Conception d'un système d'alimentation intégré dédié à la sécurisation des cartes à puce

Vincent Telandro

N° d'ordre : Année 2007

THESE

présentée devant

L'Université de Provence

Aix-Marseille I

pour obtenir le grade de

DOCTEUR

Ecole doctorale : Physique, Modélisation et Sciences pour l'Ingénieur

Spécialité : Micro- et Nano-électronique

par

Vincent TELANDRO

Ingénieur ISEN

Conception d'un système d'alimentation intégré dédié à la sécurisation des cartes à puce

Soutenue publiquement le 23 novembre 2007 devant la commission d'examen :

Président :	Jean-Luc AUTRAN	L2MP, Marseille
Rapporteurs :	Guy CATHEBRAS	LIRMM, Montpellier
	Gabriel Alfonso RINCON-MORA	Georgia Tech, Atlanta, USA
Examinateurs :	Hervé BARTHELEMY (Directeur de thèse)	USTV, Toulon
	Edith KUSSENER (Encadrante)	L2MP-ISEN, Toulon
	Pascal MASSON	LEAT, Univ. Nice Sophia-Antipolis
Invités :	Alexandre MALHERBE	STMicroelectronics, Rousset
	Laurent SOURGEN	STMicroelectronics, Rousset

Remerciements

Les travaux présentés dans ce manuscrit ont été réalisés au sein du Laboratoire Matériaux et Microélectronique de Provence (L2MP), sur le site de l'Institut Supérieur de l'Electronique et du Numérique de Toulon (ISEN-Toulon), et en collaboration avec la société STMicroelectronics-Rousset.

Je remercie Messieurs Michel Lanoo et Rachid Bouchakour, respectivement ancien et nouveau Directeurs du L2MP, de m'avoir accueilli dans leur laboratoire.

Je remercie Monsieur Bernard Petitprez, Directeur de l'ISEN-Toulon, d'avoir mis à notre disposition les moyens nécessaires à la réalisation de ces travaux et de m'avoir permis d'enseigner dans son école.

Je tiens à remercier Monsieur Jean-Luc Autran d'avoir accepté la présidence du jury chargé d'examiner mon travail.

J'exprime ma profonde reconnaissance à Messieurs Guy Cathebras et Gabriel Alfonso Rincón-Mora qui m'ont fait l'honneur d'être les rapporteurs de cette thèse. Leurs remarques, critiques et suggestions ont largement contribué à l'amélioration de ce mémoire. Je les en remercie sincèrement.

Je remercie Monsieur Pascal Masson d'avoir accepté d'examiner mon travail.

Je remercie mon directeur de thèse, Monsieur Hervé Barthélemy, pour sa confiance et ses conseils avisés. Notre passion commune pour l'analogique a alimenté de très enrichissantes discussions. Puisse le futur nous en réserver beaucoup d'autres.

J'adresse toute ma gratitude à mon encadrante, Madame Edith Kussener-Combier, pour sa disponibilité, sa patience, son soutien de tous les instants et son souci permanent d'assurer le déroulement de mon travail dans les meilleures conditions. Son enthousiasme m'a aidé à surmonter mes doutes. Je l'en remercie chaleureusement.

Je remercie mon encadrant industriel, Monsieur Alexandre Malherbe, pour le temps qu'il nous a consacré et l'étendue des connaissances dont il nous a fait profiter.

Je remercie également Monsieur Laurent Sourgen d'avoir accepté notre invitation à participer au comité d'examen.

Je tiens particulièrement à remercier Monsieur Benjamin Duval, mon co-encadrant industriel, pour la qualité de ses conseils et la confiance qu'il m'a accordé en me proposant de le rejoindre dans la société INVIA.

Je tiens également à remercier Messieurs Alain Bravaix et Didier Goguenheim, d'une part, pour la chaleur de leur accueil au sein de l'équipe Micro- et Nano-électronique du L2MP-ISEN et, d'autre part, pour la qualité et la richesse de leur enseignement.

Je remercie le Conseil Général des Bouches-du-Rhône (CG13) et la société STMicroelectronics-Rousset d'avoir soutenu financièrement ces travaux par l'intermédiaire des conventions CG13-ST-L2MP n° 2003-1-Lab2 et 2004-Lab1-Phase2.

Enfin et surtout, je souhaite remercier ma famille et mes amis. Vous avez été le soutien essentiel de ces quatre années. Merci.

Sommaire

Table des figures

Liste des tableaux

Liste des acronymes

Acronyme	Définition	Page
ABOTA	Adaptive Biasing OTA	68
AC	Alternative Current	68
AES	Advanced Encryption Standard	11
AMS	Austria Mikro Systeme	36
ANSI	American National Standards Institute	10
ASI	Asynchronous Serial Interface	7
BPA	Binary Power Analysis	22
BSIM3v3	Berkeley Short-channel IGFET Model version 3	37
C35B4	Technologie CMOS $0.35\ \mu m$ 2P/4M du fondeur AMS	36
CAR	Current Attenuation Rate	34
CG13	Conseil général des Bouches-du-Rhône	2
CM	Current Mirror	114
CNFM	Coordination Nationale pour la Formation en Micro et nanoélectronique	36
CCI	Conception de Circuits Intégrés	2
CCII	Convoyeur de courant de seconde génération	108
CCD	Charge Coupled Device	12
CMOS	Complementary Metal Oxide Semi-conductor	6
CMOSF8	Technologie CMOS $0.18\ \mu m$ du fondeur STM	35
CMP	Circuits Multi-Projets	37
CO	Chaotic Oscillator	109
CP	Charge Pump	42
CPU	Central Processing Unit	7
DBiLNA	Darlington « Pseudo-BiCMOS » Low Noise Amplifier	104
DC	Direct Current	68
DCVSL	Differential Cascode Voltage Switch Logic	24
DES	Data Encryption Standard	9

DFA	Differential Fault Analysis	14
DiPA	Direct Power Analysis	22
DPA	Differential Power Analysis	20
DRC	Design Rule Check	37
DRM	Design Rule Manual	85
DRP	Dual-Rail Pre-charge	24
DSA	Digital Secure Access	24
DyCML	Dynamic Current Mode Logic	24
ECC	Elliptic Curve Cryptography	22
ED	Edge Detector	109
EEPROM	Electrically Erasable Programmable Read Only Memory	6
EMA	Electromagnetic Analysis	15
EMV	Europay international, MasterCard international and Visa international	151
ETSI	European Telecommunications Standards Institute	151
EPS	External Power Supply	69
ESR	Equivalent Series Resistance	43
FIPS	Federal Information Processing Standards	143
GALS	Globally-Asynchronous Locally-Synchronous	23
GDSII	Graphic Data System II	37
GSM	Global System for Mobile communication	7
HMM	Hidden Markov Model	23
Ho-DPA	High-order Differential Power Analysis	22
HV	High Voltage	36
IBM	International Business Machines	10
ICMR	Input Common Mode Range	48
IEC	International Electrotechnical Commission	5
IPA	Inferential Power Analysis	22
ISEN	Institut Supérieur d'Electronique et du Numérique	2
ISO	International Standard Organisation	5
L2MP	Laboratoire Matériaux et Microélectronique de Provence	2
LDO	Low Dropout	28
LDR	Load Regulation	31
LFSR	Linear Feedback Shift Register	103
LNR	Line Regulation	30
LV	Low Voltage	69

LVLP	Low Voltage Low Power	37
LVS	Layout Versus Schematic	37
MDPL	Masked Dual-Rail Pre-charge Logic	24
MM9	MOS Model 9 (Philips)	37
MOS	Metal Oxide Semi-conductor	6
MPU	Memory Protection Unit	7
NIST	National Institute of Standards and Technology	11
NMOS	N-type MOS	36
OTA	Operational Transconductance Amplifier	42
PIN	Personnal Identification Number	9
PM	Power Manager	69
PMOS	P-type MOS	36
PODPA	Perhaps Optimal Differential Power Analysis	22
PRNG	Pseudo-Random Number Generator	102
PVC	Poly Vinyl Chloride	5
PSR	Power Supply Rejection	30
PSR^+	Power Supply Rejection (*positive rail*)	31
PSR^-	Power Supply Rejection (*negative rail*)	31
PSRR	Power Supply Rejection Ratio	34
PTAT	Proportional to Absolute Temperature	83
PVT	Process Voltage and Temperature	32
PWL	Picewise-Linear	108
QDI	Quasi Delay Insensitive	23
QSC	Quasi-Switched Capacitor	67
RAM	Random Acess Memory	7
RCG	Random Clock Generator	70
RF	Radio Frequency	6
RFA	Radio Frequency Analysis	15
RG	Reference Generator	69
RISC	Reduced Instruction Set Computer	7
RMS	Root Mean Squarre	32
RNG	Random Number Generator	7
RO	Ring Oscillator	109
ROM	Read Only Memory	7
RPA	Refined Power Analysis	22

RPI	Random Process Interrupt	24
RSA	Rivest Shamir Adleman	11
RSL	Random Switching Logic	24
SABL	Sense Amplifier Based Logic	24
S&H	Sample-and-Hold	109
SCC	Switched Capacitor Converter	70
SDC	Step-Down Converter	62
SIM	Subscriber Identification Module	5
SPA	Simple Power Analysis	17
STM	STMicroelectronics	2
SW-DPA	Sliding Window Differential Power Analysis	22
TC	Temperature Coefficient	10
TDEA	Triple Data Encryption Algorithm	10
TDES	Triple Data Encryption Standard	10
TEMPEST	Transient Electromagnetic Pulse Surveillance Technology	15
TG	Triangle-wave Generator	109
TRNG	True Random Number Generator	102
UGF	Unit Gain Frequency	45
USB	Universal Serial Bus	7
VC	Voltage Comparator	114
VCC	Voltage-to-Current Converter	109
VCO	Voltage Controlled Oscillator	102
VF	Voltage Follower	133
WDDL	Wave Dynamic Differential Logic	24
ZCS	Zero-Current Switching	62
ZPA	Zero-value Point Attacks	22
ZTC	Zero-Temperature Coefficient	90
ZVS	Zero-Voltage Switching	62

Liste des symboles

Symbole	Unité	Description	Page
$\triangleq$	-	Est défini comme étant égal à :	29
$\cong$	-	Peut être approximé par l'expression :	29
$\approx$	-	Est approximativement égal à la valeur :	48
0_k	-	Ensemble des $T_{k,l}$ tel que $D(C_{k,l},k)= 0$.	20
1_k	-	Ensemble des $T_{k,l}$ tel que $D(C_{k,l},k)= 1$.	20
A	-	Fonction de transfert d'une chaîne directe.	29
A_{cc}	-	Précision totale de la sortie d'un régulateur (en $\%$).	32
A_{cl}	-	Fonction de transfert en boucle fermé.	29
A_{ol}	-	Fonction de transfert en boucle ouverte.	29
A_{ol-dc}	-	Gain statique en boucle ouverte.	41
A_ϵ	-	Matrice carrée d'ordre 3 associée au problème (P_a).	122
$AUX1$	-	Contact auxiliaire n°1 d'une carte à puce.	6
$AUX2$	-	Contact auxiliaire n°2 d'une carte à puce.	6
B	-	Fonction de transfert de la boucle de retour.	29
CAR	-	Taux d'atténuation en courant.	34
CLK	-	Contact réservé au signal d'horloge.	6
C_L	F	Capacité de charge.	15
C_M	F	Capacité Miller.	43
C_o	F	Capacité de sortie.	43
C_p	F	Capacité parasite associée à la grille de M_p.	34
$C_{k,l}$	-	L-ième texte chiffré associé à la valeur possible k de K.	20
D	-	Fonction de sélection de l'attaque DPA.	20
D_i	-	Bloc droit de la clé secrète intervenant à la i-ème ronde de DES.	10
EN	-	Entrée de validation.	24
F_a	-	Application définissant le champs de vecteurs associé à (P_a).	117
G_i	-	Bloc gauche de la clé secrète intervenant à la i-ème ronde de DES.	10

GND	-	Contact de masse d'une carte à puce.	6
G_e	-	Erreur de gain d'un système bouclé.	29
I	-	Fonction d'interversion.	9
ID	-	Numéro d'identification d'une carte à puce.	9
I/O	-	Port de communication ASI.	6
IP	-	Fonction de permutation initiale du DES.	10
IP^{-1}	-	Fonction de permutation initiale inverse du DES.	10
Id	-	Fonction identité.	146
I_{avg}	A	Courant de consommation moyen.	21
I_L	A	Courant associé à la charge de C_L.	15
I_{DD}	A	Courant d'alimentation interne.	28
$I_{L_{max}}$	A	Amplitude maximum de I_L.	55
I_{PS}	A	Courant d'alimentation externe.	28
I_{SPS}	A	Courant d'alimentation intermédiaire.	68
$I_{SPS_{ac}}$	A	Partie AC du courant I_{SPS}.	68
$I_{SPS_{dc}}$	A	Partie AC du courant I_{SPS}.	68
I_{VCC}	A	Signal de sortie du convertisseur tension-courant (VCC).	110
I_{cc}	A	Courant d'alimentation d'une carte à puce.	152
I_{sc}	A	Courant de court-circuit d'un inverseur.	15
I_i	A	Courant d'entrée.	56
I_l	A	Courant de fuite statique d'un inverseur.	15
I_o	A	Courant de sortie.	56
$I_{o_{max}}$	A	Amplitude maximum de I_o.	34
I_{off}	A	Courant de fuite d'une technologie CMOS.	15
I_p	A	Partie de I_{PS} absorbée par les éléments de puissance.	33
I_q	A	Courant de repos.	33
J_{F_a}	-	Matrice Jacobienne de l'application $F_a(X)$.	118
K	-	Clé secrète (56 bits dans la cas du DES).	20
K_i	-	Sous-clé de 48 bits associée à la i-ème ronde de DES.	10
$K_{i,j}$	-	J-ième sextet de K_i.	20
L	m	Longueur de grille d'un transistor MOS.	6
L_i	-	Bloc gauche de K associé la i-ème ronde de DES.	10
L_{min}	m	Valeur minimale de L.	35
L_x	-	Exposant de Lyupanov associé à V_x.	126
L_y	-	Exposant de Lyupanov associé à V_y.	126

L_z	-	Exposant de Lyupanov associé à V_z.	126
M_p	-	Transistor de puissance.	40
PD	W	Bit de désactivation (*Power Down).*	87
$PSSi$	-	I-ème bit d'état de V_{PS} (*Power Supply State*).	69
P_{DD}	W	Puissance d'alimentation interne.	38
P_{PS}	W	Puissance d'alimentation externe.	38
P_a	-	Forme adimensionnée du système (P).	116
P_a^l	-	Forme linéarisée du système adimensionné (P_a).	118
$P_{k,l}$	-	L-ième texte clair associé à la valeur possible k de K.	20
$P_{i,L}$	W	Puissance consommée pour la charge de C_L.	15
$P_{i,l}$	W	Puissance associée à I_l.	15
$P_{i,sc}$	W	Puissance associée à I_{sc}.	15
P_i	W	Puissance totale consommée par un inverseur.	15
PSR^+	-	Taux de réjection du rail d'alimentation positif.	31
PSR^-	-	Taux de réjection du rail d'alimentation négatif.	31
R_{ESR}	Ω	Resistance d'ESR.	43
R_i	-	Bloc droit de K associé à la i-ème ronde de DES.	10
R_o	Ω	Résistance de sortie.	31
R_{on}	Ω	Résistance à l'état passant.	41
R_L	Ω	Résistance de charge.	43
RN_s	-	Nombre aléatoire généré par la carte à puce.	9
RN_t	-	Nombre aléatoire généré par le terminal.	9
RST	-	Contact de réinitialisation d'une carte à puce.	6
S_l	-	L-ième table de substitution du DES ($l \in [1,..,8]$).	20
T	$^\circ C$	Température.	28
$T_{k,l}$	-	Trace du courant de consommation associée à $C_{k,l}$.	20
V	-	Matrice des vecteurs propres de A.	119
U_T	V	Tension thermique.	84
V_{CO}	V	Signal de sortie de l'oscillateur chaotique (CO).	110
V_{CP}	V	Tension de sortie de la pompe de charge (CP).	42
V_{DD}	V	Tension d'alimentation interne.	28
V_{EA}	V	Tension d'Early.	44
V_{ED}	V	Signal de sortie du détecteur de front (ED).	110
V_{PS}	V	Tension d'alimentation externe.	28
V_{RC}	V	Signal de sortie du générateur d'horloge aléatoire (RCG).	101

$V_{S\&H}$	V	Signal de sortie de l'échantillonneur-bloqueur (SH).	110
V_{SPS}	V	Tension d'alimentation intermédiaire.	68
V_T	V	Tension de seuil d'un transistor MOS.	35
V_{TG}	V	Tension de sortie du générateur de triangle TG.	110
V_{cc}	V	Tension d'alimentation supérieure d'une carte à puce.	6
V_{dd}	V	Tension d'alimentation supérieure.	136
V_{do}	V	Tension de *dropout* d'un régulateur.	28
V_e	V	Tension d'erreur d'une boucle de régulation.	29
V_{fb}	V	Tension de retour d'une boucle de régulation.	40
V_i	V	Tension d'entrée d'un régulateur.	28
$V_{i_{min}}$	V	Tension d'entrée.	28
V_o	V	Tension de sortie.	28
$V_{o_{max}}$	V	Valeur maximale de V_o.	32
$V_{o_{min}}$	V	Valeur minimale de V_o.	32
V_{o_o}	V	Tension de sortie optimale.	31
V_{pp}	V	Tension de programmation de l'EEPROM d'une carte à puce.	6
V_{ref}	V	Tension de référence.	40
V_{ref_o}	V	Valeur optimale de V_{ref}.	32
V_{ss}	V	Tension d'alimentation inférieure.	136
V_{tr}	V	Réponse transitoire d'un régulateur.	32
W	m	Largeur de grille d'un transistor MOS.	35
W_{min}	m	Valeur minimale de W.	35
XOR	-	Fonction OU-exclusif.	10
$\|\|$	-	Fonction de concaténation.	9
β	-	Facteur de retour.	41
δ_X	-	Perturbation suivant la composante X.	118
ΔV_{LNR}	V	Variation de V_{DD} associé au LNR.	32
ΔV_{LDR}	V	Variation de V_{DD} associé au LDR.	32
ΔV_{PT}	V	Variation de V_{DD} induite par les variations PVT.	32
$\Delta V_{PVT_{ref}}$	V	Variation de V_{ref} résultant des variations PVT.	32
ΔV_{tr}	V	Amplitude de la réponse transitoire.	32
Δ_a	-	Pas de discrétisation du paramètre a.	123
Δ_k	-	Fonction d'évaluation de la pertinence du classement associé à k.	20
η	-	Rendement d'un convertisseur de tension.	33
η_I	-	Rendement en courant d'un régulateur.	33

η_P	-	Rendement en puissance d'un régulateur.	33
η_ϵ	-	Fonction non-linéaire modélisant un comparateur.	117
Λ	-	Racines de l'équation caractéristique III.34.	118
λ	V^{-1}	Inverse de la tension d'Early V_{EA}.	44
μ_0	cm^2/V.s	Mobilité des porteurs.	35
$\oplus$	-	Fonction OU-exclusif.	20
ω_0	rad/s	Pulsation de l'oscillateur chaotique (CO) en mode sinusoïdal.	127
ω_{0°	rad/s	Pulsation pour laquelle le gain de la chaîne directe est unitaire.	29
ω_{0dB}	rad/s	Pulsation pour laquelle le déphasage de la chaîne directe est nulle.	30
Φ_M	$^\circ$	Marge de phase.	30
ϕ_f	V	Potentiel de Fermi.	50
$\prod_\epsilon$	-	Fonction non-linéaire définie dans l'annexe B	118
f	-	Fonction intervenant à chaque ronde de DES.	10
f_ϵ	-	Champs de vecteurs non-linéaire reposant sur η_ϵ.	117
f_c	Hz	Fréquence du signal d'horloge.	37
f_{co}	Hz	Fréquence du signal V_{CO}.	128
f_j	Hz	Fréquence des sauts de f_{co}.	101
f_{rc}	Hz	Fréquence du signal V_{RC}.	101
f_s	Hz	Fréquence de commutation.	61
f_{tg}	Hz	Fréquence du signal V_{TG}.	139
γ	$\sqrt{V}$	*Body factor*.	50
k	-	Valeur possible de K.	20
k_B	J/K	Constante de Boltzmann.	104
p	-	Point fixe du système (P_a).	116
p_0	-	Point de fixe $[0,0,0]^T$ du système (P_a) .	117
p_1	-	Point de fixe $[1,0,0]^T$ du système (P_a) .	117
p_{-1}	-	Point de fixe $[-1,0,0]^T$ du système (P_a) .	117
$p_{\pm 1}$	-	Points fixes p_{-1} et p_1 du système (P_a).	119
p_t	-	Probabilité de transition d'une porte.	15
t_{ox}	m	Epaisseur d'oxyde d'un dispositif MOS.	6

Introduction

Après avoir fait ses preuves dans le secteur bancaire puis dans la téléphonie mobile, la carte à puce s'impose progressivement comme le support universel de l'identité. Une fois personnalisé, ce système sur puce portable et sécurisé permet, entre autres, d'identifier et d'authentifier son porteur légitime, de stocker ses données confidentielles et de signer électroniquement des documents officiels. Ainsi, la carte à puce s'impose dans un nombre grandissant de domaines d'application : cartes de santé, cartes d'abonnement (transports, télévision, etc.), cartes d'accès (physique ou logique), cartes d'identité électroniques et passeports biométriques sont les nouveaux vecteurs de « l'intelligence ambiante ».

Pourtant, la carte à puce est un support contraignant. En particulier, les contraintes mécaniques fixées par les normes limitent la surface silicium à seulement $25\ mm^2$. De fait, les premières cartes commercialisées comportaient uniquement une mémoire pilotée par un circuit logique simple. Par la suite, l'évolution des technologies MOS a permis de décupler les ressources matérielles embarquées; les plus sophistiqués des microcontrôleurs encartables actuels renferment un microprocesseur RISC 32 bits, plusieurs centaines de kilo de mémoire et une multitude de périphériques sécuritaires et de communication (avec ou sans contacts). L'exploitation de cette puissance via des plates-formes de développement ouvertes (Java, .Net, etc.) autorise la mise en œuvre d'applications de haut niveau alliant performance et interoperabilité.

Dans le même temps, la dématérialisation des biens et des échanges a poussée les faussaires à s'engager dans une course à l'armement technologique. Dans l'arsenal ainsi constitué, une des principales catégories d'attaques exploite les défauts liés à l'implémentation des systèmes cryptographiques : la cryptanalyse matérielle. Celle-ci se divise en deux sous-catégories : les attaques invasives et les attaques non-invasives. Ces dernières, également appelées attaques sur les « canaux cachés », reposent sur un principe découvert dans les années 70. A cette époque, la publicité commençait à financer la télévision américaine. Les chaînes n'avaient alors aucun moyen d'évaluer l'audimat. C'est à New York qu'est née l'idée d'observer la consommation d'eau et d'électricité des habitants; des variations importantes ont été mesurées pendant les pauses publicitaires des chaînes les plus regardées. La notion de « canal caché » était née [1]. Selon le même principe, l'activité d'un système électronique se traduit par des variations de son courant d'alimentation. Ainsi, menées sur le courant d'alimentation d'une carte à puce, les attaques sur les canaux cachés permettent d'extraire les données secrètes traitées au sein du système [2].

Pour repousser ces attaques, les concepteurs sont obligés de revoir constamment leur système de défense en développant sans cesse de nouvelles protections physiques et logiques visant à supprimer, ou rendre inexploitable, les corrélations existantes entre les données traitées et les canaux cachés. En défini-

tive, le nombre considérable de contre-mesures équipant actuellement les microcontrôleurs tend à pénaliser leurs performances, sans véritablement garantir leur sécurité face aux nouvelles variantes de ces attaques.

Durant les trois dernières décades, l'application des règles de mise à l'échelle formulées en 1974 par l'équipe de Robbert Dennard [3] a permis d'accroître exponentiellement la densité d'intégration des procédés MOS et de pérenniser ainsi la loi de Moore publiée 9 ans plus tôt [4]. Afin de maintenir la fiabilité des dispositifs au fil des sauts technologiques, ces homothéties successives sont, dans la mesure du possible, opérées à champs électriques constants. A cet effet, chaque réduction des dimensions s'accompagne d'une diminution de la tension d'alimentation. Or, la technologie des cartes à puce évolue plus rapidement que celle des lecteurs. Par conséquent, la tension d'alimentation délivrée par ces derniers doit, le plus souvent, être abaissée avant d'être appliquée au cœur de la puce. Cette fonction est généralement assurée par un régulateur de tension linéaire série intégré au microcontrôleur de la carte. Si ce type de régulateur présente à la fois une précision élevée et une surface restreinte, en revanche, son rendement n'est pas toujours optimum et surtout, il n'offre aucune protection contre les attaques par analyse de courant de consommation. Cependant, à notre connaissance, aucune des structures proposées dans la littérature ne permet d'atteindre simultanément tous ces objectifs.

Le travail de thèse présenté dans ce manuscrit traite de la conception et de l'intégration en technologie CMOS $0.18\ \mu m$ d'un système d'alimentation dédié à la protection des cartes à puces contre les attaques par analyse du courant d'alimentation. Il a été mené au sein de l'équipe Conception de Circuits Intégrés (CCI) du Laboratoire Matériaux et Microélectronique de Provence (L2MP - UMR CNRS 6137) localisé à l'Institut Supérieur de l'Electronique et du Numérique de Toulon (ISEN-Toulon) et en collaboration avec la division Digital Secure Access (DSA) de la société STMicroelectronics-Rousset (STM). Cette étude, conduite dans le cadre du thème de recherche intitulé « Gestion d'énergie » (PS23), a été supportée financièrement par le Conseil Général des Bouches-du-Rhône (CG13) et la société STMicroelectronics-Rousset au travers des conventions CG13-ST-L2MP n° 2003_1_Lab2 et 2004_Lab1_Phase2.

Le premier chapitre aborde les aspects sécuritaires des cartes à puce. Après une brève description de l'architecture des microcontrôleurs, nous verrons comment les ressources cryptographiques embarquées autorisent la mise en œuvre de procédures d'authentifications sécurisées. Nous présenterons ensuite succinctement les différentes catégories d'attaques, en nous focalisant plus particulièrement sur un type de canal caché : le courant d'alimentation. Enfin, nous expliquerons en quoi les contre-mesures proposées à ce jour ne répondent que partiellement aux critères industriels.

Dans un second chapitre, nous proposerons une nouvelle architecture de conversion DC-DC permettant de décorréler le courant entrant du courant sortant, tout en respectant les contraintes de surface des cartes à puces. Après avoir rappelé les différents termes et définitions liés aux régulateurs de tension, nous détaillerons le cahier des charges élaboré par la division DSA. Puis, nous verrons en quoi les différentes structures proposées dans la littérature ne permettent pas d'atteindre simultanément tous les objectifs fixés par ce dernier. Nous décrirons alors l'architecture du système proposé et son implémentation suivant un procédé CMOS $0.18\ \mu m$ fourni par STMicroelectronics. Enfin, nous analyserons les résultats des simulations Eldo (modèle MM9) réalisées via la plate-forme de conception Virtuoso de l'environnement Cadence.

Le système proposé au second chapitre comporte un générateur d'horloge aléatoire. La conception et la réalisation de ce dernier font l'objet d'un troisième et dernier chapitre. Dans une étude bibliographique préliminaire, nous verrons en quoi les structures existantes ne satisfont pas entièrement aux exigences du cahier des charges, mais peuvent servir de base pour l'élaboration d'une solution sur mesure. Nous décrirons alors la structure du générateur proposé, ainsi que son intégration en technologie STM CMOS $0.18\ \mu m$. Celui-ci repose, entre autres, sur un oscillateur chaotique de type « *double-scroll* ». L'étude mathématique et numérique du système non-linéaire décrivant ce dernier permettra de déterminer les valeurs de son paramètre de contrôle engendrant un comportement chaotique. Par ailleurs, cet oscillateur a été fabriqué suivant le procédé CMOS $0.35\ \mu m$ 2P/4M du fondeur Austria Mikro Systems (AMS); les mesures seront confrontées aux simulations numériques (MATLAB) et électriques (Spectre). Enfin, nous procéderons à une analyse statistique des simulations Eldo associées au générateur.

Chapitre I

Sécurité des cartes à puce

I.1 Présentation du support

Le terme « carte à puce » (« *smart card* » dans la littérature anglaise) désigne tout support fin de petite dimension embarquant un circuit intégré [5]. Les caractéristiques des cartes à puce sont standardisées par des normes internationales. Les standards ISO/IEC 7810 [6] et ISO/IEC 7816-1 [7] définissent, entre autres, les caractéristiques physiques et mécaniques du support. Ce dernier se présente généralement sous la forme d'une petite carte en PVC de $0.76\ mm$ d'épaisseur. Les deux formats les plus répandus sont le ID-1 (carte bancaire) et le ID-000 (carte SIM). Ils sont tous deux représentés sur le schéma de la figure I.1.

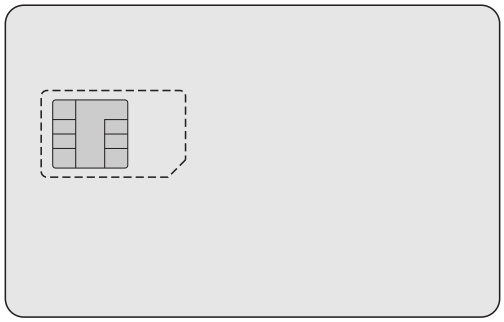


Fig. I.1 – *Formats ID-1 (trait plein) et ID-000 (trait pointillé) selon ISO/IEC 7810 [7].*

En terme d'interface de communication, les cartes à puce se divisent en deux catégories : les cartes à contact et les cartes sans contact. Dans le cas des cartes à contact, l'accès au composant électronique se fait par l'intermédiaire de plots métalliques. Leurs caractéristiques sont rassemblées dans le tableau I.1. Sauf exception [8], une carte à puce n'embarque pas de batterie, elle est alimentée par le lecteur. L'alimentation asymétrique délivrée par ce dernier est appliquée à la puce par l'intermédiaire des contacts V_{cc} (potentiel électrique le plus élevé) et GND (potentiel électrique le plus faible). Le signal d'horloge est également fourni par le lecteur. Il est transmis à la puce via CLK. L'entrée numérique RST permet de réinitialiser le circuit. Le port de communication série I/O est de type bidirectionnel semi-duplex. Le protocole de communication associé est décrit par le standard ISO 7816-3 [7]. La programmation des mémoires de type EEPROM nécessite des tensions généralement supérieures à celle supportée par le reste du circuit. Jusqu'à

la fin des années 1990, le contact V_{pp} était utilisé à cet effet. Il ne l'est plus depuis l'intégration des pompes de charge, structures permettant de générer ces niveaux de tension en interne. Enfin, les contacts $AUX1$ et $AUX2$ n'ont pas de fonction attitrée. Leur présence, même physique, reste optionnelle. Les caractéristiques des paramètres électriques (fréquence du signal d'horloge, tension d'alimentation, etc.) dépendent de la norme considérée (cf. annexe A).

Position	Numérotation	Attribution	Fonction
C1 C5 / C2 C6 / C3 C7 / C4 C8	C1	V_{cc}	Tension d'alimentation.
	C2	RST	Entrée de réinitialisation.
	C3	CLK	Entrée du signal d'horloge.
	C4	$AUX1$	Contact auxiliaire 1.
	C5	GND	Masse.
	C6	V_{pp}	Tension de programmation.
	C7	I/O	Port de communication série.
	C8	$AUX2$	Contact auxiliaire 2.

Tab. I.1 – *Caractéristiques des contacts (selon ISO/IEC 7816-2 [7]).*

Dans le cas des cartes sans contact, l'énergie et les données sont véhiculées par des champs électromagnétiques. Le module de communication radio-fréquence (RF) est intégré à la puce, et associé à une antenne embarquée dans le corps de la carte. Le protocole de transmission des cartes dites de « proximité » (distance $\leq 5\ cm$) est normalisé par le standard ISO/IEC 14443 (A ou B) [9], tandis que celui des cartes dites de « voisinage » (distance $\leq 1.5\ m$) est normalisé par le standard ISO/IEC 15693 [10].

La carte à puce est un support contraignant : sa faible épaisseur lui interdit la majorité des composants discrets, tandis que le procédé d'encartage et les contraintes mécaniques d'utilisation limitent la surface silicium à $25\ mm^2$. Cependant, l'évolution de la technologie CMOS a permis d'augmenter considérablement la complexité et les performances des circuits électroniques embarqués. En effet, depuis son introduction en 1963, la technologie CMOS a vu sa densité d'intégration doubler tous les 18 mois. En 1970, un transistor MOS occupait une surface de 1 mm^2 (L = 10 μm et t_{ox} = 1.2 μm). A surface égale, les procédés de fabrication actuels permettent d'intégrer jusqu'à 3 millions de transistors (L = 45 nm et t_{ox} = 1.3 nm), portant à plus d'un milliard le nombre de transistors par puce. Dans le même temps, la fréquence de transition d'un transistor MOS est passée de quelques mégahertz à plus de 100 GHz, tandis que le coût de fabrication en volume a chuté de 1 \$ par transistor à moins de 0.1 μ\$ par transistor. Quelles soient technologiques ou financières, ces évolutions exponentielles ont favorisé la pénétration commerciale de la technologie CMOS. A l'heure actuelle, la majorité des circuits pour cartes à puce reposent entièrement sur cette technologie.

L'apparition de nouvelles fonctionnalités a scindé la classification des cartes à puce en deux catégories : les cartes à mémoire (carte téléphonique, carte de stationnement, etc.) et les cartes à microprocesseur (carte bancaire, carte GSM, carte de santé, passeport biométrique, etc.). Les cartes à mémoire comportent

généralement une mémoire non-volatile et un bloc logique sécuritaire. Plus sophistiquées, les cartes à microprocesseurs sont de véritables micro-ordinateurs de poche. L'architecture d'un microcontrôleur pour carte à puce (ou « encartable ») est schématisée sur la figure I.2.

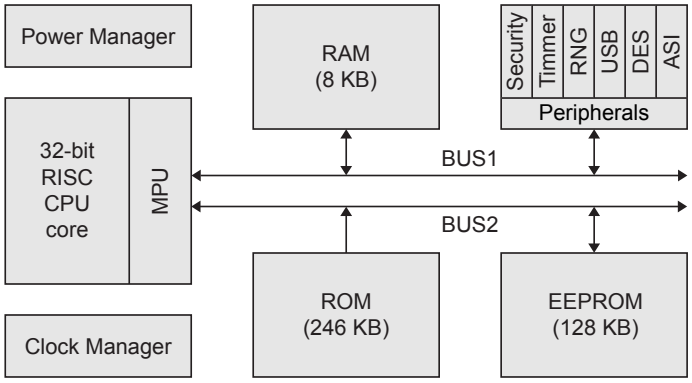


Fig. I.2 – *Architecture d'un microcontrôleur encartable (modèle ST22L128 de STM).*

Le microcontrôleur de la figure I.2 est constitué d'un microprocesseur RISC de 32 bits cadencé à 33 MHz et capable d'un adressage linéaire de la mémoire sur 24 bits. Il comporte trois types de mémoire : une mémoire morte de type ROM de 246 KB, une mémoire volatile de type RAM de 8 KB et une mémoire non-volatile réinscriptible de type EEPROM de 128 KB. Il comporte également six circuits périphériques dont : un bloc sécuritaire surveillant le système par l'intermédiaire de nombreux capteurs (tension d'alimentation, fréquence du signal horloge, etc.), un « *timer* », un générateur de nombre aléatoire (RNG), un contrôleur USB 2.0 exploitant les ports $AUX1$ et $AUX2$, un coprocesseur cryptographique dédié à l'exécution d'algorithmes de type DES et TDEA (ou triple-DES) [11], et une interface de communication ASI conforme au standard ISO 7816-3. Les différents modules sont interconnectés par l'intermédiaire de deux bus de communication distincts, ce qui autorise un accès simultané au code et aux données. Ces accès sont contrôlés par un MPU qui autorise la mise en œuvre d'un pare-feu (« *firewall* ») entre les applications. Le contrôle et la distribution des signaux d'horloge sont assurés par un gestionnaire dédié. Enfin, un contrôleur de puissance assure la gestion énergétique du système. L'encartage de ces ressources matérielles autorise la mise en œuvre d'applications sécuritaires de haut niveau.

I.2 Applications sécuritaires

La sécurité d'un grand nombre de systèmes repose sur le principe d'authentification [12]. L'objectif d'une authentification est de vérifier l'identité et l'authenticité d'un partenaire de communication. Ce type de processus fait généralement intervenir une clé secrète : si l'entité connaît la clé, on en conclut qu'elle est bien celle qu'elle prétend être. On désigne par cryptographie la discipline de la cryptologie (étymologiquement, la science du secret) s'attachant à protéger un message de telle sorte qu'il ne soit accessible qu'au destinataire légitime. La cryptanalyse s'oppose, en quelque sorte, à la cryptographie; si déchiffrer consiste à retrouver un message au moyen d'une clé, cryptanalyser c'est tenter de se passer de cette dernière.

La carte à puce est un support sécurisé qui permet de véhiculer et d'exploiter des informations confi-

dentielles tout en les gardant secrètes. Elle constitue donc un support de premier choix pour la mise en œuvre de procédures d'authentification sécurisées. Il existe principalement deux types d'algorithmes d'authentification : les algorithmes symétriques dits à « clé privée » et les algorithmes asymétriques dits à « clé publique ».

I.2.1 Les algorithmes symétriques

I.2.1.1 Introduction

Un algorithme cryptographique symétrique repose sur une clé secrète unique : la clé de chiffrement est également utilisée lors du déchiffrement. Par conséquent, cette clé doit être connue de tous les partenaires légitimes de communication, mais gardée secrète par ces derniers. Dans la majorité des applications, la méthode d'identification repose sur une procédure « *challenge-response* » de type mutuel symétrique. Son principe général est illustré sur la figure I.3.

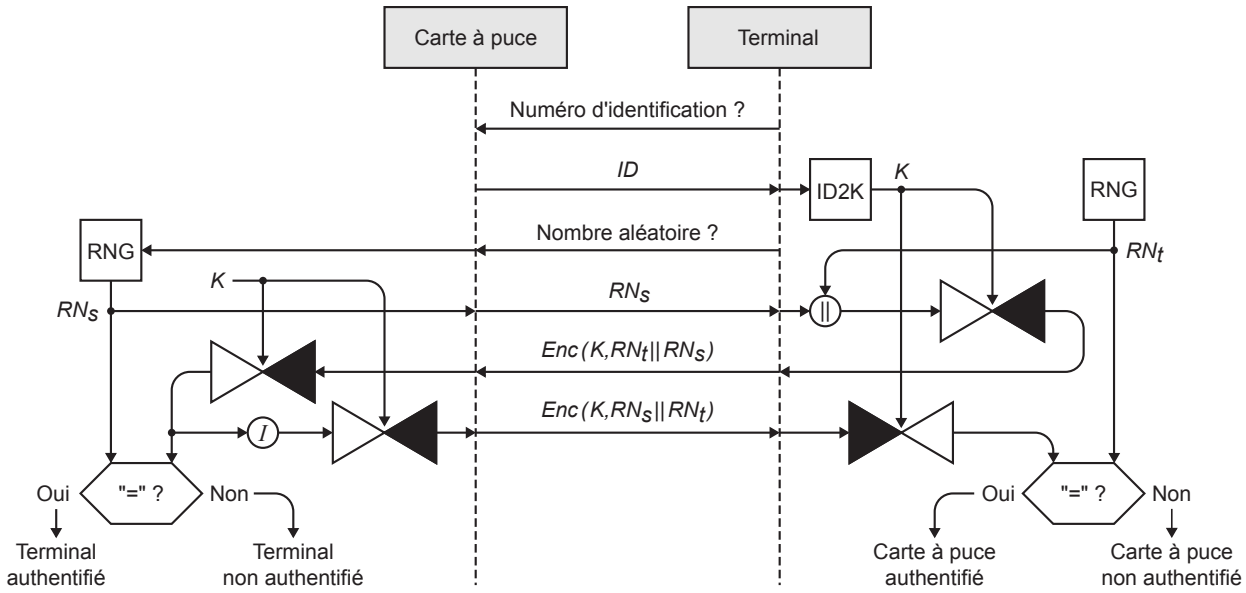


Fig. I.3 – *Principe général d'une authentification mutuelle symétrique [12].*

En premier lieu, le terminal demande à la carte de lui envoyer son numéro d'identification (ID). A partir du nombre reçu, le terminal détermine la clé secrète d'authentification spécifique à la carte (K). Ensuite, le lecteur demande à la carte de générer et de lui transmettre un nombre aléatoire (RN_s). Le terminal génère à son tour un nombre aléatoire (RN_t) qu'il concatène (fonction $||$) avec celui reçu, puis encrypte le texte clair (« *plaintext* ») résultant à l'aide de la clé secrète. Il transmet alors le texte chiffré (« *ciphertext* ») à la carte. La carte décrypte le bloc reçu et peut ainsi vérifier si le nombre aléatoire correspond à celui qu'elle a précédemment envoyé au lecteur. Si c'est le cas, le terminal est authentifié aux yeux de la carte. Ensuite, la carte intervertit les deux nombres aléatoires (fonction I), encrypte le nombre résultant à l'aide de la clé secrète, puis envoie le texte chiffré au terminal. Enfin, le terminal déchiffre le bloc et compare le nombre aléatoire reçu à celui qu'il avait précédemment envoyé. S'ils sont identiques, la carte est identifiée aux yeux du terminal ce qui clôture la procédure d'authentification. Dans le cas des cartes bancaire et des cartes SIM,

cette étape précède toujours la procédure de vérification du code PIN qui permet, quant à elle, d'authentifier l'utilisateur de la carte. Les algorithmes cryptographiques symétriques les plus courants (le DES, le TDEA et l'AES) sont détaillés dans les paragraphes suivants.

I.2.1.2 Data Encryption Standard (DES)

Adopté comme standard en 1976, le DES [11] est l'un des algorithmes cryptographiques symétriques les plus utilisés. Cette méthode de chiffrement itérative par bloc repose sur des clés de 56 bits. Son principe général est illustré sur la figure I.4 [13, 14].

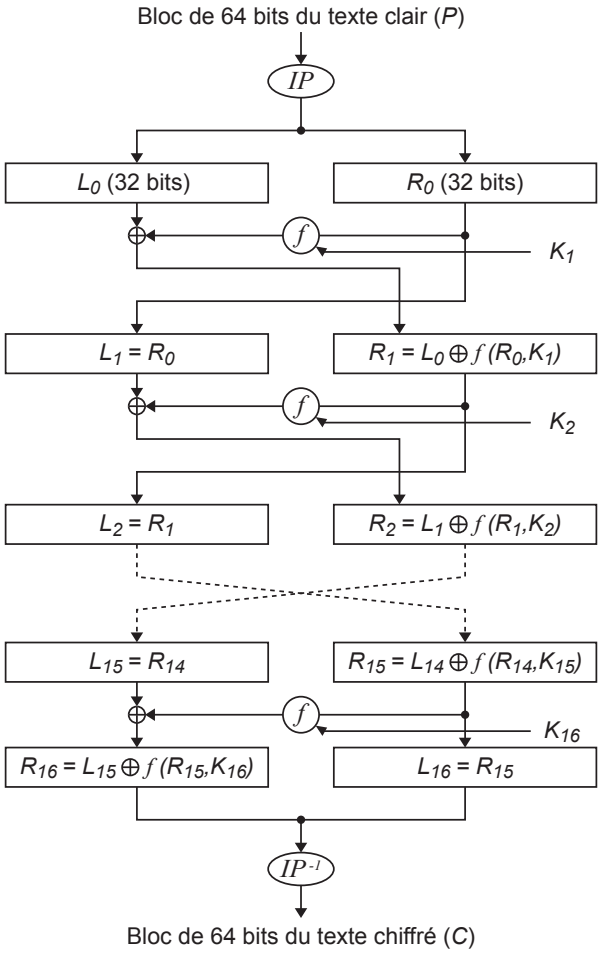


Fig. I.4 – *Principe général du DES [13].*

Le DES travaille à partir d'un bloc de texte clair (P) de 64 bits et génère un bloc de texte chiffré (C) de même dimension. Le bloc subit d'abord une permutation initiale (IP), puis il est découpé en deux blocs de 32 bits appelés respectivement bloc gauche (L_i) et bloc droit (R_i). Ces deux blocs vont alors subir 16 opérations consécutives identiques que l'on appelle des rondes de DES. Chaque ronde de DES fait intervenir la fonction f dont la structure est représentée sur la figure I.5 [13, 14]. Aprés la dernière ronde, le dernier bloc gauche est concaténé au dernier bloc droit. Enfin, le bloc résultant subit une opération permutation initiale inverse (IP^{-1}).

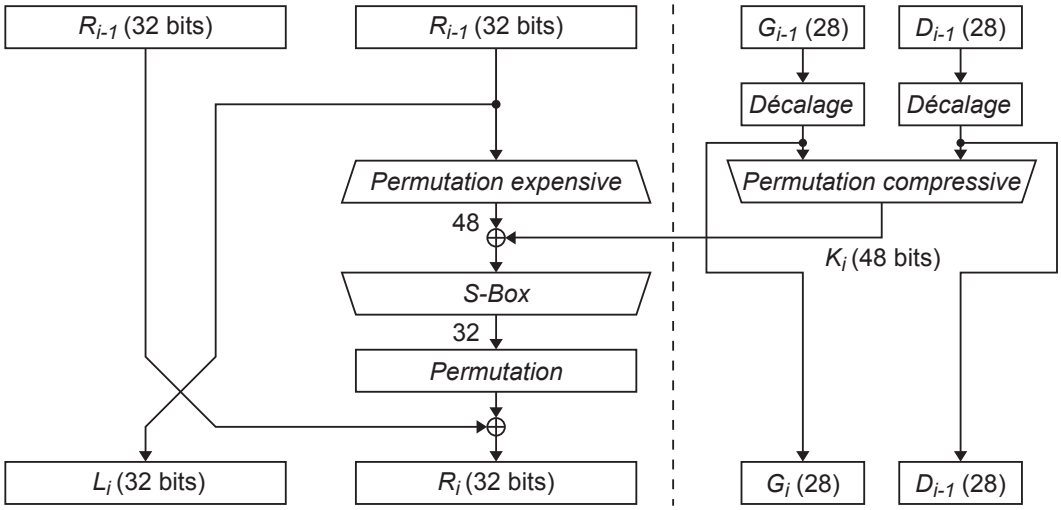


Fig. I.5 – *Structure d'une ronde de DES : fonction f (à gauche) et générateur de K_i (à droite) [13].*

Avant la première ronde de DES, la clé secrète initiale de 56 bits K est divisée en deux blocs de 28 bits : G_0 (moitié gauche de K) et D_0 (moitié droite de K). A chaque ronde i, les blocs G_{i-1} et D_{i-1} subissent un décalage normalisé (de 1 ou 2 bits vers la gauche suivant la ronde considérée). Puis les 48 bits de la sous-clé K_i sont générés par permutation compressive des blocs G_i et D_i. En parallèle, une permutation expansive est appliquée au bloc L_i qui passe de 32 à 48 bits. Il subit alors un OU-exclusif (fonction XOR) avec les 48 bits de la sous-clé K_i. Le vecteur résultant est ramené à 32 bits par l'intermédiaire d'une permutation compressive. Lors de cette permutation compressive, les 48 bits de K_i sont découpés en 8 paquets de 6 bits. Chaque paquet est ramené à 4 bits par l'intermédiaire d'une table de substitution différente de 16x4 éléments (*S-Box* pour « *Substitution Box* »). Ces *S-Box* contribuent à la « confusion » [15] en rendant l'information originale inintelligible. Elles permettent de casser la linéarité de la structure de chiffrement. Après la permutation compressive, la donnée subit une dernière permutation. Le bloc obtenu en sortie de f subit alors un XOR avec le bloc gauche précédent. Le résultat devient le bloc droit suivant, tandis que le nouveau bloc gauche n'est autre que le bloc droit précédent. Le même algorithme peut être utilisé lors du décryptage; il suffit simplement de permuter l'ordre d'utilisation des sous-clés. Contrairement à la clé qu'il exploite, le DES est un algorithme publique; la structure de ses permutations expansives et compressives, ainsi que ses 8 tables de substitution, sont entièrement définies dans la norme ANSI X3.92 [16].

I.2.1.3 Triple Data Encryption Algorithm (TDEA)

Proposé par IBM en 1978, le TDEA ou TDES (pour triple-DES) [11] a été développé afin d'augmenter le niveau de sécurité des procédures cryptographiques symétriques. Son principe est illustré sur la figure I.6. Il repose sur l'enchaînement successif de trois algorithmes DES, avec deux voire trois clés différentes. Cet algorithme permet d'augmenter considérablement le temps moyen nécessaire à la réalisation d'une attaque par force brute (« *brut-force* », cf. sous-section I.3.3) [17]. Cependant, sa force effective est réduite de 168 à 112 bits par l'attaque dite « rencontre au milieu » [17].

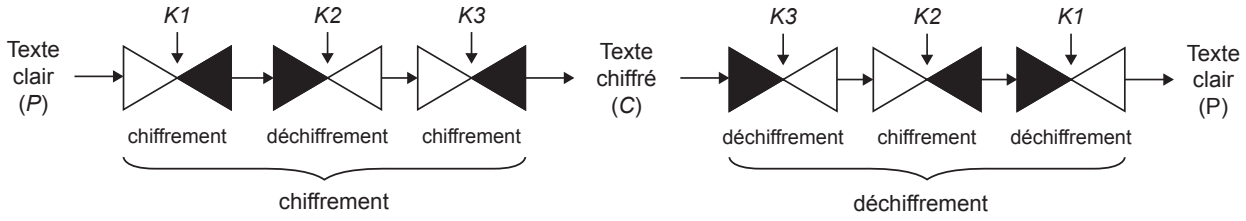


Fig. I.6 – *Principe du TDEA [12].*

I.2.1.4 Advanced Encryption Standard (AES)

Dès Janvier 1977, le NIST a initié le développement de l'algorithme de chiffrement AES [18]. Plus rapide que le triple-DES, l'AES repose sur l'algorithme de Rijndael (du nom de ces inventeurs : Vincent Rijmen and Joan Daemen). Il opère sur des blocs de 128 bits avec une clé de 128, 192 ou 256 bits. Standardisé en 2001 pour une taille de bloc de 128 bits, c'est sous cette forme qu'il est actuellement implémenté sur les cartes à puce.

Un des principaux avantages des algorithmes cryptographiques symétriques réside dans leurs vitesses d'exécution élevées. En revanche, la distribution confidentielle de la clé secrète est une étape contraignante de leur mise en oeuvre. Cette difficulté disparaît complètement dans le cas des algorithmes cryptographiques asymétriques.

I.2.2 Les algorithmes asymétriques

Un algorithme asymétrique repose sur l'utilisation de deux clés distinctes : une clé publique et une clé privée. L'une sert au chiffrement et l'autre au déchiffrement. Si, par exemple, la clé publique est utilisée pour le chiffrement, seul le détenteur de la clé privée sera en mesure de déchiffrer le message. Lorsqu'une ou plusieurs personnes souhaitent envoyer des données confidentielles à une tierce personne, cette dernière, nommée par convention Alice, prend en charge la création d'une paire de clés. Ensuite, Alice transmet sa clé publique aux personnes souhaitant communiquer avec elle (Bob, Carole, etc.). Les expéditeurs peuvent alors chiffrer les données confidentielles avec la clé publique avant de les transmettre en toute sécurité; grâce à sa clé privée, seule Alice est en mesure de les déchiffrer.

Les algorithmes asymétriques permettent de s'affranchir des contraintes associées à la distribution confidentielle des clés privées. Cependant, ils requièrent des ressources matérielles importantes, ce qui tend à limiter leur utilisation dans le cadre des systèmes embarqués. Le plus répandu des algorithmes de chiffrement asymétrique est le RSA (du nom de ses inventeurs : Rivest, Shamir et Adleman) [19]. Il repose sur l'exponentiation modulaire.

I.3 Attaques sur les cartes à puce

I.3.1 Introduction

Les attaques sur les cartes à puce se divisent en deux catégories [20, 21] : les attaques invasives et les attaques non-invasives. Les attaques invasives reposent sur l'analyse et la modification de l'intérieur du système. L'accession aux couches profondes du microcontrôleur se traduit généralement par la détérioration

du circuit, voir par sa destruction totale [22]. Par opposition, les attaques non invasives se contentent de manipuler et d'observer le système depuis l'extérieur, sans altération du support.

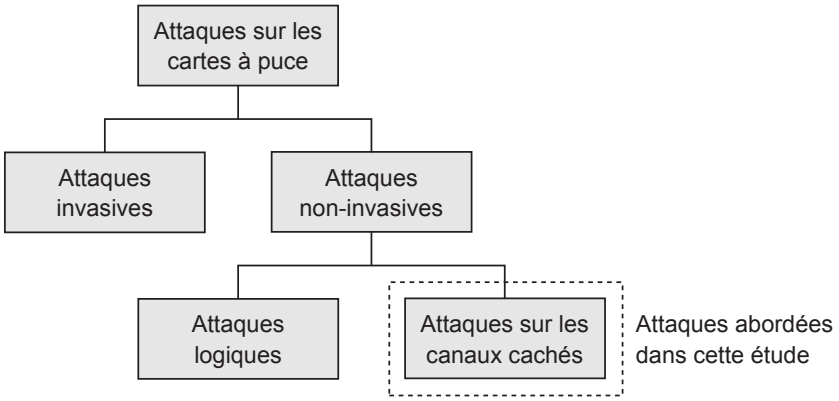


Fig. I.7 – *Arbre des attaques sur les cartes à puce.*

Les attaques non-invasives se divisent en deux catégories : les attaques logiques et les attaques sur les canaux cachés (« *side channel attacks* »). Les attaques logiques agissent uniquement par l'intermédiaire du port de communication légitime (I/O), tandis que les attaques sur les canaux cachés exploitent tous les autres canaux. Les principales catégories d'attaques sont rassemblées dans l'arbre de la figure I.7.

I.3.2 Attaques invasives

Lors d'une attaque physique, la puce est d'abord extraite de son support, puis la couche de passivation est décapée à l'aide d'un acide [23]. Lorsqu'un accès aux couches profondes est nécessaire, les niveaux de métallisation sont également retirés. Une fois ces opérations effectuées, le système devient accessible aux analyses optiques et électriques. On distingue essentiellement trois catégories d'attaques invasives :

- La rétro-ingénierie (« *reverse engineering* ») par analyse optique : l'architecture d'un système peut être déduite de l'observation de son circuit. Certains outils automatisés permettent même d'extraire l'intégralité des masques [24]. Cette attaque est généralement réalisée à l'aide d'un microscope électronique à balayage couplé à une caméra CCD [25]. Par ailleurs, la lecture des points mémoires permet de déterminer le code source du système d'exploitation et la valeur des données stockées.
- La rétro-ingénierie par analyse électrique [25] : l'utilisation d'un banc de caractérisation à micro-pointes permet de mesurer certains des signaux électriques véhiculés par les bus. L'analyse de ces données permet de compléter les résultats de la méthode évoquée précédemment. Ces micro-pointes peuvent également être utilisées pour modifier la valeur des points mémoires [26].
- La modification du circuit : un faisceau d'ion localisé peut être utilisé pour réaliser des dépôts et fabriquer ainsi des pistes, des isolants et même des composants semi-conducteurs [27]. En particulier, les fusibles des circuits de test peuvent être reconnectés afin d'autoriser la transmission des signaux cachés vers l'extérieur.

Les attaques invasives offrent de bons résultats. Cependant, elles nécessitent des moyens expérimentaux importants. Par conséquent, les pirates privilégient généralement des méthodes moins coûteuses, mais non moins complexes.

I.3.3 Attaques non-invasives

I.3.3.1 Attaques logiques

Les attaques logiques sont des méthodes purement logicielles. Elles exploitent les limites des algorithmes cryptographiques et les défauts du système d'exploitation. Tandis que les systèmes embarqués atteignent des niveaux de complexité élevés, les contraintes liées à la réduction des délais de commercialisation (« time-to-market ») n'ont jamais été aussi fortes. De ce fait, le nombre de défauts logiciels ne cesse d'augmenter, et ce, malgré la qualité des outils de vérification utilisés pendant les phases de test [28]. L'objectif des attaques logiques est donc de transformer ces limites et défauts en failles sécuritaires. On distingue essentiellement sept catégories d'attaque logique :

- ∞ L'attaque par force brute [17] : elle consiste en une recherche directe de la clé secrète par une procédure exhaustive de type essai-erreur.
- ∞ Le protocole cryptographique : il s'agit d'exploiter des défauts du protocole cryptographique. Par exemple, la faible entropie de certains générateurs de nombres pseudo-aléatoires peut rendre prévisible les séquences générées par ces derniers.
- ∞ Les commandes cachées : le système d'exploitation peut distinguer plusieurs dizaines de milliers de commandes. Certaines commandes sont destinées uniquement à la phase de développement et sont ensuite mises hors service. Cependant, la désactivation de certaines d'entres elles peut être accidentellement omise. Ces commandes rémanentes peuvent être utilisées pour manipuler les données et perturber le fonctionnement du système.
- ∞ L'empoisonnement des paramètres : une commande s'accompagne généralement d'un ou plusieurs paramètres. Un paramètre volontairement erroné, c'est-à-dire de valeur ou de dimension non autorisé, peut, au lieu d'entraîner un rejet, conduire à un dysfonctionnement du système.
- ∞ L'accès aux fichiers : le système de fichier des cartes à puce présentent une gestion précise des niveaux de permissions associés aux fichiers et aux répertoires. Cependant, il peut arriver qu'une succession complexe de procédures autorise un niveau d'accès trop élevé.
- ∞ Le microprogramme malveillant : si un pirate arrive à charger un cheval de Troie dans le système ou à abuser des défauts d'une application existante, il peut l'utiliser pour pénétrer et attaquer les autres modules du système.
- ∞ Le protocole de communication : les échanges d'informations entre une carte à puce et un terminal sont régis par un protocole normalisé (cf. section I.1). En envoyant des messages ne respectant pas ces règles, il est possible d'amener la carte à transmettre des données secrètes.

Ces attaques nécessitent un équipement restreint et sont relativement simples à mettre en œuvre, mais leurs chances de succès restent assez faibles. Par conséquent, les pirates expérimentés se tournent généralement vers des méthodes plus élaborées, comme, par exemple, les attaques sur les canaux cachées.

I.3.3.2 Attaques sur les canaux cachés

L'implémentation électronique d'une fonction cryptographique dégrade fortement son potentiel sécuritaire. En effet, l'activité d'un composant électronique engendre des variations d'une multitude de grandeurs physiques. Par conséquent, dans le cas d'une architecture complexe, ces variations sont nécessairement corrélées à l'activité du système et aux données qu'il manipule. D'un point de vue cryptographique, ces fuites sont modélisées par l'intermédiaire de canaux de communications parasites dits « canaux cachés ». Ces derniers sont illustrés sur la figure I.8.

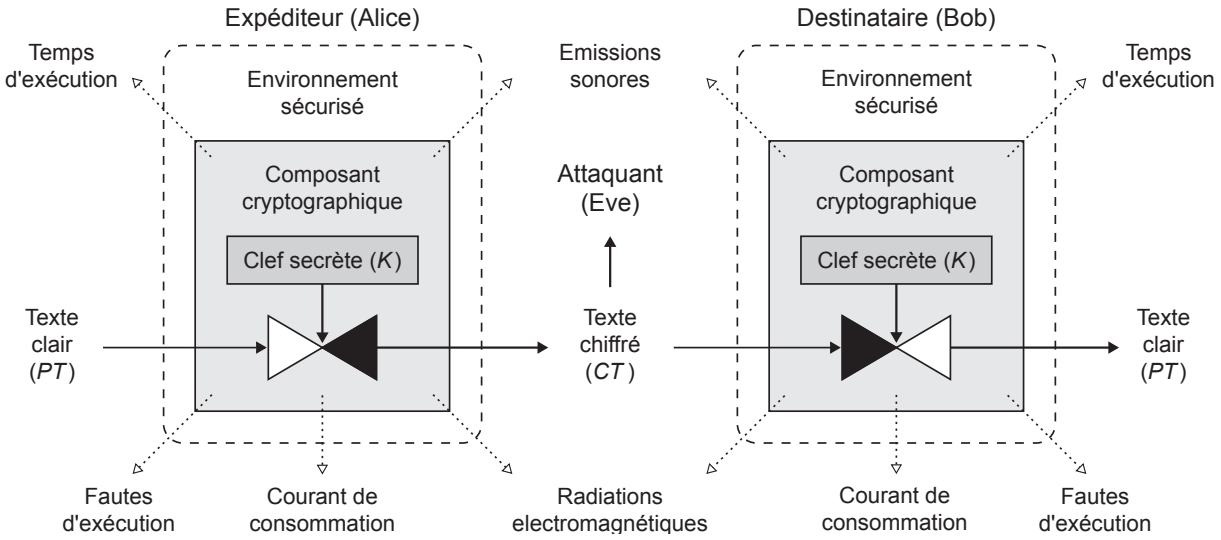


Fig. I.8 – *Canaux cachés d'un cryptosystème.*

Les types de fuites les plus exploitées sont : le temps d'exécution des tâches, les fautes d'exécution, le courant de consommation, les radiations électromagnétiques induites et les émissions sonores. Les attaques sur les canaux cachées reposent sur l'analyse des informations véhiculées par ces fuites. Leur principal objectif est de déterminer les valeurs des paramètres secrets manipulés par les algorithmes cryptographiques. Depuis leurs apparitions à la fin des années 90, elles n'ont cessé de se multiplier et de se perfectionner jusqu'à devenir une des préoccupations majeures de la cryptographie moderne. Chaque type de canal caché a donné naissance à une ou plusieurs catégories d'attaques. On en distingue essentiellement cinq :

- ∞ L'attaque temporelle : le temps d'exécution associé à une opération cryptographique peut être exploité pour déterminer la structure de l'algorithme et la valeur des paramètres [2].
- ∞ L'attaque par injection de faute : en perturbant les caractéristiques des signaux nécessaires au fonctionnement de la puce (tensions d'alimentation, fréquence du signal d'horloge, etc.), ou en plaçant cette dernière dans un environnement agressif (température, radiations électromagnétiques, lumière, rayons X, etc.), le système peut être placé dans un état de fonctionnement imprévu pouvant conduire à la divulgation d'informations secrètes. Par exemple, l'attaque DFA [29] repose sur la comparaison de textes chiffrés valides, obtenus dans des conditions normales, et de textes chiffrés erronés, obtenus par injection de fautes.

- ∞ L'attaque par analyse en courant : l'activité d'un système électronique se traduit par des variations de son courant d'alimentation. L'analyse de ces variations permet de déterminer les données confidentielles manipulées par le système [30, 31]. Dans le cas des cartes à puce, les dimensions du support obligent à externaliser la source d'énergie. Par conséquent, les signaux d'alimentation sont directement accessibles. C'est également au travers du canal de consommation que l'on obtient le canal temps [1].
- ∞ L'attaque électromagnétique (« *TEMPEST attack* » [32, 33] dans la littérature américaine) : les rayonnements électromagnétiques sont porteurs d'une information locale relative à l'activité de quelques dizaines de portes. Ainsi, ces signaux peuvent être analysés au même titre que la consommation électrique. Les techniques d'analyse de type EMA [34] reposent sur ce principe. Dans le cas des cartes à puce sans contact, le circuit est alimenté par l'énergie des ondes radios. De ce fait, aux abords de la carte, les variations du champ magnétique sont nécessairement corrélées à la consommation du produit. Cette catégorie de fuites est exploitée par les attaques de type RFA [35]. D'autres sources de rayonnement, comme par exemple la chaleur, ne font pas encore, à ce jour, l'objet d'études approfondies [1].
- ∞ La cryptanalyse acoustique [36] : l'activité des composants électriques engendre des vibrations sonores. Par conséquent, cette gamme de fréquence peut être elle-aussi exploitée.

Le travail de thèse présenté dans ce rapport portant essentiellement sur la protection des cartes à puce contre les attaques par analyse du courant de consommation, celles-ci sont développées plus en détail dans la section suivante.

I.3.4 Attaque par analyse du courant de consommation

I.3.4.1 Introduction

L'inverseur est l'une des cellules élémentaires les plus utilisées. Un inverseur en technologie CMOS est représenté sur le schéma de la figure I.9. Lorsqu'il est sollicité à la fréquence f_s, sa consommation totale est donnée par [37, 38] :

$$P_i = \underbrace{p_t.V_{DD}^2.C_L.f_s}_{P_{i,L}} + \underbrace{p_t.V_{DD}.I_{sc}.f_s}_{P_{i,sc}} + \underbrace{V_{DD}.I_l}_{P_{i,l}} \tag{I.1}$$

où p_t est la probabilité de transition du signal entrant, C_L la capacité de charge, V_{DD} la tension d'alimentation, f_s la fréquence de commutation, I_{sc} le courant de court circuit associé au chemin direct et I_l le courant de fuite en régime statique. Par conséquent, le terme $P_{i,L}$ est consécutif à la charge de C_L, le terme $P_{i,sc}$ résulte du court-circuit intervenant entre V_{DD} et la masse lorsque le transistor NMOS et le transistor PMOS sont tous deux passants, et le terme $P_{i,l}$ dépend essentiellement du courant I_{off} de la technologie CMOS employée. Un modèle probabiliste plus complet est proposé dans [39], toutefois, l'expression I.1 est suffisante pour aborder la problématique des attaques par analyse du courant de consommation.

Les figures I.9 et I.10 illustrent la consommation d'un inverseur CMOS lors d'un front montant (évènement « 0→1 » en entrée) et lors d'un front descendant (évènement « 1→0 » en entrée). Lors d'un front montant ($1ns \leq t \leq 2ns$), l'alimentation fournit simultanément les courants I_L et I_{sc}. Lors de la transition

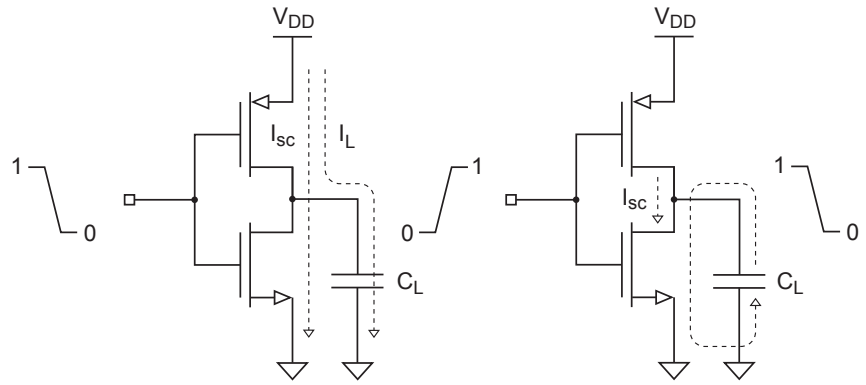


Fig. I.9 – *Consommation dynamique d'un inverseur CMOS.*

réciproque $(2.5ns \leq t \leq 3.5ns)$, l'énergie préalablement stockée dans C_L est dissipée à travers le transistor NMOS. Dans ce cas, l'alimentation délivre uniquement le courant I_{sc}. L'asymétrie de ces transferts de charge véhicule donc une information corrélée aux données manipulées par la porte. Un circuit est généralement alimenté à tension quasi-constante. Par conséquent, les variations de la puissance qu'il consomme sont proportionnelles à celles du courant qui le traverse. La simple observation du courant d'alimentation d'un inverseur permet donc de conclure sur la nature des données transmises par ce dernier.

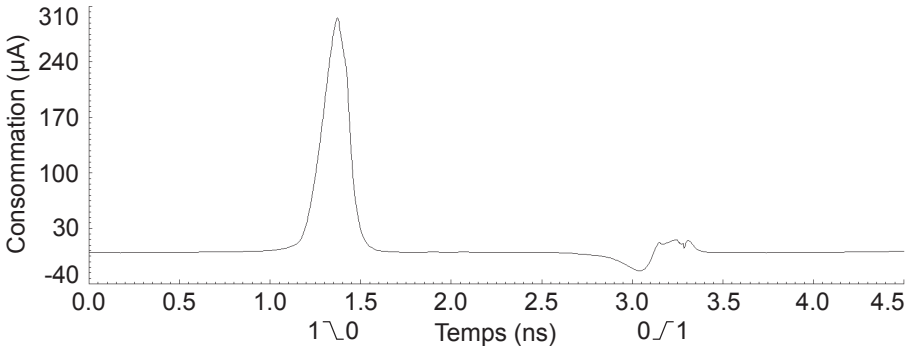


Fig. I.10 – *Courant de consommation d'un inverseur CMOS (IN : 1→0 puis 0→1).*

L'inverseur n'est pas un cas isolé; la majorité des cellules élémentaires classiques (portes logiques, registre, additionneur, multiplieur, etc.) présente la même caractéristique. Par conséquent, le principe de superposition linéaire permet d'étendre ce concept à l'échelle d'un système. En effet, aussi complexe soit il, un circuit numérique consiste principalement en la mise en parallèle d'un grand nombre de cellules élémentaires. De fait, son courant de consommation global n'est autre la somme des courants élémentaires traversant chacune de ses cellules constitutives. Ainsi, l'analyse des informations véhiculées par le courant d'alimentation d'un système permet de déterminer : la structure de son architecture, la nature des algorithmes qu'il exécute, et même, la valeur des données qu'il manipule.

D'après [40] et [41], il existe principalement deux types de corrélations entre la valeur d'une donnée manipulée et la consommation en courant : la corrélation au poids de Hamming de la donnée (c'est-à-

dire, au nombre de bits « 1 » que comporte la donnée) et la corrélation au nombre de transitions vécues par la donnée (c'est-à-dire, au poids de Hamming du XOR entre l'ancienne et la nouvelle valeur de la donnée). Lorsqu'une donnée est préchargée sur un bus, la consommation dépend du nombre de capacités à décharger, et donc, du nombre de « 1 » que comporte la donnée. Par conséquent, le poids de Hamming de la donnée est corrélé à la somme des contributions $\{P_{(inv,C_L)_i}\}_{(1\leq i\leq n)}$ (cf. eq.I.1) des n portes pilotant le bus. Lorsque la valeur d'une donnée change, la consommation dépend du nombre de bits qui sont modifiés. En effet, chaque bit du bus pilote un cône logique. Ainsi, plus le nombre de transitions est important, plus le nombre de commutations de porte l'est également. En d'autres termes, le nombre de transitions subis par une donnée est corrélé à la somme des contributions $\{P_{(inv,cc)_i}\}_{(1\leq i\leq m)}$ (cf. eq.I.1) des m portes pilotées par le bus.

Les premières attaques par analyse du courant de consommation ont été proposées en 1998 par les professeurs P. Kocher, J. Jaffe et B. Jun [30]. Les deux techniques décrites dans cet article, la SPA et la DPA, ont pour objectif avoué de déterminer la clé secrète d'un cryptosystème. Au moment de leur parution, la quasi-totalité des cartes à puce disponibles sur le marché étaient vulnérables à ces attaques. La SPA et la DPA sont respectivement à l'origine des attaques dites « simples » et des attaques différentielles. Ces deux familles constituent, à ce jour, les deux principales catégories d'attaques par analyse du courant.

I.3.4.2 Simple Power Analysis (SPA)

La méthode SPA repose sur une interprétation directe d'une trace du courant de consommation collectée pendant les opérations cryptographiques. Le dispositif schématisé sur la figure I.11 permet de réaliser cette mesure. Afin de limiter l'amplitude des perturbations, la valeur de la résistance R est prise faible.

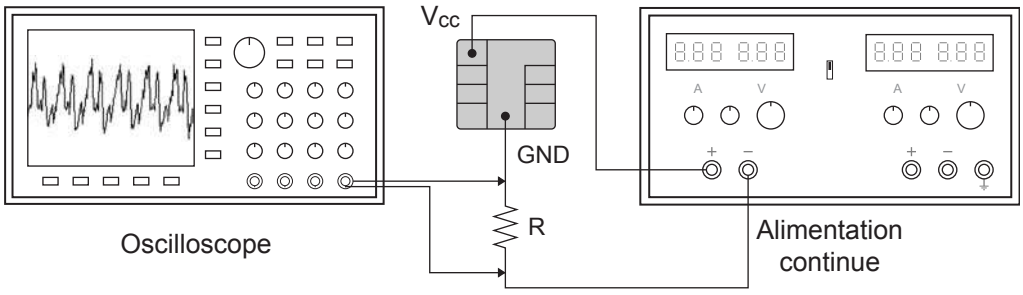


Fig. I.11 – *Dispositif de mesure du courant de consommation d'une carte à puce.*

L'exemple proposé dans [31] est représenté sur la figure I.12. Il s'agit de l'enregistrement du courant consommé par une carte à puce lors de l'exécution d'un DES. On peut facilement distinguer la présence d'un motif se répétant 16 fois. Il s'agit des 16 rondes de DES décrites dans la sous-section I.2.1.

La figure I.13 présente une vue plus détaillée des seconde et troisième rondes de DES. A cette échelle, des différences entre les rondes deviennent perceptibles. Par exemple, les 28 bits des registres de clé C et D subissent une rotation pendant la seconde ronde (flèche de gauche), tandis qu'ils en subissent deux dans la troisième ronde (flèches de droite). Ces différences sont la conséquence des branchements conditionnels

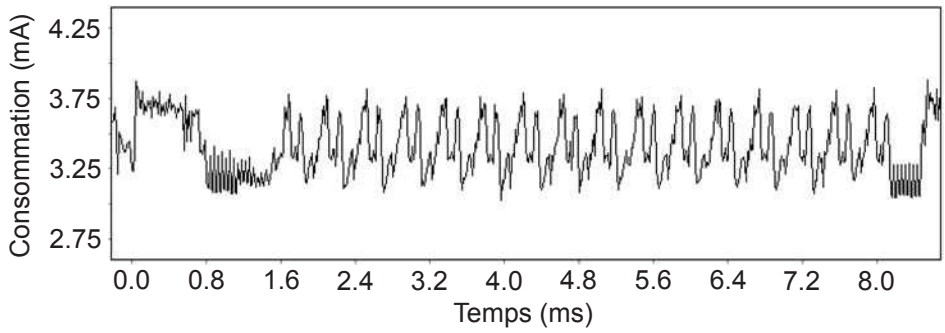


Fig. I.12 – *Courant de consommation d'une carte à puce exécutant un DES [31].*

basés sur les bits de la clé secrète K.

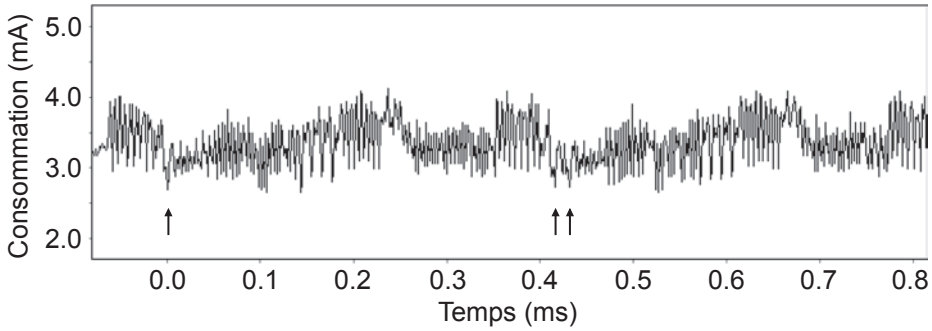


Fig. I.13 – *Courant de consommation d'une carte à puce pendant la* $2^{ème}$ *et la* $3^{ème}$ *ronde de DES [31].*

La mise en corrélation du code exécuté par un produit non sécurisé avec son courant de consommation permet donc, par adaptation de l'échelle d'observation, d'isoler les signatures moyennes associées à chaque type de commande, de boucle ou d'algorithme. Par suite, la création d'une bibliothèque de motifs classifiés permet de déterminer le code associé à une trace par identification dichotomique de ses signatures constitutives [42]. Puisque la méthode SPA permet de révéler la séquence des instructions exécutées, elle peut être utilisée pour pirater les systèmes cryptographiques dont le chemin d'exécution dépend de la valeur des données traitées. C'est par exemple le cas pour :

- Le DES : lors d'une opération de rotation de la clé, un branchement conditionnel est utilisé pour prendre en compte la valeur de son dernier bit (cf. sous-section I.2.1). La signature en courant du branchement est différente selon que le bit sortant est un « 0 » ou un « 1 ». L'observation de chacune des rondes permet donc de révéler les 56 bits de la clé. Cette différence de consommation est également perceptible dans le cas d'une opération de permutation.

- Le RSA : lors d'une exponentiation binaire, une opération de mise au carré est effectuée pour chaque bit de l'exposant. Lorsque le bit traité vaut « 1 », l'opération de mise au carré est suivie d'une multiplication. Or, une opération de multiplication requiert un plus grand nombre de manipulations qu'une opération de mise au carré. Par conséquent, la largeur relative de son pic de consommation

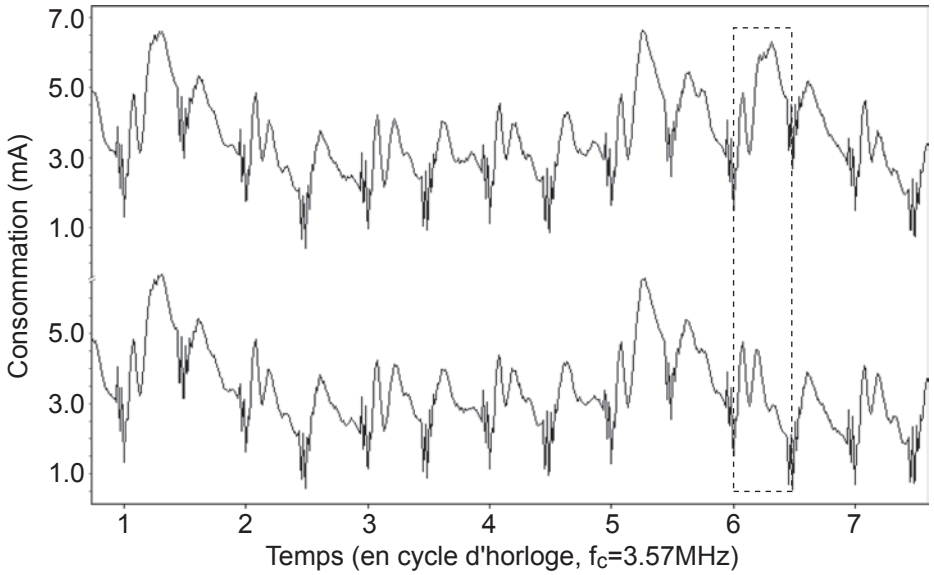


Fig. I.14 – *Signatures en courant d'un des branchements conditionnels du DES [43].*

est plus importante. La figure I.15 présente la consommation en courant d'une carte à puce calculant une signature RSA [43]. Chacun des neufs pics correspond à une opération de mise au carré ou de multiplication. La succession d'une mise au carré et d'une multiplication indique que le bit de clé est un « 1 ». L'analyse de cette trace permet donc de déterminer cinq bits de la clé : 00111.

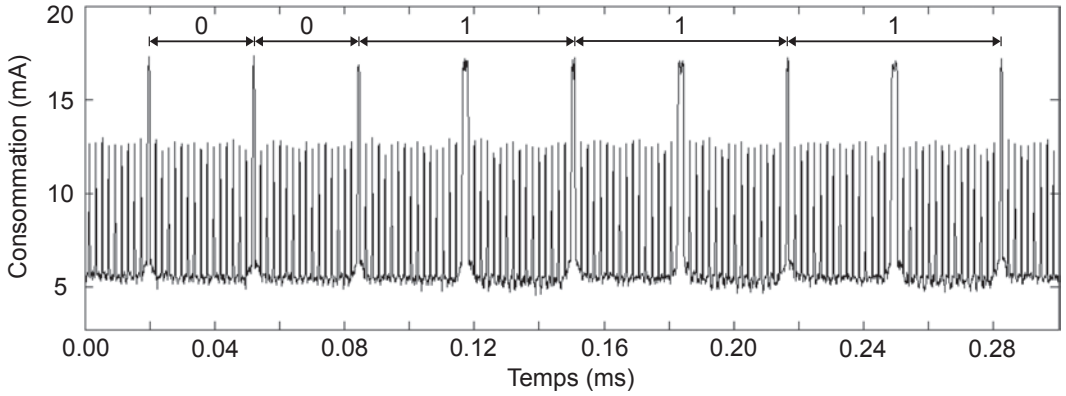


Fig. I.15 – *Courant de consommation d'une carte à puce calculant une signature RSA [43].*

Les variations à grande échelle dues aux séquences d'instructions ne sont pas les seules informations véhiculées par le courant d'alimentation. Ce dernier comporte des variations de plus faible amplitude qui sont également corrélées aux données manipulées. Lors d'une observation directe, ces variations sont indiscernables du bruit. En effet, un module cryptographique est généralement enfoui dans un système complexe. De fait, son signal de consommation est entièrement noyé dans le bruit d'alimentation global du système. Ce masquage naturel complique significativement la mise en œuvre de l'attaque SPA. L'attaque DPA permet de prendre le relais lorsqu'une inspection visuelle directe n'est plus suffisante.

I.3.4.3 Differential Power Analysis (DPA)

La DPA est une méthode d'analyse statistique différentielle permettant d'extraire des différences infinitésimales entre des mesures de consommation. Sa construction est proche de celle d'un test d'hypothèse. Son objectif est de décider si le composant cryptographique traite la donnée qui lui est fournie avec une clé supposée k. A cet effet, des caractéristiques relatives aux données qui seraient traitées sous cette hypothèse de clé, et l'observation des fuites pendant plusieurs exécutions de l'algorithme avec la clé inconnue, sont exploitées pour décider si l'hypothèse correspond ou non à la clé inconnue [1].

La première étape de l'attaque consiste à créer une fonction de sélection $D(C,K)$ dont la structure dépend de l'algorithme à cryptanalyser, du texte chiffré C et de la clé secrète à déterminer K. Puis, pour chaque valeur possible $k\in \{1,...,m\}$ de K, on encrypte n textes clairs aléatoires $\{P_{k,l}\}_{(1\leq l\leq n)}$. A chaque exécution de l'algorithme cryptographique, on mesure la consommation en courant correspondante $T_{k,l}$, on enregistre le texte chiffré résultant $C_{k,l}$ et on évalue par simulation la valeur de la fonction de sélection $D(C_{k,l},k)$. Dans le cas d'une attaque sur le DES, l'oracle D évalue la valeur d'un bit : si $D(C_{k,l},k)= 0$, la trace $T_{k,l}$ est classée dans la catégorie 0_k; sinon, la trace $T_{k,l}$ est classée dans la catégorie 1_k :

$$0_k = \{T_{k,l}|D(C_{k,l},k) = 0\}_{(1\leq l\leq n)} \tag{I.2}$$

$$1_k = \{T_{k,l}|D(C_{k,l},k) = 1\}_{(1\leq l\leq n)} \tag{I.3}$$

Si l'hypothèse sur la valeur de la clé est correcte, la prédiction faite par la fonction de sélection est correcte. La fonction D et la puissance consommée sont donc corrélées à la valeur des bits considérés. Par conséquent, le classement est correct. Dans le cas contraire, la prédiction faite par la fonction de sélection ne correspond pas à une activité particulière au sein du canal et le classement est totalement arbitraire. Pour chaque k, la pertinence du classement est évaluée en faisant la différence Δ_k entre la moyenne des courbes de consommation de la catégorie 0_k et la moyenne des courbes de consommation de la catégorie 1_k :

$$\Delta_k = \frac{1}{|0_k|}\sum_{T_{k,l}\in 0_k} T_{k,l} - \frac{1}{|1_k|}\sum_{T_{k,l}\in 1_k} T_{k,l} \tag{I.4}$$

Si k est correcte, la courbe de Δ_k présente des pics sur l'intervalle où D traite les bits correspondants. Dans le cas contraire, la courbe de Δ_k s'apparente à du bruit. La comparaison des courbes de $\{\Delta_k\}_{k\in\{1,...,m\}}$ permet donc d'identifier la valeur correcte de K.

Dans le cas du DES, l'attaque DPA permet de déterminer, par bloc de 6 bits, la sous-clé K_i de 48 bits intervenant à la i-ème ronde de DES (cf. sous-section I.2.1). Par exemple, pour déterminer la valeur du premier sextet $K_{1,1}$=$K_1[0:5]$ de la sous-clé K_1 correspondant à la première S-Box (S_1) du premier tour de DES, on peut utiliser la fonction de sélection suivante [31, 30] :

$$D\left(C_{k,l}[0],C_{k,l}[0:5],k\right) = C_{k,l}[0] \oplus S_1\left(C_{k,l}[0:5] \oplus k\right) \tag{I.5}$$

où $k \in \{000000,...,111111\}$ et $\oplus$ symbolise la fonction XOR. Pour déterminer les 48 bits de la sous-clé K_1, il suffit d'itérer cette méthode pour les 8 S-Boxs de la première ronde de DES. Une description détaillée de cette attaque et de certaines de ses variantes sont rapportées dans [44] (DES au § 1.1.2 et RSA au § 4.3).

Les courbes de la figure I.16 résultent d'une attaque DPA menée sur le DES d'une carte à puce [31]. La courbe du haut représente le courant de consommation moyen de la puce (I_{avg}) sur l'intervalle temporel correspondant à l'exécution du DES. Les trois courbes placées sous cette référence sont des traces différentielles. Chacune correspond à une sous-clé k différente; la première a été réalisée à partir de la sous-clé correcte, tandis que les deux suivantes correspondent à des sous-clés incorrectes. Chaque trace a été préparée à l'aide de 1000 enregistrements du courant de consommation (n=10^3). Bien que le niveau de bruit soit assez élevé, le pic dénonciateur apparaît clairement.

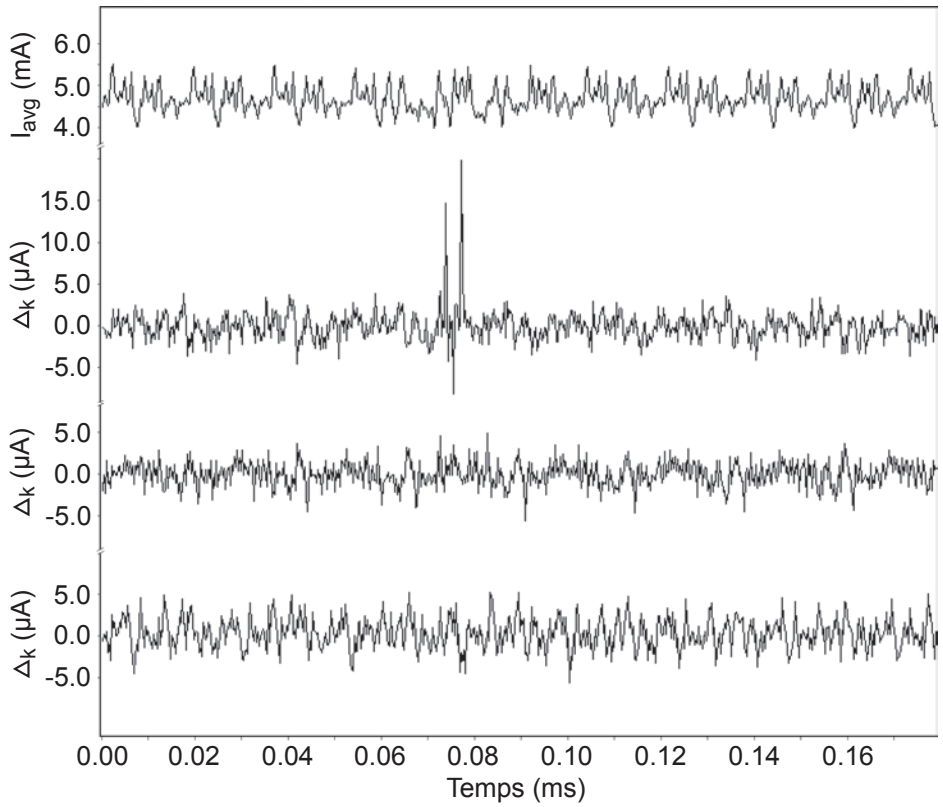


Fig. I.16 – *Traces d'une attaque DPA sur un DES : I_{avg} et 3 sous-clés k dont une correcte (n=10^3) [31].*

Alors que la signature associée à la consommation d'un transistor est quasiment impossible à identifier par le biais d'une observation directe, les traitements statistiques de la DPA permettent de mettre en évidence des différences de consommation extrêmement faibles. Toutefois, la mise en œuvre d'une attaque de ce type nécessite une bonne connaissance de l'algorithme cryptographique visé. De plus, elle n'est applicable que si le processus étudié fournit une information statistiquement observable.

Depuis 1998, un grand nombre d'attaques basées sur l'analyse de la consommation ont été proposées dans la littérature. Par exemple, dans la catégorie des attaques directes, la méthode IPA [45] permet de porter une attaque sur un système cryptographique sans avoir accès ni aux messages, ni aux chiffres. Une extension de l'attaque DPA, baptisée Ho-DPA [46, 47, 48], consiste à considérer simultanément plusieurs points de la courbe de consommation. L'attaque par caractérisation du bruit (attaque « *Template* ») repose, quant à elle, sur une approche radicalement différente. En effet, contrairement aux attaques de type DPA,

l'attaque *Template* [49] cherche à exploiter les caractéristiques du bruit d'alimentation et non à s'en défaire. D'autres attaques plus spécifiques ont également été proposées : SW-DPA [50], PODPA [40], BPA [40], DiPA [40], RPA [51], ZPA [52], etc. Cette liste, volontairement longue, n'a pas pour vocation d'être exhaustive. L'objectif est ici de faire prendre conscience au lecteur de l'importance des recherches en cours dans ce domaine.

I.4 Contre-mesures embarquées

Dans l'idéal, la consommation d'un système cryptographique doit être décorrélée de la valeur des données manipulées. D'un point de vue logiciel, ceci implique que le déroulement des algorithmes cryptographiques ne doit présenter aucune différence observable lors du traitement de deux valeurs différentes. Cette condition nécessaire n'est toutefois pas suffisante. En effet, comme nous l'avons vu à la sous-section I.3.4, la consommation au niveau porte est elle-même corrélée à la valeur des données traitées. Par conséquent, une décorrélation totale requiert également une logique adaptée. Il apparaît clairement que la réalisation d'un système cryptographique idéal présente de nombreuses difficultés. Une approche défensive complémentaire, adoptée par la majorité des contre-mesures parues à ce jour, consiste à masquer les corrélations persistantes en diminuant le rapport signal sur bruit. Dans le cadre des attaques sur le canal de consommation, on distingue essentiellement deux catégories de contre-mesures : les contre-mesures logicielles et les contre-mesures matérielles.

I.4.1 Contre-mesures logicielles

Les contre-mesures logicielles sont de loin les moins coûteuses, car elles ne nécessitent pas de modifications de la couche matérielle. Les plus répandues sont :

- ∞ Les algorithmes invariants : il s'agit d'algorithmes dont le déroulement et le temps d'exécution sont indépendants de la donnée traitée. Par exemple, la suppression des branchements conditionnels fonctions de la valeur traitée permet de diminuer significativement la faisabilité des méthodes d'analyse directes. Toutefois, dans certains cas, ces branchements sont difficilement remplaçables.

- ∞ Les courbes elliptiques [53, 54] : ces objets mathématiques peuvent être utilisés lors des opérations asymétriques (à « clé publique », cf. sous-section I.2.2). Dans ce cas, les deux partenaires de communication, Alice et Bob, se mettent publiquement d'accord sur une courbe elliptique et sur un point p de cette courbe. Secrètement, Alice choisit un entier a et Bob un entier b. Puis Alice envoie à Bob la donnée $a.p$, tandis que Bob envoie à Alice la donnée $b.p$. Chacun des deux partenaires est alors capable de calculer $a.(b.p) = b(a.p)$ qui est un point de la courbe et constituer ainsi leur clé secrète commune. Si un attaquant, nommé par convention Eve, souhaite déterminer la clé secrète, il lui faut résoudre le logarithme discret sur une courbe elliptique, ce qui, à l'heure actuelle, nécessite un temps de calcul largement supérieur à la durée moyenne d'une communication. A niveau de sécurité équivalent, un algorithmes cryptographique basé sur une courbe elliptique (ECC) requiert une clé de plus petite dimension qu'un algorithme RSA. En outre, si les attaques différentielles représentent une menace sérieuse pour les algorithmes RSA, en revanche, elles sont inefficace sur les systèmes à base de courbes elliptiques, ces derniers utilisant un secret éphémère à chaque instance du protocole.

- ∞ Le partage du secret [55, 56] : la donnée sensible est découpée en éléments, puis chaque élément est traité séparément. D'après [55], le nombre d'échantillons nécessaires à l'aboutissement d'une attaque de type DPA augmente exponentiellement avec le nombre d'éléments. Cependant, la diminution des performances du système suit une loi du même type.

- ∞ Le masquage aléatoire des données [57, 58] : comme nous l'avons vu à la sous-section I.3.4, les variations du courant de consommation sont corrélées au poids de Hamming des données manipulées (les opérandes). Par conséquent, cette information peut être masquée en ajoutant à l'opérande une valeur aléatoire qui lui est retranchée à la fin du traitement. Néanmoins, la structure du traitement doit prendre un compte les effets du masquage, au risque d'engendrer des résultats faux.

- ∞ Les algorithmes aléatoires : si un algorithmes de chiffrement repose sur des processus aléatoires, la fenêtre temporelle associée au traitement d'un bit donné sera différent d'une exécution à une autre. De nombreux processus de ce type ont été proposés : exponentiation aléatoire [59], fenêtre aléatoire [60], séquençage aléatoire des instructions [61], décalage temporel aléatoire [56], coordonnées de projection aléatoires [58, 62], etc. Dans tous les cas, la gène occasionnée est équivalente : il devient beaucoup plus difficile d'aligner les traces et d'isoler le signal d'intérêt. Toutefois, ce type de contre-mesure augmente significativement le temps d'exécution. De plus, la cryptanalyse basée sur les modèles HMM [63] a récemment démontré l'inefficacité d'un grand nombre d'entre elles.

L'apparition d'une contre-mesure donne systématiquement naissance à de nouvelles attaques. Un bon niveau de sécurité ne peut donc être atteint et conservé qu'à condition de combiner plusieurs types de protections et de faire évoluer constamment ces dernières [64]. Aussi les concepteurs sont-ils obligés d'ajouter des contre-mesures matérielles à leur arsenal algorithmique, et ce malgré le coût induit.

I.4.2 Contre-mesures matérielles

Les contre-mesures matérielles les plus répandues sont :

- ∞ La logique asynchrone [4, 65] : l'utilisation d'une logique asynchrone permet de réduire l'amplitude des signatures en courant. En effet, parce qu'à la différence de la logique synchrone, la logique asynchrone n'est pas cadencée par un signal périodique, son spectre de puissance est plus uniforme [66]. Au premier abord, cette logique dite « *data driven* » peut sembler être un mauvais candidat dans la mesure où les temps de traitement sont caractéristiques des données traitées. Cependant, la technique QDI [67] permet d'équilibrer les chemins de données afin de ne pas faire apparaître de différences observables au sein du canal de consommation. Malgré les déséquilibres réintroduits par la phase de placement-routage, cette méthode offre de bons résultats. Une autre catégorie de logique, la GALS [66], propose un compromis entre l'approche synchrone et l'approche asynchrone.

- ∞ La logique dupliquée à fonctionnement complémentaire : comme nous l'avons vu à la sous-section I.3.4, c'est la dissymétrie des transferts de charges qui est à l'origine de l'information portée par le canal. Par conséquent, si chaque porte logique présente une porte jumelle au fonctionnement complémentaire, la signature de l'ensemble est théoriquement équilibrée et donc indépendante de

l'événement traité. Néanmoins, un circuit à logique conjuguée consomme quasiment deux fois plus d'énergie que son homologue à logique simple.

∞ Les logiques dynamiques et différentielles : la logique SABL [68] est une logique dynamique (à pré-charge) et différentielle (deux fils par signal) issue de la logique DCVSL [69]. Contrairement à une porte classique, une porte SABL présente un événement de commutation par cycle, quelle que soit la valeur en entrée. De plus, la charge absorbée est quasiment indépendante du type de la transition. Par conséquent, quel que soit l'évènement traité, les différences de consommation sont difficilement perceptibles. La logique WDDL [70] adopte un principe équivalent, mais repose uniquement sur des cellules CMOS standards. Par rapport à une logique traditionnelle, la surface est multipliée par 3.5 et les performances sont divisées par 2. La réalisation de fils complémentaires à charge équilibrée est une des difficultés majeures associées à l'implémentation des logiques citées précédemment. Pour améliorer l'équilibrage des charges de commutation, la logique Dual-Spacer DRP [71] alterne, à chaque cycle, entre deux états de pré-charge différents. Pour échapper à cette même contrainte, la logique MDPL [72], qui repose sur des cellules standards, opère un masquage par randomisation des signaux. Cependant, la commutation systématique des portes entraîne une dissipation énergétique importante. La logique DyCML [73] permet de limiter cette surconsommation grâce à l'utilisation d'une source de courant dynamique. Le résultat est identique avec un rendement énergétique supérieur et un meilleur délai de transmission.

∞ La logique à commutation aléatoire : la logique RSL [39] utilise une entrée aléatoire par porte et introduit un signal de validation (EN pour « *enable* »). Le signal EN force la sortie de la porte à une valeur définie jusqu'à ce que tous les signaux d'entrées soient stables. Elle permet ainsi d'équilibrer la probabilité de transition des portes. Cependant, elle requiert une synchronisation trés précise des signaux de validation.

∞ L'injection directe de bruit sur l'alimentation : l'objectif est de noyer l'information dans du bruit. Cette contre-mesure fut une des premières mises en œuvre pour contrer les attaques directes. Cependant, pour qu'elle soit efficace, le signal du courant d'alimentation doit tendre vers un bruit blanc, ce qui implique une surconsommation très importante. En outre, le bruit injecté est généralement additif, par conséquent, cette protection résiste mal aux attaques statistiques différentielles.

∞ Les interruptions aléatoires de processus [50] : les RPI sont les pendants matériels des interruptions algorithmiques. Au lieu d'exécuter séquentiellement le code, le microprocesseur alterne aléatoirement entre les algorithmes d'intérêt et des instructions factices. Cette désynchronisation engendre un effet connu en traitement du signal sous le nom de moyennage incohérent (« *incoherent averaging* ») [74].

∞ Un signal d'horloge aléatoire [55] : en cadençant le système à l'aide d'un signal d'horloge à fréquence ou à gigue de phase aléatoire, on produit un effet de masquage similaire à celui obtenu dans le cas des interruptions aléatoires.

∞ Le filtrage de l'alimentation : l'utilisation d'un régulateur linéaire à dérivation (« *shunt regulator* ») permet de diminuer significativement l'amplitude des signatures en courant [75]. Encore plus efficace, l'intégration d'un régulateurs à commutation permet de décorréler quasi-totalement le cou-

rant d'alimentation externe (celui fourni par le lecteur) du courant d'alimentation interne (celui consommé par le microcontrôleur) [76]. Cependant, comme nous le verrons au chapitre suivant, ces convertisseurs ne permettent pas d'atteindre simultanément tous les objectifs fixés par STMicroelectronics.

En définitive, la majorité des contre-mesures matérielles nécessite de mettre en œuvre des librairies et des circuits spécifiques devant évoluer aux rythmes des attaques et des technologies. Par ailleurs, le remplacement d'une logique classique par une logique sécurisée se traduit généralement par une surconsommation importante et une diminution significative des performances. Toutefois, la dernière catégorie de contre-mesures évoquée précédemment ne présente pas toutes ces contraintes. En effet, la structure d'un convertisseur de tension est quasiment indépendante du circuit à protéger et, réciproquement, son implémentation n'a quasiment aucune influence sur les performances de ce dernier. Une nouvelle contre-mesure de ce type sera proposée au prochain chapitre.

Chapitre II

Système d'alimentation sécurisé

II.1 Introduction

Depuis plus de trente ans, l'application du principe de changement d'échelle [4] suivant les règles de Dennard [3] permet d'accroître la densité d'intégration et la vitesse de commutation des dispositifs MOS, tout en minimisant la dissipation de puissance. Pour des questions de fiabilité, ces homothétie sont opérées à champs électriques constants. Ainsi, toute réduction des dimensions d'un facteur donné impose une diminution des tensions suivant le même facteur [3]. Durant les années 70 et 80, la densité d'intégration à été ainsi multipliée par deux tous les trois ans. Dans le même temps, l'augmentation de la surface des puces s'est traduite par un doublement du nombre de transistors par puce tous les dix-huit mois. Depuis le milieu des années 90, le rythme des sauts technologiques s'est accéléré, tandis que l'accroissement de la surface a subi un ralentissement. En définitive, densité et nombre de transistors sont actuellement doublés tous les deux ans.

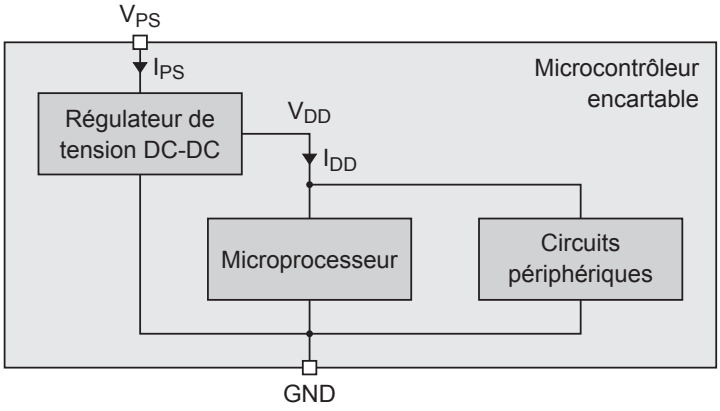


Fig. II.1 – *Système d'alimentation d'un microcontrôleur encartable.*

Pour des raisons logistiques et financières, l'évolution technologique du parc de lecteurs est plus lente que celle des cartes à puce. De fait, la tension d'alimentation supportée par le cœur de la puce est généralement inférieure à celle délivrée par le lecteur. Par conséquent, cette dernière doit être abaissée par l'intermédiaire d'un circuit embarqué sur la carte. C'est précisément le rôle du régulateur de tension continu-continu

(DC-DC) représenté sur la figure II.1; il a pour objectif de générer une tension d'alimentation interne continue (V_{DD}) à partir de la tension d'alimentation externe elle-même continue (nommée V_{PS} dans la nomenclature STM, en lieu et place de V_{cc}). La tension V_{DD} doit atteindre rapidement une valeur constante, précise et stable, quelles que soient les variations de la tension V_{PS}, du courant de charge (I_{DD}), de la température et du procédé de fabrication.

En complément de sa fonction de convertisseur, le régulateur peut être utilisé pour protéger le circuit alimenté contre les attaques par analyse en courant. En effet, certaines méthodes de conversion permettent d'atténuer significativement l'amplitude des informations véhiculées par ce dernier, voire, de décorréler complètement le courant d'alimentation externe (I_{PS}) du courant d'alimentation interne (I_{DD}). Cependant, leur implémentation n'est pas toujours compatible avec les contraintes technologiques associées aux cartes à puce. Dans le cadre de cette étude, ces contraintes ont été fixées par le partenaire industriel.

II.2 Spécifications des régulateurs de tension DC-DC

Les spécifications des régulateurs de tension DC-DC sont généralement classifiées en quatre catégories [77] : les plages de fonctionnement, la stabilité, les performances de régulation et le rendement en puissance. Les caractéristiques associées à chacune d'entre elles sont détaillées dans les sections suivantes. Dans le cadre de cette étude, nous examinerons deux critères supplémentaires : la surface et le niveau de sécurité.

II.2.1 Plages de fonctionnement

Les conditions de fonctionnement sont habituellement définies par plage de valeurs. On distingue essentiellement : la plage de tension d'entrée, la plage de tension de sortie, la plage de courant de charge et la plage de température.

Soient V_i et V_o les tensions d'entrée et de sortie du régulateur. La tension dite de (« *dropout* » désigne la tension différentielle V_i-V_o en-dessous de laquelle le circuit cesse de réguler correctement la tension de sortie [77]. Les régulateurs capables de descendre à des tensions de *dropout* (V_{do}) inférieures à $600\ mV$ sont dits « à faible chute de tension » (LDO pour « *Low Dropout* »). La tension d'entrée minimum du régulateur ($V_{i_{min}}$) peut donc se mettre sous la forme :

$$V_{i_{min}} = V_o + V_{do} \tag{II.1}$$

A l'opposé, la tension d'entrée maximum supportée par le régulateur dépend principalement de la technologie employée. Dans les filières CMOS avancées, la tension de destruction (« *breakdown voltage* ») des transistors haute tension (HV pour « *High Voltage* ») est généralement supérieure à $15\ V$.

Si la valeur maximum de plage de fonctionnement en courant du régulateur se situe sous la barre de l'ampère, ce dernier peut être classé dans la catégorie des régulateurs de faible puissance. Dans le cas contraire, il appartient à la catégorie des régulateurs de forte puissance.

II.2.2 Stabilité

Les régulateurs de tension reposent généralement sur une boucle de contre-réaction. Son principe est illustré sur le schéma de la figure II.2. La chaîne directe ($A(s)$) est constituée d'un amplificateur à fort gain,

tandis que la boucle de retour ($B(s)$) repose sur des éléments passifs de précision.

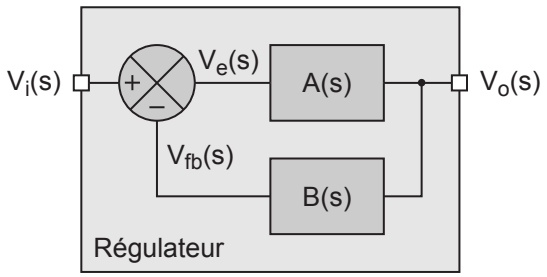


Fig. II.2 – *Système électronique bouclé à contre-réaction.*

Les amplificateurs électroniques présentent généralement un gain important mais relativement peu précis. La structure de la figure II.2 permet de convertir le surplus de gain en une fonction de transfert précise, ne dépendant que des éléments de la boucle de retour [78]. La fonction de transfert en boucle ouverte est définie par :

$$A_{ol}(s) \triangleq \frac{V_{fb}(s)}{V_e(s)} = A(s) \cdot B(s) \tag{II.2}$$

où $V_{fb}(s)$ est le tension de retour, $V_e(s)$ le tension d'erreur, $A(s)$ la fonction de transfert de la chaîne directe et $B(s)$ la fonctions de transfert de la boucle de retour. La fonction de transfert en boucle fermée est quant à elle définie par :

$$A_{cl}(s) \triangleq \frac{V_o(s)}{V_i(s)} = \frac{A_{ol}(s)}{1 + A_{ol}(s) \cdot B(s)} \tag{II.3}$$

où $V_i(s)$ et $V_o(s)$ sont, respectivement, les tensions d'entrée et de sortie du système. Si le gain de la fonction de transfert en boucle ouverte vérifie la condition $|A_{ol}(s)| \gg 1$, la fonction de transfert en boucle fermée est approximativement égale à $B(s)^{-1}$. L'erreur relative de $A_{cl}(s)$ par rapport à sa valeur idéale $B(s)^{-1}$ est donnée par :

$$G_e(s) = \frac{B(s)^{-1} - A_{cl}(s)}{B(s)^{-1}} = \frac{1}{1 + A_{ol}(s) \cdot B(s)} \cong \frac{1}{A_{ol}(s) \cdot B(s)} \tag{II.4}$$

Par rapport au système en boucle ouverte, le système en boucle fermé présente une bande passante plus large, une sensibilité moins élevée aux perturbations et une distortion plus faible. En contrepartie, la présence d'une rétroaction peut engendrer une instabilité (i.e., un régime libre ne s'amortissant pas) [78]. En effet, s'il existe une pulsation où la fonction de transfert en boucle ouverte ($A_{ol}(s)$) présente simultanément un déphasage inférieur à $0°$ et un gain supérieur ou égal à l'unité alors, à cette fréquence, la contre-réaction devient positive; le signal va se régénérer à travers la boucle et le système devient instable. En particulier, si le gain est unitaire à la pulsation ou le déphasage devient inférieur à $0°$ ($\omega_{0°}$), le critère de Barkhausen est vérifié :

$$A(j\omega_{0°}) \cdot B(j\omega_{0°}) = -1 \tag{II.5}$$

Le circuit est alors équivalent à un oscillateur sinusoïdal de pulsation $\omega_{0°}$. La pureté spectrale de ces oscillations dépend de la dérivée du déphasage en $\omega_{0°}$; la fréquence d'oscillation est d'autant plus stable que la pente du déphasage est élevée. Si le gain est supérieur à l'unité, le signal diverge jusqu'à ce que la saturation vienne limiter son amplitude. Pour un régulateur, l'apparition de ces phénomènes n'est évidemment

pas souhaitable. D'après ce qui précède, un système bouclé à contre-réaction sera stable (i.e., ne sera pas le siège d'oscillations entretenues) à condition que [78] :

$$Arg\left[A_{ol}(j\omega_{0dB})\right] > 0^{\circ} \tag{II.6}$$

où la pulsation ω_{0dB} est telle que :

$$|A_{ol}(j\omega_{0dB})| = 1 \tag{II.7}$$

La fonction de transfert en boucle ouverte est généralement de type passe-bas. Par conséquent, le tracé de son diagramme de Bode en gain présente un unique passage à $0\ dB$. Dans ce cas, le système bouclé peut être considéré comme stable si la courbe de $|A_{ol}(j\omega)|$ traverse le point à $0\ dB$ avant que la courbe $Arg\left[A_{ol}(j\omega)\right]$ atteigne 0°. Il est à noter que ce test de stabilité est une approche simplifiée du critère plus général de Nyquist [79].

La marge de phase de la fonction de transfert en boucle ouverte (Φ_M) est un critère permettant d'évaluer la stabilité d'un système bouclé. Elle est donnée par :

$$\Phi_M \triangleq Arg\left[A_{ol}(j\omega_{0dB})\right] \tag{II.8}$$

Par définition, la marge de phase conditionne le niveau d'oscillation des réponses transitoires du système bouclé (phénomène dit de « *ringing* »). Afin de limiter l'amplitude (dépassement ou « *overshoot* ») et la durée des oscillations, la marge de phase doit être supérieure à 45°. Il est communément admis qu'une marge de phase de 60° est adaptée à la plupart des situations [79].

II.2.3 Performances de régulation

La qualité de la régulation est quantifiée par l'intermédiaire de : la précision statique, la précision transitoire, la précision totale et le bruit de sortie. Ces critères sont développés dans les paragraphes suivants.

II.2.3.1 Précision statique

Les critères relatifs à la précision statique sont : le factor de regulation amont, le taux de réjection de l'alimentation, la facteur de regulation aval, la dépendance en température et en procédé de fabrication.

Le facteur de regulation amont (LNR pour « *Line Regulation* ») est la variation relative, en régime statique (i.e, établi ou permanent), de la tension de sortie par rapport à la tension d'entrée :

$$LNR \triangleq \left.\frac{\Delta V_o}{\Delta V_i}\right|_{V_{ref},I_o} \tag{II.9}$$

La réjection d'alimentation (PSR pour « *Power Supply Rejection* ») est une analyse fréquentielle du facteur de regulation amont. En d'autres termes, le facteur de régulation amont correspond à la valeur statique du PSR. On dissocie la réjection associée au nœud d'alimentation V_i (PSR^{+}) de celle associée à la masse (PSR^{-}). Le taux de réjection de l'alimentation ($PSRR$ pour « *Power Supply Rejection Ratio* ») est quant à lui défini comme l'inverse du PSR :

$$PSRR(s) \triangleq \left.\frac{\Delta V_i(s)}{\Delta V_o(s)}\right|_{V_{ref},I_o} \tag{II.10}$$

Le $PSRR$, comme le PSR, s'exprime généralement en décibel.

Le courant de charge varie en fonction de l'activité du produit alimenté. Le facteur de régulation aval (LDR pour « *Load Regulation* ») est à I_o ce que la régulation de ligne est à V_i : la variation relative, en régime permanent, de la tension de sortie par rapport au courant de charge. En d'autres termes, il s'agit de la résistance de sortie statique du régulateur (R_o):

$$LDR \triangleq R_o \triangleq \left.\frac{\Delta V_o}{\Delta I_o}\right|_{V_i, V_{ref}} \tag{II.11}$$

Les pires cas interviennent lorsque le courant de charge transite de sa valeur minimale à sa valeur maximale et vice versa.

La dépendance en température est généralement mesurée à l'aide du coefficient en température fractionnel normalisé (TC pour « *Temperature Coefficient* ») [78]:

$$TC \triangleq \frac{1}{V_{o_o}} . \frac{\partial V_o}{\partial T} \tag{II.12}$$

où V_{o_o} est la valeur optimale de la tension de sortie. Une autre mesure consiste à déterminer, sur la plage de température considérée, l'erreur relative maximum de V_o par rapport à sa valeur optimale.

La précision d'un régulateur dépend directement de la précision de ses éléments constitutifs. Or, les caractéristiques des composants intégrés sont fonction de leurs géométries et des propriétés de leurs matériaux. En particulier, la précision absolue de ces caractéristiques dépend de la tolérance des paramètres du procédé de fabrication. Certains de ces paramètres présentent une tolérance relativement élevée (parfois supérieure à $10\ \%$). Afin d'annuler les effets de ces variations globales, la structure des circuits analogiques reposent sur des ratios (de résistance, de capacité, de transistors, etc.). Ainsi, la précision du circuit est quasiment indépendante de la précision absolue de ces éléments. Cependant, elle reste sensible à d'autres effets : les fluctuations aléatoires des procédés (effet local), les gradients de procédé à « grande » échelle (effet de distance), l'influence des structures adjacentes (effet de proximité) et les caractéristiques non-isotropiques des matériaux (effet d'orientation). Ces phénomènes se traduisent par un désappariement (« *mismatch* ») des éléments unitaires supposés identiques; ils dégradent la précision relative des composants. Toutefois, certaines techniques de dessin des masques (cf. § III.4.3.2.d) permettent de réduire les effets de ces phénomènes et d'atteindre ainsi une précision relative élevée (inférieure à 1%).

De nombreux outils de simulation permettent de déterminer l'influence des précisions absolue et relative des éléments sur les performances globales des circuits. Les plus utilisés sont : l'analyse de type « *corner* » et l'analyse de type « Monte-Carlo ». La première méthode permet d'étudier les effets induits par les déviations globales du procédé de fabrication. Elle consiste à simuler le comportement du circuit en affectant aux paramètres du procédé les jeux de valeurs conduisant aux pires-cas. Bien que relativement pessimiste, cette méthode permet de vérifier rapidement si le circuit respecte les spécifications du cahier des charges. L'analyse Monte-Carlo permet, quant à elle, d'étudier l'influence du *mismatch*. Plus réaliste, cette méthode distributive nécessite cependant des temps de simulations plus importants.

Les éléments d'un même circuit présentent généralement des températures de fonctionnement différentes. Les circuits sont donc le siège de gradients de température. Ces gradients sont une source supplémentaire de *mismatch*. De plus, ils provoquent un stress mécanique qui dégrade la fiabilité des circuits. Ainsi, les dépendances en température et en procédé de fabrication sont fortement corrélées. Leurs effets sont difficilement dissociables et, s'il arrive qu'ils se compensent, ils peuvent également conduire à une synergie. Il est donc préférable de les simuler conjointement.

II.2.3.2 Précision transitoire

La réponse transitoire (ΔV_{tr}) est la variation transitoire maximale de la tension de sortie engendrée par une variation transitoire donnée du courant de charge. Elle dépend principalement du temps de réponse du régulateur et de la capacité équivalente de son nœud de sortie.

II.2.3.3 Précision totale

La précision totale du régulateur (A_{cc}) est le pourcentage d'erreur maximum de la tension V_o par rapport à sa valeur optimale. Elle prend en compte les effets : de la régulation de ligne (ΔV_{LNR}), de la régulation de charge (ΔV_{LDR}), de la dépendance en procédé de fabrication et en température du régulateur (ΔV_{PT}), de la réponse transitoire (ΔV_{tr}), ainsi que de la dépendance en procédé de fabrication, en tension d'alimentation et en température de la référence de tension (PVT pour « *Process Voltage and Temperature* »). Une hypothèse pessimiste consiste à supposer que l'erreur totale est égale à la somme linéaire des erreurs systématiques. Dans ce cas, les valeurs minimum ($V_{o_{min}}$) et maximum ($V_{o_{max}}$) de V_o sont données par [80] :

$$V_{o_{min}} \leq \Delta V_{LNR} + \Delta V_{LDR} + \Delta V_{PT} + \Delta V_{tr} + G_e \cdot V_o + V_{ref} \cdot \frac{V_{o_o}}{V_{ref_o}} \leq V_{o_{max}} \tag{II.13}$$

où V_{ref} est la tension de référence et V_{ref_o} est la valeur optimale de V_{ref} :

$$V_{ref} = V_{ref_o} + \Delta V_{PVT_{ref}} \tag{II.14}$$

où G_e est l'erreur relative de gain (cf. § II.3), $\Delta V_{PVT_{ref}}$ la variation de V_{ref} induite par les déviations cumulées du procédé de fabrication, de la température et de la tension d'alimentation. Leurs définitions sont analogues à celles données dans le cadre du régulateur. Par suite, la précision du régulateur est donnée par :

$$A_{cc} \triangleq \frac{V_{o_{max}} - V_{o_{min}}}{V_{o_o}} \cdot 100 \tag{II.15}$$

II.2.3.4 Bruit de sortie

Le bruit de sortie du régulateur est l'amplitude RMS (*Root Mean Square*) du bruit présent sur le nœud de sortie V_o en l'absence de variation du courant de charge ou de la tension d'entrée. En d'autres termes, il s'agit du bruit intrinsèque du régulateur. Les régulateurs à découpage sont généralement plus « bruyants » que leurs homologues linéaires.

Les signaux d'alimentation délivrés par les lecteurs de cartes à puces sont souvent très bruités. Les caractéristiques du bruit dépendent du type de régulateur employé par le lecteur. Lorsque ce dernier est un

régulateur à découpage, ce qui est généralement le cas pour une question de rendement, son bruit de sortie résulte principalement du mécanisme de commutation. Dans ce cas, le spectre du bruit s'étale autour de la fréquence de commutation. Cette dernière est généralement comprise entre $1\ KHz$ et $1\ MHz$ [80]. Si le régulateur du lecteur est un régulateur linéaire, les caractéristiques du bruit d'alimentation dépendent, entre autres, de son PSR^+ et de son LDR. En particulier, si son LDR est de mauvaise qualité, le bruit est alors fonction des caractéristiques du courant charge; son spectre est centré sur la fréquence de fonctionnement de la carte. Par conséquent, le PSR^+ du régulateur intégré à la carte doit être suffisamment élevé sur cette plage de fréquence.

II.2.4 Rendement en puissance

Le courant d'entrée d'un régulateur (I_i) peut se décomposer en la somme de deux courants : le courant d'entrée du ou des éléments de puissance (I_p) et le courant de repos (I_q) :

$$I_i = I_p + I_q \tag{II.16}$$

Le courant de repos désigne le courant absorbé par le régulateur en l'absence de courant de charge. Il correspond donc au courant de consommation intrinsèque du régulateur. Si le courant de fuite des éléments de puissance peut être considéré comme négligeable (ce qui est généralement le cas) le courant de repos est égal au courant de consommation du circuit de contrôle. C'est cette hypothèse qui a été retenue dans le schéma-bloc de la figure II.3.

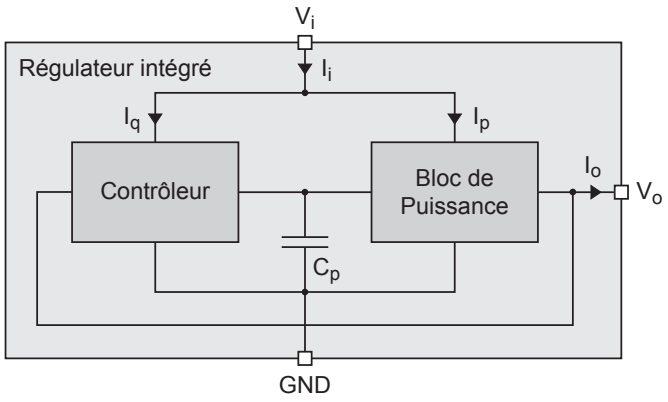


Fig. II.3 – *Schéma-bloc d'un régulateur de tension DC-DC intégré.*

Le rendement en puissance d'un régulateur (η_P) est donné par :

$$\eta_P \triangleq \frac{P_o}{P_i} = \frac{V_o \cdot I_o}{V_i \cdot I_i} \cong \frac{V_o \cdot I_o}{V_i \cdot (I_p + I_q)} \tag{II.17}$$

Les tensions V_o et V_i étant fixées par l'application, l'optimisation du rendement en puissance passe nécessairement par la maximisation du rendement en courant (η_I). Celui-ci est donné par :

$$\eta_I \triangleq \frac{I_o}{I_i} \cong \frac{I_o}{I_q + I_p} \tag{II.18}$$

Quel que soit le type de régulateur considéré, la valeur moyenne de I_q dépend fortement de la taille de la capacité parasite associée au nœud de contrôle des éléments de puissance (C_p). Dans le cas d'un régulateur linéaire, l'augmentation de I_q permet de repousser le pôle $jC_p\omega$ et donc, d'augmenter la bande passante de la chaîne directe. Dans le cas d'un régulateur à découpage, le courant $I_{o_{max}}$ augmente à la fois avec la fréquence de commutation et la taille des éléments commutés. Ainsi, pour un courant $I_{o_{max}}$ donné, l'augmentation de la fréquence de commutation permet de minimiser la surface des éléments commutés. En contrepartie, l'accélération du rythme des charges/décharges de C_p se traduit par une augmentation significative de I_q.

Par ailleurs, le choix des paramètres à optimiser dépend également des caractéristiques de la charge [81]. Si l'ordre de grandeur de la valeur moyenne du courant de charge est comparable à celle du courant de repos, ce dernier est un facteur déterminant. Dans le cas contraire, le rendement en courant I_p/I_o devient prédominant.

II.2.5 Aspect sécuritaire

En première approche, le niveau de sécurité d'un régulateur linéaire peut être évalué par le biais du taux d'atténuation en courant (CAR pour « *Current Attenuation Rate* »). Les tensions V_{ref} et V_i étant supposées constantes, le CAR est défini comme la variation relative du courant entrant par rapport à celle du courant de charge :

$$CAR(s) \triangleq \left.\frac{\Delta I_i(s)}{\Delta I_L(s)}\right|_{V_i,V_{ref}} \tag{II.19}$$

où $\Delta I_i(s)$ symbolise la variation du courant d'entrée et $\Delta I_L(s)$ celle du courant de charge. Par définition, un niveau de sécurité optimal est atteint lorsque $CAR(s) = 0$. En d'autres termes, le régulateur doit absorber un courant constant quelles que soient les variations du courant de charge. Certaines structures linéaires permettent théoriquement d'atteindre ce résultat (cf. § II.4.2.2). En pratique, les défauts des composants (éléments parasites, courants de fuite, etc.) tendent à limiter le taux d'atténuation. Une alternative efficace consiste à utiliser un régulateur à découpage. Cependant, comme nous le verrons plus tard, ce type de circuit est difficilement compatible avec une intégration sous fortes contraintes de surface. Une architecture hybride pourrait néanmoins permettre d'allier efficacité et efficience. Quelle que soit la solution retenue, l'évaluation du niveau de corrélation entre les signaux $I_i(t)$ et $I_o(t)$ nécessite de faire appel à des outils mathématiques issus du traitement du signal (autocorrélation, intercorrélation, etc.) et du traitement d'image (mesure de similitude de forme, reconnaissance de formes, etc.). Ces approches ont été menées, respectivement, dans les thèses de Fabien Chaillan [82] et Mike Fournigault [83]. Nos trois thèses se sont déroulées en parallèle au sein du laboratoire L2MP et en collaboration avec la division DSA de la société STMicroelectronics-Rousset.

II.3 Cahier des charges

Le cahier des charges de cette étude à été établi en collaboration avec la division *Smartcard* de la société STMicroelectronics. L'ojectif initial était de réaliser une protection matérielle contre les attaques par analyse du courant. En accord avec les encadrants industriels, nous avons décidé d'intégrer cette contremesure au système d'alimentation. Le nouveau système d'alimentation doit donc jouer un double rôle : il

doit réguler la tension d'alimentation interne tout en protégeant le circuit alimenté contre les attaques par analyse du courant.

II.3.1 Contexte technologique

Au démarrage de cette thèse, la division DSA de STMicroelectronics-Rousset utilisait une technologie propriétaire de type CMOS $0.18\ \mu m$ à 6 niveaux de métallisation (CMOSF8). Cette division a ensuite vécu deux sauts technologiques en 3 ans; un premier vers une technologie CMOS $0.15\ \mu m$, puis un second vers une technologie CMOS $0.13\ \mu m$. Un des objectifs de cette étude étant de mettre en œuvre une solution indépendante du procédé de fabrication, nous n'avons pas suivi ces migrations technologiques; l'ensemble des circuits issues de la collaboration avec STMicroelectronics repose sur la technologie de départ. Quoi qu'il en soit, dans la plupart des cas, le portage d'un circuit analogique vers un procédé de fabrication inférieure à $0.18\ \mu m$ présente bien plus d'inconvénients que d'avantages [84].

Paramètre	Symbole	Valeur (typique)		Unité
		NMOS	PMOS	
Longueur de grille minimale.	L_{min}	0.18	0.18	μm
Largeur de grille minimale.	W_{min}	0.28	0.28	μm
Epaisseur d'oxyde de grille.	t_{ox}	3.5	3.5	nm
Tension d'alimentation.	V_{DD}	$1.8\ \pm 10\%$	$1.8\ \pm 10\%$	V
Tension de seuil (10x10).	V_T	494	-530	mV

Tab. II.1 – *Caractéristiques des transistors standards de la technologie CMOSF8 (STM).*

Paramètre	Symbole	Valeur (typique)		Unité
		NMOS	PMOS	
Longueur de grille minimale.	L_{min}	0.9	0.9	μm
Largeur de grille minimale.	W_{min}	1.48	1.48	μm
Epaisseur d'oxyde de grille.	t_{ox}	20	20	nm
Tension d'alimentation.	V_{DD}	< 17	< 15.5	V
Tension de seuil (10x10).	V_T	760	-780	mV

Tab. II.2 – *Caractéristiques des transistors HV de la technologie CMOSF8 (STM).*

Les transistors standards de la technologie $0.18\ \mu m$ fournis par STMicroelectronics (modules LV pour « *Low Voltage* » dans la nomenclature STM) sont des dispositifs de type faible fuite (i.e, à tension de seuil relativement élevée). Les valeurs de leurs paramètres électriques sont rassemblées dans le tableau II.1. Ces transistors supportent une tension d'alimentation de $1.8\ V \pm 10\%$. En complément des dispositifs standards, cette technologie dispose de transistors haute tension (HV). Un transistor HV doit être utilisé dès lors qu'une des tensions appliquées entre deux des bornes du dispositif dépasse $1.98\ V$ ($1.8\ V\ + 10\%$). Les

caractéristiques des transistors HV sont répertoriées dans le tableau II.2. Par rapport à un transistor standard de même dimension, un transistor HV occupe une surface plus importante et son dessin de masque est plus complexe (règles de dessin plus nombreuses). Aussi vaut-il mieux privilégier la technologie standard.

Une partie des circuits a été également réalisée à partir du procédé CMOS $0.35\ \mu m$ à 2 niveaux de polysilicium et 4 niveaux de métallisation (2P/4M) du fondeur AMS (technologie C35B4). Cette technologie a été mise a disposition du laboratoire par la Coordination Nationale pour la Formation en Micro et nanoélectronique (CNFM). Seuls les transistors standards de ce procédé (modules $3.3\ V$ dans la nomenclature AMS) ont été utilisés. Leurs caractéristiques sont reportées dans le tableau II.3.

Paramètre	Symbole	Valeur (typique)		Unité
		NMOS	PMOS	
Longueur de grille minimale.	L_{min}	0.35	0.35	μm
Largeur de grille minimale.	W_{min}	0.4	0.4	μm
Epaisseur d'oxyde de grille.	t_{ox}	7.6	7.6	nm
Tension d'alimentation.	V_{DD}	3.3 $\pm 10\%$	3.3 $\pm 10\%$	V
Tension de seuil (10x10).	V_T	460	-680	mV
Mobilité effective.	μ_0	370	126	$cm^2/V.s$

Tab. II.3 – *Caractéristiques des transistors standards de la technologie C35B4 (AMS).*

Les technologies CMOSF8 et C35B4 sont des procédés CMOS à double-caisson sur substrat de type P. Leur vue en coupe est schématisée sur la figure II.4. Contrairement aux procédés à triple-caisson, ces technologies présentent une contrainte intrinsèque; les prises substrats des transistors NMOS sont indissociables et nécessairement connectées à la masse. Par conséquent, de nombreuses techniques de conception de circuit ne leur sont pas applicables (réduction du V_T par effet substrat, attaque par le substrat [85], booster de courant [86], etc.).

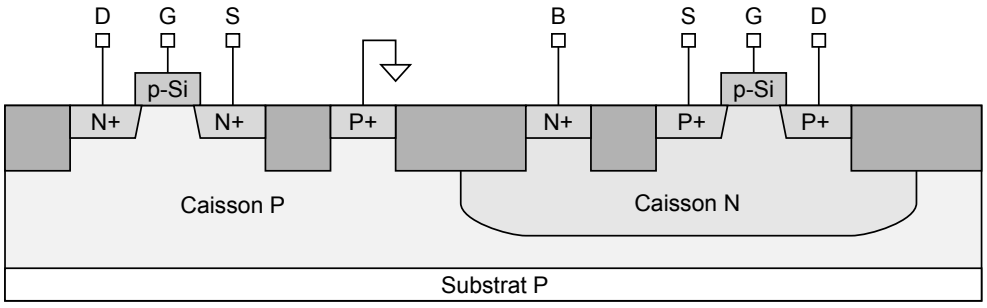


Fig. II.4 – *Coupe transversale d'une technologie CMOS à double-caisson sur substrat P.*

L'ensemble des circuits a été simulé via la plate-forme de conception Virtuoso de l'environnement Cadence (version 4.4.6 et 5.0). Les circuits en technologie CMOSF8 ont été simulés avec Eldo (Mentor

Graphics), en utilisant les paramètres MM9 [87] fournis par STMicroelectronics. En ce qui concerne les circuits en technologie C35B4, ils ont été simulés avec Spectre (Cadence), à partir des paramètres BSIM3v3 du *Hit-Kit 3.70* mis à disposition par le CNFM.

II.3.2 Spécifications du système d'alimentation

Le système doit alimenter un microcontrôleur RISC 32 bits cadencé à $20\ MHz$ (cf. figure I.2). Ses caractéristiques sont rassemblées dans le tableau II.4. En mode veille, la valeur moyenne de son courant de consommation ($\overline{I_{DD}}$) est de $100\ \mu A$. A pleine charge, la valeur moyenne de I_{DD} passe à $28\ mA$, tandis que sa valeur instantanée peut atteindre $100\ mA$. Les vitesses de variation maximales de $\overline{I_{DD}}$ et de I_{DD} sont, respectivement, de $25\ mA/\mu s$ et $150\ mA/ns$. L'ensemble de ces valeurs place le régulateur dans la catégorie des convertisseurs de faible puissance.

Paramètre		Symbole	Valeur	Unité
Tension d'alimentation.		V_{DD}	$1.8\ \pm 10\%$	V
Valeur moyenne de I_{DD}	Mode veille.	-	100	μA
	Pleine charge.	-	28	mA
Valeur instantanée maximale de I_{DD}		-	100	mA
Vitesse de variation maximale de $\overline{I_{DD}}$		-	25	$mA/\mu s$
Vitesse de variation maximale de I_{DD}		-	150	mA/ns

Tab. II.4 – *Caractéristiques de la charge (microcontrôleur RISC 32 bits cadencé à* $20\ MHz$*).*

La tension d'alimentation externe fournie par le lecteur (V_{PS}) est de type continu, simple (mono-tension) et asymétrique (« *single supply* »). Si nécessaire, l'alimentation peut être symétrisée en interne par génération d'une masse virtuelle de niveau $V_{PS}/2$. En effet, l'absence de symétrie interdit l'utilisation de certaines topologies. Par exemple, la plupart des circuits analogiques à base de convoyeurs de courant requièrent un point milieu à faible impédance [88].

Les spécifications du cahier des charges sont rassemblées dans le tableau II.5. Le régulateur doit être compatible avec toutes les classes des principaux standards (cf. tableau de l'annexe A). Ainsi, la tension d'entrée (V_{PS}) peut prendre trois valeurs : $5\ V \pm 10\%$, $3.3\ V \pm 10\%$ et $1.8\ V \pm 10\%$. La tension délivrée par le régulateur (V_{DD}) doit respecter les contraintes associées à la charge (cf. tableau II.4). Ainsi, la valeur moyenne de V_{DD} doit être égale à $1.8\ V$. De plus, par souci de compatibilité avec les technologies avancées ($90\ nm$), cette valeur doit pouvoir descendre jusqu'au volt. La précision de V_{DD} doit respecter les $\pm 10\%$ de tolérance supportés par la technologie $0.18\ \mu m$, quelles que soit les variations de V_{PS}, de I_{DD}, de la température ($-40°C$ à $125°C$) et du procédé de fabrication (3σ). En particulier, lorsque V_{PS} est fixée à $1.8\ V$, la chute de tension aux bornes du régulateur ne doit pas dépasser $180\ mV$ sous $28\ mA$, ce qui équivaut à une résistance à l'état ouvert (R_{on}) d'environ $6.4\ \Omega$. En terme de régulation, la réponse transitoire du régulateur (V_{tr}) ne doit pas excéder $180\ mV$. Concernant le PSR^+, la rejection de V_{PS} doit rester inférieure à $-10\ dB$ sur la bande de fréquence allant du DC à $100\ MHz$. Enfin, le temps de montée de

V_{PS} étant fixé à 1 μs, le temps de démarrage du régulateur doit rester inférieur à 50 μs.

Paramètre	Symbole	Valeur(s)	Unité
Plages d'entrée.	V_{PS}	5 $\pm 10\%$, 3.3 $\pm 10\%$ et 1.8 $\pm 10\%$	V
Tension de sortie.	V_{DD}	1.8	V
Tension de *dropout* ($\overline{I_{DD}}$ = 28 mA).	V_{do}	< 180	mV
Précision statique (V_{tr} exclu).	A_{cc}	$< \pm 10\%$	-
Réponse transitoire.	V_{tr}	< 180	mV
Réjection de V_{PS} (du DC à 100 MHz).	PSR^+	< -10	dB
Temps de démarrage ($t_r(V_{PS})$=1 μs).	-	< 50	μs
Rendement en puissance.	η_P	> V_{DD}/V_{PS}	-
Plage de fonctionnement en température.	-	-40 à 125	°C
Déviation du procédé de fabrication.	-	3σ	-
Surface silicium.	-	< 1	mm^2

Tab. II.5 – *Cahier des charges du système d'alimentation.*

En 2005, le segment des cartes SIM a représenté plus de 60% du marché des cartes à microprocesseurs. Comme la majorité des appareils portatifs, les téléphones GSM sont alimentés par des batteries. De fait, la consommation de la carte SIM est un critère commercial important. Un module SIM est peu solicité par le téléphone dont il est l'hôte. Cependant, lorsqu'il est actif, son courant de consommation est généralement élevé. Par conséquent, le rendement en puissance doit faire l'objet d'un soin particulier. D'après les spécifications fixées par STMicroelectronics, le rendement du convertisseur doit être supérieur à celui d'un régulateur linéaire série idéal (i.e. V_{DD}/V_{PS}, cf. § II.4.2.1).

En ce qui concerne les contraintes d'implantation, les composants discrets sont interdits et la surface totale du circuit ne doit pas excéder 1 mm^2. Par conséquent, le régulateur doit être compensé en interne (i.e., sans capacité externe) et l'utilisation d'inductances de puissance est à proscrire.

II.3.3 Rôle sécuritaire

D'un point de vue sécuritaire, le régulateur doit protéger le système alimenté contre les attaques par analyse en courant. Il doit donc décorreler le courant d'alimentation externe (celui fourni par le lecteur) du courant d'alimentation interne (celui consommé par la charge). A notre connaissance, peu de contre-mesures basées sur le système d'alimentation ont été proposées dans la littérature; d'après nos recherches bibliographiques, seules trois protections de ce type ont fait l'objet de publications ou de brevets ([76], [75] et [89]). Sur ces trois techniques, seule la première permet d'atteindre un niveau de décorrelation quasi-total. Les deux autres, qui sont d'ailleurs assez proches, se contentent d'atténuer l'amplitude des informations. Par ailleurs, comme nous le verrons dans la section suivante, aucune de ces solutions ne permet de respecter simultanément l'ensemble des spécifications du cahier des charges (cf. tableau II.5).

II.4 Etude de l'existant

II.4.1 Introduction

Les régulateurs de tension DC-DC se divisent en deux catégories : les régulateurs linéaires et les régulateurs à découpage (« *switching regulator* »). Les régulateurs linéaires agissent par modulation linéaire et continue de la conductance d'un élément série, tandis que les régulateurs à découpage agissent par modulation du rythme d'un transfert séquentiel de charges. Les différentes catégories et sous-catégories de régulateurs sont répertoriées dans l'arbre de la figure II.5.

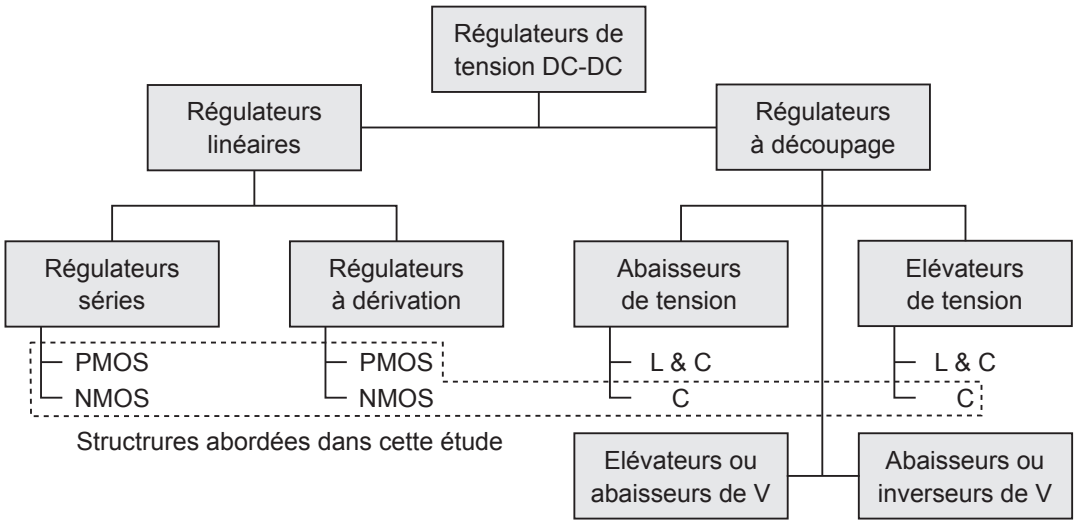


Fig. II.5 – *Arbre des régulateurs de tension DC-DC.*

On distingue principalement deux familles de régulateurs linéaires : les régulateurs linéaires séries et les régulateurs linéaires à dérivation (« *shunt regulator* »). Ces régulateurs tirent leur nom de leur topologie; le transistor de puissance d'un régulateur série est connecté en série entre le nœud d'entrée et le nœud de sortie, tandis que celui d'un régulateur en dérivation est connecté en parallèle entre le nœud de sortie et la masse. Les régulateurs linéaires peuvent être également classés suivant le type du transistor de puissance utilisé (NMOS ou PMOS) et le type de compensation employée (interne ou externe). Les topologies relatives aux deux types de transistors sont détaillées dans les sections suivantes. En revanche, pour les raisons exposées précédemment, seule la compensation interne sera abordée.

Plus vaste, la famille des régulateurs à découpage présente un grand nombre de sous-familles. Leur classification dépend, entre autre, du mode de conversion et du type des éléments commutés. Il existe principalement quatre modes de conversion : les abaisseurs de tension (« *step-down converter* » ou « *buck converter* »), les élévateurs de tension (« *step-up converter* » ou « *boost converter* »), les élévateurs ou abaisseurs de tension (« *buck-boost converter* »), et les abaisseurs ou inverseurs de tensions (« *inverting converter* »). Etant données les spécifications du cahier des charges, nous ne nous intéresserons qu'aux circuits de type abaisseurs de tension. En ce qui concerne le type des éléments commutés, l'utilisation combinée de capacités et d'inductances permet d'atteindre un rendement élevé (supérieur à 90%). Cependant,

ces composants, et en particulier les inductances, sont difficilement intégrables. Pour cette raison, les régulateurs entièrement intégrés reposent le plus souvent sur des topologies linéaires. Néanmoins, dans le cadre d'une application sécuritaire, les circuits à commutation offrent un avantage supplémentaire non négligeable; le transfert séquentiel des charges permet de décorréler le courant d'entrée du courant de sortie. De plus, une catégorie de convertisseurs à découpage repose uniquement sur des capacités : les pompes de charge (« *charge pump* ») [90]. Plus adaptées à nos contraintes, ces topologies seront détaillées dans les sections suivantes.

II.4.2 Régulateurs linéaires

II.4.2.1 Régulateurs linéaires séries

II.4.2.1.a Topologies et plages de fonctionnement

La structure d'un régulateur linéaire série en technologie CMOS est schématisée sur la figure II.6. Le terme « série » provient de la topologie du régulateur; le transistor de puissance (M_p), également appelé transistor de « ballast », est connecté en série entre les nœuds d'entrée (V_i) et de sortie (V_o) du régulateur. Son niveau de conduction est contrôlé par l'intermédiaire d'une boucle de contre-réaction.

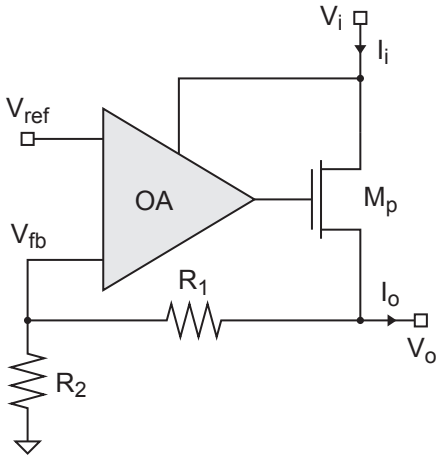


Fig. II.6 – *Structure générale d'un régulateur linéaire série en technologie CMOS.*

La chaîne directe est constituée d'un amplificateur opérationnel A et du transistor de puissance. La chaîne de retour repose sur un pont diviseur de tension (R_1 et R_2). Son point milieu ramène une fraction de V_o sur l'une des entrées de A. Si M_p est un transistor NMOS, le signal de retour (V_{fb}) est appliqué à l'entrée inverseuse de A. Dans le cas contraire, elle est appliquée à l'entrée non-inverseuse de A. La tension de consigne (V_{ref}) est délivrée par une référence de tension. Elle est appliquée à la seconde entrée du comparateur. L'erreur commise sur V_o (i.e., V_{fb}-V_{ref}) est amplifiée par A. Le signal résultant est appliqué à la grille de M_p. Ainsi, les variations de la tension de grille s'opposent aux variations de V_o qui lui ont donné naissance. Conformément à la relation II.3, le gain statique en boucle fermée est donnée par :

$$A_{cl-dc} = \frac{V_o}{V_{ref}} = \frac{A_{ol-dc}}{1 + A_{ol-dc} \cdot \beta} \tag{II.20}$$

où A_{ol-dc} est le gain statique en boucle ouverte et $\beta = R_2/(R_1 + R_2)$ le facteur de retour. Si le gain statique en boucle ouverte est suffisamment élevé, le gain statique en boucle fermée est approximativement égal à $1/\beta$. Par suite, la valeur statique de V_o est quasiment indépendante de la précision de la boucle. En revanche, elle dépend directement de la précision de V_{ref} et de celle des résistances. La réalisation de ces cellules doit donc faire l'objet d'un soin particulier.

Le choix du type de transistors de puissance (NMOS ou PMOS) dépend des priorités du cahier des charges. En termes de plage de fonctionnement en tension, le transistor NMOS est désavantagé; la source du transistor NMOS étant nécessairement connecté à V_{DD}, le passage d'un courant I_p requiert une tension de grille égale à $V_{DD} + V_{GS_p}(I_p)$. Soit $I_{p_{max}}$ le courant maximum véhiculé par le transistor de puissance. Si l'amplificateur est alimenté par V_{PS} et si sa tension de sortie peut atteindre cette valeur (sortie « *rail-to-rail* »), alors la tension de *dropout* du régulateur est donnée par :

$$V_{do_N} = V_{DD} + V_{GS_p(I_{pmax})} \tag{II.21}$$

Dans le cas d'un transistor PMOS, la tension de *dropout* n'est limitée que par la résistance à l'état passant (R_{on}) du transistor de puissance :

$$V_{do_P} = R_{on}.I_p \tag{II.22}$$

Au-delà d'un certain niveau de conduction, la résistance du canal devient négligeable devant les résistances d'accès (source et drain). Dans ces conditions, la valeur de R_{on} est faible (quelques Ω) et d'autant plus faible que le transistor est large. De fait, l'utilisation d'un transistor PMOS permet d'atteindre une tension de *dropout* beaucoup plus basse que la limite fixée par l'expression II.21, relative à un transistor NMOS. A ce titre, le terme LDO désigne généralement les régulateurs linéaires séries reposant sur un transistor PMOS. Néanmoins, l'intégration d'une pompe de charge dans la boucle de régulation (cf. figure II.7) permet aux régulateurs à transistor NMOS de faire jeu égal avec leurs homologues à transistor PMOS.

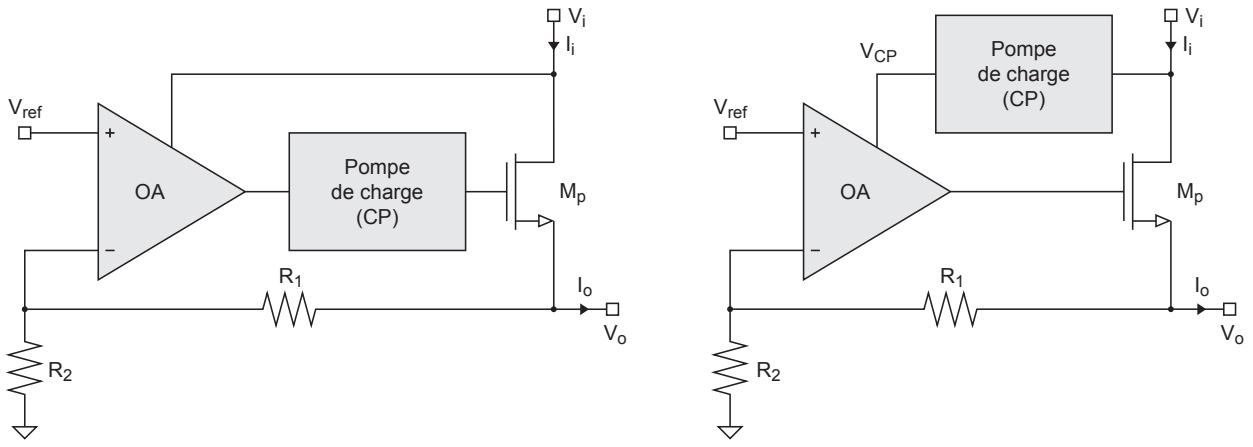


Fig. II.7 – *Régulateurs linéaires séries à transistor NMOS et pompe de charge [91, 92].*

Un élévateur de tension à pompe de charge (« CP pour *Charge Pump* ») est un convertisseur à capacités commutées permettant de générer une tension de sortie supérieure à sa tension d'entrée [90]. En particulier,

la tension de sortie de la pompe de charge (V_{CP}) peut être supérieure à la tension d'alimentation. Ainsi, l'utilisation directe ou indirecte de la tension V_{CP} pour piloter la grille du transistor de puissance permet de s'affranchir de la limite fixée par la relation II.21. Il existe différentes manières d'intégrer une pompe de charge dans la boucle de régulation. Trois d'entre elles sont représentées sur les figures II.7 et II.8. La solution ilustrée à gauche de la figure II.7 consiste à placer la pompe de charge en série entre la sortie de l'amplificateur opérationnel de transconductance (OTA pour *Operationnal Transconductance Amplifier*) et la grille du transistor de puissance [91]. Dans ce cas, la pompe de charge consomme uniquement l'énergie nécessaire à la polarisation de la grille (V_{G_p}). En contrepartie, le temps de latence existant entre l'entrée et la sortie de la pompe de charge dégrade significativement la bande passante de la fonction de transfert en boucle ouverte. Néanmoins, ce facteur n'à qu'une influence limitée sur la rapidité du régulateur (cf. § II.4.2.1.c). La seconde technique, représentée à droite de la figure II.7, consiste à alimenter l'OTA par l'intermédiaire de la pompe de charge [92]. Contrairement à la technique précédente, cette configuration n'affecte pas la rapidité de la boucle. En revanche, elle se traduit par une consommation plus importante.

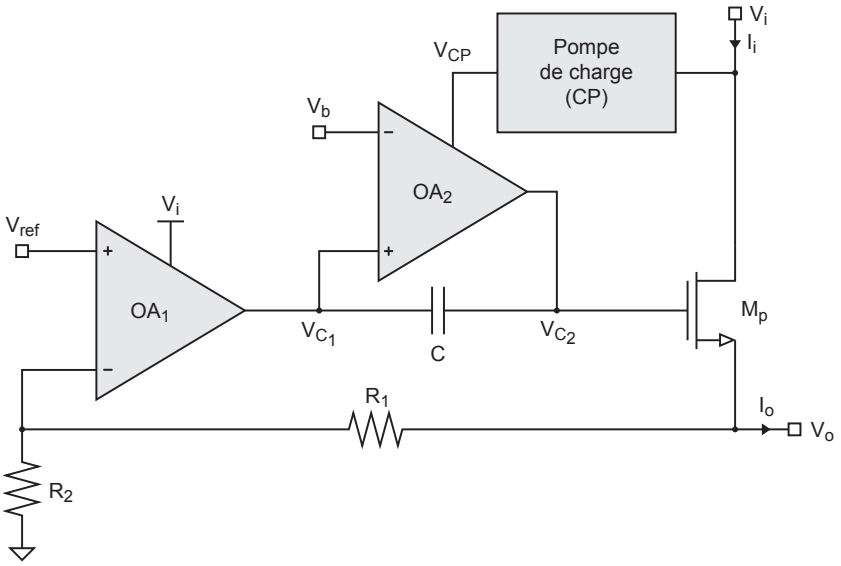


Fig. II.8 – *Régulateur linéaire série à transistor NMOS et pompe de charge [93].*

La troisième solution est schématisée sur la figure II.8 [93]. Une capacité flottante (C) est connectée en série entre la sortie de l'amplificateur associé à la boucle (OA_1) et la grille du transistor de puissance. Cette capacité de découplage joue le rôle d'un décaleur de tension. Le mode commun ($V_{C_{cm}} = (V_{C_1} + V_{C_2})/2$) de la tension différentielle aux bornes de C ($V_C = V_{C_1} - V_{C_2}$) est contrôlé par un amplificateur (OA_1) alimenté par la tension d'alimentation externe. L'amplitude de V_C est contrôlée par un amplificateur (OA_2) alimenté via une pompe de charge. Ainsi, les variations de V_o agissent directement sur la grille du transistor de puissance par décalage de $V_{C_{cm}}$. L'amplificateur OA_2 maintient quand à lui la valeur moyenne de V_{C_1} au milieu de sa plage d'excursion, par réajustement dynamique de V_C. Cette solution garantit une rapidité de régulation élevée. En contrepartie, la multiplication du nombre de cellules entraîne une surconsommation importante. Quelle que soit la solution considérée, la tension de *dropout* du régulateur n'est plus limitée que par la résistance R_{on} du transistor NMOS. Sa nouvelle valeur est donc donnée par l'expression II.22.

II.4.2.1.b Rendement en puissance

Le courant de repos du régulateur linéaire est la somme de trois contributions : le courant d'alimentation de l'amplificateur, le courant de polarisation du pont résistif (I_{res}) et le courant d'alimentation de la référence de tension. Dans le cas d'un régulateur à transistor PMOS, le courant de consommation de l'amplificateur est au cœur du compromis vitesse-consommation; parce que sa valeur conditionne la bande passante de la chaîne directe, il doit être maintenue à un niveau suffisant pour garantir une réponse transitoire en accord avec le cahier des charges. Afin de limiter I_{res}, on utilise des résistances de grandes valeurs. Cependant, les résistances de précision intégrées occupent une surface relativement importante ce qui limite leur taille à quelques centaines de kilo Ohms. De plus, le courant I_{res} doit être maintenu à un niveau suffisant de sorte que l'influence du pôle associé à la capacité d'entrée de l'amplificateur reste négligeable. Il est à noter que l'adjonction d'une pompe de charge à la boucle de régulation augmente sérieusement la valeur moyenne du courant de repos. Toutefois, si l'on suppose le courant de repos négligeable devant le courant de charge, alors le courant d'entrée du régulateur est quasiment égal au courant de charge ($I_i \cong I_o \cong I_L$). Dans ce cas, le rendement du régulateur tend vers sa valeur idéale :

$$\eta_P = \frac{V_o \cdot I_o}{V_i \cdot (I_L + I_q)} \frac{V_o}{V_i} \tag{II.23}$$

et le rendement idéal maximum du régulateur linéaire ne dépend plus que de sa tension de *dropout* :

$$\eta_{P_{max}} \cong \frac{V_o}{V_o + V_{do}} \tag{II.24}$$

La diminution de la tension différentielle $V_i - V_o$ permet notamment de réduire la puissance $I_L \cdot (V_i - V_o)$ dissipée par effet joule aux bornes du transistor de puissance et, par voie de conséquence, l'échauffement du circuit.

II.4.2.1.c Etude fréquentielle

Transistor de puissance PMOS et compensation interne

Un régulateur linéaire intégré à transistor de puissance PMOS est schématisé sur la figure II.9. L'OTA présente une transconductance g_{m_a} et une résistance de sortie r_a. La charge est modélisée par une source de courant (I_L) en parallèle avec une résistance (R_L) et un réseau constitué d'une capacité (C_L) et de l'ESR (« *Equivalent Series Resistance* ») associé à C_L (R_E). L'ESR d'une capacité intégrée est généralement faible, mais sa valeur a tendance à croître avec la densité de routage. Lorsque le transistor de puissance est polarisé en inversion forte et en régime saturé, sa capacité grille-drain (C_{gd_p}) peut être considérée comme négligeable devant sa capacité grille-source (C_{gs_p}). Cependant, l'influence de la capacité C_{gd_p} est amplifiée par effet Miller. Cet effet sera pris en compte par l'intermédiaire d'une capacité équivalente dite « capacité Miller » (C_M). La grille de M_p est généralement localisée à proximité de la sortie de l'OTA. A ce titre, l'ESR de la capacité équivalente associée à la grille de M_p peut être considérée comme négligeable. Afin de respecter les contraintes de surface imposées par le cahier des charges, aucune capacité de découplage n'a été ajoutée en sortie du montage. Par conséquent, la capacité équivalente du nœud de sortie est approximativement égale à la capacité intrinsèque de la charge ($C_o \cong C_L$).

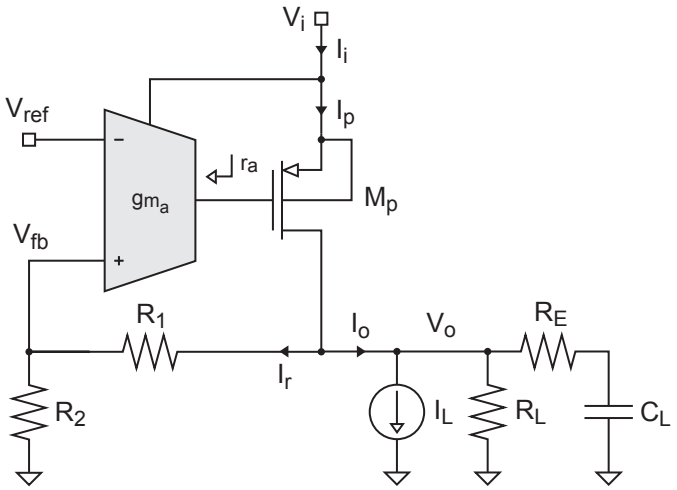


Fig. II.9 – *Régulateur linéaire série à transistor de puissance PMOS et compensation interne.*

L'ouverture du schéma de la figure II.9 au niveau du nœud V_{fb} permet de déterminer la fonction de transfert en boucle ouverte. Le schéma équivalent petit signal du circuit de la figure II.9 en boucle ouverte est représenté sur la figure II.10. Une fois linéarisé autour de son point de fonctionnement, le transistor M_p peut être modélisé par une transconductance (g_{m_p}) en parallèle avec une résistance (r_{ds_p}). La résistance drain-source r_{ds_p} modélise l'effet de modulation de la longueur du canal. Son expression est donnée par :

$$r_{ds_p} \triangleq \frac{V_{EA_p}}{I_{DS_p}} = \frac{1}{\lambda \cdot I_{DS_p}} \tag{II.25}$$

où V_{EA} est la tension d'Early, λ l'inverse de V_{EA} et I_{DS_p} le courant de polarisation du transistor de puissance. Afin de minimiser la surface du transistor de puissance, la longueur du transistor de puissance (L) est fixée à la valeur minimale autorisée par la technologie (L_{min}), ce qui implique un effet de modulation important.

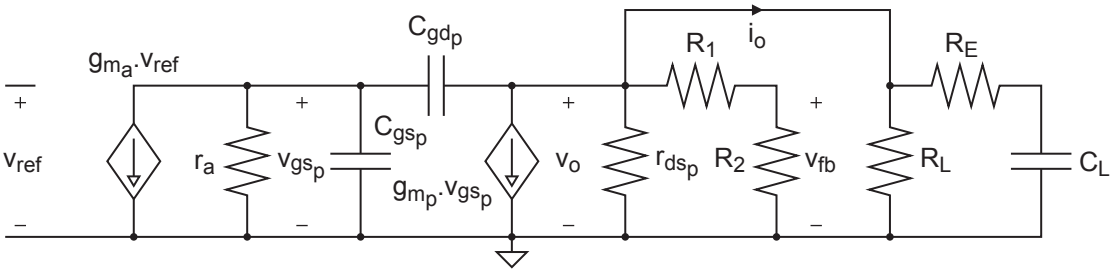


Fig. II.10 – *Schéma équivalent petit signal du circuit de la figure II.9 en boucle ouverte.*

La fonction de transfert en boucle ouverte est donnée par :

$$A_{ol}(s) = \left.\frac{v_{fb}(s)}{v_{ref}(s)}\right|_{V_i, I_L} \cong \beta \cdot g_{m_a} \cdot Z_g(s) \cdot g_{m_p} \cdot Z_o(s) \tag{II.26}$$

où $Z_g(s)$ est l'impédance équivalente du nœud associé à la grille du transistor de puissance et $Z_o(s)$ l'im-

pédance équivalente du nœud de sortie :

$$Z_g(s) \cong \frac{r_a}{1 + s \cdot r_a \cdot \left(C_{gs_p} + C_M\right)} \tag{II.27}$$

$$Z_o(s) \cong r_{ds_p} // \left(R_1 + R_2\right) // R_L // \left(R_E + \frac{1}{s \cdot C_L}\right) \tag{II.28}$$

où C_M est la capacité Miller induite par C_{gd_p} :

$$C_M \cong g_{m_p} \cdot \left[r_{ds_p} // \left(R_1 + R_2\right) // R_L\right] \cdot C_{gd_p} \tag{II.29}$$

A fort courant de charge, la résistance r_{ds_p} peut être considérée comme négligeable devant R_1, R_2 et R_L. Dans ce cas, les expressions II.28 et II.29 peuvent être approximées par :

$$Z_o(s) \cong \frac{r_{ds_p} \cdot (1 + s \cdot R_E \cdot C_L)}{1 + s \cdot \left(r_{ds_p} + R_E\right) \cdot C_L} \tag{II.30}$$

$$C_M \cong g_{m_p} \cdot r_{ds_p} \cdot C_{gd_p} \tag{II.31}$$

Par suite, l'expression II.26 peut se réécrire sous la forme :

$$A_{ol}(s) \cong \beta \cdot A_{ol-dc} \cdot \frac{1 + s \cdot R_E \cdot C_L}{\left[1 + s \cdot r_a \cdot \left(C_{gs_p} + C_M\right)\right] \cdot \left[1 + s \cdot \left(r_{ds_p} + R_E\right) \cdot C_L\right]} \tag{II.32}$$

où le gain statique en boucle ouverte est donné par :

$$A_{ol-dc} \cong g_{m_a} \cdot r_a \cdot g_{m_p} \cdot r_{ds_p} \tag{II.33}$$

La fonction de transfert en boucle ouverte (cf. eq. II.32) présente deux pôles (p_g et p_o) et un zéro (z_o) :

$$p_g \cong \frac{1}{2 \cdot \pi \cdot r_a \cdot \left(C_{gs_p} + C_M\right)} \tag{II.34}$$

$$p_o \cong \frac{1}{2 \cdot \pi \cdot \left(r_{ds_p} + R_E\right) \cdot C_L} \tag{II.35}$$

$$z_o \cong \frac{1}{2 \cdot \pi \cdot R_E \cdot C_L} \tag{II.36}$$

Par conséquent, le système bouclé est potentiellement instable. Dans un régulateur entièrement intégré, la somme des capacités C_{gs_p} et C_M est généralement grande devant C_L. De fait, le pôle interne (p_g) domine le pôle relatif au nœud de sortie (p_o); la compensation est dite « interne ». Si l'on suppose que la fréquence du zéro est grande devant la fréquence de gain unitaire (UGF pour « *Unit Gain Frequency* »), le diagramme asymptotique de Bode associé à $|A_{ol}(s)|$ correspond à la courbe de la figure II.11. Dans ce cas, si le pôle secondaire apparaît avant l'UGF, le système bouclé sera sujet à l'instabilité.

Lorsque le transistor de puissance est en inversion forte et en régime saturé, sa transconductance est proportionnelle à $\sqrt{I_p}$, tandis que sa résistance drain-source est proportionnelle à $1/I_p$. Ainsi, dans ce régime de fonctionnement, A_{ol-dc} est proportionnel à $1/\sqrt{I_p}$, le pôle dominant (p_g) est proportionnel à $\sqrt{I_p}$

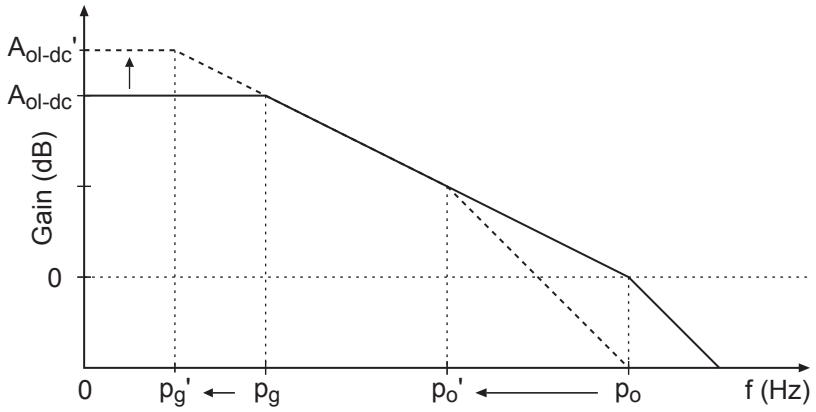


Fig. II.11 – *Réponse fréquentielle de la boucle de transmission d'un régulateur à transistor PMOS.*

tandis que le pôle secondaire (p_o) est proportionnel à I_p. Compte tenu de ces dépendances, les pires conditions de stabilité interviennent lorsque I_p prend sa valeur la plus faible. En effet, sous cette hypothèse, le pôle secondaire se rapproche du pôle dominant. Par conséquent, la fréquence de gain unitaire et la vitesse de rotation de la phase augmentent simultanément ce qui se traduit par une diminution de la marge de phase. Bien que leurs effets soient moindres, les variations en température et en procédé de fabrication ont également une influence sur la position des pôles; ils doivent être également pris en compte.

Dans la configuration PMOS, le bruit d'alimentation agit directement sur la source du transistor de puissance (cf. figure II.9). Il apparaît donc amplifié sur le nœud de sortie. Toutefois, le bruit d'alimentation est également injecté sur la grille du transistor de puissance par l'intermédiaire de l'OTA. De fait, le PSR^+ du régulateur dépend directement de celui de l'OTA. Le principe de superposition linéaire permet d'étudier séparément ces deux effets. Le schéma équivalent petit signal de la figure II.12 en boucle fermée permet de déterminer le PSR^+ résultant du chemin direct (le PSR^+ de l'OTA étant supposé nul).

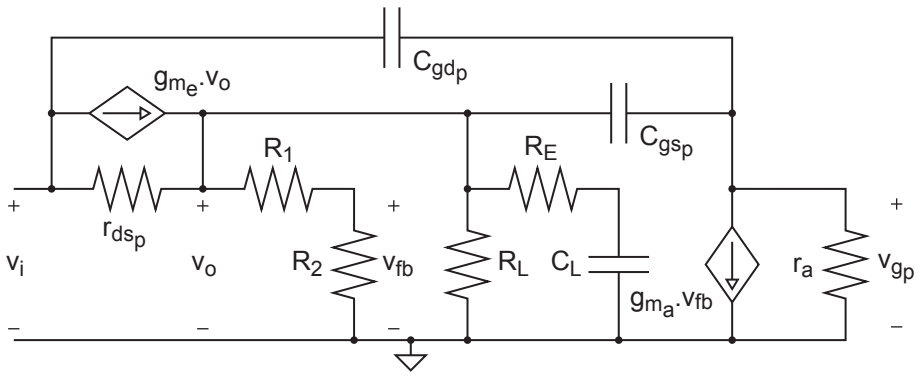


Fig. II.12 – *Schéma équivalent petit signal du circuit de la figure II.9 en boucle fermée.*

La tension V_{ref} et le courant I_L étant supposés constants, la tension de sortie petit signal du système

bouclé est donnée par :

$$v_o(s)|_{V_{ref},I_L} \cong Z'_o(s) \cdot \left[\frac{v_i(s) - v_o(s)}{r_{ds_p}} + g_{m_p} \left(v_i(s) - v_{g_p}(s) \right) \right] \tag{II.37}$$

où l'impédance $Z'_o(s)$ est donnée par :

$$Z'_o(s) \cong (R_1 + R_2) \,//R_L// \left(R_E + \frac{1}{s \cdot C_L} \right) \tag{II.38}$$

La réorganisation de la relation II.37 permet d'établir l'expression du taux de réjection :

$$PSR^+(s) = \left. \frac{v_o(s)}{v_i(s)} \right|_{V_{ref},I_L} \cong \frac{\left(1 + g_{m_p} \cdot r_{ds_p}\right) \cdot Z'_o(s)}{r_{ds_p} + \left(1 + \beta \cdot g_{m_a} \cdot Z_g(s) \cdot g_{m_p} \cdot r_{ds_p}\right) \cdot Z'_o(s)} \tag{II.39}$$

On en déduit l'expression du facteur de régulation amont (cf. § II.2.3) :

$$LNR \triangleq PSR^+(0) \cong \frac{1}{\beta \cdot g_{m_a} \cdot r_a} \tag{II.40}$$

A basse fréquence, le PSR^+ dépend uniquement du gain statique de la boucle de transmission. Lorsque la fréquence augmente, la réponse de la boucle se détériore, ce qui conduit à une augmentation de la résistance de sortie et par voie de conséquence, à une augmentation du PSR^+. Au-delà d'une certaine fréquence, la capacité C_{gs_p} commence à court-circuiter la grille et la source du transistor de puissance. De fait, cette configuration grille-commune dégrade significativement le PSR^+. Dans le même temps, sous l'effet de la capacité C_o, la résistance de sortie du régulateur commence à diminuer. Ces phénomènes contribuent à faire redescendre le PSR^+. Ce dernier atteint généralement sa valeur la plus basse aux alentours de l'UGF [94]. En définitive, quelle que soit la plage de fréquence considérée, l'injection directe du bruit par la transconductance du transistor de puissance dégrade significativement la réjection de l'alimentation.

L'influence du PSR^+ de l'OTA sur celui du régulateur dépend du type de transistor de puissance utilisé. Dans la configuration PMOS de la figure II.9, le bruit d'alimentation (δV_i) est nécessairement présent sur la source du transistor de puissance (V_{S_p}). Pour qu'il ne soit pas injecté par g_{m_p} sur V_o, la seule solution consiste à s'assurer que δV_i est également présent (avec la même amplitude et la même phase) sur V_{G_p}. En d'autres termes, le bruit d'alimentation doit apparaître dans le mode commun des tensions V_{S_p} et V_{G_p} [94]. Par conséquent, la maximisation du PSR^+ du régulateur passe par l'utilisation d'un OTA à PSR^+ unitaire. C'est le cas des deux OTA de la figure II.13.

Le circuit représenté à gauche sur la figure II.13 est un OTA simple terminaison (« *single-ended-output* ») à paire différentielle NMOS chargée par un miroir. Le schéma du centre représente un OTA cascode replié (« *folded-cascode* ») à paire différentielle PMOS. Du point de vue du PSR^+, ces deux OTA présentent un schéma petit signal équivalent. Celui-ci est représenté sur la figure II.14.

La paire différentielle et les miroirs étant supposés appairés ($r_{ds_{p1}} = r_{ds_{p2}} = r_{ds_1}, r_{ds_{n1}} = r_{ds_{n2}} = r_{ds_2}$ et $g_{m_{p1}} = g_{m_{p2}} = g_{m_m}$), le PSR^+ de ces OTA non-chargés est donné par :

$$PSR^+_{OTA} = \left. \frac{v_{oa}}{v_{sa}} \right|_{V_{ia}} = \frac{r_{ds_2}}{r_{ds_1} + r_{ds_2}} + \frac{i_{r_{ds_2}}}{v_{sa}} \cdot (r_{ds_1} // r_{ds_2}) \approx 1 \tag{II.41}$$

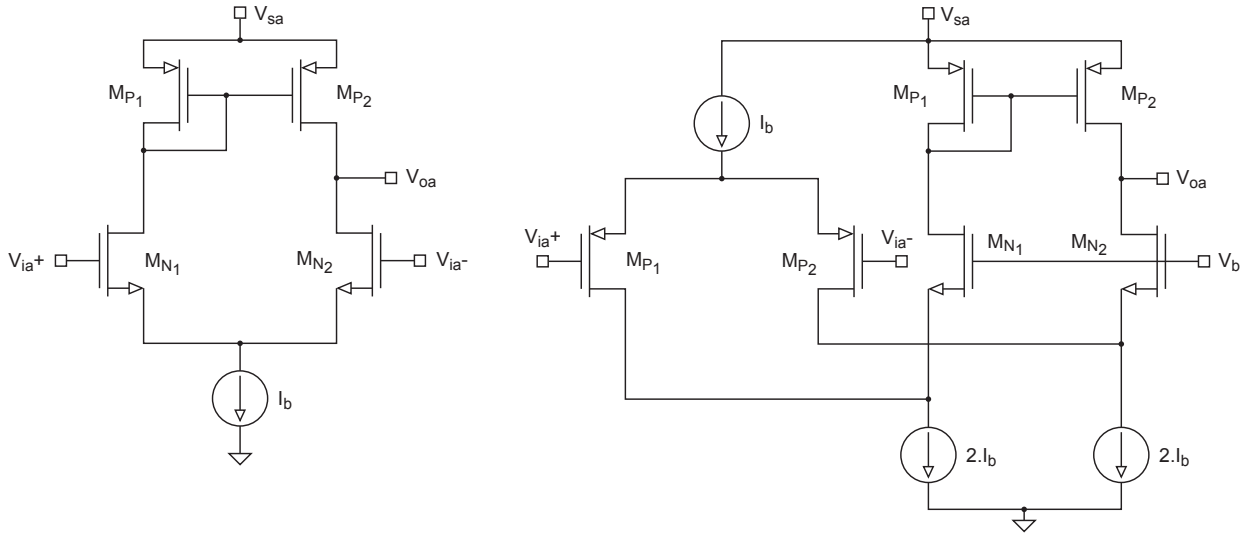


Fig. II.13 – *Circuits d'OTA permettant de maximiser le PSR^+ d'un régulateur à transistor PMOS [94].*

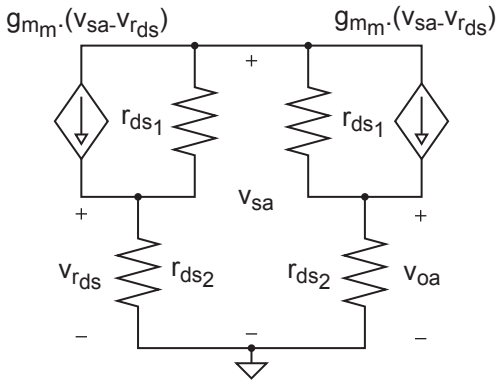


Fig. II.14 – *Schéma équivalent petit signal des OTA de la figure II.13 [94].*

où v_{ia}, v_{oa} et v_{sa} sont respectivement les tensions d'entrée, de sortie et d'alimentation de l'amplificateur. Il apparaît donc que l'utilisation de ces structures permet d'augmenter le PSR^+ du régulateur. Le choix entre l'une ou l'autre de ces deux topologies doit être guidé par les spécifications du régulateur. L'OTA replié présente deux fois plus de branches que l'OTA à simple terminaison. Par conséquent, à performances fréquentielles équivalentes, sa consommation est nécessairement plus grande. Un plus grand nombre de transistors implique également un bruit équivalent en entrée supérieur et une tension d'*offset* ramenée sur l'entrée plus importante. En contrepartie l'OTA replié présente une plage d'entrée en mode commun (ICMR pour « *Input Common Mode Range* ») plus étendue. A taille et polarisation identiques, une paire différentielle PMOS est environ trois fois moins rapide qu'une paire différentielle NMOS ($\mu_{0_N} \cong 3 \cdot \mu_{0_P}$). En contrepartie, la valeur minimale de la tension d'entrée en mode commun d'une paire NMOS est limitée à $V_{T_N} + V_{DS_{sat}}$; une paire différentielle PMOS permet d'utiliser une tension de référence (V_{ref}) de plus faible amplitude.

Afin de déterminer la régulation de charge, on applique un courant de test (i_t) à la sortie v_o du circuit

bouclé non chargé (cf. figure II.10). Les tensions V_{ref} et V_i étant supposées constantes, la tension de test résultante est donnée par :

$$v_t(s)|_{V_{ref},V_i} \cong \left[r_{ds_p} // \left(R_1 + R_2\right)\right] \cdot \left(i_t(s) - g_{m_p} \cdot v_{g_p}(s)\right) \tag{II.42}$$

L'impédance de sortie intrinsèque du régulateur est donc donnée par :

$$R_o(s) = \left.\frac{v_t(s)}{i_t(s)}\right|_{V_{ref},V_i} \cong \frac{r_{ds_p} // \left(R_1 + R_2\right)}{1 + \beta \cdot g_{m_a} \cdot Z_g(s) \cdot g_{m_p} \cdot \left[r_{ds_p} // \left(R_1 + R_2\right)\right]} \tag{II.43}$$

Par définition, la régulation de charge est égale à l'impédance de sortie statique du système en boucle fermé :

$$LDR \triangleq R_o(0) \cong \frac{r_{ds_p}}{\beta \cdot A_{ol-dc}} \tag{II.44}$$

En définitive, l'augmentation du gain statique en boucle ouverte permet d'améliorer la régulation de charge.

En présence d'un courant de charge petit signal $i_L(s)$, le comportement du circuit bouclé de la figure II.12 est décrit par le système d'équations suivant :

$$\begin{cases} i_i(s) \cong -g_{m_p} \cdot v_{g_p}(s) - \frac{v_o(s)}{r_{ds_p}} \\ v_o(s) \cong \left(r_{ds_p} // Z'_o(s)\right) \cdot \left(-g_{m_p} \cdot v_{g_p}(s) - i_L(s)\right) \end{cases} \tag{II.45}$$

où l'expression de l'impédance $Z'_o(s)$ est donnée par la relation II.38. La résolution du système II.45 permet de dériver l'expression du CAR :

$$CAR(s) = \left.\frac{i_i(s)}{i_L(s)}\right|_{V_{ref},V_i} \cong \frac{\left(1 + \beta \cdot g_{m_a} \cdot Z_g(s) \cdot g_{m_p} \cdot r_{ds_p}\right) \cdot Z'_o(s)}{r_{ds_p} + \left(1 + \beta \cdot g_{m_a} \cdot Z_g(s) \cdot g_{m_p} \cdot r_{ds_p}\right) \cdot Z'_o(s)} \tag{II.46}$$

Par conséquent, la valeur basse fréquence du taux d'atténuation en courant est donnée par :

$$CAR_{dc} \cong \frac{\left(1 + \beta \cdot A_{ol-dc}\right) \cdot R_E}{r_{ds_p} + \left(1 + \beta \cdot A_{ol-dc}\right) \cdot R_E} \approx 1 \tag{II.47}$$

Pour r_{ds_p} grand devant R_E, la valeur haute fréquence (i.e., $f>>$UGF) du CAR tend quant à elle vers :

$$CAR|_{f>>UGF} \cong \frac{R_E}{r_{ds_p} + R_E} \approx 0 \tag{II.48}$$

Puisque l'expression du CAR est fonction de la fréquence, le régulateur engendre une distortion du signal informationnel. Si la partie du spectre située au delà l'UGF subit une atténuation significative, en revanche, celle située avant le premier pôle ne présente quasiment aucune déformation. D'un autre coté, la régulation ne peut être correcte que si la majorité du spectre du courant de charge s'inscrit dans la bande passante du régulateur. Par conséquent, un régulateur linéaire série ne peut pas simultanément réguler et sécuriser. De plus, une atténuation invariante du signal ne constitue une contre mesure suffisante. En effet, dans le cas d'une DPA, une simple augmentation du nombre d'échantillons permet de compenser la dégradation du rapport signal à bruit [55].

Transistor de puissance NMOS et compensation interne

Un régulateur linéaire intégré à transistor de puissance NMOS est schématisé sur la figure II.15. Contrairement à la configuration drain-commun du transistor PMOS, la configuration suiveur du transistor NMOS n'engendre pas d'inversion de phase. De fait, la boucle est refermée sur l'entrée inverseuse de l'OTA. Alors que la prise substrat du transistor de puissance PMOS était connectée à sa source, la technologie employée impose de connecter celle du transistor NMOS à la masse. La présence d'une tension non nulle entre le substrat et la source du transistor de puissance se traduit par un décalage de sa tension de seuil. Ce phénomène, connu sous le nom d'« effet substrat », vaut à la prise substrat le surnom de « grille arrière » (« *back-gate* »). Si V_{BS_p} est la tension substrat-source du transistor de puissance, alors sa tension de seuil est donnée par :

$$V_{T_p} = V_{T0_p} + \gamma \cdot \left(\sqrt{2 \cdot |\phi_f| - V_{BS_p}} - \sqrt{2 \cdot |\phi_f|} \right) \tag{II.49}$$

où V_{T0_p} est la tension de seuil à V_{BS_p} nul, γ le « *body factor* » et ϕ_f le potentiel de Fermi. Par construction, la tension V_{BS_p} est égale à la tension de sortie du régulateur. Ainsi, la modulation du niveau d'inversion du transistor s'oppose aux variations de V_{BS_p} qui lui ont donné naissance. En d'autres termes, l'effet substrat participe à la régulation de la tension de sortie. Comme précédemment, l'OTA présente une transconductance g_{m_a} et une résistance de sortie r_a.

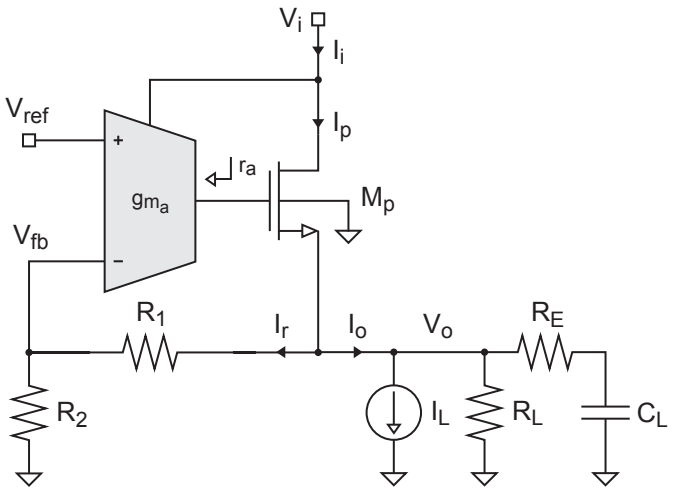


Fig. II.15 – *Régulateur linéaire série à transistor de puissance NMOS et compensation interne.*

L'ouverture du schéma de la figure II.15 au niveau du nœud V_{fb} permet de déterminer la fonction de transfert en boucle ouverte. Le schéma équivalent petit signal du circuit de la figure II.15 en boucle ouverte est représenté sur la figure II.16. La transconductance g_{mb_p} modélise l'effet substrat. La fonction de transfert en boucle ouverte est donnée par :

$$A_{ol}(s) = \left. \frac{v_{fb}(s)}{v_{ref}(s)} \right|_{V_i, I_L} \cong \frac{\beta \cdot g_{m_a} \cdot Z_g(s) \cdot g_{m_p} \cdot Z_o(s)}{1 + g_{m_e} \cdot Z_o(s)} \tag{II.50}$$

où $g_{m_e} = g_{m_p} + g_{mb_p}$, $Z_o(s)$ correspond à la relation II.28 et $Z_g(s)$ est l'impédance équivalente du nœud

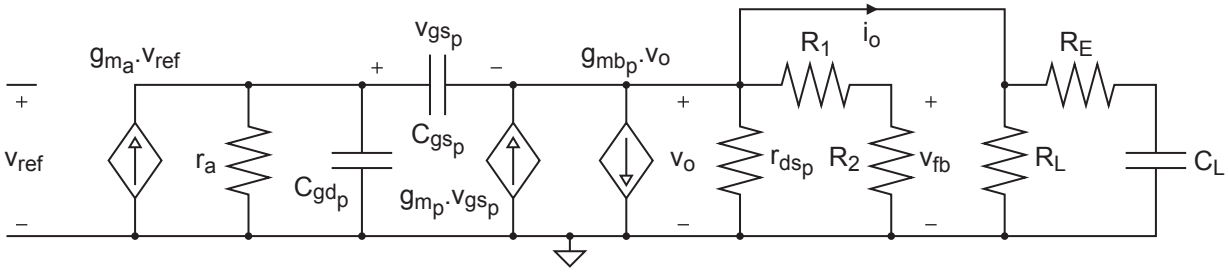


Fig. II.16 – *Schéma équivalent petit signal du circuit de la figure II.15 en boucle ouverte.*

associé à la grille du transistor de puissance :

$$Z_g(s) \cong \frac{r_a}{1 + s \cdot r_a \cdot C_{gd}} \tag{II.51}$$

La résistance r_{ds_p} pouvant être considérée comme faible devant R_1, R_2 et R_L, l'équation II.50 conduit à :

$$A_{ol}(s) \cong \frac{\beta \cdot g_{m_a} \cdot r_a \cdot g_{m_p} \cdot r_{ds_p} \cdot (1 + s \cdot R_E \cdot C_L)}{\left(1 + g_{m_e} \cdot r_{ds_p}\right) \cdot (1 + s \cdot r_a \cdot C_{gd}) \cdot \left\{1 + s \cdot \left[\frac{R_E + r_{ds_p} \cdot (1 + g_{m_e} \cdot R_E)}{1 + g_{m_e} \cdot r_{ds_p}}\right] \cdot C_L\right\}} \tag{II.52}$$

Par ailleurs, R_E est petite devant r_{ds_p}, et g_{mb_p} négligeable devant g_{m_p}. L'expression II.52 peut donc se simplifier sous la forme :

$$A_{ol}(s) \cong \beta \cdot A_{ol-dc} \cdot \frac{1 + s \cdot R_E \cdot C_L}{(1 + s \cdot r_a \cdot C_{gd}) \cdot \left(1 + s \cdot \frac{C_L}{g_{m_p}}\right)} \tag{II.53}$$

où le gain statique en boucle ouverte est approximativement égal à :

$$A_{ol-dc} \cong g_{m_a} \cdot r_a \tag{II.54}$$

En configuration suiveur, les caractéristiques du transistor de puissance n'interviennent pas dans l'expression du gain statique en boucle ouverte. Ainsi, à conditions équivalentes, la valeur de ce dernier est plus basse dans le cas d'un transistor NMOS que dans le cas d'un transistor PMOS. En contrepartie, la faible résistance de sortie induite par la topologie NMOS permet de repousser l'UGF à des fréquences plus élevées. A nouveau, la fonction de transfert en boucle ouverte présente deux pôles et un zéro :

$$p_g \cong \frac{1}{2 \cdot \pi \cdot r_a \cdot C_{gd}} \tag{II.55}$$

$$p_o \cong \frac{g_{m_p}}{2 \cdot \pi \cdot C_L} \tag{II.56}$$

$$z_o \cong \frac{1}{2 \cdot \pi \cdot R_E \cdot C_L} \tag{II.57}$$

Par rapport à la configuration drain commun du transistor PMOS, la configuration suiveur du transistor NMOS se traduit par l'absence d'effet Miller et une résistance de sortie plus faible. Par conséquent, les pôles p_g et p_o sont positionnées à des fréquences plus élevées. En d'autres termes, la bande passante de la boucle de transmission est plus large dans le cas d'un transistor NMOS. A nouveau, la compensation

est de type « interne » et la fréquence du zéro est supposée grande devant l'UGF. La forme générale du diagramme asymptotique de Bode associée à $|A_{ol}(s)|$ est représenté sur la figure II.17. Comme précédemment, la présence du pôle secondaire aux alentours de l'UGF rend le système potentiellement instable.

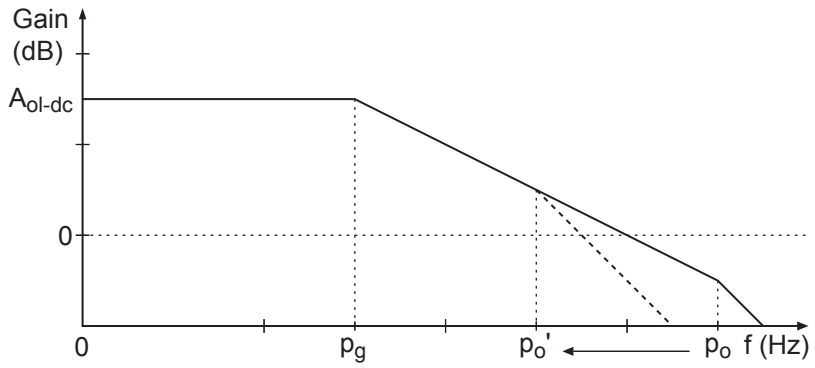


Fig. II.17 – *Réponse fréquentielle de la boucle de transmission d'un régulateur à transistor NMOS.*

Lorsque le transistor de puissance est en inversion forte et en régime saturé, le gain statique en boucle ouverte (A_{ol-dc}) et le pôle dominant (p_g) sont indépendants de I_p, tandis que le pôle secondaire (p_o) est proportionnel à $\sqrt{I_p}$. Par conséquent, lorsque I_p diminue, le pôle secondaire se rapproche du pôle dominant. Ainsi, comme dans le cas du transistor PMOS, les pires conditions de stabilité interviennent lorsque I_p prend sa valeur la plus faible. Cependant, la configuration suiveur du NMOS présente une résistance de sortie beaucoup plus faible que la configuration drain-commun du PMOS. Ainsi, à courant I_g identique, la distance entre les pôles, et par voie de conséquence, la marge de phase, sont plus élevées dans le cas d'un régulateur à transistor NMOS. En contrepartie, le gain statique en boucle ouverte de la topologie NMOS est plus faible que celui de la topologie PMOS.

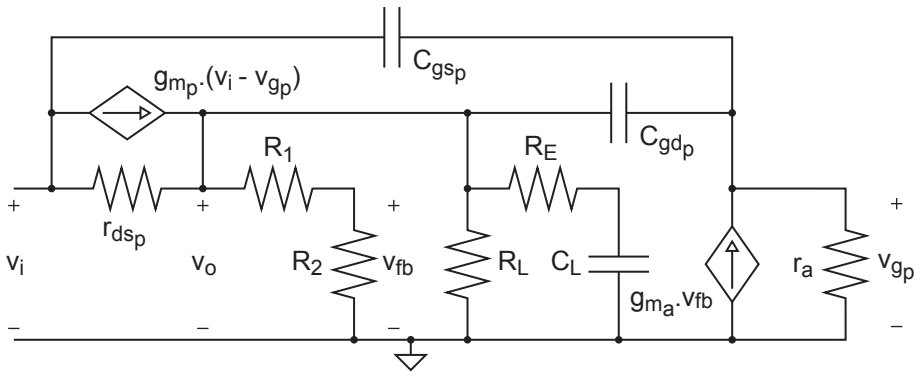


Fig. II.18 – *Schéma équivalent petit signal du circuit de la figure II.15 en boucle fermée.*

Le PSR^+ de l'OTA étant supposé nul, le schéma équivalent petit signal de la figure II.12 permet de déterminer le PSR^+ résultant du chemin directe. Si l'on suppose la tension V_{ref} et le courant I_L constants,

la tension de sortie du système bouclé est donnée par :

$$v_o(s)|_{V_{ref},I_L} \cong Z'_o(s) \cdot \left[\frac{v_i(s) - v_o(s)}{r_{ds_p}} + g_{m_p} \cdot \big(v_{g_p}(s) - v_o(s)\big) - g_{mb_p} \cdot v_o(s) \right] \tag{II.58}$$

où l'impédance $Z'_o(s)$ correspond à la relation II.38. La réorganisation de l'expression II.58 conduit à :

$$PSR^+(s) = \left. \frac{v_o(s)}{v_i(s)} \right|_{V_{ref},I_L} \cong \frac{Z'_o(s)}{r_{ds_p} + \big\{1 + r_{ds_p} \cdot \big[g_{mb_p} + g_{m_p} \cdot (1 + \beta \cdot g_{m_a} \cdot Z_g(s))\big]\big\} \cdot Z'_o(s)} \tag{II.59}$$

La régulation de ligne est donc donnée par :

$$LNR \triangleq PSR^+(0) \cong \frac{1}{\beta \cdot g_{m_p} \cdot r_{ds_p} \cdot A_{ol-dc}} \tag{II.60}$$

Si l'on fait abstraction du chemin indirect (i.e. l'OTA), la transconductance du transistor NMOS ne participe pas à la transmission du bruit d'alimentation. Par conséquent, à conditions équivalentes, un régulateur à transistor NMOS présente une meilleur réjection intrinsèque du bruit d'alimentation.

La configuration suiveur du transistor NMOS implique que toute variation de sa tension de grille est directement transmise à sa source. Par conséquent, l'OTA doit impérativement filtrer le bruit d'alimentation. Ainsi, la maximisation du PSR^+ du régulateur passe par l'utilisation d'un OTA à PSR^+ nul. C'est le cas des deux OTA de la figure II.19.

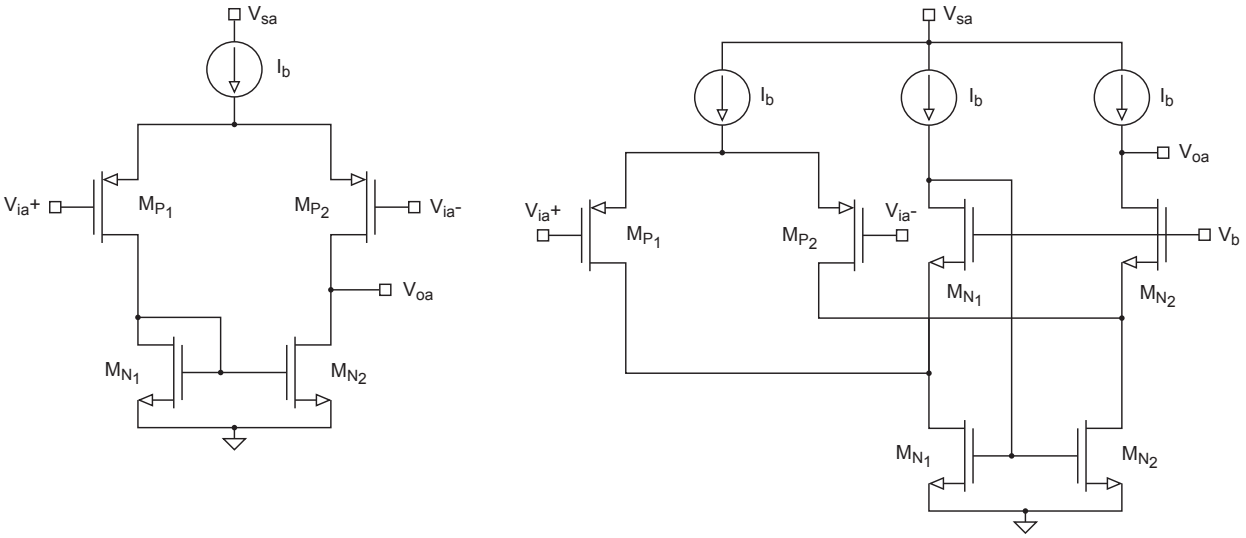


Fig. II.19 – *Structures d'OTA permettant de maximiser le PSR^+ d'un régulateur à transistor NMOS [94].*

Le circuit représenté à gauche sur la figure II.19 est un OTA simple terminaison à paire différentielle PMOS chargée par un miroir. Le schéma du centre représente un OTA cascode replié à paire différentielle NMOS. Du point de vue du PSR^+, ces deux OTA présentent un schéma petit signal équivalent. Ce dernier est représenté sur la figure II.20.

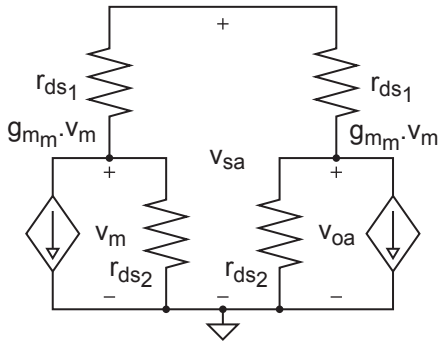


Fig. II.20 – *Schéma équivalent petit signal des OTA de la figure II.19 [94].*

La paire différentielle et les miroirs étant supposées appairés ($r_{ds_{p1}} = r_{ds_{p2}} = r_{ds_1}$, $r_{ds_{n1}} = r_{ds_{n2}} = r_{ds_2}$ et $g_{m_{n1}} = g_{m_{n2}} = g_{m_m}$), le PSR^+ de ces OTA est donné par :

$$PSR^+_{OTA} = \left.\frac{v_{oa}}{v_{sa}}\right|_{V_{ia}} = \frac{r_{ds_2}}{r_{ds_1} + r_{ds_2}} - \frac{i_{r_{ds_1}}}{v_{sa}} \cdot (r_{ds_1} // r_{ds_2}) \approx 0 \tag{II.61}$$

où V_{ia}, V_{oa} et V_{sa} sont respectivement les tensions d'entrée, de sortie et d'alimentation de l'amplificateur. Par conséquent, l'utilisation de ces structures permet d'augmenter le PSR^+ d'un régulateur à transistor NMOS. A nouveau, le choix de l'une ou l'autre dépend des spécifications du cahier des charges.

Afin de déterminer la régulation de charge, on applique un courant de test (i_t) à la sortie v_o du circuit bouclé non chargé (cf. figure II.16), les tensions V_{ref} et V_i étant supposées constantes. L'expression de la tension de test résultante est donnée par :

$$v_t(s)|_{V_{ref},V_i} \cong \left[r_{ds_p} // \left(R_1 + R_2\right)\right] \cdot \left[i_t(s) + g_{m_p} \cdot \left(v_{g_p}(s) - v_t(s)\right) - g_{mb_p} \cdot v_t(s)\right] \tag{II.62}$$

L'impédance de sortie intrinsèque du régulateur est donc donnée par :

$$R_o(s) = \left.\frac{v_t(s)}{i_t(s)}\right|_{V_{ref},V_i} \cong \frac{r_{ds_p} // \left(R_1 + R_2\right)}{1 + \left[g_{mb_p} + g_{m_p} \cdot (1 + \beta \cdot g_{m_a} \cdot Z_g(s))\right] \cdot \left[r_{ds_p} // \left(R_1 + R_2\right)\right]} \tag{II.63}$$

On en déduit l'expression de la régulation de charge :

$$LDR \triangleq R_o(0) \cong \frac{1}{\beta \cdot g_{m_p} \cdot A_{ol-dc}} \tag{II.64}$$

En définitive, si la régulation de charge d'un régulateur à transistor PMOS est égale à celle d'un régulateur à transistor NMOS, en revanche, la bande passante plus élevée de ce dernier lui garantit de meilleurs performances fréquentielles.

En présence d'un courant de charge petit signal $i_L(s)$, le comportement du circuit bouclé de la figure II.18 est régi par le système d'équation suivant :

$$\begin{cases} i_i(s) \cong g_{m_p} \cdot v_{g_p}(s) - \frac{v_o(s)}{r_{ds_p}} \\ v_o(s) \cong \left(r_{ds_p} // Z'_o(s)\right) \cdot \left(g_{m_p} \cdot v_{g_p}(s) - i_L(s)\right) \end{cases} \tag{II.65}$$

où l'expression de l'impédance $Z'_o(s)$ est donnée par la relation II.38. La résolution du système II.65 permet de dériver l'expression du CAR :

$$CAR(s) = \left.\frac{i_i(s)}{i_L(s)}\right|_{V_{ref},V_i} \cong \frac{\left[1 + r_{ds_p} \cdot \left(g_{m_e} + \beta \cdot g_{m_a} \cdot Z_g(s) \cdot g_{m_p}\right)\right] \cdot Z'_o(s)}{r_{ds_p} + \left[1 + \left(g_{m_e} + \beta \cdot g_{m_a} \cdot Z_g(s) \cdot g_{m_p}\right) \cdot r_{ds_p}\right] \cdot Z'_o(s)} \tag{II.66}$$

Par suite, la valeur statique du taux d'atténuation en courant est donnée par :

$$CAR_{dc} \cong \frac{\left(1 - \beta \cdot A_{ol-dc} \cdot g_{m_p} \cdot r_{ds_p}\right) \cdot R_E}{r_{ds_p} + \left(1 - \beta \cdot A_{ol-dc} \cdot g_{m_p} \cdot r_{ds_p}\right) \cdot R_E} \approx 1 \tag{II.67}$$

Pour R_E négligeable devant r_{ds_p}, ce qui est généralement le cas, la valeur haute fréquence du CAR tend quant à elle vers :

$$CAR|_{f>>UGF} \cong \frac{R_E}{r_{ds_p} + R_E} \approx 0 \tag{II.68}$$

En définitive, la bande passante élevée du régulateur à transistor NMOS se traduit par un niveau de sécurité encore plus bas que dans le cas du transistor PMOS.

II.4.2.1.d Réponse transitoire

La réponse transitoire d'un régulateur linéaire série dépend de son temps de réponse Δt), de la taille de sa capacité de sortie (C_o), de l'ESR de C_o et de l'amplitude maximale du courant de charge $I_{L_{max}}$ [81]:

$$V_{tr_{max}} = \frac{I_{L_{max}}}{C_o}\Delta t + \Delta V_{ESR} \tag{II.69}$$

où ΔV_{ESR} est la chute de tension induite par l'ESR. Dans le cas d'un dispositif NMOS, sa source est connectée directement à la tension de sortie du régulateur. Par conséquent, le transistor de puissance assure une régulation intrinsèque extrêmement rapide; si l'on fait abstraction des effets de couplage source-grille et des effets quasi-statiques, la réponse du régulateur est quasi-instantanée. Lorsque le transistor de puissance est de type PMOS, son temps de réaction est égal, aux effets non-quasi-statiques prés, au temps de réaction de sa grille. Il dépend donc directement du délai de propagation à travers la boucle de transmission (Δt). L'expression de Δt est fonction de la bande passante du régulateur en boucle fermé (BW_{cl}) et de la vitesse de variation maximale de la tension associée à la sortie de l'amplificateur chargé (i.e., du « *slew rate* » de l'amplificateur). Elle peut être approximée par :

$$\Delta t \cong \frac{1}{BW_{cl}} + \frac{C_p \cdot \Delta V_p}{I_{a_{max}}} \tag{II.70}$$

où C_p est la capacité de charge de l'amplificateur, $I_{a_{max}}$ le courant de sortie maximum de l'amplificateur et ΔV_p la variation de tension aux bornes de C_p permettant de passer du point de polarisation pré-transitoire au point de polarisation post-transitoire. Par construction, un régulateur à transistor NMOS offre une vitesse de réaction nettement plus élevée qu'un régulateur à transistor PMOS. En termes de réponse transitoire, ce facteur est d'autant plus important que la nécessité d'une intégration totale limite significativement la taille de C_o. Notons qu'en contrepartie, la proximité des capacités intégrées leur confère des ESR beaucoup plus faibles que celles de leurs homologues discrets.

II.4.2.1.e Conclusion

Un régulateur linéaire série est à la fois rapide, précis et compact. De plus, dans sa configuration PMOS, il offre une faible tension de *dropout*. A courant de repos équivalent, un régulateur à transistor NMOS présente une tension de *dropout* plus importante. En contrepartie, ce dernier permet d'atteindre une vitesse de régulation plus élevée, tout en conservant une marge de phase supérieure. Enfin, quel que soit le type de transistor considéré, un régulateur linéaire série rapide n'engendre, par nature, quasiment aucune atténuation du signal informationnel. La protection d'une charge contre les attaques par analyse du courant nécessite donc de faire appel à d'autres types de topologies.

II.4.2.2 Régulateur linéaire à dérivation

La structure d'un régulateur linéaire à dérivation (« *shunt regulator* ») en technologie CMOS est représentée sur la figure II.21. La chaîne directe et la chaîne de retour sont analogues à celles d'un régulateur linéaire série. En revanche, à la différence de ce dernier, le transistor de puissance (M_p) est disposé parallèlement à la charge. De fait, ces deux types de régulateur présentent des fonctionnements antagonistes. La chute de tension est ici obtenue par le biais d'une résistance (R_s) connectée en série entre l'entrée (V_i) et la sortie (V_o) du régulateur. Le courant d'entrée (I_i) traversant R_s est la somme du courant de sortie (I_o) et du courant dérivé par le transistor de puissance (I_p). Ainsi, pour stabiliser V_o, la boucle de régulation s'oppose aux variations de V_i et I_o en ajustant dynamiquement l'amplitude de I_p. Dans cette topologie, le transistor de puissance PMOS surclasse son homologue sur quasiment tous les points, ce qui explique sa popularité.

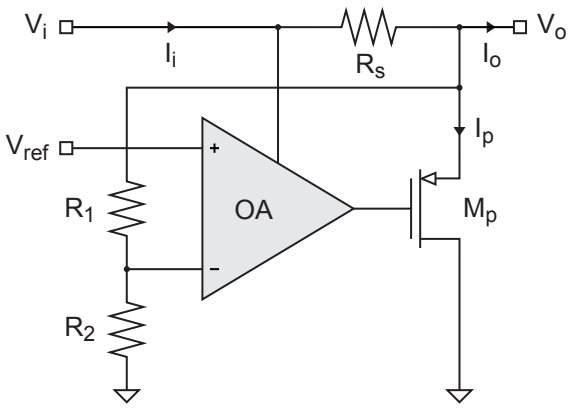


Fig. II.21 – *Régulateur linéaire à dérivation (« shunt regulator) » en technologie CMOS [89].*

La tension de *dropout* d'un régulateur linéaire à dérivation est indépendante du type de transistor de puissance utilisé. Elle est atteinte dès lors que le courant I_p du transistor de dérivation s'annule. On a alors $I_i \cong I_o$, ce qui conduit à :

$$V_{do} \cong R_s \cdot I_o|_{I_p=0} \tag{II.71}$$

Ainsi, la valeur minimale de V_{do} ($V_{do_{min}}$) dépend de l'amplitude maximale du courant de charge ($I_{o_{max}}$). Par conséquent, pour un jeu de conditions aux limites $\{V_{do_{max}}, I_{o_{max}}\}$ donné, la valeur maximale possible de R_s ($R_{s_{max}}$) est celle conduisant à la fermeture de M_p (i.e., à $V_{GS_p} \approx V_{T_p}$). Cette valeur doit évidemment

prendre en compte les déviations du procédé du fabrication. Par ailleurs, la surface d'une résistance intégrée dépend à la fois de sa valeur et de sa densité de courant maximale admissible. Ainsi, la surface d'occupation de la résistance de puissance peut également constituer un facteur limitant. La valeur minimale de R_s dépend quant à elle du rendement minimum admissible.

Le rendement en puissance d'un régulateur linéaire à dérivation dépend à la fois de la marge $R_s - R_{s_{max}}$ et de la différence $\overline{I_o} - I_{o_{max}}$; si une valeur de R_s petite devant $R_{s_{max}}$ autorise une marge de fonctionnement importante, en revanche, elle conduit à une surconsommation permanente. Dans ce cas, même à pleine charge, le transistor de dérivation dissipe une quantité d'énergie non négligeable. Si R_s est proche de $R_{s_{max}}$ et si la valeur moyenne du courant de charge tangente sa valeur maximale, alors le rendement du régulateur à dérivation tend vers celui d'un régulateur linéaire série idéal. Ces circonstances sont toutefois peu réalistes, car difficilement atteignables en pratique. En définitive, dans le cadre de l'application visée, le rendement apparaît comme le principal point faible des régulateurs *shunt*.

De par leur mode d'alimentation, les cartes à puce sans contact sont soumises à des variations de puissance très importantes. Le surplus d'énergie présent à un instant t ne pouvant être stocké, il doit être impérativement évacué au risque d'engendrer une surtension. Pour cette raison, le système d'alimentation des cartes à puce sans contact repose généralement sur un régulateur linéaire à dérivation. Dans ce cas, le rendement du régulateur conditionne la distance maximale à partir de laquelle la carte cesse de fonctionner.

En terme de régulation de charge et de réjection d'alimentation, un régulateur *shunt* à transistor de puissance PMOS présente des performances élevées, équivalentes à celles d'un régulateur série à transistor NMOS. En outre, dans cette configuration, l'utilisation d'un OTA à PSR^+ nul permet de maximiser le PSR^+ du régulateur. Par ailleurs, si nécessaire, la technique proposée dans [86] permet de tirer profit de l'effet substrat pour accroître dynamiquement le courant de sortie du transistor de puissance.

A l'inverse des régulateurs linéaires séries, le taux d'atténuation en courant d'un régulateur à dérivation est directement proportionnel à sa régulation de charge; si les variations du courant de charge sont instantanément compensées par le transistor de dérivations, elles n'entraînent pas de variations de la tension de sortie. Dans ce cas, si la tension d'entrée est constante, le courant d'entrée l'est également; vu de l'extérieur, tout se passe comme si la charge consommait un courant constant. Par conséquent, un régulateur *shunt* idéal présente un CAR nul. En réalité, le comportement fréquentiel du CAR suit une évolution inverse de celle de la résistance de sortie; l'atténuation en courant, élevée en DC, diminue lorsque la fréquence du courant de charge augmente. Par rapport au régulateur *shunt* classique (i.e., à résistance passive), la structure de la figure II.22 permet d'améliorer significativement le taux d'atténuation en courant [75].

La méthode illustrée sur la figure II.22 consiste à isoler les nœuds d'entrée et de sortie du régulateur en remplaçant la résistance R_s par un transistor de puissance fonctionnant en source de courant (M_{p_2}). Cette structure ayant été spécifiquement conçue pour un système télé-alimenté, la source de courant est contrôlée par une boucle de régulation visant à limiter l'effondrement de la tension d'entrée. Par conséquent, le courant injecté dans M_{p_2} est quasiment indépendant du courant de charge. Cependant, l'effet Early et le couplage capacitif existant entre le drain et la grille de M_{p_2} tendent à limiter le niveau d'isolation effectif.

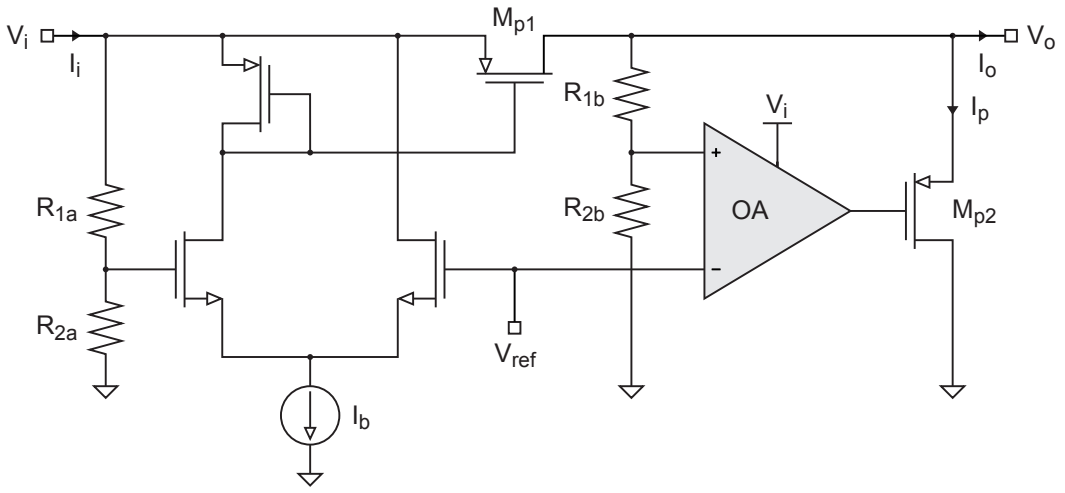


Fig. II.22 – *Régulateur de tension intégré pour cartes à puce sans contact [75].*

Néanmoins, d'après les mesures présentées dans [75], cette structure permet d'atteindre un taux d'atténuation de $-66\ dB$. Or, la réalisation d'une attaque de type DPA nécessite de doubler le nombre d'échantillon à chaque atténuation de $-3\ dB$ du signal informationnel [75]. Ainsi, la contre-mesure de la figure II.22 permet de multiplier le temps de traitement par 2^{22}; la durée moyenne d'une attaque passe alors de moins d'une minute à plus de 7 ans [75].

En définitive, les régulateurs linéaires à dérivation offrent une régulation de qualité et un niveau de sécurité intéressant. En contrepartie, leurs principes de fonctionnement se traduit nécessairement par un rendement en puissance inférieur à ceux des régulateurs séries. Néanmoins, un régulateur de ce type occupant une surface relativement restreinte, il pourrait être utilisé en complément d'un régulateur principal, pour alimenter uniquement les cellules nécessitant un niveau de protection accru. De la sorte, il n'aurait qu'un impact limité sur le rendement global du système. Cependant, les modules cryptographiques comptent généralement parmi les circuits les plus gourmands en énergie. Par conséquent, en l'état, ce type de régulateur n'est pas adapté à nos contraintes.

II.4.3 Régulateurs à découpage

II.4.3.1 Structure générale

Dans le marché des systèmes embarqués, l'autonomie est un critère commercial dominant. Aussi, le rendement en puissance des régulateurs linéaires n'est généralement pas adapté à ce type de produit. Au prix d'une augmentation substantielle de la surface et du bruit de sortie, les régulateurs à découpage permettent d'atteindre des rendements nettement plus élevés, pouvant atteindre 90%. La structure générale d'un régulateur à découpage est représentée sur la figure II.23.

Un régulateur à découpage est généralement constitué d'un bloc de puissance doublé d'un système de contrôle. Le bloc de puissance est formé d'un ou plusieurs éléments réactifs interconnectés par le biais d'interrupteurs de puissance. Comme dans le cas d'un régulateur linéaire, le système de contrôle repose gé-

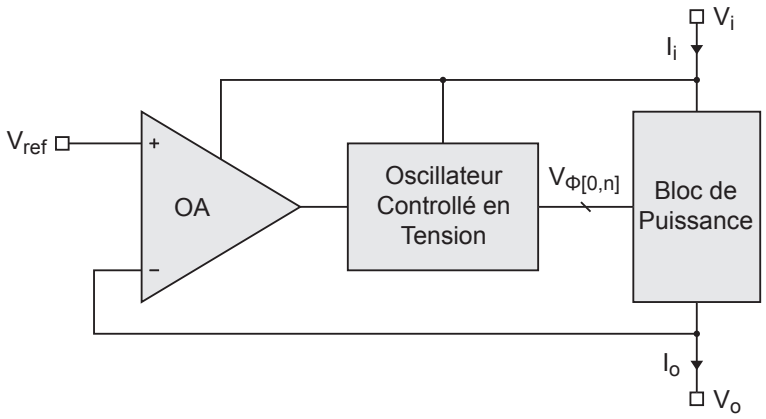


Fig. II.23 – *Structure générale d'un régulateur à découpage.*

néralement sur une boucle de contre-réaction. En revanche, le signal de sortie de l'amplificateur ne contrôle pas directement les transistors de puissance mais la fréquence d'un oscillateur. Les signaux d'horloge résultants sont utilisés pour piloter les interrupteurs. Leurs commutations périodiques engendrent un transfert séquentiel d'énergie de l'entrée vers la sortie du régulateur. Ainsi, le convertisseur régule la tension de sortie par modulation continue de la fréquence de commutation des éléments réactifs. L'intégrabilité et les performances d'un régulateur à découpage dépendent principalement des caractéristiques du bloc de puissance. En outre, sa topologie conditionne le fonctionnement du générateur de phases. En ce qui concerne la boucle de contrôle, sa structure varie peu d'un convertisseur à l'autre et son intégration ne présente pas de difficultés majeures.

II.4.3.2 Hacheur série

Le plus utilisé des abaisseurs de tension à découpage est le hacheur série (« *buck converter* »). La structure de son bloc de puissance est schématisée sur la figure II.24.

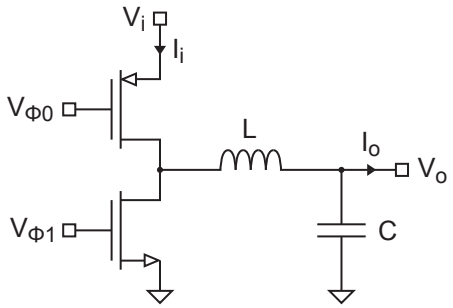


Fig. II.24 – *Bloc de puissance d'un hacheur série (« buck converter »).*

Le fonctionnement du hacheur série repose sur l'utilisation conjuguée d'une inductance et d'une capacité. Le courant d'une impédance purement réactive est déphasé de 90° par rapport à la tension à ses bornes; elle ne dissipe pas l'énergie, mais la stocke sous la forme d'un champs électromagnétique. Ainsi, dans le schéma de la figure II.24, les valeurs moyennes des puissances aux bornes de L et C sont toutes

les deux nulles. Cette topologie permet donc de transférer l'énergie en minimisant les pertes; la puissance stockée pendant la phase de charge est restituée pendant la phase de décharge, ce qui assure un flux continu et un rendement théorique idéal de 100%. Afin d'éviter l'apparition d'un courant de court-circuit lors de la commutation, les signaux de contrôles ($V_{\phi 0}$ et $V_{\phi 1}$) doivent être à phases non-recouvrantes. En terme de sécurité, cette méthode de conversion garantit une atténuation efficace; lors de la charge, l'inductance filtre les variations du signal informationnel, et lors de la décharge, l'entrée est entièrement coupée de la sortie. La taille de l'inductance conditionne le rendement et la précision du régulateur [95]. Un niveau de performance correct conduit généralement à des valeurs difficilement intégrables. Toutefois, certaines techniques permettent de réduire significativement les dimensions de l'élément réactif, tout en conservant un effet inductif équivalent. Deux d'entres elles sont illustrées sur le schéma de la figure II.25.

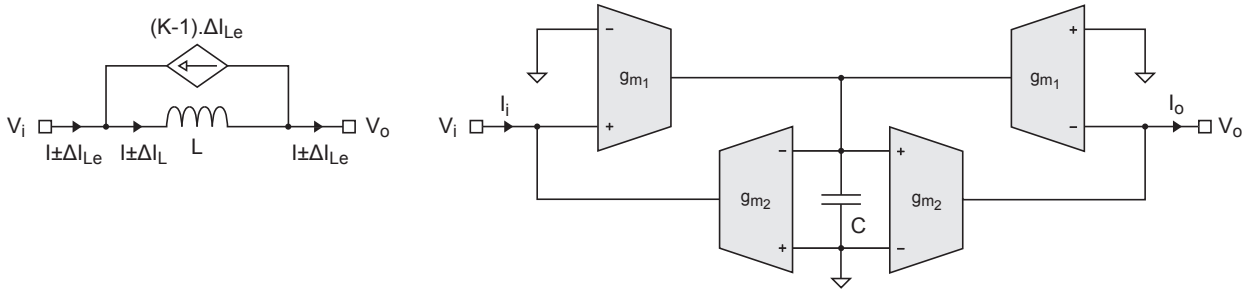


Fig. II.25 – *Multiplieur actif d'inductance [95] (à gauche) et inductance simulée (à droite).*

En mode courant, la technique du multiplieur actif d'inductance [95] consiste à amplifier l'amplitude des ondulations du courant traversant l'inductance par un facteur K. L'impédance ainsi obtenue présente une réactance effective K fois supérieure à celle de l'inductance implémentée. Proposée par le même auteur, la technique dite du multiplieur actif de capacité permet, comme son nom l'indique, d'obtenir un résultat équivalent avec une capacité [96]. Implémentée avec succès, cette technique a permis de réaliser un convertisseur *buck* entièrement intégré, dont l'inductance de $150\ nH$ conduit à des performances proches de celles obtenues pour un composant de dimensions dix fois supérieures [95]. Cependant, dans notre cas, le peu de surface disponible conduirait à une valeur de K excessivement élevée et par la même, à un rendement trop faible.

La seconde technique consiste à simuler un comportement inductif à l'aide d'un circuit actif. C'est l'objectif du circuit gyrateur de la figure II.25. Pour des OTA supposés idéaux, l'impédance différentielle $(v_1 - v_2)/(i_1 - i_2)$ est purement réactive et vaut $C_L/(gm_1 \cdot gm_2)$. En réalité, le facteur de qualité et les plages de fonctionnements (tension, courant, fréquence, etc.) de l'inductance simulée sont limitées par les défauts des OTA. De plus, chaque OTA doit consommer un courant au moins égal à celui traversant le dipôle. Le faible rendement résultant n'est donc pas adapté au filtrage d'un signal de forte puissance. En définitive, l'implémentation d'une inductance n'est pas compatible avec nos contraintes.

II.4.3.3 Convertisseur à capacités commutées

II.4.3.3.a Cas général

Egalement appelés pompe de charge (« *charge pump* »), les convertisseurs à capacités commutées sont des circuits constitués uniquement d'interrupteurs et de capacités de transfert. On distingue principalement deux catégories de convertisseurs à capacités commutées : les élévateurs de tension (« *boost-converter* ») et les abaisseurs de tension (« *buck-converter* »). Le rendement d'un convertisseur à capacités est limité par deux types de pertes : les pertes de conduction et les pertes de commutation.

Les pertes de conduction correspondent à la puissance rayonnée par effet Joule dans les éléments dissipatifs (R_{on} des interrupteurs, R_{ESR} des capacités, etc.). Pour un convertisseur à capacités commutées, elles sont données par [97] :

$$P_{(l,c)_{tot}} = R_o(f_s).I_o^2 \tag{II.72}$$

où I_o est le courant de sortie et $R_o(f_s)$ la résistance de sortie calculée à la fréquence de commutation.

Les pertes de commutation se divisent en deux catégories : les pertes de charge et l'énergie nécessaire au pilotage des interrupteurs. Même en l'absence d'éléments dissipatifs, le rendement d'un convertisseur idéal est intrinsèquement limité par les pertes de charge. En effet, lorsqu'une capacité C est mise au contact d'une source de tension indépendante, dont l'amplitude diffère d'une quantité ΔV_c de celle initialement présente à ses bornes, le transfert de charge s'accompagne d'une perte d'énergie égale à [98] :

$$E_{l,s_c} = \frac{1}{2} \cdot C \cdot (\Delta V_c)^2 = \frac{1}{2} \cdot Q \cdot \Delta V_c \tag{II.73}$$

où Q est la charge totale transférée. Cette perte d'énergie est indépendante de la valeur des résistances parasites.

En ce qui concerne les pertes par pilotage, l'énergie nécessaire à l'ouverture d'un transistor NMOS ou la fermeture d'un transistor PMOS est donnée par :

$$E_{l,s_d} = C_{gs} \cdot (\Delta V_{gs})^2 + C_{gd} \cdot (\Delta V_{gd})^2 \tag{II.74}$$

Ainsi, pour un convertisseur cadencé à la fréquence f_s, faisant intervenir N boucles de charge et M transistors par cycle de commutation, la perte totale de puissance est approximativement égale à :

$$P_l \cong P_{(l,c)_{tot}} + \underbrace{\frac{f_s}{2} \cdot \sum_{i=1}^{N} Q_i \cdot \Delta V_{c_i}}_{P_{(l,s_c)_{tot}}} + \underbrace{f_s \cdot \sum_{j=1}^{M} \left[C_{gs_j} \cdot (\Delta V_{gs_j})^2 + C_{gd_j} \cdot (\Delta V_{gd_j})^2 \right]}_{P_{(l,s_d)_{tot}}} \tag{II.75}$$

Par suite, le rendement global d'un convertisseur à capacités commutées est donné par :

$$\eta \triangleq \frac{P_{out}}{P_{in}} \cong \frac{P_{out}}{P_{out} + P_l} \tag{II.76}$$

où P_{in} et P_{out} désignent respectivement les puissances en entrée et en sortie du convertisseur. Le rendement théorique maximum d'un convertisseur idéal (i.e., sans élément dissipatif et à pertes de pilotages nulles) est donc intrinsèquement limité à [98] :

$$\eta_{max} = 1 - \frac{P_{(l,s_c)_{tot}}}{P_{out} + P_{(l,s_c)_{tot}}} \tag{II.77}$$

D'aprés les expressions II.75 et II.77, l'amélioration du rendement passe, entre autres, par la diminution des ΔV_{c_i}. Plusieurs solutions sont envisageables : un gain en tension proche de l'unité, la diminution du courant de charge, l'augmentation de la taille des capacités ou l'augmentation de la fréquence de commutation. Si la dernière de ces solutions est de loin la moins contraignante, elle s'accompagne cependant d'une augmentation des pertes de pilotage qui tend à inverser ses conséquences sur le rendement. Tout se joue alors sur l'optimisation du compromis entre pertes de charge et pertes de pilotage. L'introduction d'une inductance en série entre l'interrupteur et la capacité permet d'éliminer les pertes de charge; elle freine la variation du courant tandis que la différence de tension apparaît immédiatement à ses bornes. De fait, le rendement d'un hacheur série est généralement supérieur à celui d'un convertisseur à capacités commutées. Par ailleurs, des techniques visant à réaliser des convertisseurs à capacités commutées sans perte (« *lossless converter* » [98]) ont été proposées dans la littérature. Par exemple, les méthodes dites de « commutation douce » (« *soft switching* ») permettent de supprimer les pertes associées aux recouvrements tension-courant par commutation des interrupteurs lorsque la tension (ZVS pour *Zero-Voltage Switching*) ou le courant (ZCS pour *Zero-Current Switching*) s'annule [99].

II.4.3.3.b Abaisseur de tension à pompe de charge

Un abaisseur de tension à pompe de charge (ou SDC pour « *Step Down Converter* ») [100, 101] est schématisé sur la figure II.26. Ce circuit fait intervenir deux capacités flottantes (C_{f0} et C_{f1}), une capacité de sortie à la masse (C_o) et neufs interrupteurs (M_0 à M_8). Il permet de réaliser une conversion fractionnelle de la tension avec un rendement relativement élevé. Le gain en tension dépend, d'une part, des ratios entre les tailles des capacités et, d'autre part, de la topologie des phases de transfert. Ainsi, une structure comme celle de la figure II.26 permet de réaliser quatre gains distincts. Pour trois capacités identiques, ces derniers valent : $1/3$, $1/2$, $2/3$ et 1. Quel que soit le mode de fonctionnement considéré, le principe de conservation de la charge permet de démontrer que le gain en courant est l'inverse du gain en tension.

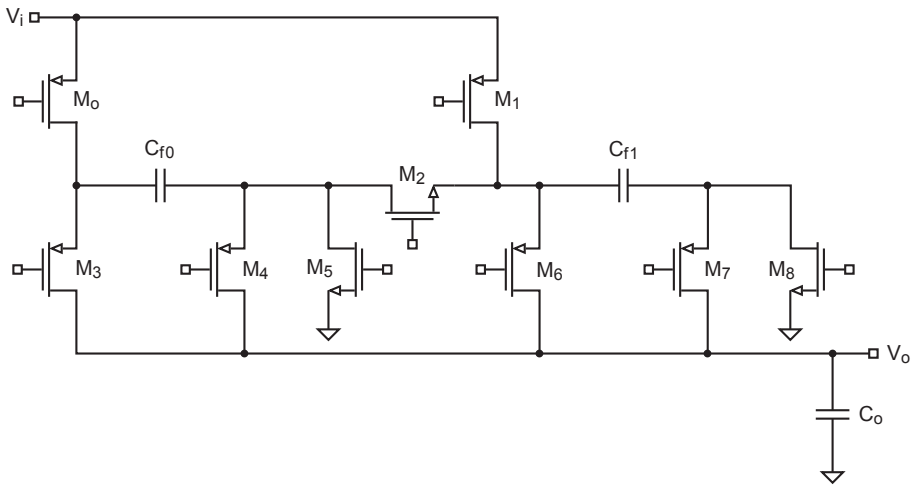


Fig. II.26 – *Abaisseur de tension à pompe de charge [100, 101].*

Les phases de charge et de décharge des modes $1/3$ et $2/3$ sont schématisées, respectivement, sur les

figures II.27 et II.28. L'entrée du convertisseur (V_i) est connectée à un générateur de tension idéal. La sortie du convertisseur (V_o) est quant à elle connectée à une source de courant continu puisant une charge Q_L à chaque demi-période. Dans la suite de cette étude, on supposera que : tous les transistors présentent des caractéristiques équivalentes, les capacités sont identiques et de taille C, les temps de charge et de décharge sont petits devant la demi-période d'un cycle de commutation, les éléments dissipatifs sont négligeables, la tension de sortie est proche de sa valeur idéale et que ses ondulations sont négligeables.

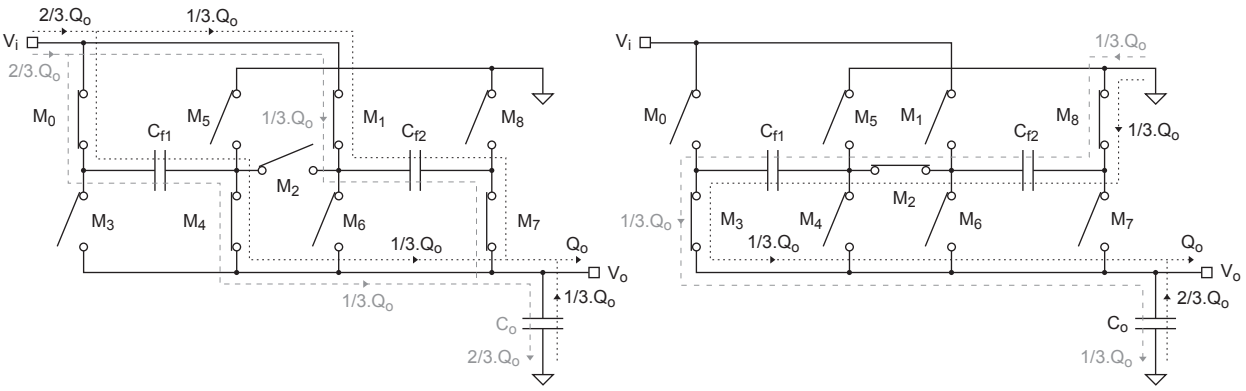


Fig. II.27 – *Abaisseur de tension à pompe de charge en mode* $2/3$.

Pendant la phase de charge de la configuration $2/3$ (cf. schéma gauche de la figure II.27), les deux capacités flottantes sont connectées en parallèle, puis chargées en série entre V_i et V_o. A la commutation, chaque capacité récupère la charge perdue pendant la phase de décharge; une charge égale aux $2/3$ de Q_L est fournie quasi-instantanément par V_i (trait gris à pointillés larges). A l'instant précédent la commutation vers la phase de charge, la différence entre la tension V_i et la tension aux bornes des capacités (i.e., ΔV_c) est égale à Q_L/C. Par conséquent, la commutation vers la phase de charge engendre une perte d'énergie égale à :

$$E_{(l,s_c)_{(2/3,ch)}} = \frac{1}{2} \cdot \frac{2 \cdot Q_L}{3} \cdot \frac{Q_L}{C} = \frac{Q_L^2}{3 \cdot C} \tag{II.78}$$

Immédiatement, la tension aux bornes des capacités flottantes atteint $1/3$ de V_i tandis que la tension aux bornes de la capacité de sortie atteint $2/3$ de V_i. Puis, pendant la demi-période de la phase de charge, une charge Q_L est débitée sur V_o (trait noir à pointillés fins). Le tiers de cette charge est délivré par C_o, le reste étant fourni par le générateur. A la fin de la phase de charge, la variation de charge a engendré une diminution de la tension V_o de $Q_L/(3C)$.

Pendant la phase de décharge de la configuration $2/3$ (cf. schéma droit de la figure II.27), les capacités flottantes sont connectées en série entre la masse et le nœud de sortie. La commutation entraîne instantanément un ré-équilibrage des charges entre les capacités; la charge $Q_L/3$ transite des capacités flottantes vers la capacité de sortie (trait gris à pointillés larges) et la tension de sortie se stabilise immédiatement à $2/3$ de V_i. A l'instant précédent la commutation vers la phase de décharge, la différence entre la tension présente aux bornes de C_o et celle présente aux bornes des deux capacités flottantes en série est égale à Q_L/C. Par conséquent, la diffusion des charges entraîne une perte d'énergie égale à :

$$E_{(l,s_c)_{(2/3,dch)}} = \frac{1}{2} \cdot \frac{Q_L}{3} \cdot \frac{Q_L}{C} = \frac{Q_L^2}{6 \cdot C} \tag{II.79}$$

Sur la totalité de la phase de décharge, une charge Q_L est fournie à la sortie; $2/3$ de cette charge proviennent de C_o, le reste étant fourni par les capacités flottantes (trait noir à pointillés fins). Cette variation de charge engendre une diminution de la tension de sortie égale à $2/3$ de Q_L/C. Elle est à l'origine du ΔV_c précédent la phase de charge.

En définitive, la valeur moyenne de la tension de sortie est approximativement égale aux $2/3$ de V_i. Lors d'un cycle de commutation, la charge totale délivrée par le générateur (Q_i) est égale aux $4/3$ de Q_L, tandis que la charge totale transférée en sortie (Q_o) est égale à $2Q_L$. Par suite, le gain en courant vaut $3/2$.

En ce qui concerne les pertes associées au pilotage des grilles (cf. équation II.74), on a $\Delta V_{gs} = V_i$, $\Delta V_{gd} < V_i$ et $C_{gd} \cong C_{gs}/10$. Par conséquent, l'expression II.74 peut se simplifier sous la forme :

$$E_{l,s_d} \cong C_{gs} \cdot V_i^2 \tag{II.80}$$

Ainsi, l'énergie de pilotage consommée par le SDC en mode $2/3$ lors d'un cycle de commutation vaut :

$$E_{(l,s_d)_{(2/3,tot)}} \cong 9 \cdot C_{gs} \cdot V_i^2 \tag{II.81}$$

Par suite, si l'on néglige les pertes de conduction, l'énergie totale perdue pendant un cycle de commutation est approximativement égale à :

$$E_{l_{(2/3)}} \cong E_{(l,s_c)_{(2/3,ch)}} + E_{(l,s_c)_{(2/3,dch)}} + E_{(l,s_d)_{(2/3,tot)}} = \frac{Q_L^2}{2} + 9 \cdot C_{gs} \cdot V_i^2 \tag{II.82}$$

En définitive, le rendement global du convertisseur fonctionnant en mode $2/3$ est donné par :

$$\eta_{2/3} = \frac{E_{o_{(2/3)}}}{E_{i_{(2/3)}} + E_{l_{(2/3)}}} = \frac{V_{o_{(2/3)}} \cdot Q_o}{V_i \cdot Q_{i_{(2/3)}} + E_{l_{(2/3)}}} \cong \frac{\frac{2}{3} \cdot V_i \cdot 2 \cdot Q_L}{V_i \cdot \frac{4}{3} \cdot Q_L + \frac{Q_L^2}{2} + 9 \cdot C_{gs} \cdot V_i^2} \tag{II.83}$$

Pour une structure idéale sans perte, le rendement en puissance tend bien vers 100%.

Pendant la phase de charge de la configuration $1/3$ (cf. schéma gauche de la figure II.28), les deux capacités flottantes sont connectées en série entre V_i et V_o. A la commutation, chaque capacité récupère immédiatement la charge perdue pendant la phase de décharge; une charge égale au tiers de Q_L est instantanément puisée sur V_i (trait gris à pointillés larges). A l'instant précédent la commutation vers la phase de charge, la différence entre la tension V_i et celle présente aux bornes des capacités est égale à Q_L/C. Par conséquent, la commutation vers la phase de charge s'accompagne d'une perte d'énergie égale à :

$$E_{(l,s_c)_{(1/3,ch)}} = \frac{1}{2} \cdot \frac{Q_L}{3} \cdot \frac{Q_L}{C} = \frac{Q_L^2}{6 \cdot C} \tag{II.84}$$

Immédiatement, la tension aux bornes de chaque capacité atteint $1/3$ de V_i. A nouveau, durant la demi-période de la phase de charge, une charge Q_L est débitée sur V_o (trait noir à pointillés fins). Les $2/3$ de cette charge sont fournis par C_o, le tiers restant étant délivré par le générateur. A la fin de la phase de charge, la variation de charge se traduit par une diminution de la tension V_o de $2/3$ de Q_L/C.

Pendant la phase de décharge de la configuration $1/3$ (cf. schéma droit de la figure II.28), les trois capacités sont connectées en parallèle entre la masse et le nœud de sortie. La commutation est immédiatement suivie d'un ré-équilibrage des charges; chaque capacité flottante communique une charge $Q_L/3$ à la

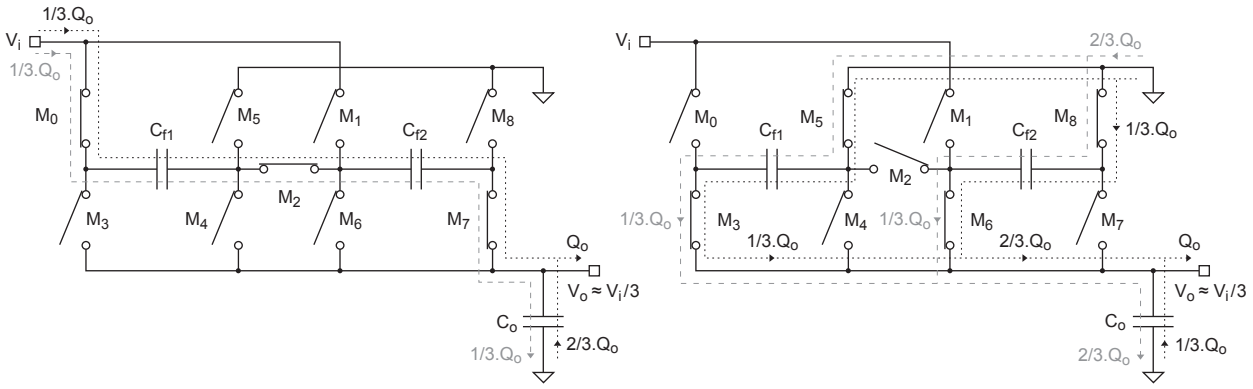


Fig. II.28 – *Abaisseur de tension à pompe de charge en mode* $1/3$.

capacité de sortie (trait gris à pointillés larges). Quasi-instantanément, la tension de sortie se stabilise à $1/3$ de V_i. A l'instant qui précède la commutation vers la phase de décharge, la différence entre la tension aux bornes de C_o et celle aux bornes des capacités flottantes est égale à Q_L/C. De fait, le transfert des charges s'accompagne d'une perte d'énergie égale à :

$$E_{(l,s_c)_{(1/3,dch)}} = \frac{1}{2} \cdot \frac{2 \cdot Q_L}{3} \cdot \frac{Q_L}{C} = \frac{Q_L^2}{3 \cdot C} \tag{II.85}$$

Lors de la phase de décharge, une charge Q_L est débitée sur la sortie; chaque capacité fournit $1/3$ de cette charge (trait noir à pointillés fins). Ce transfert de charge engendre une diminution de la tension de sortie égale à $Q_L/3C$. Elle est à l'origine des pertes induites par la commutation suivante.

Au final, la valeur moyenne de la tension de sortie est approximativement égale à $1/3$ de V_i. Durant un cycle complet, la charge totale délivrée par le générateur est égale aux $2/3$ de Q_L tandis que la charge totale délivrée en sortie est égale à $2Q_L$. Par conséquent, le gain en courant du convertisseur est égal à 3. Les expressions des pertes de pilotage et des pertes totales sont identiques à celles de la configurations $2/3$ (cf. expression II.81 et II.82). Par suite, le rendement du convertisseur en mode 1/3 est donné par :

$$\eta_{1/3} = \frac{E_{o_{(1/3)}}}{E_{i_{(1/3)}} + E_{l_{(1/3)}}} = \frac{V_{o_{(1/3)}} \cdot Q_o}{V_i \cdot Q_{i_{(1/3)}} + E_{l_{(1/3)}}} \cong \frac{\frac{1}{3} \cdot V_i \cdot 2 \cdot Q_L}{V_i \cdot \frac{2}{3} \cdot Q_L + \frac{Q_L^2}{2} + 9 \cdot C_{gs} \cdot V_i^2} \tag{II.86}$$

En mode $1/2$, la phase de charge est identique à celle du mode $2/3$, tandis que la phase de décharge est équivalente à celle du mode $1/3$. Ainsi, le gain en courant est proche de 2 et la valeur moyenne de la tension de sortie est approximativement égale à $V_i/2$. A chaque commutation, la tension différentielle ΔV_c est approximativement égale à $V_i/3$, ce qui est nettement supérieur aux valeurs rencontrées dans les cas précédents. Par conséquent, les pertes de charge sont plus élevées. En contrepartie, les capacités flottantes et les interrupteurs travaillent toujours en parallèle, ce qui tend à réduire les pertes de conduction. Enfin, en mode « gain unitaire », les interrupteurs relient directement l'entrée et la sortie du convertisseur.

L'abaisseur de tension à pompe de charge peut être utilisé comme bloc de puissance d'un régulateur à découpage. En complément du contrôle de sa fréquence de commutation, l'ajustement dynamique de sa configuration permet d'optimiser le rendement tout en améliorant la qualité de la régulation [100]. Néanmoins, ce type de convertisseur présente une capacité de régulation relativement faible car, d'une part, le

gain est quantifié et, d'autre part, la tension de sortie varie avec la tension d'entrée. Ainsi, le bruit de sortie et le rendement sont fonction de l'écart entre le gain visé et le gain natif le plus proche (i.e., $1/3$, $1/2$, $2/3$ ou 1); ils se dégradent dès lors que l'écart augmente. En d'autres termes, le régulateur est d'autant plus performant que le gain recherché est proche d'un des gains intrinsèques de la structure. Bien que l'augmentation du nombre d'étages permette d'affiner le pas de la plage de gain, la multiplication du nombre d'interrupteurs se traduit, quand à elle, par une augmentation significative des pertes de pilotage. L'unité de contrôle repose généralement sur une batterie de comparateurs à seuil et un circuit logique simple. Une solution plus élaborée consiste à confier le contrôle du convertisseur à un microcontrôleur [80]. Toutefois, cette solution n'est envisageable que si les ressources matérielles disponibles sont suffisantes pour assurer l'exécution des processus « temps-réel » nécessaires à son fonctionnement. Dans notre cas, l'implémentation d'un microprocesseur dédié conduirait à une consommation excessive d'énergie et d'espace.

D'un point de vue sécuritaire, le niveau de protection dépend de la phase considérée. Quel que soit le mode de fonctionnement, la phase de charge donne lieu à un couplage capacitif direct entre l'entrée et la sortie du régulateur. De plus, la faible résistance des interrupteurs limite l'effet de filtrage. Par conséquent, une partie importante du signal informationnel est transmise au nœud d'entrée. A l'opposé, la phase de décharge offre un niveau de protection élevé; si l'on néglige les courants de fuite, le nœud de sortie est alimenté exclusivement par les capacités. Pour améliorer la continuité du flux énergétique, une méthode consiste à utiliser deux cellules connectées en parallèle et fonctionnant en opposition de phase. Cependant, cette topologie engendre une fuite continuelle d'informations.

II.4.3.3.c Hacheur de courant

Le premier convertisseur DC-DC dédié à la protection contre les attaques par analyse en courant fut proposé en 2000 par A. Shamir [76, 102]. Son principe est illustré sur la figure II.29. Ce « hacheur de courant » repose uniquement sur deux capacités à la masse (C_1 et C_2) et quatre interrupteurs (M_0 à M_3). L'allure des signaux de contrôle ($V_{\phi 1}$ et $V_{\phi 2}$) est représentée sur la figure II.29.

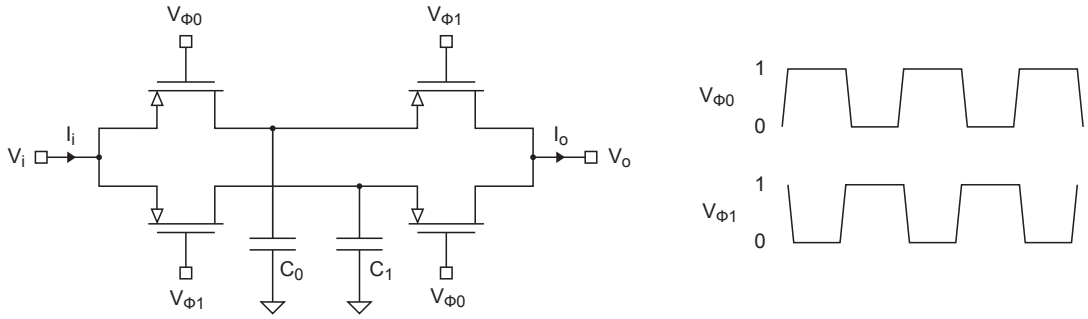


Fig. II.29 – *Hacheur de courant [76].*

Pendant la première moitié du cycle, la capacité C_1 est chargée sur V_i alors que C_2 est déchargée sur V_o. Pendant la seconde moitié du cycle, les rôles sont inversés. La valeur moyenne du courant transitant sur V_i lors d'un cycle de charge est égale à la valeur moyenne du courant transitant sur V_o lors du cycle de décharge précédent. Le plus souvent, un microprocesseur RISC exécute une instruction par cycle d'horloge. Par

conséquent, le niveau de corrélation entre I_i et I_o sera d'autant plus faible que la fréquence de commutation du convertisseur (f_s) sera petite devant la fréquence d'horloge du processeur alimenté (f_c). En contrepartie, la réduction de la fréquence de commutation a pour effet d'augmenter l'amplitude des ondulations de la tension de sortie.

Les gains en tension et en courant d'un hacheur de courant sont unitaires. Par conséquent, l'utilisation d'une cellule de ce type comme bloc de puissance d'un régulateur de tension se traduit par la génération d'un courant pulsé. De fait, le bruit de sortie est élevé et les pertes de charge importantes. Néanmoins, certaines techniques, comme par exemple celles des capacités quasi-commutées (QSC pour « *Quasi-Switched Capacitor* ») [103], permettent de réduire les pertes de commutation par le biais d'une charge à courant constant. A fréquence de commutation fixée et pour un courant de sortie donné, la taille des capacités conditionne le niveau d'ondulation de la tension sortie et par voie de conséquence, l'importance des pertes de charges. Le dimensionnement des capacités est donc au cœur du compromis entre régulation, sécurité et surface. Comme suggéré dans [102], les capacités peuvent être soit intégrées à la puce, soit encapsulées dans le corps de la carte. Au vue des spécifications du cahier des charges, l'intégration des capacités nécessiterait une surface trop importante. Si l'encapsulation permet de s'affranchir des problèmes de surface, en revanche, elle facilite l'accès aux signaux internes et occasionne un surcoût non-négligeable du procédé d'encartage. Cette solution n'est donc pas adaptée à nos contraintes.

II.4.4 Synthèse et conclusion

Les principaux avantages et inconvénients des différents types de convertisseur sont synthétisés dans le tableau II.6. Le choix entre l'une de ces topologies est une question de priorité. En terme de régulation et d'encombrement, les régulateurs linéaires sont de loin les plus performants. De plus, les régulateurs linéaires à dérivation permettent d'atténuer significativement les fuites d'informations. En revanche, leur rendement est encore plus bas que celui des régulateurs linéaires séries. Lorsque le rendement est l'objectif principal, les régulateurs à découpages deviennent incontournables. Si la surface n'est pas limitée, l'utilisation d'un hacheur série à inductance permet d'atteindre un rendement élevé. Dans le cas contraire, l'utilisation d'une pompe de charge permet d'atteindre un meilleurs compromis entre rendement et surface. En outre, l'effet de moyennage induit par le transfert séquentiel des charges permet de décorréler le courant entrant du courant sortant. Cependant, la nature pulsée du courant se traduit par un bruit de sortie plus élevé que dans le cas d'un régulateur linéaire. Quoi qu'il en soit, l'implémentation d'une pompe de charge nécessiterait une surface largement supérieure à celle prévue par le cahier des charges. En définitive, aucune de ces structures ne répond entièrement à nos attentes.

Type de convertisseur		Régulation	Rendement	Sécurité	Surface
Linéaire	Série	+ +	-	- -	+ +
	A dérivation (« *Shunt regulator* »)	+ +	- -	+	+
A découpage	Hacheur série (« *Buck converter* »)	+	+ +	+	- -
	Abaisseur à pompe de charge	-	+	+	-
	Hacheur de courant	- -	-	+ +	-

Tab. II.6 – *Comparatif des différents types de convertisseur.*

II.5 Système proposé

II.5.1 Principe

Le courant d'alimentation d'un microcontrôleur encartable est représenté sur la partie gauche de la figure II.30. Il peut se décomposer en la somme de deux courants : un courant lentement variable (composante DC) et un courant à variations rapides (composante AC). La composante DC véhicule la majorité de la puissance, tandis que la composante AC véhicule la majorité du signal informationnel. Ainsi, en transférant la composante DC par un convertisseur linéaire (canal DC) et la composante AC par un convertisseur à découpage (canal AC), la structure bi-canal du système proposé permet de décorréler le courant entrant du courant sortant tout en minimisant la surface.

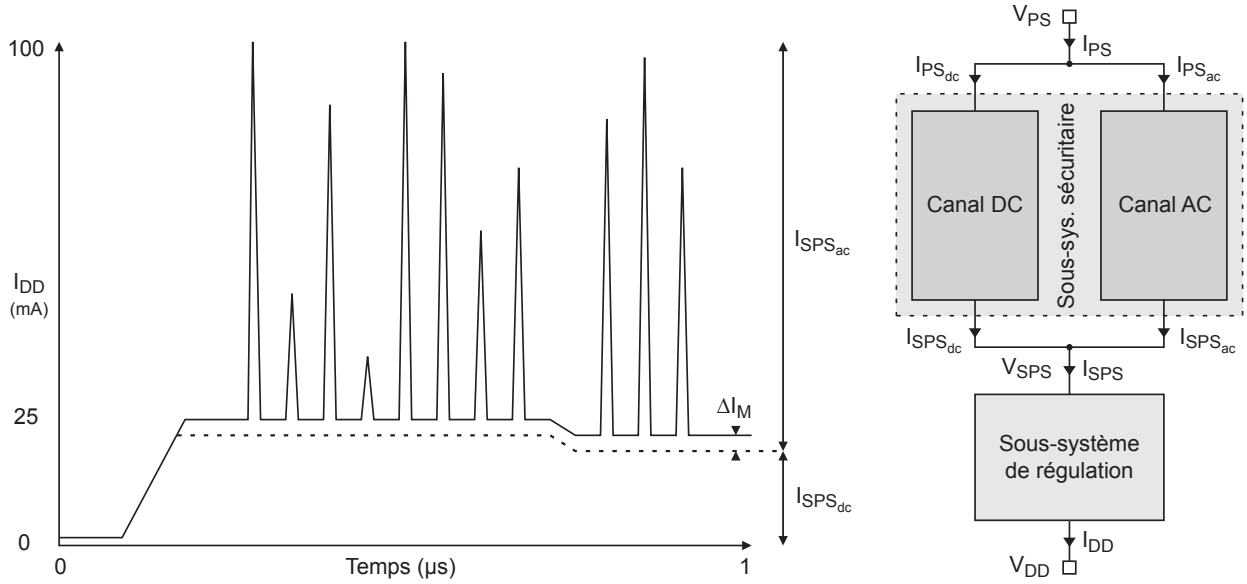


Fig. II.30 – *Principe de fonctionnement du système proposé.*

L'architecture du système proposé est schématisée à droite de la figure II.30. Elle repose sur deux sous-systèmes en série : un sous-système sécuritaire connecté entre le nœud d'alimentation externe (V_{PS}) et un nœud d'alimentation intermédiaire (V_{SPS}), et un sous-système de régulation connecté entre V_{SPS} et le nœud d'alimentation interne (V_{DD}). Le sous-système sécuritaire repose sur une structure bi-canal constituée d'un régulateur linéaire série (canal DC) en parallèle avec un convertisseur à découpage (canal AC). La bande passante du régulateur linéaire est volontairement limitée de sorte qu'il ne délivre que la partie lentement variable du courant d'alimentation ($I_{SPS_{dc}}$). Ainsi, la partie AC du courant d'alimentation ($I_{SPS_{ac}}$) est nécessairement transmise par le convertisseur à découpage. Par conséquent, le courant d'alimentation externe (I_{SPS}) est bien décorrélé du courant d'alimentation interne (I_{DD}). D'après les spécifications du cahier des charges, la valeur moyenne de la composante AC est petite devant celle de la composante DC. Or, à courant équivalent, la surface d'un régulateur linéaire est petite devant celle d'un convertisseur à découpage. Par conséquent, l'architecture proposée permet également de minimiser la surface totale du système.

L'activité du convertisseur à découpage engendre un bruit de sortie relativement important, d'où la

nécessité d'intercaler un sous-système de régulation entre V_{SPS} et la charge. Par ailleurs, afin d'améliorer la réponse transitoire, le canal AC véhicule également une partie du courant DC. En effet, la marge de courant ΔI_M (cf. figure II.30) permet de limiter les ondulations de V_{SPS} au cas où la valeur moyenne du courant I_{SPS} viendrait à varier plus rapidement que la bande passante du canal DC. En outre, le rendement du canal AC est généralement supérieur à celui du canal DC. Par conséquent, le rendement global du système augmente avec ΔI_M. Cependant, à fréquence de commutation fixée, une augmentation de ΔI_M ne peut être atteinte que pour un accroissement de la surface du convertisseur. Il s'agit donc de trouver un compromis approprié entre régulation, rendement, sécurité et surface.

II.5.2 Architecture

II.5.2.1 Vue d'ensemble

L'architecture du système proposé est représentée sur la figure II.31. Le regroupement des blocs par fonctionnalité permet de distinguer quatre ensembles : le sous-système sécuritaire, le sous-système de régulation, le gestionnaire de puissance (PM pour « *Power Manager* ») et le générateur de références (RG pour « *Reference Generator* »).

Le système s'adapte automatiquement à l'amplitude de la tension d'alimentation externe. Il présente trois modes de fonctionnement distincts : un mode sécurisé à haut rendement lorsque $V_{PS} = 5\,V \pm 10\%$, un mode ultra-sécurisé lorsque $V_{PS} = 3.3\,V \pm 10\%$ et un mode LDO non-sécurisé lorsque $V_{PS} = 1.8\,V \pm 10\%$. Le gestionnaire de puissance assure le démarrage et la configuration dynamique du système. Il contrôle l'ensemble du système par l'intermédiare des bus $OTACTRL$, $S3CTRL$, $RCGCTRL$ et $CPCTRL$. Ces bus comportent des signaux de contrôle numériques, un courant de référence (I_{ref}) et une tension de référence (V_{ref}). Enfin, le générateur de références à faible tension d'alimentation (LV pour « *Low Voltage* ») produit une référence de tension ($V_{ref_{LV}}$) et une référence de courant ($I_{ref_{LV}}$) qu'il délivre au gestionnaire de puissance par l'intermédiaire du bus REF.

La vue d'ensemble du circuit réalisé sous Cadence Virtuoso est représentée sur la figure II.32. Par rapport au schéma de principe de la II.31, il comporte deux cellules supplémentaires : l'alimentation externe (EPS pour « *External Power Supply* ») et la charge (« *Load* »). Les entrées numériques PM et RCG sont destinées au microcontrôleur. Elles autorisent, respectivement, la mise en veille du gestionnaire de puissance et l'activation du générateur d'horloge aléatoire.

Le gestionnaire de puissance contrôle l'ensemble du système par le biais des bits $PSS(i)$ et des courants de polarisation $Ib\_sn2u\_(i)$. Les bits $PSS0$ et $PSS1$ indiquent l'état de la tension d'alimentation externe. Les cellules constitutives des différents blocs sont détaillées dans les sections suivantes.

II.5.2.2 Sous-système sécuritaire

Le canal DC du sous-système sécuritaire repose sur un régulateur linéaire série à transistor de puissance PMOS (M_P). La tension V_{ref} intervient comme signal de consigne de la boucle de régulation. Le canal AC repose sur un convertisseur à capacités commutées (SCC pour « *Switched Capacitor Converter* »). Afin

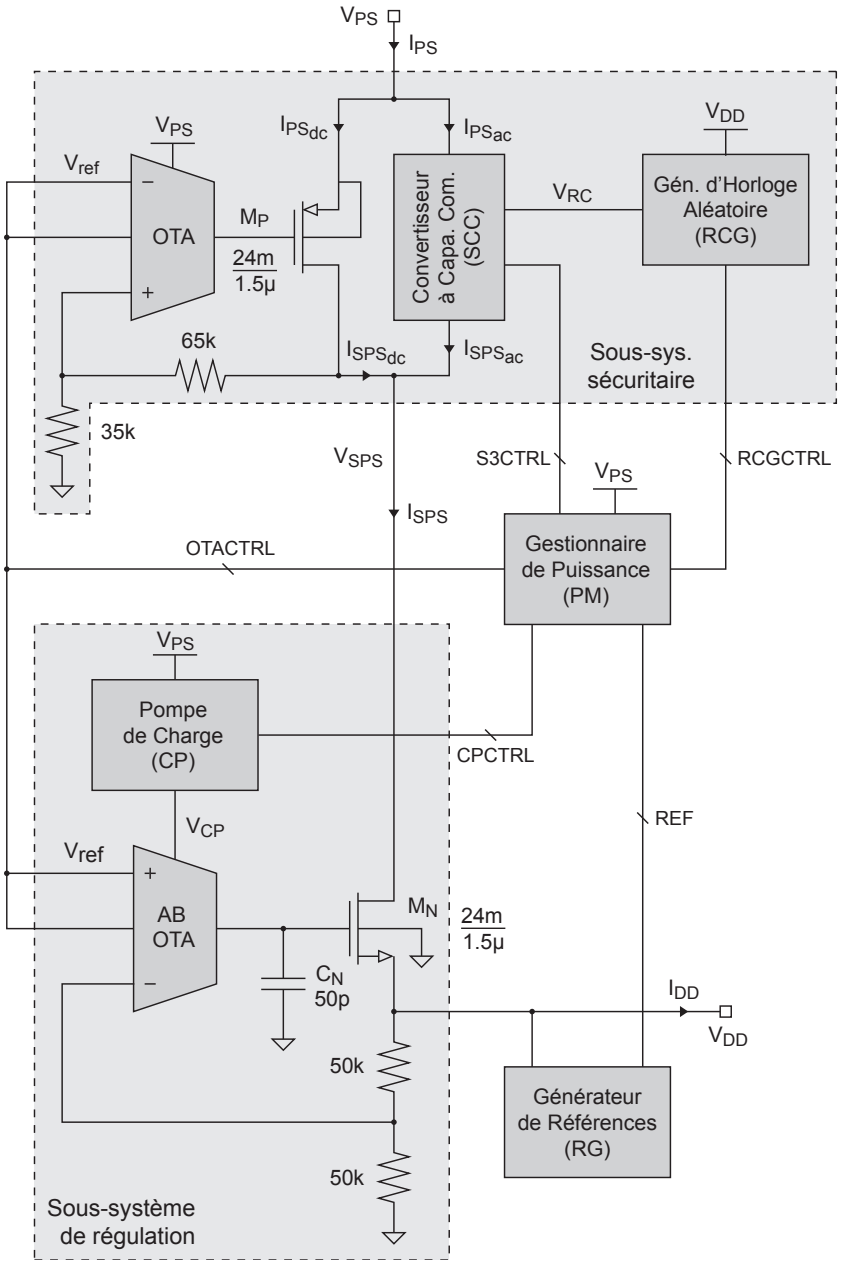


Fig. II.31 – *Architecture du système proposé.*

de masquer les fuites d'information résiduelles, le convertisseur à capacités commutées est cadencé par un générateur d'horloge aléatoire (RCG pour « *Random Clock Generator* »). La valeur moyenne du courant délivré par le convertisseur est proportionnelle à la différence entre sa tension de sortie non-chargée et la tension de sortie du régulateur linéaire. Ainsi, plus la valeur moyenne de V_{SPS} fixée par le canal DC est basse, plus la quantité de courant transitant par le canal AC est importante. Cependant, l'amplitude du bruit de sortie est également proportionnelle à cette différence, et la marge de tension $V_{SPS} - V_{DD}$ doit être maintenue à un niveau suffisant pour garantir le bon fonctionnement du sous-système de régulation. Il convient donc de déterminer la valeur moyenne de V_{SPS} offrant le meilleur rapport régulation-sécurité.

Le fonctionnement du système est synthétisé dans le tableau II.7. Lorsque V_{PS} est égale à $5\ V \pm 10\%$,

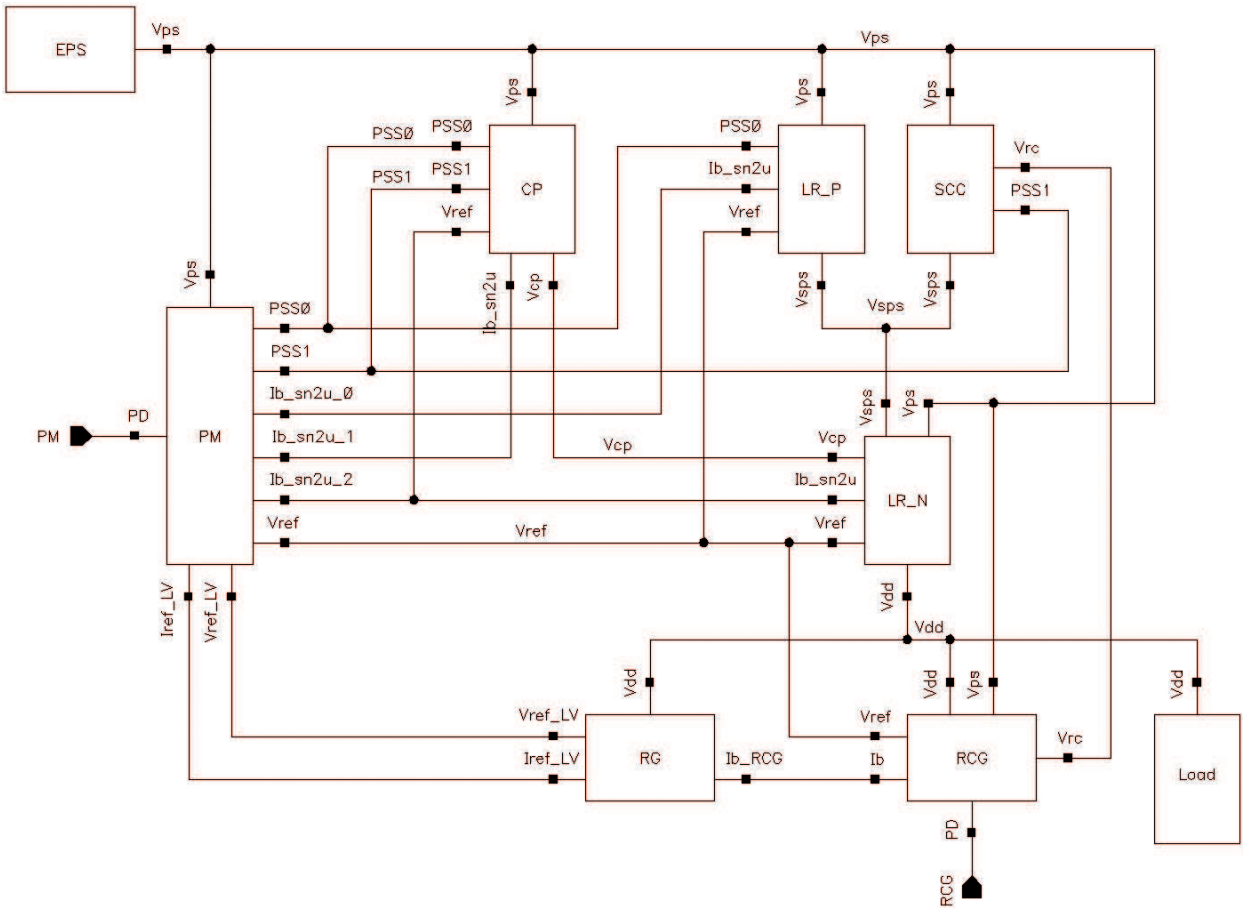


Fig. II.32 – *Schéma-bloc du système proposé.*

Tension d'alim. externe	Mode	Fonctionnement		Bits de ctrl.	
		LR_P	SCC	$PSS0$	$PSS1$
$V_{PS} > 4\ V$	Sécurisé haut-rend.	$V_{SPS} \approx 2.6\ V$	Pompe de charge $2/3$	1	1
$2.5\ V < V_{PS} < 4\ V$	Ultra-sécurisé	$V_{SPS} \approx 2.6\ V$	Hacheur de courant	1	0
$V_{PS} < 2.5\ V$	Non-sécurisé LDO	$V_{SPS} \approx V_{PS}$	Désactivé	0	0

Tab. II.7 – *Modes de fonctionnement du système proposé.*

le convertisseur linéaire régule la tension V_{SPS} à $2.6\ V$ tandis que le convertisseur à capacités commutées fonctionne en pompe de charge à gain $2/3$. Cette combinaison permet de tirer profit de la différence importante entre V_{PS} et V_{DD} pour protéger la charge, tout en maximisant le rendement global du convertisseur. Lorsque V_{PS} est égale à $3.3\ V \pm 10\%$, le régulateur linéaire continue à réguler la tension V_{SPS} à $2.6\ V$. En revanche, la marge de tension devient insuffisante pour faire fonctionner le convertisseur à découpage en mode pompe de charge tout en conservant une différence $V_{SPS} - V_{DD}$ suffisante. Ce dernier fontionne alors en mode hacheur de courant ce qui, faute d'améliorer le rendement, assure une protection élevée contre les attaques par analyse de courant. Dans les deux cas, la valeur moyenne de la tension de sortie du convertisseur à capacités commutées non-chargé est approximativement égale à $3.3\ V$; les $700\ mV$ d'écart entre

cette valeur et les $2.6\ V$ fixés par le régulateur linéaire garantissent un niveau de courant AC suffisant. Enfin, lorsque V_{PS} est égale à $1.8\ V \pm 10\%$, la marge de tension devient insuffisante pour activer le sous-système sécuritaire. Il est alors désactivé et court-circuité par le biais du transistor de puissance (M_P).

II.5.2.2.a Régulateur linéaire série

Afin de limiter le niveau de corrélation entre les courants I_{PS} et I_{SPS}, le régulateur ne doit transmettre que la partie lentement variable de I_{SPS}. L'objectif est donc de ralentir la régulation de charge, sans toutefois sacrifier la régulation de ligne. Dans un régulateur linéaire série, l'utilisation d'un transistor de puissance de type PMOS limite intrinsèquement la vitesse de régulation de charge (cf. § II.4.2.1.e). Cette spécificité a motivé notre choix. Le circuit du régulateur linéaire (LR_P) est représenté sur la figure II.33.

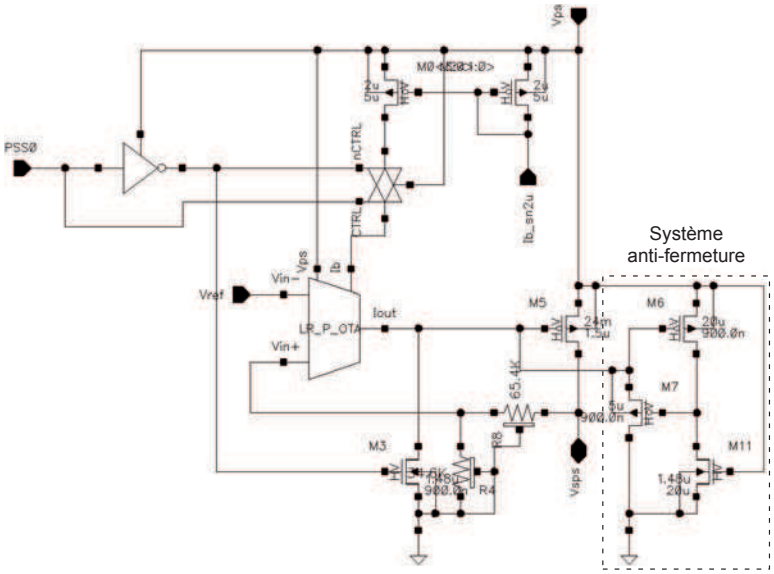


Fig. II.33 – *Régulateur linéaire série (LR_P) intégré au sous-système sécuritaire.*

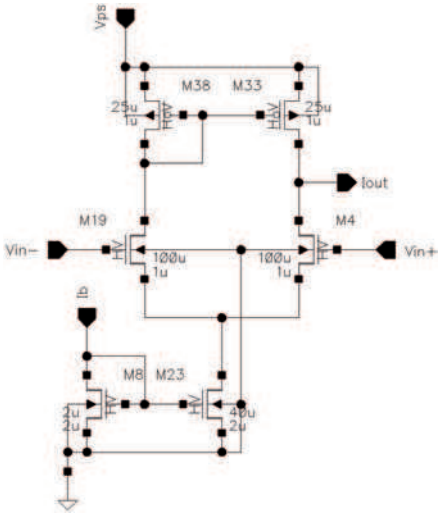


Fig. II.34 – *OTA (LR_P_OTA) du régulateur linéaire série (LR_P).*

Comme démontré au § II.4.2.1.c, la marge de phase diminue avec le courant de charge. Afin de garantir la stabilité de V_{SPS} pendant les phases à faible courant de charge (démarrage et mode veille), le transistor de puissance (M_5) est muni d'un dispositif anti-fermeture; l'action conjuguée des transistors M_6, M_7 et M_{11} empêche la tension V_{GS_5} de descendre en-dessous d'un certain seuil. Ainsi, lorsque le courant de charge devient trop faible, le transistor M_7 court-circuite la boucle de régulation. Le transistor de puissance PMOS repose sur un bloc précaractérisé équivalent à un transistor de largeur $24\ mm$ et de longueur $= 1.5\ \mu m$. Sa surface avoisine les $0.2\ mm^2$ et sa capacité équivalente de grille atteint $60\ pF$. La résistance totale du pont résistif est fixée à $100\ K\Omega$. Cette valeur offre un compromis approprié entre courant de repos et surface silicium. La logique de contrôle interface le régulateur avec le gestionnaire de puissance. Lorsque la tension d'alimentation externe est à $1.8\ V$, le bit $PSS0$ est à 0; la porte de transmission coupe la polarisation de l'OTA et le transistor de rappel court-circuite la grille du transistor de puissance à la masse. Par suite, la tension V_{SPS} suit la tension V_{PS}.

D'après les conclusions du § II.4.2.1.e, un régulateur linéaire série à transistor PMOS présente un

PSR^+ intrinsèquement moins élevé que celui d'un régulateur linéaire série à transistor NMOS. Néanmoins, l'utilisation d'un OTA adéquat permet de limiter cet effet secondaire indésirable (cf. § II.4.2.1.c). C'est le cas de l'OTA utilisé dans le sous-système sécuritaire (cf. figure II.34). Il s'agit d'un OTA simple terminaison à paire différentielle NMOS chargée par un miroir.

L'ajustement des caractéristiques de l'OTA permet de régler la bande passante de la boucle de transmission. D'après le cahier des charges, la fréquence de fonctionnement du microcontrôleur à alimenter est fixée à $20\ MHz$. Dans ce cas, les résultats obtenus en simulation montrent qu'une fréquence de gain unitaire de $2\ MHz$ offre un compromis adéquat entre régulation et taux d'atténuation en courant. A pleine charge, la marge de phase est prise supérieure à $60°$. La consommation moyenne de l'OTA est de $42\ \mu A$.

II.5.2.2.b Générateur d'horloge aléatoire

La faible surface disponible impose de fixer la longueur des transistors de puissance au minimum autorisé par la technologie. Or, comme évoqué au paragraphe II.4.2.1.c, ce choix se traduit par un effet de modulation important. Si ce dernier améliore la régulation de charge, en revanche, il dégrade significativement le taux d'atténuation en courant. En effet, les variations de I_{DD} provoquent des variations de V_{DD} qui agissent directement sur le courant I_{SPS}. Ces dernières entraînent des variations de V_{SPS} qui agissent par effet Early sur le courant I_{PS}. Ainsi, bien qu'ils soient très nettement atténués et déformés, les pics de consommation de la charge restent tout de même visibles sur le courant d'alimentation externe. Pour masquer ces fuites, le convertisseur à capacités commutées (SCC) est cadencé par un signal d'horloge aléatoire (V_{RC}). Ainsi, les signatures résiduelles de la charge deviennent indissociables des appels de courant du SCC. Pour que le masquage soit efficace, la charge et le SCC doivent être activés simultanément et la fréquence de commutation moyenne du SCC doit être égale à la fréquence de fonctionnement du microcontrôleur alimenté. A cet effet, la plage de variation fréquentielle de V_{RC} est centrée sur $20\ MHz$ et s'étend symétriquement sur $30\ MHz$. Dans ces conditions, la consommation moyenne du générateur d'horloge aléatoire (RCG) est inférieure à $1\ mW$. L'étude approfondie du RCG fait l'objet du chapitre III.

II.5.2.2.c Convertisseur à capacités commutées (SCC)

Le circuit du convertisseur à capacités commutées (SCC) est représenté sur la figure II.35. Il est constitué de deux blocs HV : un bloc de puissance (SCC_PE) et un générateur de phases (SCC_Clk). Le bloc de puissance comporte les éléments réactifs et les interrupteurs de puissance. Sa configuration est fonction de l'état du bit $PSS1$. Le second bloc génère les 4 signaux de pilotage destinés aux interrupteurs du bloc de puissance ($V_{clk[0...3]}$). Ces signaux sont dérivés du signal V_{RC} produit par le générateur d'horloge aléatoire.

Le circuit du bloc SCC_PE est représenté sur la figure II.36. Il est constitué de deux cellules de puissance identiques (A et B) et d'une logique de contrôle. Les cellules A et B sont connectées en parallèles et fonctionnent en alternance; lorsque la cellule A est en phase de charge, la cellule B est phase de décharge et vice-versa. Leur structure est équivalente à celle de la pompe de charge à gain $2/3$ présentée au paragraphe II.4.3.3.b (cf. figure II.26). Cependant, la structure proposée présente deux transistors NMOS supplémentaires. Cette nouvelle topologie offre deux modes de fonctionnement distincts : un mode identique à celui du circuit original et un mode hacheur de courant analogue à celui de la figure II.29. La configuration des

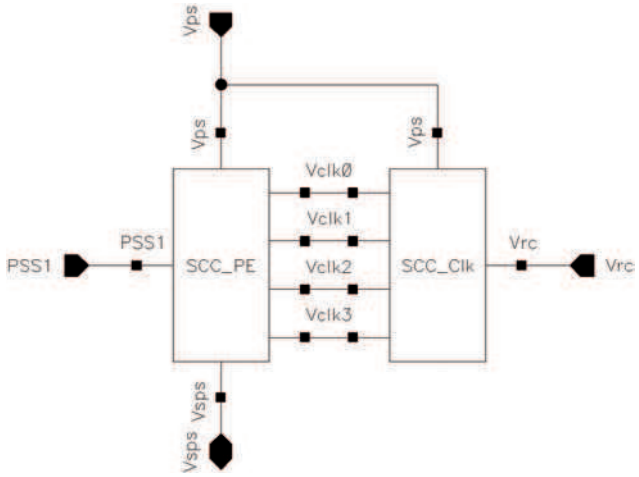


Fig. II.35 – *Schéma du convertisseur à capacités commutées (SCC).*

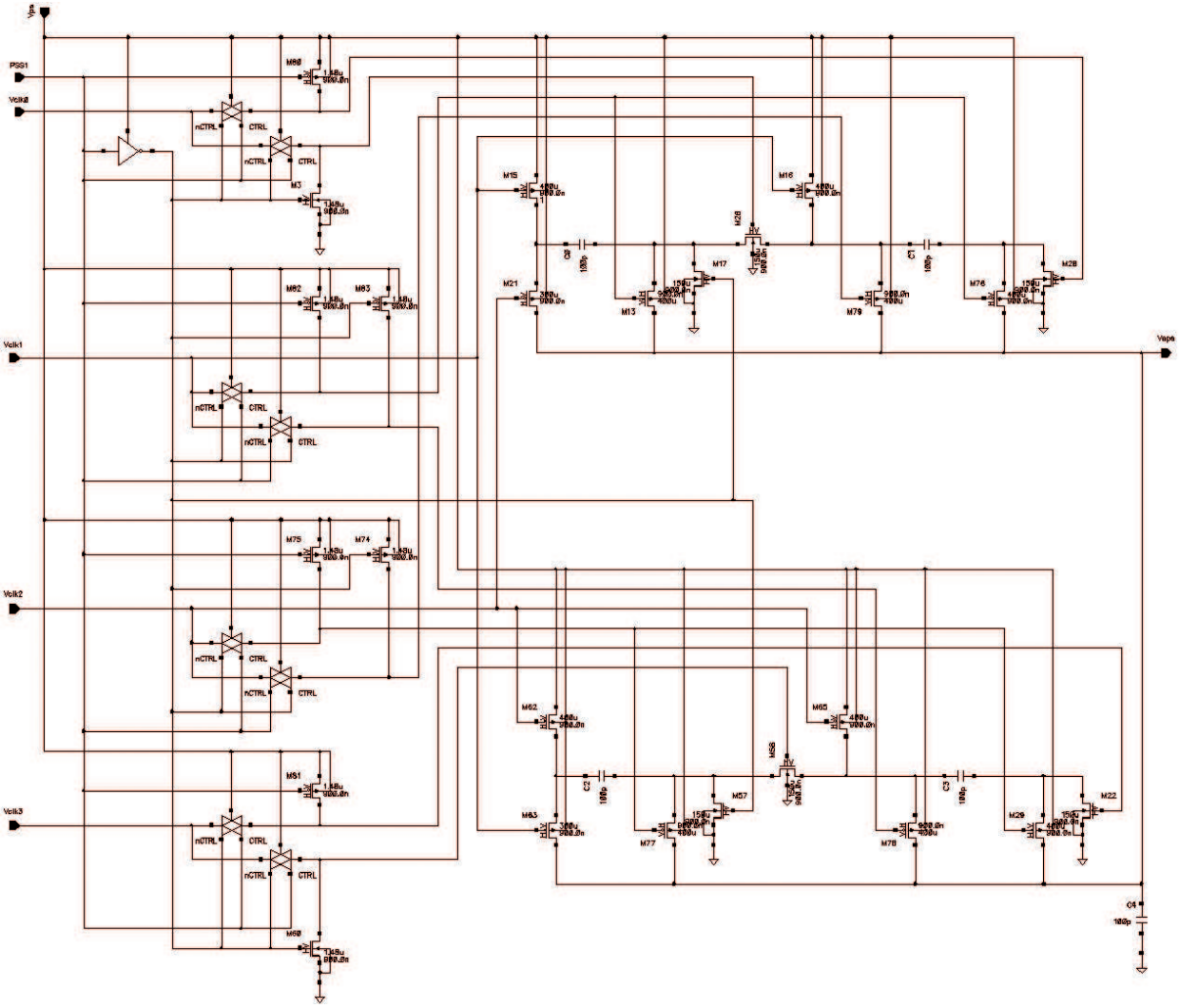


Fig. II.36 – *Bloc de puissance (SCC_PE) du convertisseur à capacités commmutées (SCC).*

cellules est fonction de l'état du bit $PSS1$; lorsqu'il est à 1, les cellules fonctionnent en pompe de charge et lorsqu'il est à 0, les cellules fonctionnent en hacheur de courant. Les portes de transmission du bloc logique assurent la configuration du bloc SCC_PE par aiguillage des signaux de phase. Au total, le bloc de puissance fait intervenir cinq capacités poly1-poly2 de $100\ pF$ chacune. Leur implémentation nécessite une surface globale d'environ $0.22\ mm^2$. Concernant les interrupteurs de puissance, leur longueur est fixée au minimum ($0.9\ \mu m$), la largeur des transistors NMOS est fixée à $150\ \mu m$ et la largeur des transistors PMOS est fixée à $400\ \mu m$.

Le générateur de phases est représenté sur la figure II.37. Il est constitué de trois cellules HV : un circuit anti-recouvremment (SCC_Clk_NO) et deux buffeurs de tension (SCC_Clk_Buf).

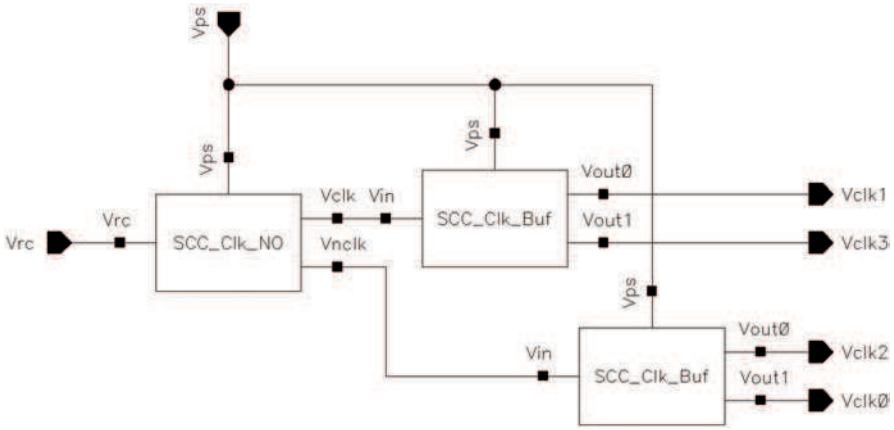


Fig. II.37 – *Schéma du générateur de phases (SCC_Clk).*

Afin d'éviter tout court-circuit lors des commutations, les signaux de pilotage des interrupteurs doivent être à phases non-recouvrantes. La première cellule de la chaîne (cf. figure II.38) permet de générer deux signaux à phases non-recouvrantes (V_{clk} et V_{nclk}) à partir du signal d'horloge aléatoire (V_{RC}) [104].

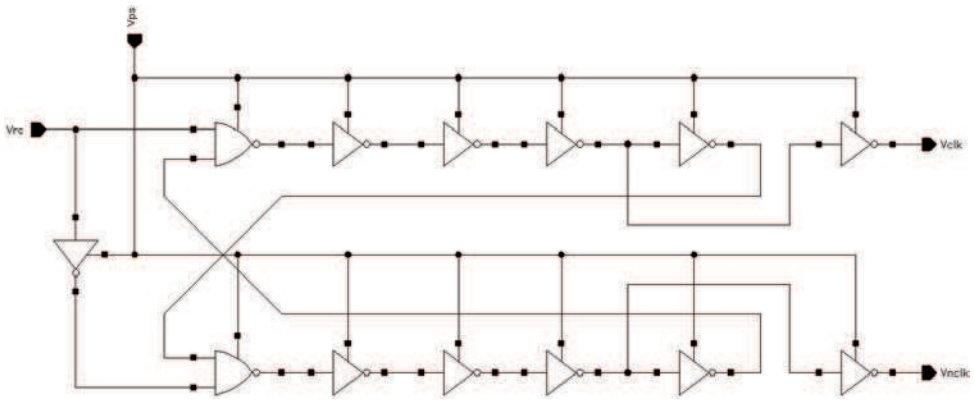


Fig. II.38 – *Circuit anti-recouvremment (SCC_Clk_NO) du générateur de phases (SCC_Clk) [104].*

Les chaînes d'inverseurs entrant dans la composition des buffers de la figure II.39 convertissent les signaux V_{clk} et V_{nclk} en quatres signaux à phases non-recouvrantes bufférisés. Le dimensionnement des

inverseurs passe par un compromis entre consommation et ouverture du diagramme de l'oeil : la consommation doit être minimisée, sans toutefois perdre le caractère non-recouvrant des signaux de phase. En raison des dimensions importantes des interrupteurs et du caractère élevé de la fréquence de commutation, la consommation du générateur de phases constitue la principale dépense énergétique du système. Pour $\overline{f_s} = 20\ MHz$, elle s'élève à $5.55\ mW$ en mode pompe de charge ($1.1\ mA$ sous $5\ V$) et à $1.72\ mW$ en mode hacheur de courant ($0.52\ mA$ sous $3.3\ V$).

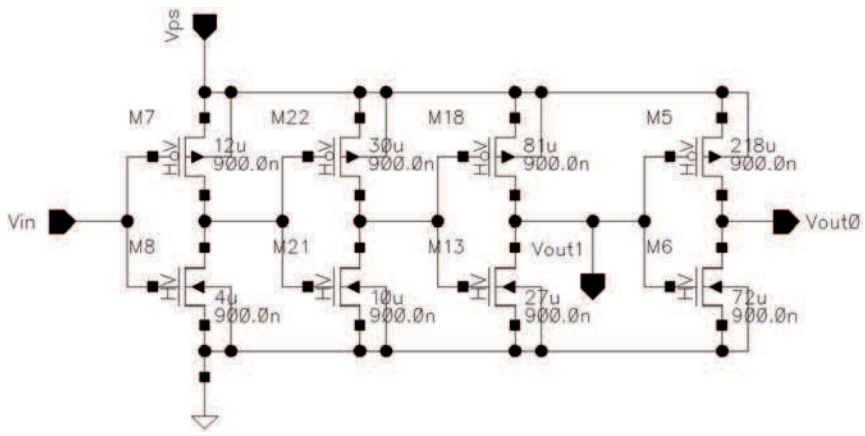


Fig. II.39 – *Buffer (SCC_Clk_Buf) du générateur de phases (SCC_Clk).*

II.5.2.3 Sous-système de régulation

De par son principe de fonctionnement, le sous-système sécuritaire engendre un bruit de sortie élevé. Par conséquent, la tension V_{SPS} ne peut pas être utilisée directement pour alimenter la charge. L'objectif du sous-système de régulation (LR_N) est de réguler V_{DD} à partir de V_{SPS}. Son circuit est schématisé sur la figure II.40.

Compte tenu des variations importantes de I_{DD} et de V_{SPS}, le convertisseur doit présenter à la fois une régulation de charge efficace et un PSR^+ élevé. C'est précisément le cas du régulateur linéaire série à transistor NMOS. Dans sa configuration suiveur, le transistor NMOS (M_N) permet d'isoler efficacement V_{DD} de V_{PS}, tout en garantissant une réponse rapide aux appels du courant de charge (cf. § II.4.2.1.c). Comme dans le cas du régulateur LR_P, le transistor de puissance du régulateur LR_N repose sur une cellule précaractérisée équivalente à un transistor tel que $W_p = 24\ mm$, $L_p = 1.5\ \mu m$ et $C_p = 60\ pF$. La polarisation de ce dernier devient problématique des lors que la tension d'alimentation externe ne prend pas sa valeur la plus haute. Afin de surmonter cette difficulté, nous avons opté pour la seconde solution proposée au paragraphe II.4.2.1.a : l'alimentation de l'OTA par une pompe de charge (CP) [92]. Cette technique présente l'avantage de détruire les informations véhiculées par le courant de consommation de l'OTA. En contrepartie, elle entraîne une surconsommation relativement importante et son implémentation requiert une surface non négligeable. La minimisation de cette dernière se paye au prix d'un augmentation du bruit de sortie. Par conséquent, l'OTA doit présenter à la fois une consommation faible et un PSR^+ élevé [94].

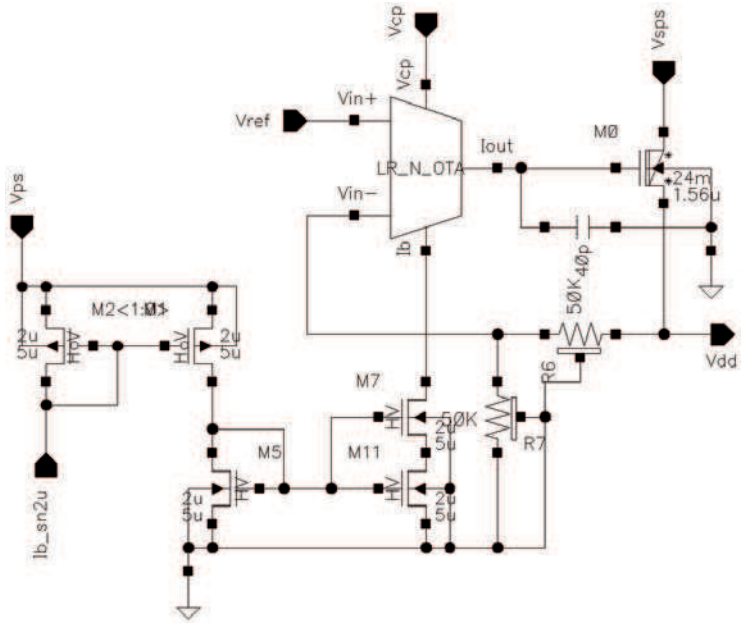


Fig. II.40 – *Régulateur linéaire série à transistor NMOS (LR_N) du sous-système de régulation.*

La vitesse de réaction de l'OTA ne joue qu'un rôle secondaire dans la qualité de la réponse transitoire d'un régulateur linéaire série à transistor NMOS. En effet, la vitesse de boucle de transmission sera toujours plus lente que la réponse intrinsèque du transistor monté en suiveur [91]. A ce titre, l'utilisation d'un OTA à polarisation adaptative permet de réduire significativement la valeur moyenne du courant de repos, tout en minimisant la dégradation de la réponse transitoire. En effet, l'augmentation du courant de polarisation en fonction de la tension différentielle d'entrée garantit un *slew rate* élevé lorsqu'il est nécessaire et une consommation faible le reste du temps. Ainsi, l'OTA régule principalement la partie DC de V_{DD}, tandis que la source du transistor de puissance offre une régulation intrinsèque de la partie AC. Le niveau de recouvrement entre ces deux modes est au cœur du compromis entre régulation et consommation.

L'OTA à polarisation adaptative (ABOTA pour « *Adaptive Biasing OTA* ») est inspiré du circuit proposé dans [105]. Sa structure symétrique repose sur deux paires différentielles PMOS au fonctionnement complémentaire (cf. figure II.41). Dans notre cas, l'utilisation de paires différentielles à transistors PMOS présente deux avantages : l'OTA possède un PSR^+ élevé et un ICMR adapté à de faibles valeurs de V_{ref} [106, 107]. Chaque paire différentielle est polarisée en inversion faible par une source de courant principale (I_{b_0}) doublée d'une boucle de retour de gain en courant K. Lorsque la tension différentielle d'entrée ($V_{in} = V_{in_+} - V_{in_-}$) est nulle, les courants de polarisation des paires différentielles (I_{b_1} et I_{b_2}) sont donnés par [105] :

$$I_{b_{1(2)}} = \frac{I_{b_0} + K \cdot I_{b_{1(2)}}}{2} = \frac{I_{b_0}}{2 - K} \tag{II.87}$$

Si l'on suppose que pour V_{in} non nulle, les transistors restent polarisés en inversion faible, alors les expressions des courants de polarisations sont donnés par [105, 108] :

$$I_{b_{1(2)}} = \frac{I_{b_0}}{1 - K + e^{-(+)\frac{V_{in}}{n \cdot V_{th}}}} \tag{II.88}$$

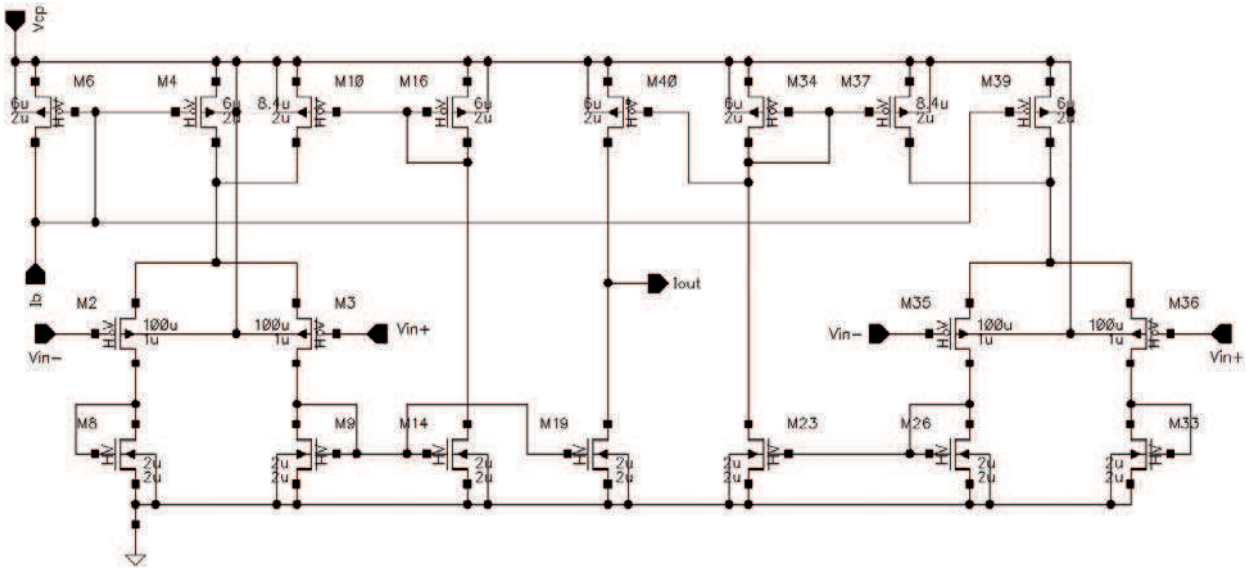


Fig. II.41 – *OTA à polarisation adaptative (LR_N_OTA) du sous-système de régulation [105].*

Le courant de sortie, qui est égal à la différence $I_{b_1} - I_{b_2}$, peut alors se mettre sous la forme [105] :

$$I_{out} = \frac{I_{b_0} \cdot \left(e^{\frac{V_{in}}{n \cdot V_{th}}} - 1 \right)}{1 - (K-1) \cdot e^{\frac{V_i}{n \cdot V_{th}}}} \tag{II.89}$$

Ainsi, en-deçà d'une limite fixée par le changement de régime des transistors, le courant de sortie augmente exponentiellement avec la tension différentielle d'entrée. Comme cela est démontré dans [105], ce circuit non-linéaire possède un unique point d'équilibre stable auquel il retourne systématiquement, quelle que soit l'amplitude de la tension différentielle d'entrée. Dans l'implémentation proposée, le facteur de gain en courant K est fixé à 1.4. Cette valeur offre un bon compromis entre consommation à V_{in} nul et réactivité. Lorsque V_{in}=0, la consommation de l'OTA est inférieure à $8\ \mu A$. Dans notre cas, ce n'est pas le changement de régime des transistors de la paire différentielle qui limite l'augmentation du courant de polarisation, mais l'effondrement de la tension d'alimentation fournie par la pompe de charge (V_{CP}).

Pour garantir le bon fonctionnement de l'OTA, la pompe de charge (CP) doit générer une tension (V_{CP}) supérieure à $4\ V$. Dans ce but, la configuration de sa structure HV est adaptée dynamiquement à la valeur de la tension d'alimentation externe. Le schéma-bloc de son circuit est représenté sur la figure II.42. Il comporte : un transistor de dérivation, un décaleur de tension (CP_HV_to_HV2), un générateur d'horloge (CP_Clk), un bloc de puissance (CP_PE) et un bloc de régulation (CP_Reg). La pompe de charge est contrôlée à la fois par les bits $PSS(i)$ et par le bloc de régulation local. Lorsque la tension d'alimentation externe prend sa valeur la plus haute, le bit $PSS1$ (positionné à 1) désactive la pompe de charge et la court-circuite par le biais du transistor de puissance. On a alors $V_{CP} \cong V_{PS}$. Dans les autres cas, le bloc de puissance est cadencé par l'oscillateur local. La fréquence de ce dernier est contrôlée en courant par le bloc de régulation. La configuration des blocs de puissance et de régulation est fonction de l'état du bit $PSS0$.

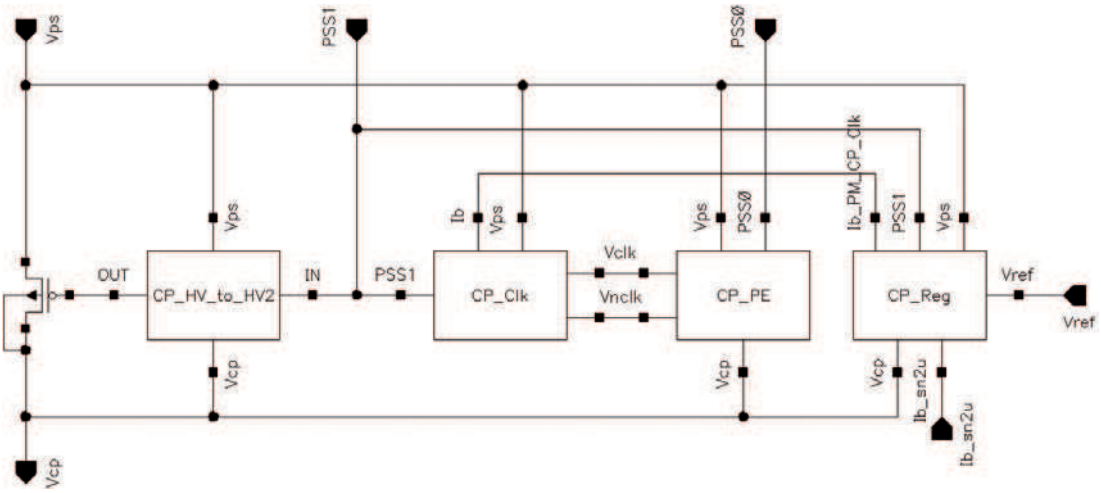


Fig. II.42 – *Pompe de charge (CP) du sous-système de régulation.*

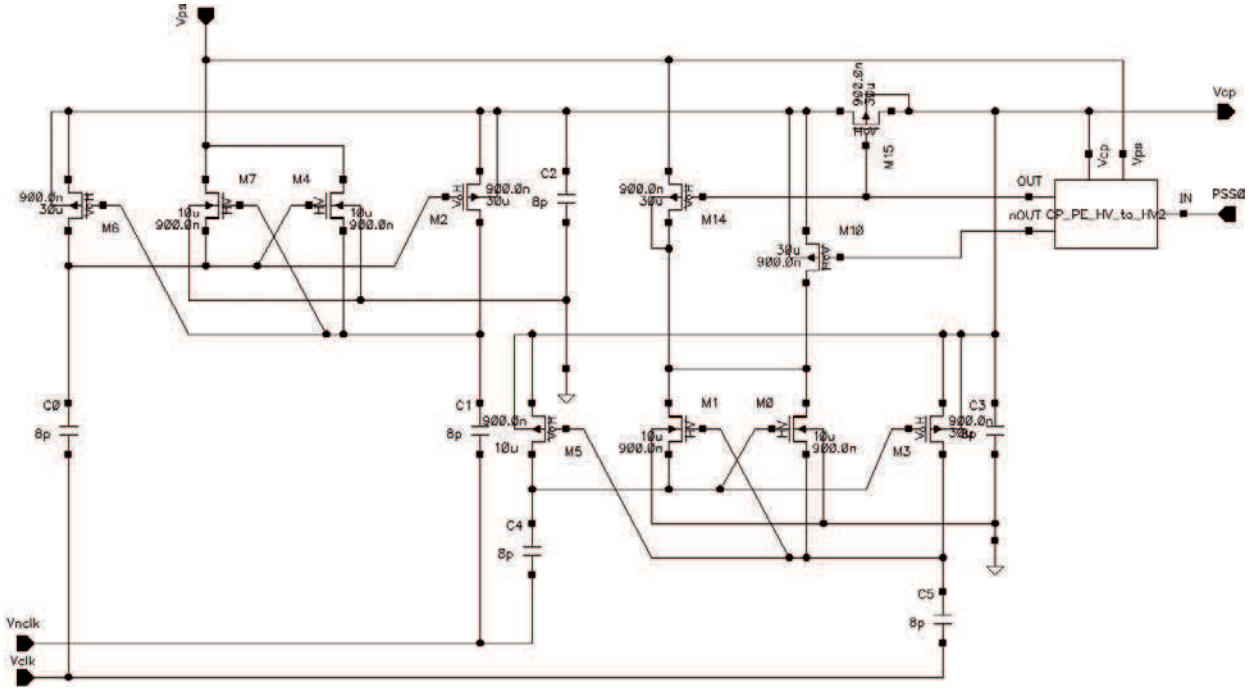


Fig. II.43 – *Bloc de puissance (CP_PE) de la pompe de charge (CP).*

Le bloc de puissance de la pompe de charge (CP_PE) est représenté sur la figure II.43. Il est constitué de deux doubleurs de tension identiques (cellules A et B) [109] et d'une logique de contrôle. Chaque doubleur repose sur trois capacités poly1-poly2 de $8\ pF$: deux capacités de pompage (C_p) et une capacité de sortie (C_o). L'interconnection des doubleurs dépend de la valeur du bit $PSS0$. Lorsque V_{PS}=$1.8\ V$, ils fonctionnent en série; l'entrée du doubleur A est alimentée par V_{PS}, la sortie du doubleur A est connectée à l'entrée du doubleur B, et la sortie du doubleur B constitue la sortie de la pompe de charge (V_{CP}). Si l'on fait abstraction des pertes, le gain théorique de la structure résultante est approximativement égal à quatre.

L'amplitude pic-pic des ondulations de la tension de sortie (δV_{CP}) est donnée par [110] :

$$\Delta V_{CP} = \frac{I_o}{2 \cdot f_s \cdot (C_p + C_o)} \tag{II.90}$$

où I_o est le courant de sortie de la pompe de charge. Si l'on néglige la résistance série des interrupteurs et si l'on suppose ΔV_{CP} petit devant V_{CP}, alors le rendement d'un doubleur est donné par [110] :

$$\eta_{CP} = \frac{I_o \cdot V_{CP}}{2 \cdot I_o \cdot V_i + 2 \cdot f_s \cdot C_a \cdot V_i^2} \tag{II.91}$$

où V_i est la tension d'entrée de la pompe de charge qui est ici égale à V_{PS}.

Lorsque V_{PS}=3.3 V, les doubleurs sont connectés en parallèle entre V_{PS} et V_{CP} et fonctionnent en opposition de phase. Dans ce cas, le gain théorique n'est plus que de deux. En contrepartie, à fréquence de commutation égale, l'amplitude des ondulations de V_{CP} est divisée par deux, ce qui permet de réduire les pertes de commutation.

L'ensemble des décaleurs de tension intervenant au sein du système, tout comme ceux de la pompe de charge (CP_HV_to_HV2 et CP_PE_HV_to_HV2), reposent sur le circuit de la figure II.44 [104]. Celui de la figure II.43 transforme le signal $PSS0$ d'amplitude V_{PS} en un signal opposé d'amplitude V_{CP}.

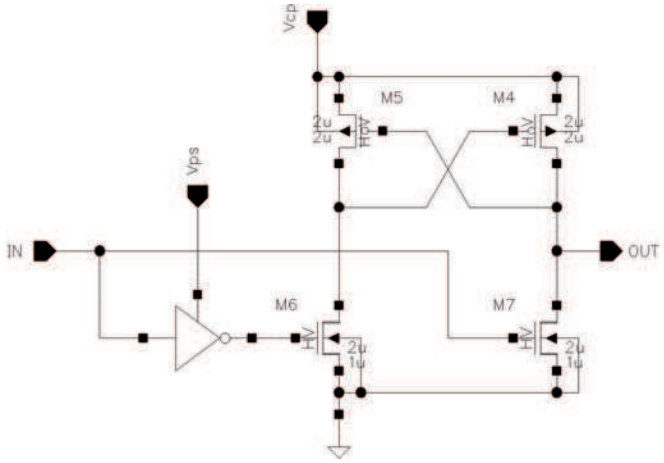


Fig. II.44 – *Schéma des décaleurs de tension (CP_HV_to_HV2 et CP_PE_HV_to_HV2) [104].*

Le régulateur de la pompe de charge (CP_Reg) est représenté sur la figure II.45. Lorsque $PSS1$=1 (i.e., lorsque V_{PS}=5 V), toutes les cellules de la pompe de charge sont désactivées. Lorsque $PSS1$=0 (i.e., lorsque V_{PS}=1.8 V ou 3.3 V), l'amplificateur à hystérésis (CP_Reg_HC) compare la tension de référence (V_{ref}) à une fraction de la tension V_{CP}. La précision du pont diviseur de tension n'ayant qu'une importance relative, celui-ci repose sur une structure à transistor; le remplacement des résistances par des transistors polarisés en régime linéaire permet de réduire la consommation de la branche tout en limitant la surface du circuit. Si V_{CP} devient inférieur à 5 $V \pm 20\%$, le comparateur ouvre la porte de transmission connectée à sa sortie, ce qui a pour effet de doubler le courant de polarisation de l'oscillateur local ($Ib\_PM\_CP\_Clk$). Par suite, la fréquence de commutation de la pompe de charge est multipliée par deux

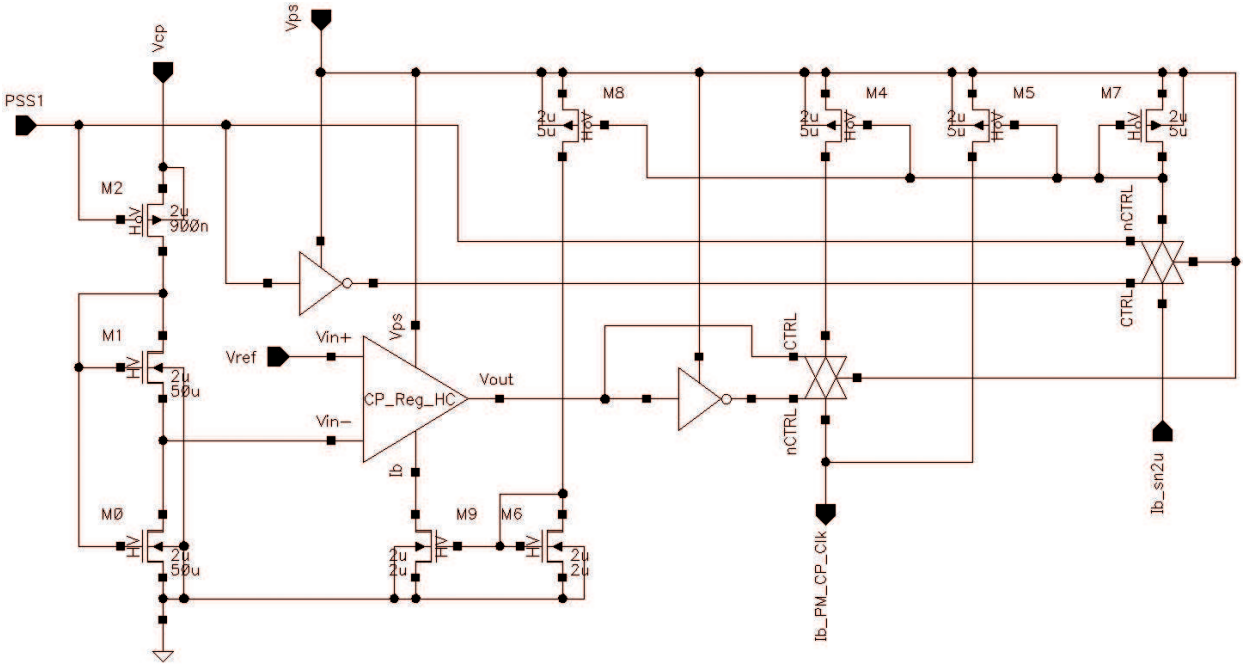


Fig. II.45 – *Régulateur (CP_Reg) de la pompe de charge (CP).*

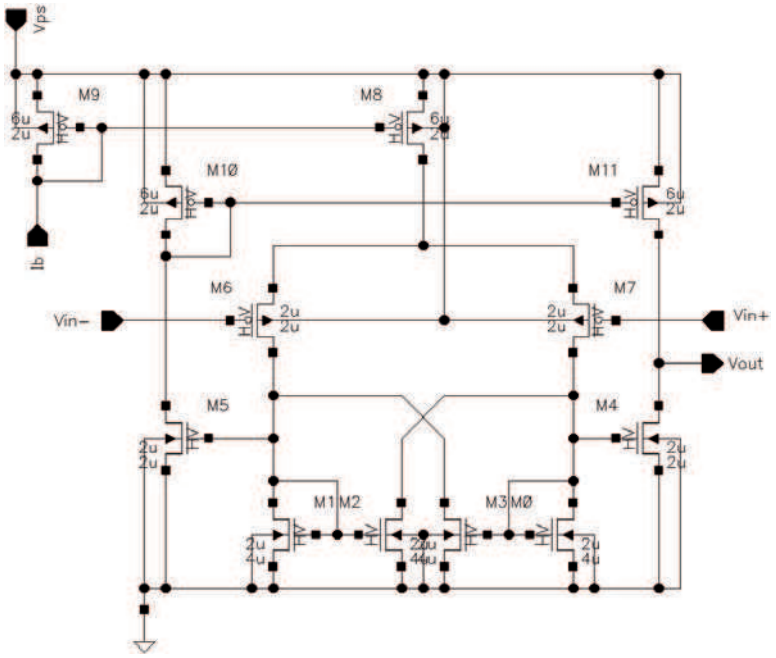


Fig. II.46 – *Comparateur à hystérésis (CP_Reg_HC) du régulateur (CP_Reg) [78].*

et la tension V_{CP} remonte.

Le circuit du comparateur à hystérésis (CP_Reg_HC) est schématisé sur la figure II.46 [78]. L'utilisation d'un comparateur à hystérésis permet de limiter le phénomène d'oscillation autour du seuil. L'ensemble des comparateurs à hystérésis du système reposent sur un circuit similaire à celui de la figure II.45.

Le générateur d'horloge de la pompe de charge (CP_Clk) est représentée sur la figure II.47. Il repose sur un oscillateur en anneau contrôlé en courant (CP_Clk_Osc), une cellule anti-recouvrement (CP_Clk_NO) et deux buffeurs de tension (CP_Clk_Buf). Les cellules CP_Clk_Osc et CP_Clk_NO sont analogues, respectivement, aux cellules SCC_Clk_NO et SCC_Clk_Buf du convertisseur à capacités commutées (cf. figure II.37).

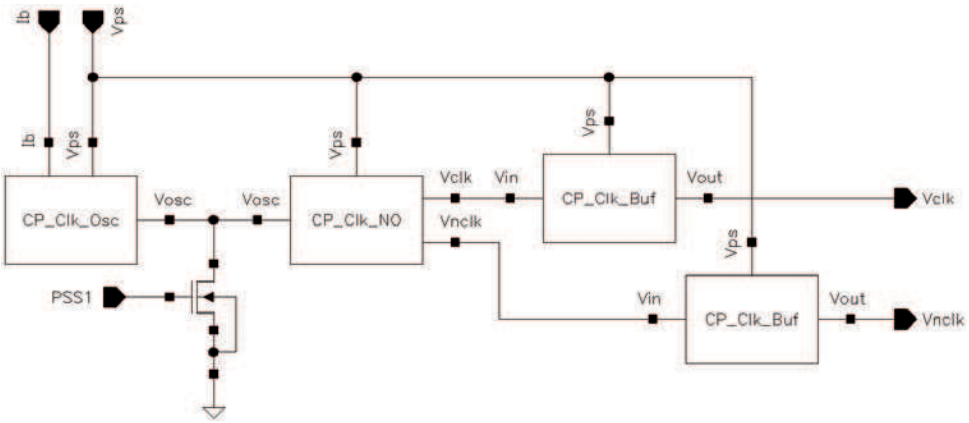


Fig. II.47 – *Générateur d'horloge (CP_Clk) de la pompe de charge (CP).*

Le circuit de l'oscillateur (CP_Clk_Osc) est représenté sur la figure II.48. La fréquence de son signal de sortie (V_{osc}) est linéairement proportionnelle à son courant de polarisation (I_b). En mode normal, I_b=2 μA, la fréquence moyenne de V_{osc} est de 8.7 MHz et la consommation totale de la cellule s'élève à environ 12 μA. En mode accéléré, toutes ces valeurs sont approximativement multipliées par deux.

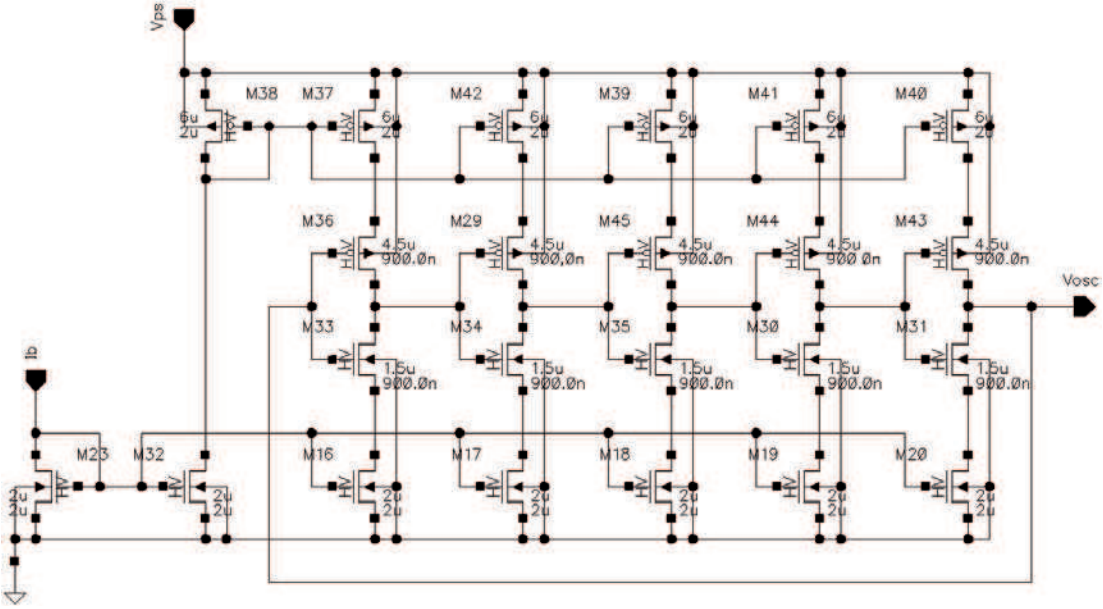


Fig. II.48 – *Oscillateur en anneau (CP_Clk_Osc) du générateur d'horloge (CP_Clk) [111].*

II.5.2.4 Générateur de références

Le générateur de références (RG) est constitué de deux cellules LV autonomes : une référence de tension (RG_VR) de 900 mV ($V_{ref_{LV}}$) et une référence de courant (RG_CR) de 2 μA ($I_{ref_{LV}}$). Pour des raisons de confidentialité, le circuit de la référence de tension ne peut être divulgué dans ce rapport. Dans les conditions PVT fixées par le cahier des charges (cf. tableau II.5), la tension $V_{ref_{LV}}$ présente une déviation maximale inférieure à 9 $\%$.

La référence de courant doit présenter une précision équivalente à celle de la référence de tension. De plus, afin de répondre aux critères industriels, sa plage de fonctionnement en courant doit s'étendre du microampère au nanoampère, sa structure doit privilégier les dispositifs MOS (pas de transistor bipolaire, même sous sa forme latérale) et sa surface doit être aussi petite que possible. En outre, par souci de compatibilité avec les technologies avancées, sa tension d'alimentation doit pouvoir descendre au volt. Le développement des références de courant est intimement lié à celui des références de tension. Il constitue l'un des domaines les plus actifs de la recherche en conception de circuits intégrés. De fait, un grand nombre de topologies a été proposé dans la littérature. Cependant, peu d'entre elles répondent simultanément à l'ensemble des critères formulés précédemment. C'est le cas de la structure schématisée sur la figure II.50.

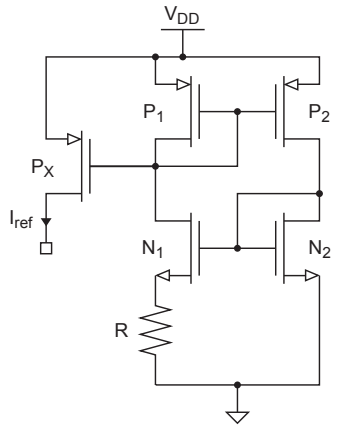


Fig. II.49 – *Référence de courant en technologie CMOS avec résistance [108].*

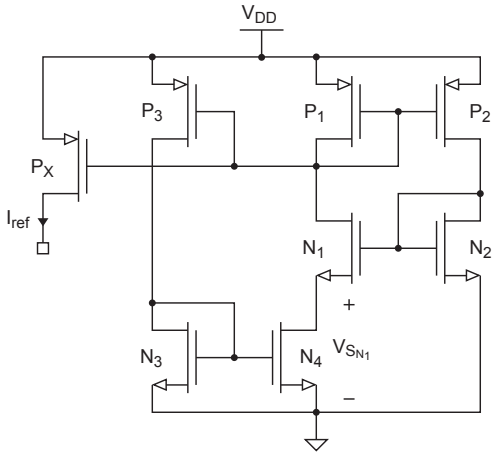


Fig. II.50 – *Référence de courant en technologie CMOS sans résistance [112].*

Le circuit de la figure II.50 peut se décomposer en deux structures : une référence de tension (P_1, P_2, N_1 et N_2) proportionnelle à la température absolue (PTAT pour « *Proportional to Absolute Temperature* ») et une résistance active (P_3, N_3 et N_4). Ces deux structures forment une boucle; la tension PTAT ($V_{S_{N_1}}$) est appliquée aux bornes de la résistance active (N_4), et le courant résultant ($I_{DS_{N_4}}$) est miroité dans toutes les branches du circuit. La référence de tension PTAT repose sur un convoyeur de courant de première génération (CCI) à quatre transistors [113] : deux transistors PMOS polarisés en inversion forte saturée (P_1 et P_2) et deux transistors NMOS saturés en inversion faible (N_1 et N_2). Les équations asymptotiques standards permettent d'exprimer la tension de source du transistor N_1 comme étant [112] :

$$V_{S_{N_1}} = U_T \cdot ln\left(\frac{S_{N_1} \cdot S_{P_2}}{S_{N_2} \cdot S_{P_1}}\right) \tag{II.92}$$

où U_T=$K.T/q$ est la tension thermique, et S_{N_1}, S_{N_2}, S_{P_1}, S_{P_2} les rapports W/L des transistors correspondants. Dans le circuit original, le courant $I_{ref_{LV}}$ est généré par application de $V_{S_{N1}}$ aux bornes d'une résistance R à la masse (cf. figure II.49[108]). Cependant, la surface associée à la résistance devient importante dès lors que le courant de référence passe sous la barre du microampère. La solution proposée dans [112] consiste à remplacer cette dernière par un transistor polarisé en inversion forte et en régime de conduction (N_4). La polarisation de N_4 est assurée par le biais de deux transistors supplémentaires (P_3 et N_3), polarisés quant à eux en inversion forte et en régime saturé. Le gain du miroir P_1-P_x étant supposé unitaire, l'expression du courant de référence est donnée par [112] :

$$I_{ref_{LV}} = n^2 \cdot \beta_{N_4} \cdot U_T^2 \cdot \left[\frac{S_{N_4} \cdot S_{P_3}}{S_{N_3} \cdot S_{P_1}} - 0.5 + \sqrt{\frac{S_{N_4} \cdot S_{P_3}}{S_{N_3} \cdot S_{P_1}} \cdot \left(\frac{S_{N_4} \cdot S_{P_3}}{S_{N_3} \cdot S_{P_1}} - 1 \right)} \right] \cdot ln^2 \left(\frac{S_{N_1} \cdot S_{P_2}}{S_{N_2} \cdot S_{P_1}} \right) \quad \text{(II.93)}$$

où n désigne la pente sous le seuil et β_{N_4} est donné par :

$$\beta_{N_4} = \mu_N \cdot C_{ox} \cdot \frac{W_{N_4}}{L_{N_4}} \quad \text{(II.94)}$$

D'après l'expression II.93, le courant $I_{ref_{LV}}$ est de type PTAT. Cependant, fait non signalé par son concepteur, le transistor en conduction peut être polarisé de telle sorte que les effets induits par les variation en température de ses tensions de polarisation se compensent mutuellement [114]. Dans ce cas, le courant $I_{ref_{LV}}$ devient quasi-indépendant de la température. Le circuit de la figure II.51 a été dimensionné dans cette optique.

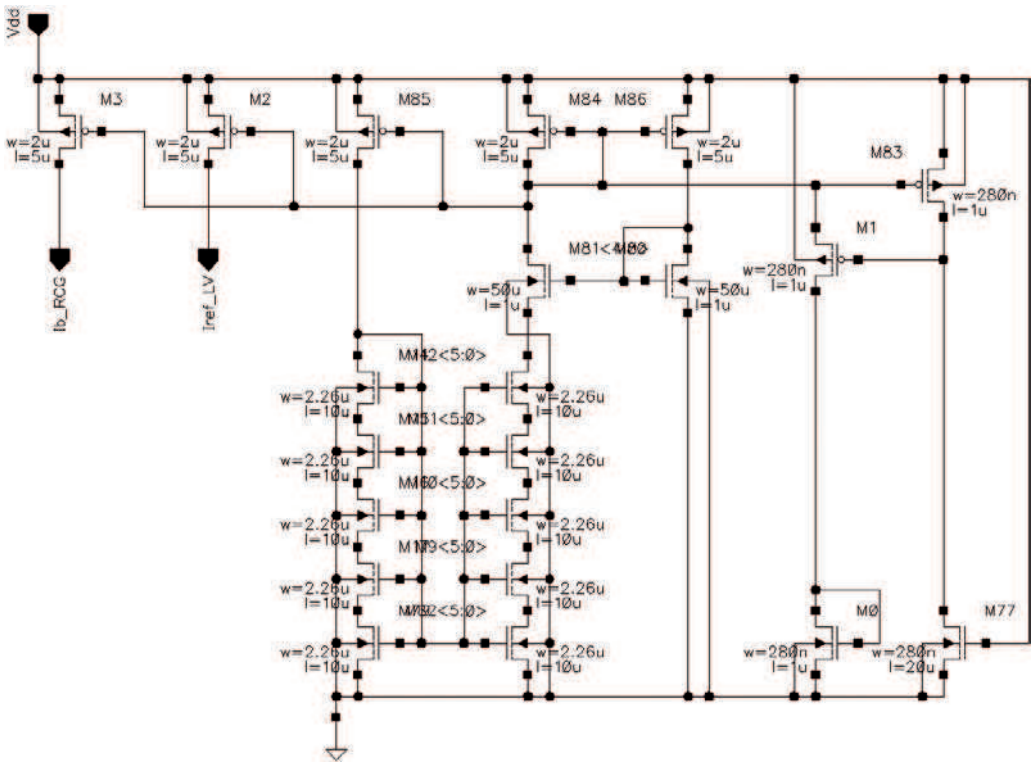


Fig. II.51 – *Circuit de la référence de courant LV (RG_CR).*

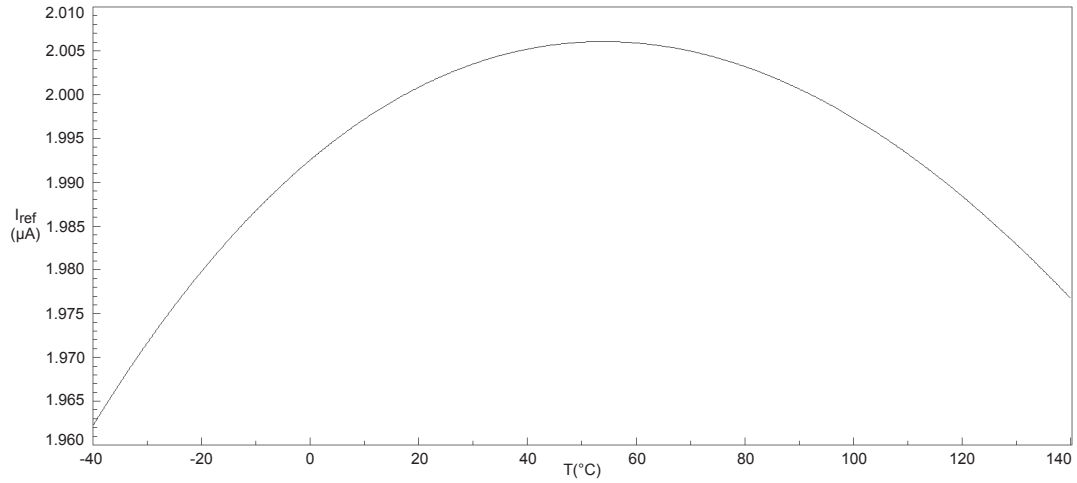


Fig. II.52 – *Comportement de $I_{ref_{LV}}$ en fonction de la température T (process typique et $V_{DD} = 1.8\ V$).*

Par rapport au schéma de principe, le circuit de la figure II.51 fait intervenir un bloc supplémentaire : le circuit de démarrage [115] (« *startup* »). Le régime de fonctionnement visé correspond au seul point d'équilibre stable du circuit [112]. Cependant, son temps de démarrage naturel est long au regard des spécifications du cahier des charges (cf. tableau II.5). Le *startup* a pour vocation d'accélérer la mise route du circuit et non d'empêcher un hypothétique blocage. Pour $T = 27°C$, $V_{DD} = 1.8\ V$ et les valeurs typiques des paramètres technologiques, le courant $I_{ref_{LV}}$ atteint 90% de sa valeur statique en moins de $40\ ns$. Afin de prendre en compte les effets physiques relatifs aux formes des transistors, le dessin des masques doit être anticipé dès la phase de simulation pré-*layout*. A cet effet, les transistors de la figure II.51, correspondant aux transistors N_3 et N_4 de la figure II.50, sont divisés en transistors unitaires identiques à faible ratio d'aspect ($L = 10\ \mu m$ et $W = 2.26\ \mu m$). Cette technique de *layout* permet d'améliorer le *matching*; elle autorise l'interdigitalisation des transistors celon une disposition matricielle de type « *common-centroid* » [116, 117, 118]. Par ailleurs, la mise en série de transistors unitaires permet de s'affranchir du L maximum fixé par les régles de dessin (DRM pour « *Design Rule Manual* »). Enfin, les outils d'extraction post-*layout* permettent de prendre en compte les éléments parasites plus difficilement anticipables (capacités d'interconnection, résistances d'interconnection, etc.).

La courbe de la figure II.52 illustre le comportement du courant $I_{ref_{LV}}$ en fonction de la température. Sur la plage comprise entre -40 et 125°C, il varie au maximum de 2%. De plus, pour des variations cumulées du procédé de fabrication, de la tension d'alimentation et de la température, la déviation de $I_{ref_{LV}}$ reste inférieure à 12%. Une implémentation en technologie AMS CMOS $0.35\ \mu m$ sera présentée au trosième chapitre (cf. § III.4.3.2.d).

II.5.2.5 Gestionnaire de puissance

Les différentes boucles de régulation intervenant dans notre système exploitent la tension de référence V_{ref} comme signal de consigne. Cette tension est délivrée par la référence LV fournie par STMicroelectronics. Or, la totalité des cellules LV sont alimentées par l'intermédiaire de la tension V_{DD}. Par conséquent, elles ne sont pas opérationnelles à la mise sous tension du circuit. Cette interdépendance entre V_{DD} et

V_{ref} rend la phase de démarrage délicate et le système potentiellement instable. En effet, même brève, une tension V_{DD} trop élevée pourrait aboutir à la destruction des dispositifs. Une solution proposée dans la littérature consiste à alimenter la référence de courant LV par l'intermédiaire d'un prérégulateur indépendant [119]. Cependant, cette méthode nécessite un pont résistif additionnel. La solution proposé ici fait intervenir une seconde référence de tension ($V_{ref_{HV}}$). Cette tension est délivrée par un circuit HV alimenté directement sur V_{PS}. Il est ensuite désactivé dès lors que la référence LV ($V_{ref_{LV}}$) devient opérationnelle. Puisqu'elle ne sert qu'au démarrage, la consommation et la précision de référence HV ont peu d'importance. En revanche, sa surface doit être aussi faible que possible.

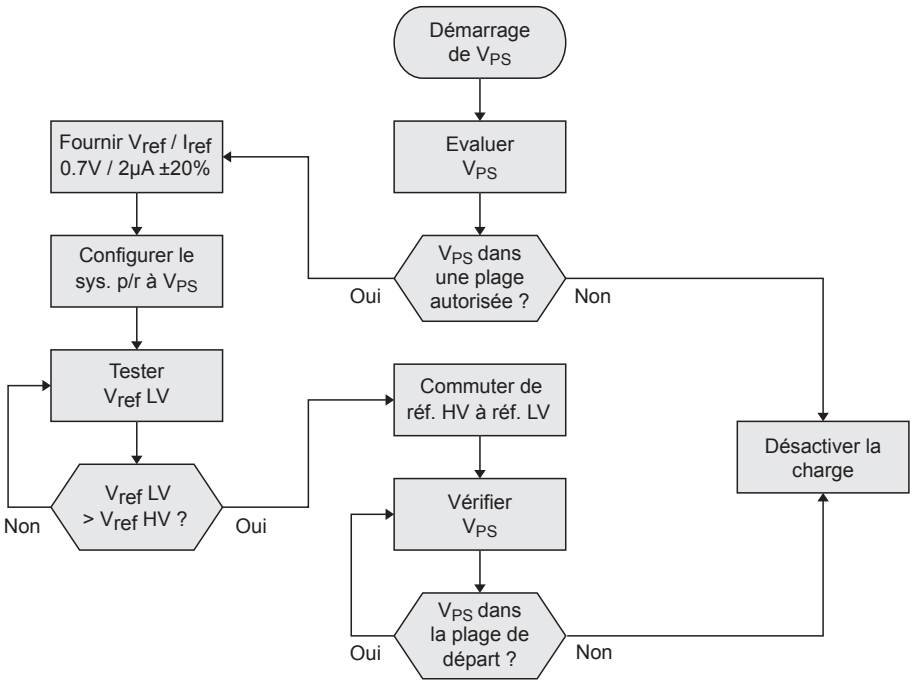


Fig. II.53 – *Diagramme fonctionnel de la stratégie de démarrage.*

La stratégie de démarrage est synthétisée par le diagramme fonctionnel de la figure II.53. En premier lieu, le gestionnaire de puissance évalue la valeur de la V_{PS}. Si elle n'appartient à aucune des trois plages autorisées, la charge n'est pas activée. Dans le cas contraire, le gestionnaire démarre le système en générant une référence de tension de 700 $mV \pm 20\%$ ($V_{ref_{HV}}$) et une référence de courant de 2 μA $\pm 20\%$ ($I_{ref_{HV}}$). Dans le même temps, il configure le système en fonction de la plage détectée, via les signaux numériques et les courants de polarisation des bus de contrôle. Lorsque V_{DD} atteint 1.2 V, la référence de tension LV devient opérationnelle. Dès que l'amplitude de $V_{ref_{LV}}$ devient supérieure à celle de $V_{ref_{HV}}$, le gestionnaire bascule V_{ref} vers sa valeur définitive (i.e., 900 mV). Ainsi, pour garantir le bon démarrage du système, la précision minimum de la référence HV doit être telle que la valeur statique de $V_{ref_{HV}}$ ne dépasse jamais celle de $V_{ref_{LV}}$. Lorsque V_{DD} atteint 1.8 V, le microcontrôleur devient opérationel. Il commute I_{ref} de $I_{ref_{HV}}$ à $I_{ref_{LV}}$, puis il désactive la référence HV. Enfin, le gestionnaire passe en mode surveillance; il vérifie le maintien de la tension V_{PS} dans sa plage de départ. S'il détecte une déviation anormale, il désactive immédiatement la charge afin de protéger cette dernière contre une éventuelle tentative de piratage.

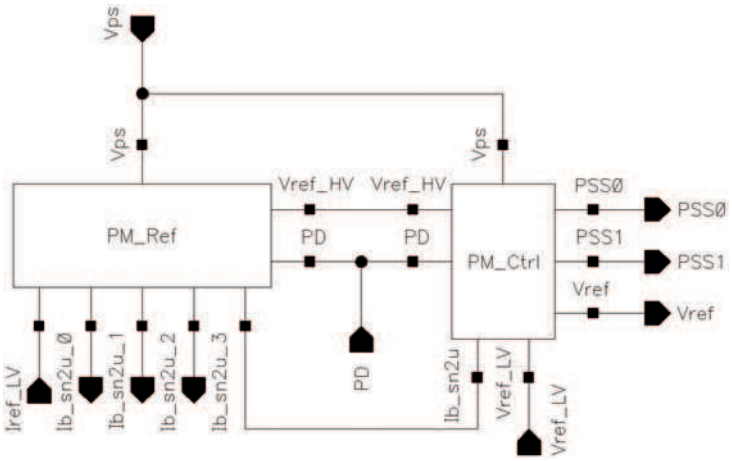


Fig. II.54 – *Schéma du gestionnaire de puissance (PM).*

La vue d'ensemble du gestionnaire de puissance est représentée sur la figure II.54. Le gestionnaire de puissance est constitué de deux cellules HV : le bloc de contrôle (PM_Ctrl) et le bloc de référence (PM_Ref). Le contrôleur est le cerveau du système. Il génère les bits d'état $PSS0$ et $PSS1$ et assure l'aiguillage des références de tension et de courant. Le bloc de référence HV génère les signaux $V_{ref_{HV}}$ et $I_{ref_{HV}}$. Il assure également la duplication et la distribution des courants de polarisation pour l'ensemble du système. Le bit PD (« *Power Down* ») permet de désactiver le gestionnaire de puissance.

Le bloc de contrôle est représenté sur la figure II.55. Il comporte deux comparateurs à seuil, un sélectionneur de référence autonome (PM_Ctrl_Ref) et un circuit logique dédié au verrouillage des signaux de contrôle (PM_Ctrl_L). Les bits $COMP0$ et $COMP1$ sont à l'origine, respectivement, des bits $PSS0$ et $PSS1$. Ils résultent de la comparaison des tensions issues du pont résistif avec les 700 mV de la référence HV. Par souci d'économie d'espace, la résistance totale du pont résistif est limitée à 30 $K\Omega$. Puisqu'il n'est utilisé qu'au démarrage, la consommation induite reste négligeable.

Le circuit de la cellule de verrouillage (PM_Ctrl_L) est schématisé sur la figure II.56. La valeur initiale par défaut des bits $PSS0$ et $PSS1$ est fixée à zéro; elle ne tient pas compte des valeurs effectives des bits $COMP0$ et $COMP1$. Pour mémoire, dans ce mode de fonctionnement, le sous-système sécuritaire est court-circuité, tandis que la pompe de charge du sous-système de régulation fonctionne à plein régime (cf. tableau II.7). Cette configuration permet d'accélérer le démarrage de V_{DD}. Lorsque la tension $V_{ref_{HV}}$ atteint sa valeur statique, le bit HVR passe à 0 et les valeurs des bits $COMP0$ et $COMP1$ sont transmises, respectivement, aux bits $PSS0$ et $PSS1$. Après désactivation du bloc via PD, les valeurs définitives des bits $PSS0$ et $PSS1$ sont maintenues par des points mémoires à deux inverseurs rebouclés [104].

Le sélectionneur de référence (PM_Ctrl_Ref) est représenté sur la figure II.57. Le comparateur, dont le circuit est schématisé sur la figure II.58, amplifie la différence entre les tensions $V_{ref_{LV}}$ et $V_{ref_{HV}}$. Le signal résultant pilote l'aiguillage de V_{ref} par l'intermédiaire des portes de transmissions. Enfin, le passage du bit PD à 1 verrouille la tension V_{ref} sur $V_{ref_{LV}}$ et plonge les cellules du contrôleur en mode veille.

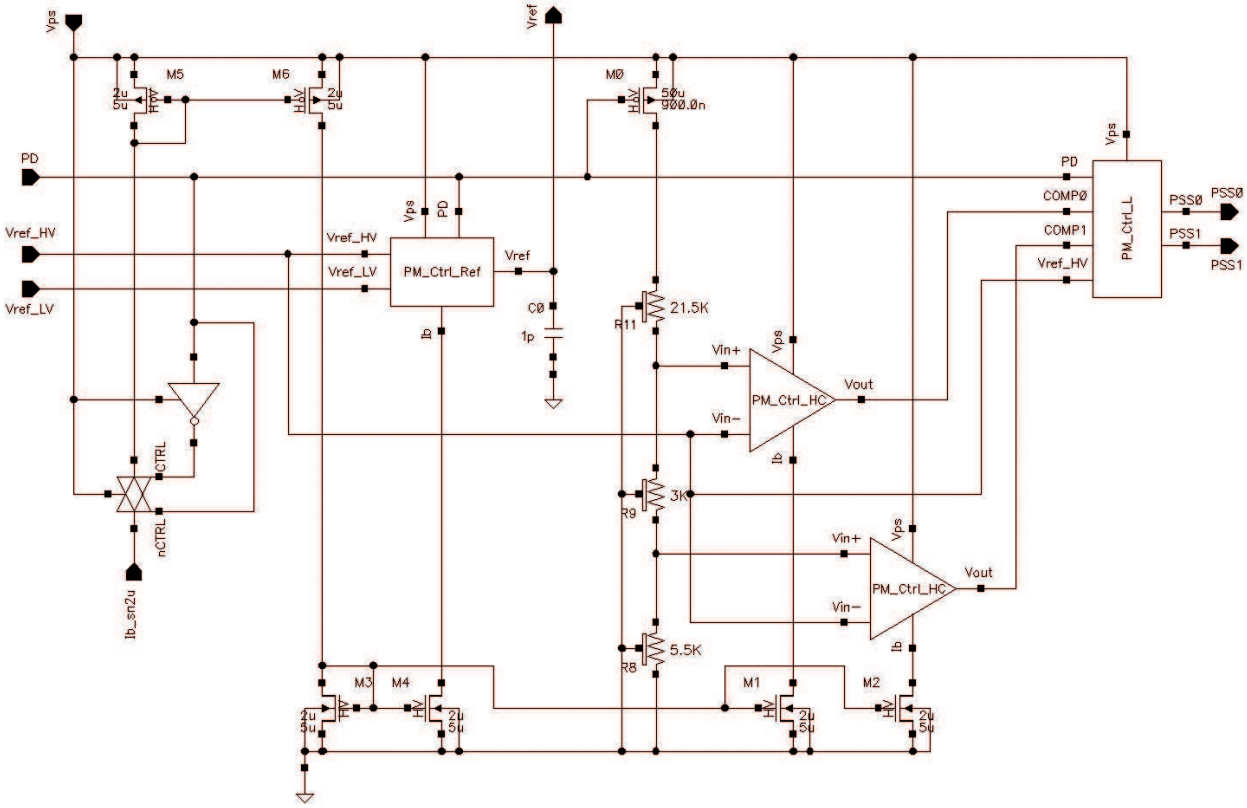


Fig. II.55 – *Bloc de contrôle (PM_Ctrl) du gestionnaire de puissance (PM).*

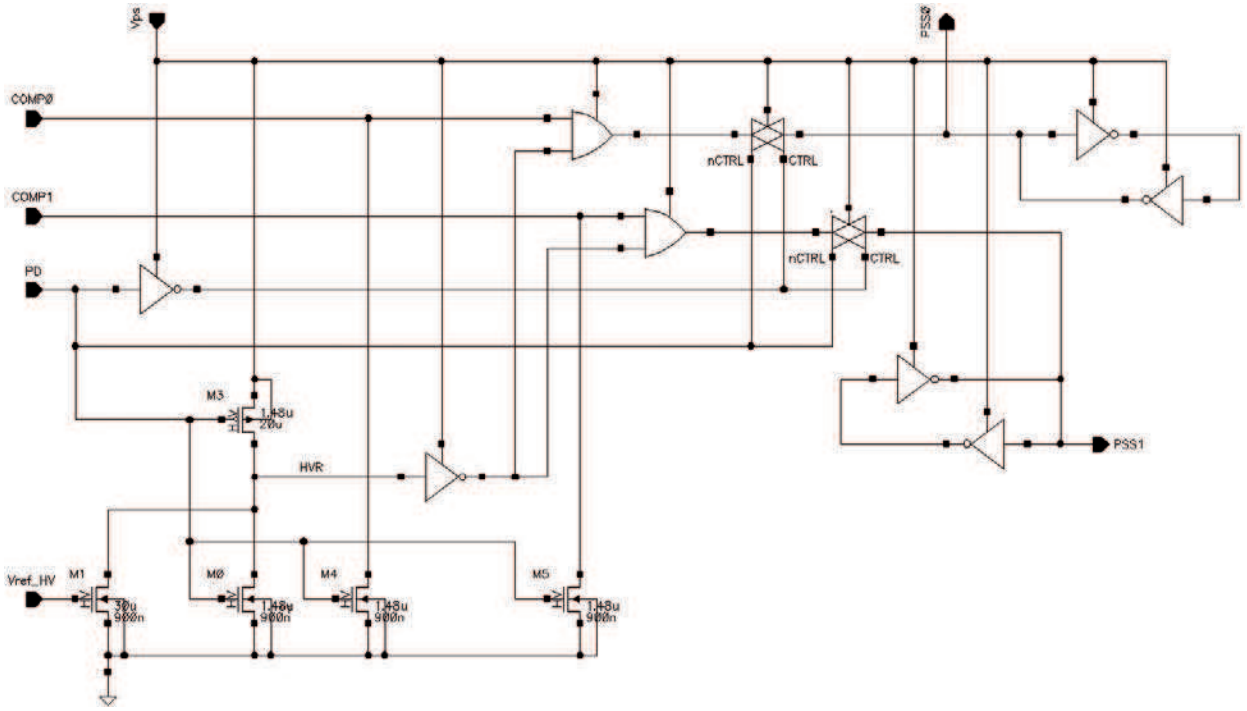


Fig. II.56 – *Circuit de verrouillage (PM_Ctrl_L) des signaux de contrôle.*

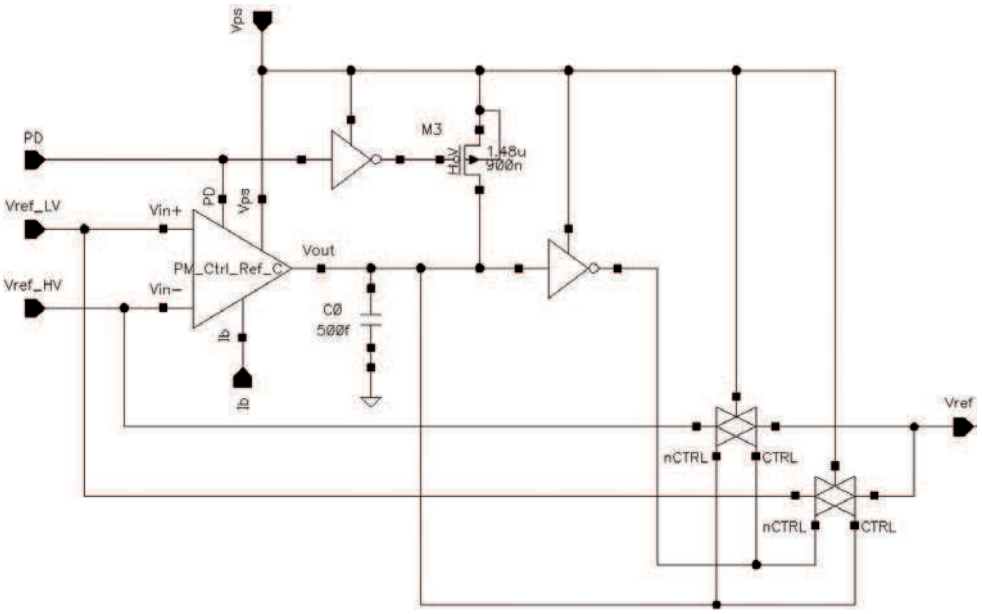


Fig. II.57 – *Schéma du sélectionneur de référence (PM_Ctrl_Ref).*

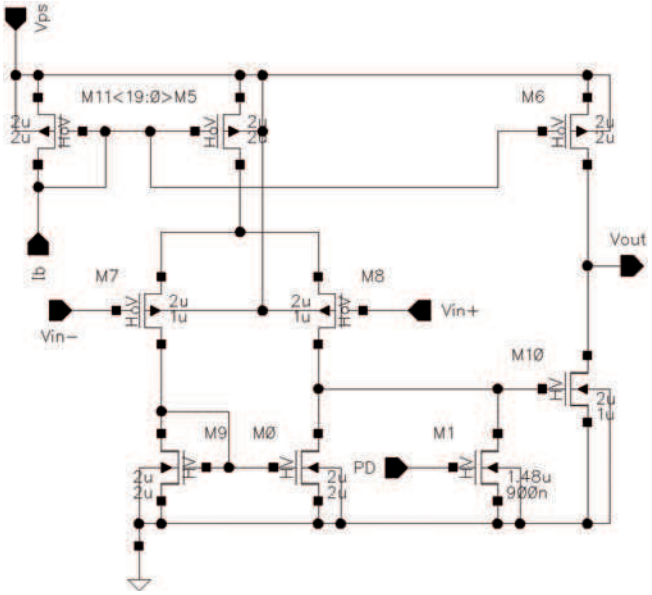


Fig. II.58 – *Comparateur (PM_Ctrl_Ref_C) du sélectionneur de référence (PM_Ctrl_Ref).*

Le bloc de référence (PM_Ref) est représenté sur la figure II.59. Par un jeu de miroir, il polarise l'ensemble des cellules du système à partir du courant de référence. Le temps de démarrage de la référence de courant LV fournie par le fondeur est supérieur au temps de démarrage spécifié par le cahier des charges. Pour palier à ce problème, le passage de $I_{ref_{LV}}$ à $I_{ref_{HV}}$ est déclenché à la mise en veille du bloc de référence (i.e., par le microcontrôleur via PD). Contrairement à V_{ref}, la faible précision de $I_{ref_{HV}}$ n'a pas d'influence significative sur le bon déroulement de la phase de démarrage.

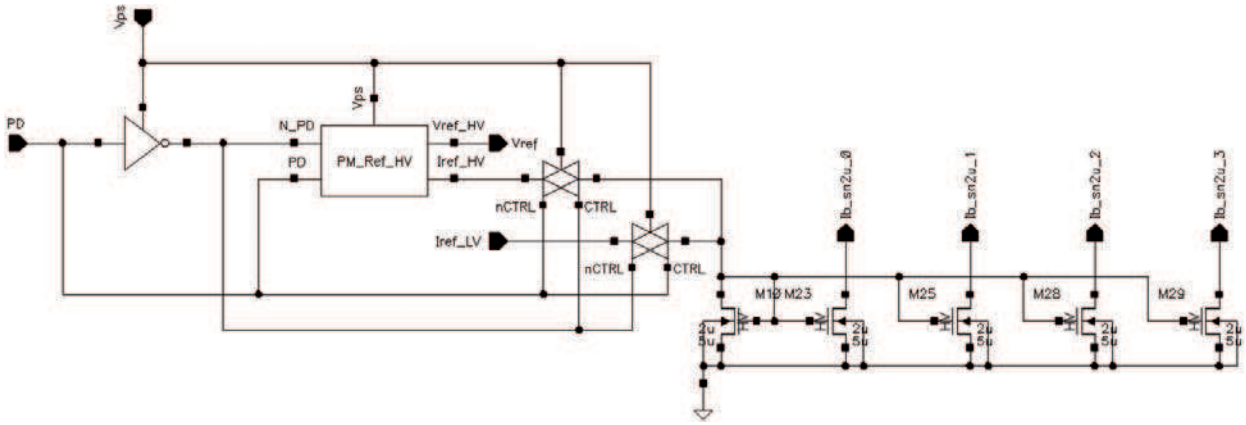


Fig. II.59 – *Schéma du bloc de référence (PM_Ref).*

La référence HV (PM_Ref_HV) repose sur la structure à résistance de la figure II.50 [112]. Contrairement au circuit LV présenté précédemment (cf. figure II.51), le circuit HV est utilisée à la fois comme référence de tension ($V_{ref_{HV}}$=700 mV) et de courant ($I_{ref_{HV}}$=2 μA). La tension $V_{ref_{HV}}$ est générée par injection du courant $I_{ref_{HV}}$ dans un transistor connecté en diode. D'aprés l'expression II.93, le courant $I_{ref_{HV}}$ est de type PTAT. Ainsi, en dimensionnant le transistor connecté en diode de sorte à ce que son point de polarisation se situe légèrement en-dessous de son point à coefficient en température nul (ZTC pour « *Zero Temperature Coefficient* »), on réduit significativement la dépendance en température de $V_{ref_{HV}}$ [120]. Pour les raisons évoquées au paragraphe précédent, la cellule (PM_Ref) a été optimisée principalement en terme de surface. Bien que relativement faible, sa précision de $\pm 20\%$ est néanmoins suffisante pour garantir le bon déroulement de la phase de démarrage (i.e., $V_{ref_{HV}}$>$V_{ref_{LV}}$), et ce, dans toutes les conditions PVT prévues par le cahier des charges. Dans tout les cas, la tension $V_{ref_{HV}}$ atteint 90% de sa valeur statique en moins de $40\ ns$.

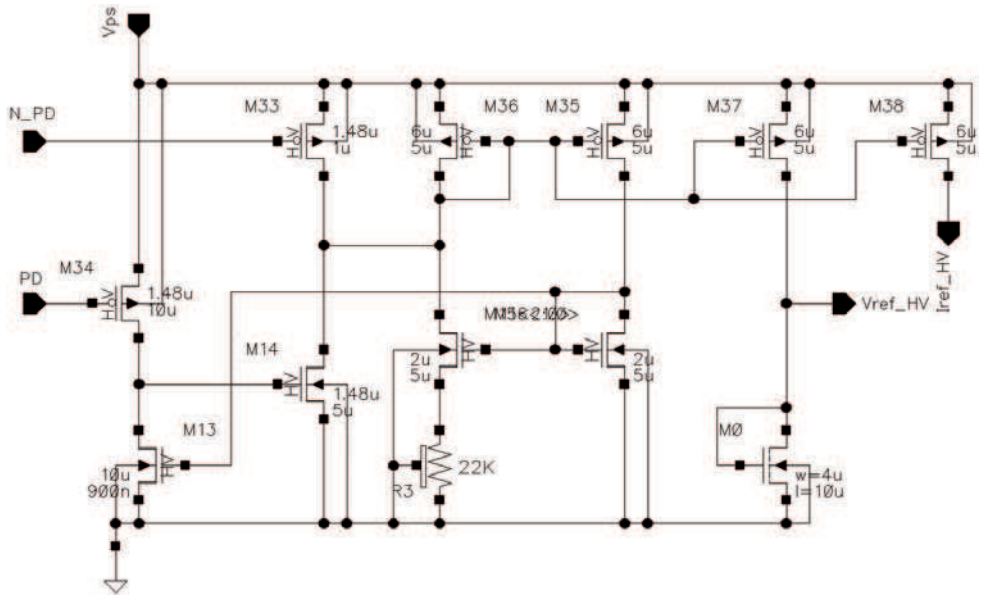


Fig. II.60 – *Schéma du générateur de références HV (PM_Ref_HV).*

II.5.3 Bilan

Au total, le circuit analogique « *full-custom* » proposé comporte 2138 cellules élémentaires et 1189 nœuds. Sa surface a été estimée à $0.8\ mm^2$.

II.5.4 Résultats simulés

II.5.4.1 Etude fréquentielle

II.5.4.1.a Stabilité du régulateur linéaire associé au sous-système sécuritaire (LR_P)

La réponse fréquentielle en boucle ouverte du régulateur linéaire associé au sous-système sécuritaire (LR_P) est représentée sur la figure II.61. Elle a été simulée à pleine charge ($\overline{I_{DD}} = 28\ mA$, courbes rouges) et en mode veille ($\overline{I_{DD}} = 100\ \mu A$, courbes bleues), le système anti-fermeture ayant été supprimé. A pleine charge, le gain statique vaut $71.7\ dB$, la fréquence de gain unitaire est égale à $2.03\ MHz$ et la marge de phase atteint $80.2°$. En mode veille, le gain statique vaut $85.1\ dB$, la fréquence de gain unitaire atteint $1.47\ MHz$ et la marge de phase n'est plus que de $48°$. Comme attendu, la diminution du courant de charge se traduit par une dégradation importante de la marge de phase (cf. § II.4.2.1.c). Lorsqu'il est présent, le système anti-fermeture permet d'éviter cette zone d'instabilité.

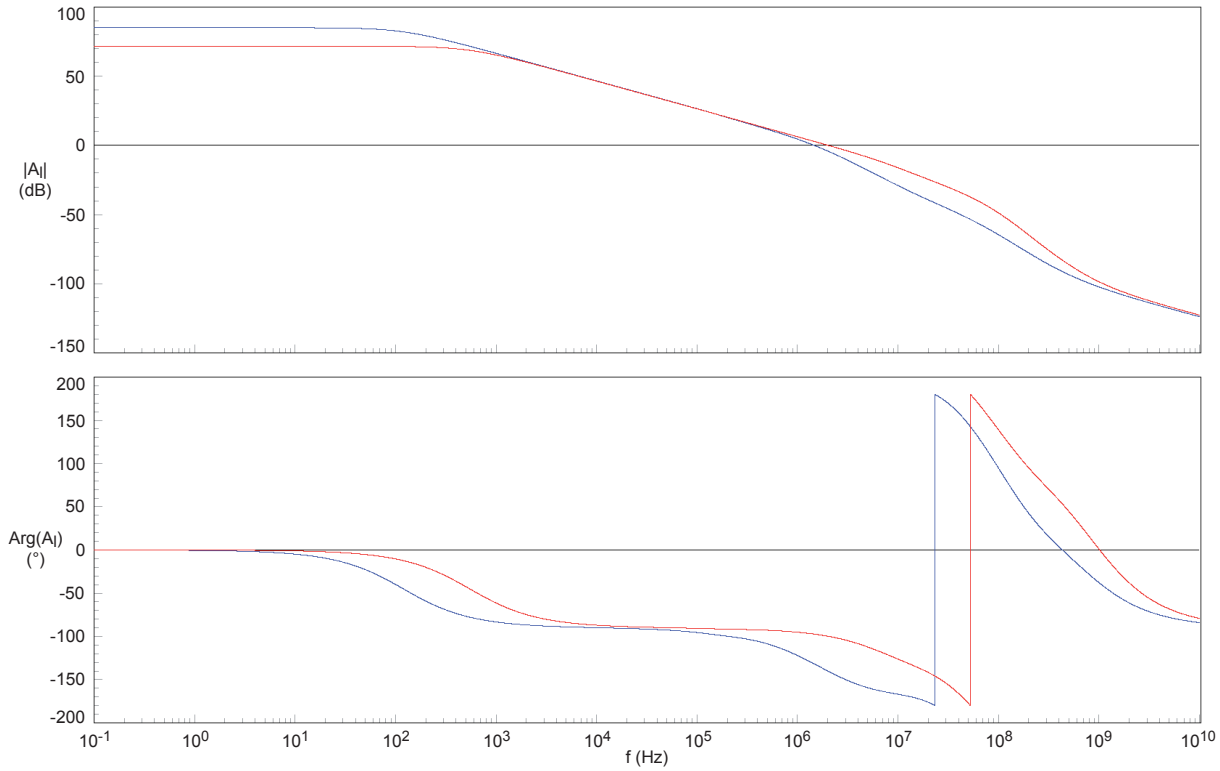


Fig. II.61 – *Réponse fréquentielle en B.O. de LR_P pour* $\overline{I_{DD}}$=28 mA *(rouge) et* $\overline{I_{DD}}$=100 μA *(bleu).*

II.5.4.1.b Stabilité du régulateur linéaire associé au sous-système de régulation (LR_N)

La réponse fréquentielle en boucle ouverte du sous-système de régulation (LR_N) a été simulée à pleine charge (courbes rouges) et en mode veille (courbes bleues). Les diagrammes de Bodes résultant sont représentés sur la figure II.62. A pleine charge, le gain statique vaut $67.8\ dB$, la fréquence de gain unitaire est égale à $277\ KHz$ et la marge de phase atteint $81.4°$. En mode veille, le gain statique vaut $67.4\ dB$, la fréquence de gain unitaire est égale à $239\ KHz$ et la marge de phase atteint $80.8°$. Contrairement au régulateur à transistor PMOS, le régulateur à transistor NMOS offre une stabilité quasi inconditionnelle.

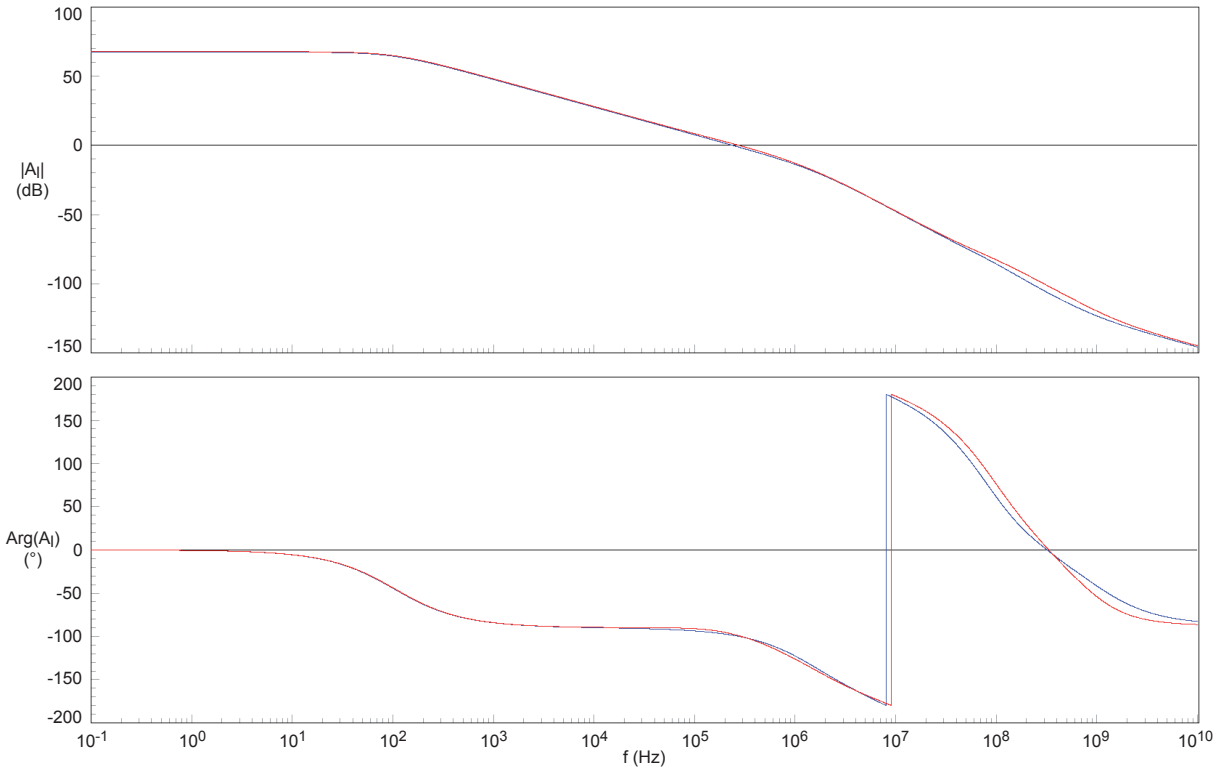


Fig. II.62 – *Réponse fréquentielle en B.O. de LR_N pour* $\overline{I_{DD}}$=28 mA *(rouge) et* $\overline{I_{DD}}$=100 μA *(bleu).*

II.5.4.1.c Régulation de ligne

Le comportement fréquentiel du taux de réjection d'alimentation PSR^+) est illustré sur la figure II.63. Il a été simulé à pleine charge (courbes rouges) et en mode veille (courbes bleues). A pleine charge, la valeur statique du PSR^+ est de $-85.9\ dB$. Sur la plage étudiée, la valeur la plus haute est de $-13.3\ dB$; cette valeur est atteinte pour $4.46\ MHz$. Lorsque la charge fonctionne en mode veille, la valeur statique du PSR^+ est de $-84.4\ dB$. Sa valeur la plus élevée, $-12.7\ dB$, est atteinte aux alentours de $378\ KHz$. Dans les deux cas, les spécifications du cahier des charges sont respectées.

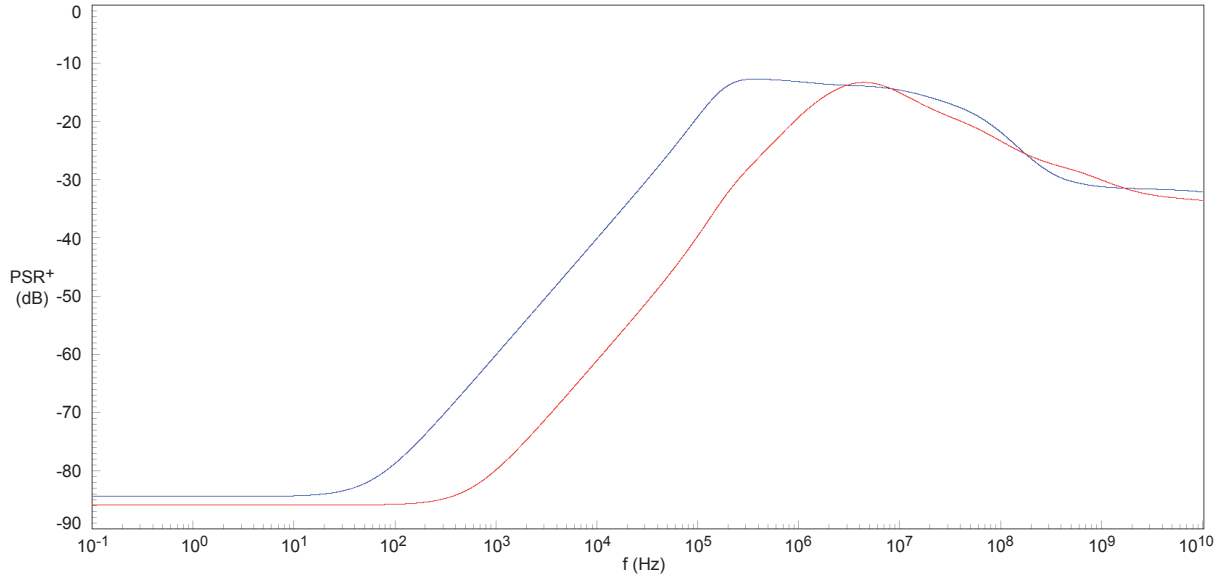


Fig. II.63 – *Evolution fréquentielle du PSR^+ pour $\overline{I_{DD}}$=28 mA (rouge) et $\overline{I_{DD}}$=100 μA (bleu).*

II.5.4.2 Etude transitoire

II.5.4.2.a Structure de test

Afin de simuler le comportement du système dans des conditions plus réalistes, le générateur de tension externe (EPS) et la charge (« *Load* ») sont modélisés à l'aide de macrocellules paramétrables (cf. figure II.64). La résistance de sortie du générateur de tension externe est réglée de telle sorte que l'amplitude des ondulations de V_{PS} corresponde au pire cas envisagé par la norme, soit $\pm 10\%$ de sa valeur moyenne (cf. tableau A.1). Cette disposition permet d'étudier l'impact du bruit d'alimentation sur le fonctionnement du système.

La charge est modélisée à l'aide du macromodèle proposé dans [121, 122] (cf. figure II.64). Elle repose sur dix-sept éléments en parallèle : un transistor NMOS et une matrice de seize suiveurs $\{buf_{ij}\}_{i,j\in[0...3]}$ chargés chacun par une capacité $\{C_{ij}\}_{i,j\in[0...3]}$. Chaque élément est piloté par un générateur de fronts paramétrable. Les signaux impulsionnels délivrés par ces générateurs idéaux présentent des discontinuités. Afin de limiter l'impact des artefacts résultant, seul le second inverseur de chaque doublet participe à la génération de I_{DD}. Les pics de courant ainsi généré présentent des vitesses de variation plus réalistes (i.e., des coudes de déclenchement moins anguleux). Les dimensions des éléments et les caractéristiques des générateurs sont passées en paramètre; les paramètres associées aux transistors NMOS permettent d'ajuster l'amplitude de la composante DC du courant de charge, tandis que les paramètres associées aux inverseurs permettent de contrôler les caractéristiques de sa composante AC. Par ailleurs, la commutation séquentielle

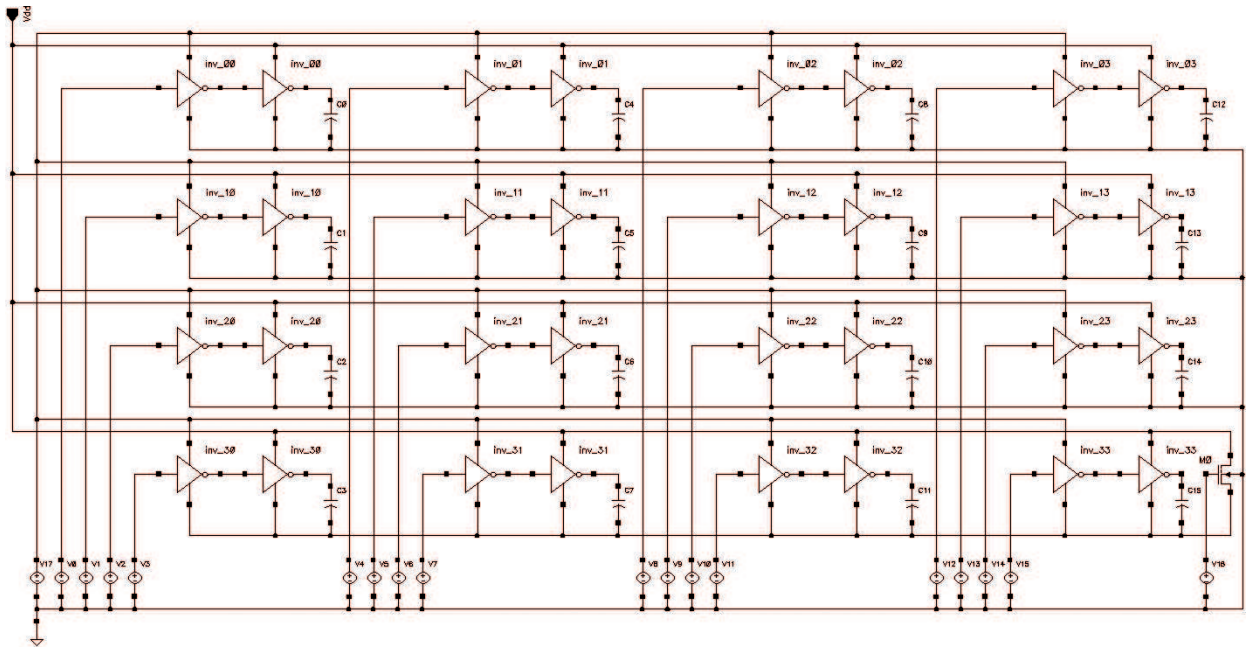


Fig. II.64 – *Schéma du macromodèle relatif à la charge (Load) [121, 122].*

des inverseurs permet de générer des motifs complexes, proches des signaux réels. Les signatures engendrées par l'activité d'un microcontrôleur exécutant des algorithmes cryptographiques ont été étudiées dans le cadre de deux thèses menées conjointement au sein du L2MP : une thèse en traitement du signal [82] et une thèse en traitement d'image [83]. Les résultats de ces études ont été exploités, entre autres, lors de la mise en œuvre des signatures de test.

Le courant délivré par la macrocellule (I_{DD}) est représenté en haut de la figure II.65. Il comporte trois phases distinctes : une phase de démarrage, une phase d'activité et une phase de mise en veille. Au début de la phase de démarrage, la charge présente une consommation correspondant à son mode veille ($100\ \mu A$). La montée en charge débute après un délais initial de $20\ \mu s$. Conformément au cahier des charges, la valeur moyenne de I_{DD} passe de $100\ \mu A$ à $25\ mA$ en une microseconde. La phase d'activité est amorcée au temps $t = 23\ \mu s$ et sa durée est fixée à $10\ \mu s$. Dans cet intervalle, la valeur moyenne de I_{DD} est de $28\ mA$ et les pics de consommation atteignent $100\ mA$ avec une vitesse de variation de l'ordre de $150\ mA/ns$; la composante AC constitue moins de 12% de la consommation totale. Enfin, à l'instant $t = 35\ \mu s$, la charge amorce son passage en veille; la valeur moyenne de I_{DD} chute à $100\ \mu A$ en moins d'une microseconde.

II.5.4.2.b Régulation

Le comportement transitoire du système à été simulé pour trois valeurs de $\overline{V_{PS}}$. Les courbes de $V_{PS}(t)$, $V_{SPS}(t)$, $V_{CP}(t)$, $V_{DD}(t)$ et $V_{ref}(t)$ sont représentées sur la figure II.65 pour $\overline{V_{PS}} \approx 5\ V$, $3.3\ V$ et $1.8\ V$. Conformément au cahier des charges, le temps de montée de V_{PS} est fixé à $1\ \mu s$.

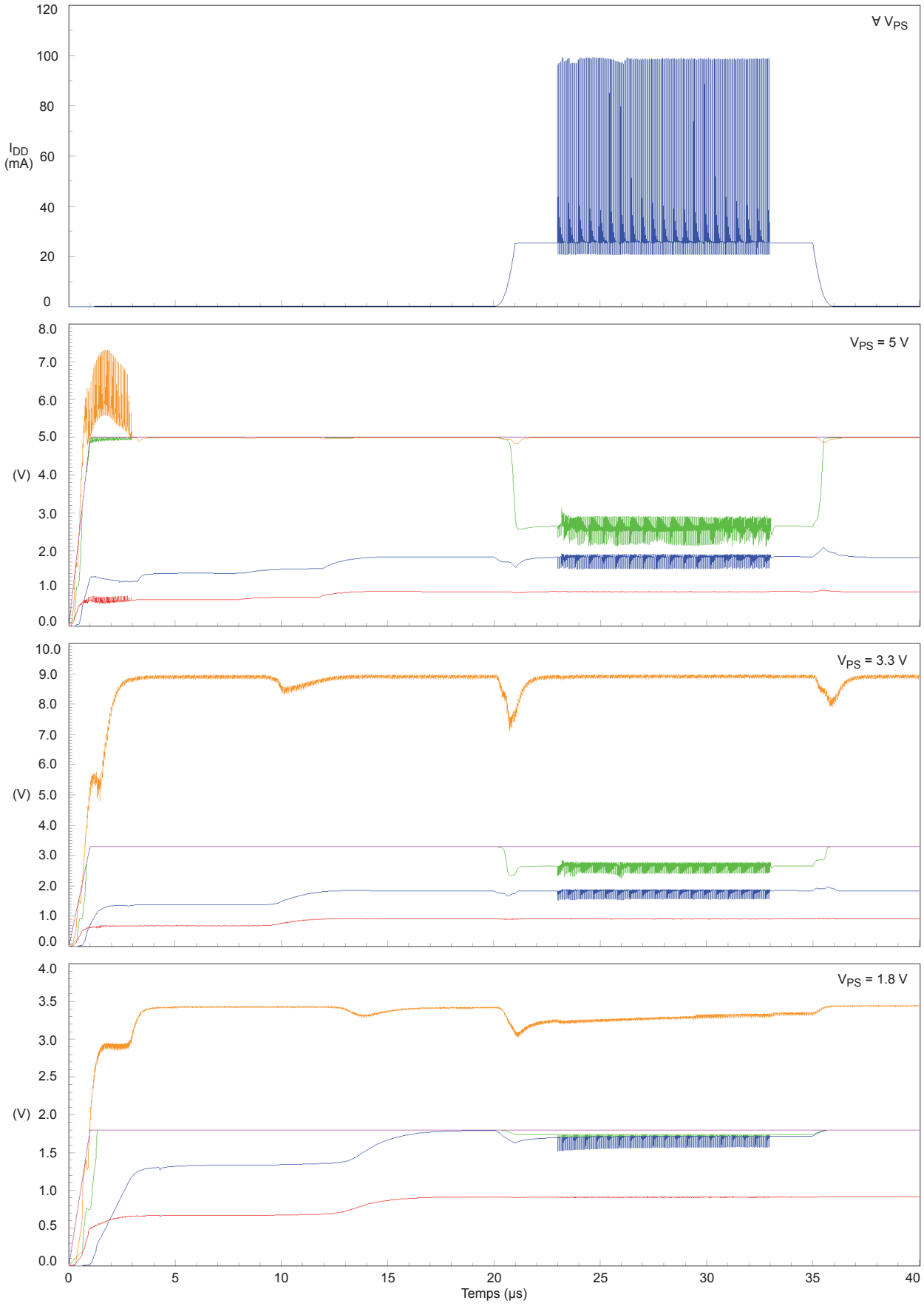


Fig. II.65 – *Courbes de I_{DD}, V_{PS}, V_{SPS}, V_{CP}, V_{DD} et V_{ref} pour $\overline{V_{PS}} \approx 5\ V$, $3.3\ V$ et $1.8\ V$.*

Quelle que soit la réalisation considérée, la courbe représentative de $V_{DD}(t)$ marque un palier à $1.4\ V$ avant de transiter vers sa valeur définitive ($1.8\ V$). Ce point d'inflexion correspond à l'instant ou V_{ref} passe de $V_{ref_{HV}}$ ($\approx 700\ mV$) à $V_{ref_{LV}}$ ($\approx 900\ mV$). Dans tous les cas, la tension V_{DD} atteint 90% de sa valeur statique en moins de $15\ \mu s$.

Lorsque $V_{PS} \approx 5\ V$, le contrôleur de puissance désactive immédiatement la pompe de charge de sorte que $V_{CP} = V_{PS}$. A la montée en charge, la boucle de régulation du sous-système sécuritaire (LR_P) reprend la main sur le système anti-fermeture. A partir de cet instant,la tension V_{SPS} atteint 90% de sa valeur statique ($2.6\ V$) en moins de $1\mu\ s$. Cette variation rapide de V_{SPS} tend à dégrader la qualité de la régulation; la réponse transitoire de V_{DD} atteint $240\ mV$ ce qui est supérieur aux $180\ mV$ autorisés par le cahier des charges. Pour améliorer ce point, une solution pourrait consister a augmenter l'amplitude du courant de veille de sorte à pouvoir supprimer le système anti-fermeture. Pendant la phase d'activité, la réponse transistoire de V_{DD} est de $260\ mV$ alors que l'amplitude des ondulations de V_{SPS} atteint $760\ mV$. Au moment du passage en veille, le système anti-fermeture est réactivé; le dépassement de V_{DD} atteint $210\ mV$.

Lorsque $\overline{V_{PS}} \approx 3.3\ V$, la pompe de charge hisse la tension V_{CP} à $8.9\ V$ en moins de $3\ \mu s$. La tension V_{SPS} présente un comportement analogue à celui obtenu pour $\overline{V_{PS}} \approx 5\ V$. En revanche, l'influence du système anti-fermeture est moins marquée que dans le cas précédent; lors de la montée en charge, la réponse transitoire de V_{DD} reste inférieure à $140\ mV$. Pendant la phase d'activité, l'amplitude des ondulations de V_{SPS} atteint $370\ mV$, tandis que la réponse transitoire de V_{DD} est égale à $220\ mV$. Enfin, lors du passage en mode veille, le dépassement de V_{DD} n'est plus que de $120\ mV$.

Lorsque $\overline{V_{PS}} \approx 1.8\ V$, la tension V_{CP} monte à $3.4\ V$ en moins de $4\ \mu s$. Lors de la montée en charge, la réponse transitoire de V_{DD} atteint $180\ mV$. A pleine charge, on obtient $\overline{V_{SPS}} \approx 1.74\ V$ et $\overline{V_{DD}} \approx 1.72\ V$. L'amplitude des ondulations de V_{DD} reste inférieure à $210\ mV$.

II.5.4.2.c Masquage du signal informationnel

Les courbes représentatives de $I_{DD}(t)$ et $I_{PS}(t)$ sont superposées sur les figures II.66 et II.67 pour, respectivement, $\overline{V_{PS}} \approx 5\ V$ et $\overline{V_{PS}} \approx 3.3\ V$. Lorsque $\overline{V_{PS}} \approx 5\ V$, le convertisseur à capacités commutées fonctionne en mode pompe de charge. En raison du couplage direct induit par cette topologie (cf. § II.4.3.3.b), les pics de courant de $I_{DD}(t)$ apparaissent sur $I_{PS}(t)$. Néanmoins, le sous-système sécuritaire uniformise la répartition de l'énergie; le taux d'atténuation en courant (CAR) atteint tout de même $-25.5\ dB$; les appels de courant sont fortement moyennés et leurs formes deviennent quasiment inexploitable. Par ailleurs, les variations induites par l'activité de la pompe de charge complexifient significativement la détection des instants relatifs aux déclenchements des pics du courant de charge.

Lorsque $\overline{V_{PS}} \approx 3.3\ V$ (cf. figure II.67), le convertisseur à capacités commutées fonctionne en mode hacheur de courant. Dans ce cas, seul l'effet Early associé aux transistors de puissance limite la perméabilité du système (cf. § II.4.3.3.c); le CAR atteint $-32\ dB$; les fuites résiduelles sont quasiment indissociable des signatures du hacheur de courant.

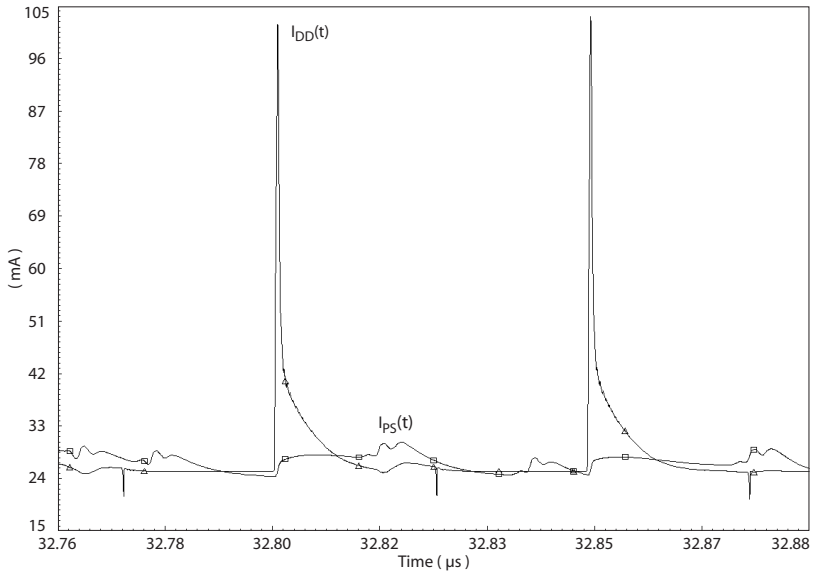


Fig. II.66 – *Courbes représentatives de $I_{DD}(t)$ et $I_{PS}(t)$ pour $\overline{V_{PS}} \approx 5\ V$.*

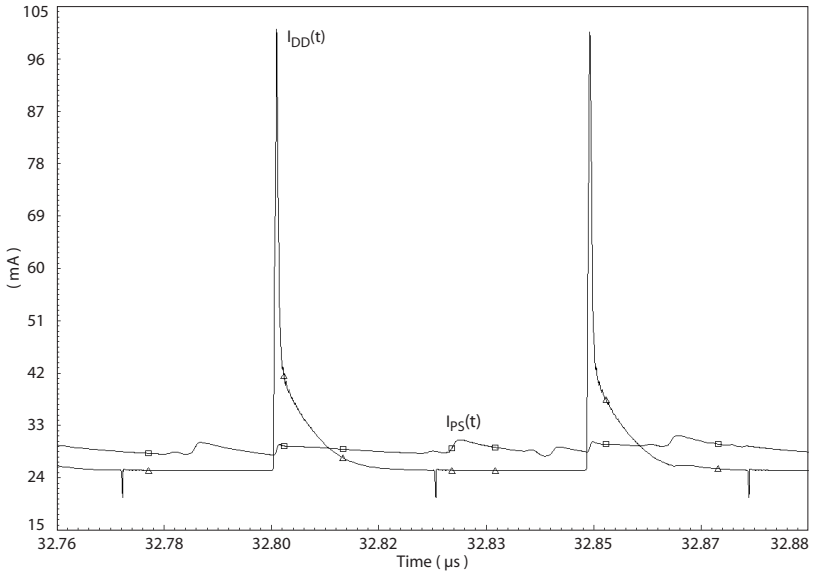


Fig. II.67 – *Courbes représentatives de $I_{DD}(t)$ et $I_{PS}(t)$ pour $\overline{V_{PS}} \approx 3.3\ V$*

Pour que le masquage résiste aux méthodes d'analyse statistique, il suffirait d'introduire un délai aléatoire entre l'activation du SCC et le démarrage de la charge. Cette contre-mesure complexifierait sérieusement la synchronisation des traces, et par voie de conséquence, la mise en œuvre des techniques de moyennage statistique. Il est à noter que, malgré la macrocellule employée pour la charge, les pics de courant présentent des discontinuités relativement pessimistes. Par conséquent, les résultats expérimentaux devraient confirmer les résultats simulés.

Lorsque la marge de tension devient trop faible (i.e., inférieur à $600\ mV$), le système proposé ne permet plus de protéger la charge. En effet, si le mode LDO permet de réguler V_{DD} à faible V_{PS}, en revanche, il

Paramètre	Valeur			Unité
$\overline{V_{PS}}$	5	3.3	1.8	V
$\overline{V_{DD}}$	1.82	1.82	1.72	V
$\overline{I_{DD}}$	27.97	27.98	28.00	mA
$\overline{I_{PS}}$	27.10	29.24	28.18	mA
$\overline{I_{PS_{ac}}}$	7.04	4.44	–	mA
$\overline{I_{SPS_{ac}}}$	8.61	3.92	–	mA
Consommation du SCC	5.55	1.72	–	mW
Rendement du SCC	63.5	69.6	–	%
Consommation du système	7.1	3.2	0.33	mW
Rendement du système	37.1	52.2	95.0	%

Tab. II.8 – *Consommation et rendement du système pour* $\overline{V_{PS}} \approx 5\ V$, $3.3\ V$ *et* $1.8\ V$ *(à pleine charge).*

n'offre aucune protection contre les attaques par analyse du courant. Aussi, dans le cadre d'une application sécuritaire, ce mode de fonctionnement ne devrait pas être autorisé. Toutefois, si l'application visée doit impérativement fonctionner à faible tension d'alimentation, une solution pourrait consister à remplacer le mode LDO proposé par une régulateur *shunt* analogue à celui de la figure II.22. En outre, dans ce mode LDO sécurisé, le générateur d'horloge aléatoire pourrait être utilisé pour injecter du bruit dans le canal d'alimentation et masquer ainsi les variations résiduelles non-atténuées par le régulateur.

II.5.4.2.d Rendement en puissance

Si la comparaison des courbes II.66 et II.67 tend à démontrer la supériorité du mode hacheur de courant en terme de masquage, en revanche, la conclusion est toute autre en ce qui concerne le rendement. En effet, lorsque $\overline{V_{PS}} \approx 5\ V$ (cf. figure II.66), la valeur moyenne de $I_{PS}(t)$ est approximativement égale à celle de $I_{DD}(t)$, tandis que pour $\overline{V_{PS}} \approx 3.3\ V$ (cf. figure II.67), la valeur moyenne de $I_{PS}(t)$ est supérieure à celle de $I_{DD}(t)$. En particulier, le ratio des écarts $I_{PS}(t) - I_{DD}(t)$ est nettement supérieur au ratio $5/3.3$. Ce constat est confirmé par les résultats répertoriés dans le tableau II.8.

Le tableau II.8 rassemble, pour trois valeurs de $\overline{V_{PS}}$, les caractéristiques énergétiques du système fonctionnant à pleine charge. Lorsque $\overline{V_{PS}} \approx 5\ V$, le gain en courant intrinsèque du SCC atteint 1.45, ce qui est proche de la valeur théorique idéale (i.e. $3/2$, cf. § II.4.3.3.b). Cependant, si l'on prend en compte sa consommation propre, le gain en courant effectif ($I_{SPS_{ac}}/I_{PS_{ac}}$) n'est plus que de 1.22. Néanmoins, puisqu'une proportion importante du courant I_{DD} est ici véhiculée par le canal AC (plus de 30%), cette valeur de gain suffit à rendre négatif le courant de repos du système ($\overline{I_{PS}} < \overline{I_{DD}}$). Ainsi, le rendement global de ce dernier atteint 37.1 %, ce qui est supérieur au rendement d'un régulateur linéaire idéal opérant dans les mêmes conditions (i.e. 36 %, cf. equation II.17). Lorsque $\overline{V_{PS}} \approx 3.3\ V$, le gain en courant intrinsèque du SCC est égal à sa valeur théorique (i.e. 1, cf. § II.4.3.3.c), mais son gain effectif n'est que de 0.88. Par

ailleurs, la diminution de la marge de tension $V_{PS} - V_{SPS}$ se traduit par une réduction du courant véhiculé par le canal AC. Celui-ci ne représente alors plus que $14\ \%$ du courant I_{DD} total. De fait, le rendement du système ($52.2\ \%$) devient alors inférieur à celui d'un régulateur linéaire idéal (i.e. $54.5\ \%$). Enfin, lorsque $\overline{V_{PS}} \approx 1.8\ V$, la désactivation du sous-système sécuritaire diminue significativement la consommation totale du système; celui-ci est alors équivalent à un régulateur linéaire série dont le rendement, $94.9\ \%$, est proche de sa valeur idéale (i.e. $95.5\ \%$).

II.6 Conclusion

En traitant séparément les composantes DC et AC du courant de charge, le système proposé permet d'atteindre un compromis approprié entre régulation, rendement et sécurité, tout en respectant les contraintes technologiques associées aux cartes à puce. Deux types de canaux AC ont été implémentés : une pompe de charge et un hacheur de courant. Dans le premier cas, le gain en courant de la pompe de charge compense entièrement la consommation du système. De fait, le rendement du régulateur est supérieur à celui d'un régulateur linéaire idéal. En contrepartie, le couplage capacitif induit par cette topologie tend à dégrader le masquage du signal informationnel. De plus, l'utilisation d'une structure de ce type nécessite une marge de tension relativement importante. Par rapport à la pompe de charge, le hacheur de courant permet de réduire la tension de *dropout* du sous-système sécuritaire. Par ailleurs, en diminuant l'amplitude des fuites d'informations, il améliore significativement la qualité du masquage; les signatures résiduelles deviennent quasiment indissociables des pics de consommation du SCC. En revanche, à marge de tension équivalente, le rendement du hacheur de courant est moins élevé que celui de son homologue. Quel que soit le mode de fonctionnement considéré, le rendement de la structure proposé est supérieur à celui d'un régulateur *shunt*. En contrepartie, l'utilisation d'un régulateur *shunt* permettrait de protéger la charge avec une marge de tension beaucoup plus faible. Ainsi, la combinaison de ces deux solutions, selon le principe évoqué au § II.5.4.2.c, devrait permettre de protéger la charge en toutes circonstances, tout en maximisant le rendement.

Dans le circuit présenté, l'accent a été mis sur l'intégrabilité. Or, une augmentation raisonnable de la longueur des transistors de puissance et de la taille des capacités de puissance permettrait de réduire significativement l'amplitude des fuites d'information, tout en conservant un niveau de régulation acceptable. D'autre part, comme suggéré au paragraphe II.4.2.2, le système proposé peut être utilisé pour protéger uniquement les cellules sécuritaires, les autres cellules étant alimentées par un régulateur linéaire traditionnel. A la fois efficace et efficiente, cette solution hybride permettrait, au prix d'une complexité accrue, de réduire significativement la surface de l'implémentation présentée dans ces pages. Quoi qu'il en soit, à performances équivalentes, un régulateur basé uniquement sur un convertisseur à découpage nécessiterait une surface au moins cinq fois supérieure à celle du circuit présenté. Le système proposé a fait l'objet de deux brevets mondiaux et deux articles en conférences internationales (cf. annexe D).

Suite à des problèmes conjoncturels, notre collaborateur industriel a été dans l'obligation d'annuler la fabrication des prototypes initialement planifiés. Par conséquent, les résultats présentés dans ce chapitre n'ont pu être vérifiés expérimentalement. Néanmoins, comme nous le verrons au chapitre suivant, la cellule clé du générateur d'horloge aléatoire a été fabriqué avec succès en technologie AMS CMOS $0.35\ \mu m$.

Chapitre III

Générateur d'horloge aléatoire

III.1 Introduction

Le générateur d'horloge aléatoire (RCG pour « *Random Clock Generator* ») est une des cellules clés du sous-système sécuritaire proposé au second chapitre (cf. figure II.30). Son rôle est de générer le signal d'horloge (V_{RC}) destiné à cadencer le convertisseur à capacités commutées (SCC). Les caractéristiques de V_{RC} doivent permettre au SCC de masquer les fuites résiduelles associées à l'activité de la charge (cf. § II.5.2.2.b). L'étude du RCG est au cœur de ce troisième et dernier chapitre. Elle a été menée conjointement avec F. Chaillan, dont les travaux de thèse ont visé, entre autres, à lui donner un cadre mathématique rigoureux [82].

III.2 Cahier des charges

Afin d'optimiser le masquage du signal informationnel, la fréquence f_{rc} du signal d'horloge V_{RC} doit varier continuellement de manière aléatoire. De plus, sa plage de variation fréquentielle (Δf_{rc}) doit être continue, uniformément distribuée et centrée sur la fréquence de fonctionnement de la charge (f_c). Pour limiter la durée des états stables de V_{RC}, la fréquence moyenne des sauts de f_c ($\overline{f_j}$) doit être au moins égale à f_{rc}. Puisque la quantité d'énergie véhiculée par le SCC est proportionnelle à sa fréquence de commutation, cette dernière ne doit jamais descendre en dessous d'un certain seuil. A cet effet, la largeur de la plage de variation fréquentielle doit être facilement ajustable. Les spécifications du cahier des charges sont rassemblées dans le tableau III.1. Elles ont été fixées en collaboration avec la division DSA de la société STMicroelectronics.

En vue d'une intégration au cœur du microcontrôleur, le générateur doit reposer, de préférence, sur les éléments LV de la technologie STM $0.18\ \mu m$. De fait, sa tension d'alimentation (V_{DD}) est fixée à $1.8\ V\ \pm 10\%$. Pour des valeurs de $\overline{f_{rc}}$ et $\overline{f_j}$ fixées à $20\ MHz$, le générateur doit consommer moins de $1\ mW$. Dans les conditions PVT établies au second chapitre (cf. tableau II.5), la précision de $\overline{f_{rc}}$ doit être supérieure à 10%. De plus, afin de répondre aux exigences du sous-système sécuritaire, le temps de démarrage du générateur doit être inférieur à $0.5\ \mu s$. Enfin, sa surface doit être aussi faible que possible.

Paramètre	Symbole	Valeur	Unité
Tension d'alimentation.	V_{DD}	$1.8 \pm 10\%$	V
Fréquence moyenne du signal d'horloge.	$\overline{f_{rc}}$	20	MHz
Fréquence moyenne des sauts de f_{rc}.	$\overline{f_j}$	> 20	MHz
Largeur de la plage de variation fréquentielle.	Δf_{rc}	30	MHz
Précision de f_{rc} (pour les conditions PVT du tableau II.5).	-	< 10	$\%$
Temps de démarrage.	-	< 0.5	μs
Consommation.	-	< 1	mW

Tab. III.1 – *Cahier des charges du générateur d'horloge aléatoire.*

III.3 Etat de l'art

III.3.1 Introduction

Le développement des générateurs d'horloge aléatoire est étroitement lié à celui des générateurs de nombres aléatoires (RNG pour « *Random Number Generator* »). Les RNG se divisent en deux catégories : les RNG dits « pseudo-aléatoires » (PRNG pour « *Pseudo-Random Number Generator* ») et les RNG dits « vraiment aléatoires » (TRNG pour « *True Random Number Generator* »). Les techniques mises en œuvre pour les PRNG peuvent être utilisées pour générer un signal d'horloge aléatoire. Réciproquement, la majorité des TRNG repose sur l'échantillonnage d'un signal d'horloge aléatoire qui, dans notre cas, peut être utilisé directement. Ainsi, on distinguera deux familles de générateurs d'horloge aléatoire : les générateurs numériques (utilisation détournée des PRNG), et les générateurs analogiques (utilisation directe des cellules initialement développées pour les TRNG). La famille des générateurs numériques se divise en deux catégories : les générateurs matériels et les générateurs logiciels. En ce qui concerne les générateurs analogiques, un grand nombre de méthodes ont été proposées dans la littérature, parmi lesquelles : l'amplification directe d'une source de bruit [123, 124], le pilotage d'un oscillateur contrôlé en tension (VCO pour « *Voltage Controlled Oscillator* ») par une source de bruit [125] et les générateurs de chaos [126, 127] (en temps continu [128, 129] ou discret [130, 131]).

III.3.2 Générateurs numériques

La famille des PRNG se divise en deux catégories : les PRNG matériels et les PRNG logiciels. Le plus répandu des PRNG matériels est le registre à décalage avec rétroaction linéaire (LFSR pour « *Linear Feedback Shift Register* »). Son schéma de principe est représenté sur la figure III.1. Les bits de sortie des registres subissent une série d'opérations (par exemple, des XOR) avant d'être réinjectés en entrée du premier registre. Le flot ainsi généré constitue une suite récurrente linéaire. Cette dernière est périodique : pour un registre de profondeur égale à n, la période maximale est limitée à $2^n - 1$ [132]. Ce type de registre est utilisé en cryptographie pour les implémentations matérielles de certains algorithmes de chiffrement de flot. Le chiffrement par flot (« *stream cipher* » dans la littérature anglaise) est une des deux grandes catégories de chiffrements modernes en cryptographie symétrique, le second étant le chiffrement par bloc évoqué au § I.2.1.2. A la différence de ce dernier, le chiffrement par flot permet de traiter les données de

longueur quelconque, sans les découper.

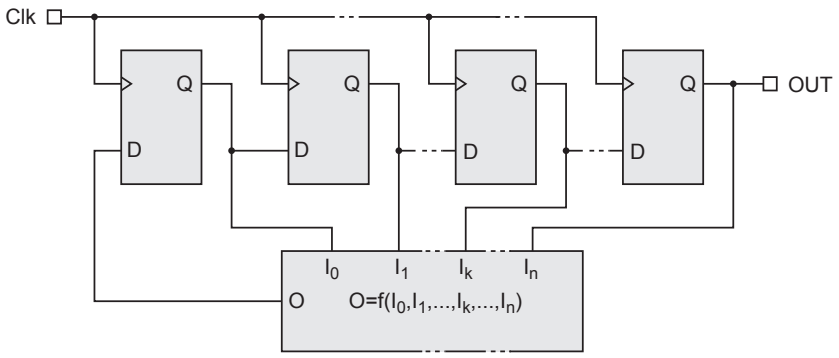


Fig. III.1 – *Registre à décalage avec rétroaction linéaire (LFSR) [132].*

Un PRNG logiciel repose sur un algorithme exécuté par un microprocesseur. Dans ce cas, la périodicité de la suite dépend à la fois de l'algorithme employé et de la taille des données manipulées par le microprocesseur. Introduit en 1948 par D.H Lehmer, le générateur congruentiel linéaire est un des algorithmes les plus utilisés. Il repose sur la formule de récurrence suivante :

$$X_{n+1} = (a \cdot X_n + c) \mod m \tag{III.1}$$

où a est le multiplicateur, c l'incrément et X_o le germe. La période du flux est au maximum de m, dont la valeur est généralement prise égale à la largeur du bus de données. Par rapport aux solutions matérielles, les solutions logicielles facilitent la mise en œuvre d'opérations complexes. De plus, elles présentent l'avantage d'être reprogrammables à la volée. En contrepartie, un circuit dédié permet d'atteindre des débits plus important et, le cas échéant, de décharger le processeur central. Quel que soit le type d'implémentation retenu, le flux de sortie d'un PRNG peut être utilisé comme signal d'horloge aléatoire. Cependant, le signal ainsi généré est nécessairement périodique et sa fréquence décrit un ensemble discret dont la valeur maximale est limitée par la fréquence de fonctionnement du générateur. Par conséquent, cette solution n'est pas adaptée à l'application sécuritaire envisagée. Néanmoins, certaines techniques permettent de transformer le flux d'un LFSR en une source de bruit analogique [133].

III.3.3 Générateurs analogiques

III.3.3.1 Amplification directe d'un bruit blanc

Un bruit blanc est un signal aléatoire qui véhicule la même puissance quelle que soit la fréquence considérée [134]. En réalité, un bruit ne peut être blanc que sur une plage de fréquence donnée. En électronique, on distingue principalement deux sources de bruit blanc : le bruit de grenaille (« *shot noise* ») et le bruit thermique. Dans les deux cas, le bruit généré présente une amplitude à densité de probabilité normale (gaussienne). Par conséquent, s'il est comparé à sa valeur moyenne, le signal binaire résultant sera aléatoire et uniformément distribué [123]. Le bruit de grenaille résulte des fluctuations associées à un phénomène d'injection. Il est lié à la nature corpusculaire du courant. Par exemple, dans une jonction PN, il résulte de la fluctuation du nombre de porteurs franchissant la barrière de potentiel. Le bruit thermique, également

nommé bruit de résistance, bruit Johnson ou bruit de Johnson-Nyquist résulte quant à lui des fluctuations de vitesse des porteurs. Il est associé au mouvement Brownien (agitation thermique) des porteurs de charge. Contrairement au bruit de grenaille, le bruit thermique existe même en l'absence de polarisation. D'aprés l'expression formulée par Nyquist, la valeur efficace du bruit thermique présent aux bornes d'une résistance R est donnée par [135] :

$$\overline{v_n} = \sqrt{4 \cdot k_B \cdot T \cdot R \cdot \Delta f} \tag{III.2}$$

où k_B est la constante de Boltzmann, T la température en degré Kelvin et Δf la bande spectrale considérée. C'est sur une source de ce type que repose générateur de la figure III.2 [123].

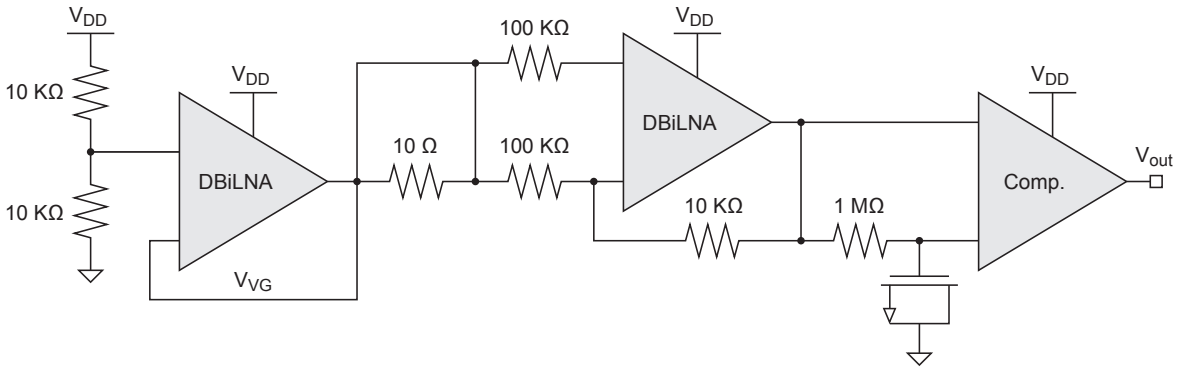


Fig. III.2 – *Amplification et seuillage d'un bruit thermique [123].*

Dans le générateur de la figure III.2, le bruit thermique de deux résistances est d'abord préamplifié avant d'être seuillé. Lors du seuillage, le bruit amplifié est comparé à sa valeur moyenne. Comme évoqué au § II.3.2, l'utilisation d'une alimentation asymétrique impose de recourir à une masse virtuelle (V_{VG}). Cette dernière permet de centrer les signaux d'intérêt au milieu de la plage de fonctionnement des amplificateurs. L'étage de préamplification est rendue indispensable par la faible amplitude du bruit thermique. En effet, elle n'est que de $40\ nV/\sqrt{Hz}$ pour une résistance en polysilicium de $100\ K\Omega$. L'amplification différentielle (une résistance par entrée de l'amplificateur) améliore la réjection du bruit de mode commun (bruit d'alimentation, couplage substrat, couplage électromagnétique, etc.). Cependant, les résistances, tout comme les transistors de l'amplificateur, sont également des sources de bruit « *flicker* ». Le bruit *flicker* est attribué aux fluctuations aléatoires du nombre de porteurs associés aux processus de génération, de recombinaison et de capture [135]. Avec son spectre en $1/f$, ce bruit « rose » tend à colorer le bruit souhaité blanc. Ainsi, l'objectif consiste ici à maximiser la largeur spectrale et l'amplitude du bruit blanc tout en minimisant la composante en $1/f$. En d'autres termes, il faut abaisser, autant que faire se peut, la fréquence à partir de laquelle le bruit en $1/f$ et le bruit blanc ont même amplitude (« $1/f$ *noise corner frequency* »). Cependant, la réalisation d'un amplificateur faible bruit à fort gain se traduit généralement par une consommation élevée; dans [123], les amplificateurs faible bruit à étage d'entrée Darlington « pseudo BiCMOS » (DBiLNA pour « *Darlington Pseudo-BiCMOS Low Noise Amplifier* » [136]) engendrent une consommation de $5\ mW$, ce qui est cinq fois supérieur au budget énergétique total alloué par le cahier des charges.

III.3.3.2 VCO piloté par une source de bruit

Le générateur de nombres aléatoires proposé par Intel est schématisé sur la figure III.3 [125]. Ce TRNG repose sur l'échantillonnage d'un signal d'horloge rapide par un signal d'horloge lent. Le flux numérique ainsi généré est rendu aléatoire par les fluctuations du déphasage entre les deux signaux. Il est ensuite ré-équilibré par un correcteur de type von Neumann.

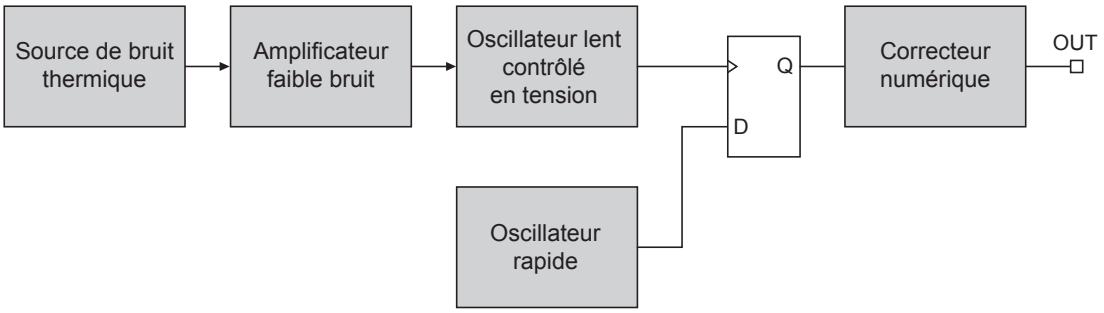


Fig. III.3 – *Générateur de nombres aléatoires proposé par Intel [125].*

Afin d'augmenter le bruit de phase du signal lent, le VCO dont il est issu est contrôlé par un signal analogique aléatoire. Ce dernier est généré selon la méthode décrite au § III.3.3.1. Dans la mesure où le bruit amplifié n'est pas exploité directement, sa « blancheur » revêt ici une importance moins critique. Au-delà d'une simple dérive de la phase, cette technique pourrait aboutir à la génération d'un signal d'horloge présentant une période aléatoire. Cependant, pour ce faire, le signal de contrôle doit alors présenter une amplitude relativement importante.

III.3.3.3 Générateurs de chaos

III.3.3.3.a Introduction

Un système chaotique est un système dynamique non-linéaire déterministe présentant un phénomène d'instabilité appelé « sensibilité aux conditions initiales » qui, associé à une propriété supplémentaire de récurrence, le rend non prédictible sur le long terme. Deux trajectoires initialement proches l'une de l'autre s'éloignent exponentiellement au cours du temps. D'après [137], il est difficile de distinguer un signal chaotique d'un signal non-déterministe. En particulier, les spectres fréquentiels des signaux chaotiques sont analogues à ceux des bruits résultant de processus stochastiques [137]. Par conséquent, les circuits chaotiques constituent une alternative efficiente pour la génération de signaux pseudo-aléatoires non prédictibles et non périodiques [127]. De fait, ils sont exploités dans de multiples domaines d'applications : traitement analogique du signal, cryptographie chaotique (communication numérique sécurisée), etc.

En terme de dynamique, les modèles permettant de générer du chaos peuvent être classés en temps continu ou discret selon que l'évolution du système est décrite par une équation aux différences non-linéaire ou par une équation différentielle non-linéaire. On distingue également les systèmes autonomes, dans lesquels les oscillations s'auto-entretiennent, des systèmes non-autonomes qui requièrent quant à eux une source d'excitation externe [127]. L'implémentation électronique des systèmes en temps discret repose

le plus souvent sur des circuits à courants ou capacités commutés. Dans les deux cas, la bande passante du signal chaotique est limitée à une fraction de la fréquence d'horloge. Par conséquent, les circuits de ce type ne peuvent pas garantir simultanément une fréquence élevée et une consommation faible. Par conséquent, ils ne sont pas adaptés aux contraintes de cette étude. Nous nous intéresserons donc principalement aux systèmes chaotiques en temps continu.

III.3.3.3.b Générateurs chaotiques en temps continu autonomes

Les générateurs de chaos à temps-continu autonomes appartiennent à l'espace $L_{n,m}$ des systèmes dynamiques n-D à m éléments non-linéaires, définis par l'équation d'état [127] :

$$\tau \cdot \frac{d}{dt} X\,(t) = F\,[X(t),P] = A \cdot X\,(t) + B \cdot f\,[X(t)] + C \tag{III.3}$$

où τ est une matrice diagonale définissant les constantes de temps du système, $X(t) = [x_i(t)]_{1 \leq i \leq n} \in \mathbb{R}^{n \times 1}$ est le vecteur d'état du système, $A \in \mathbb{R}^{n \times n}$, $B \in \mathbb{R}^{n \times m}$, $C \in \mathbb{R}^{n \times 1}$ et $f(\cdot) = [f_j(\cdot)]_{1 \leq j \leq m} \in \mathbb{R}^{m \times 1}$ est un champ de vecteurs non-linéaire. Cette forme canonique est illustrée par le schéma bloc de la figure III.4. Il consiste en un chemin direct contenant un sous-système linéaire temporellement invariant (cadre en pointillé) et une boucle de retour incluant les éléments de $f(\cdot)$.

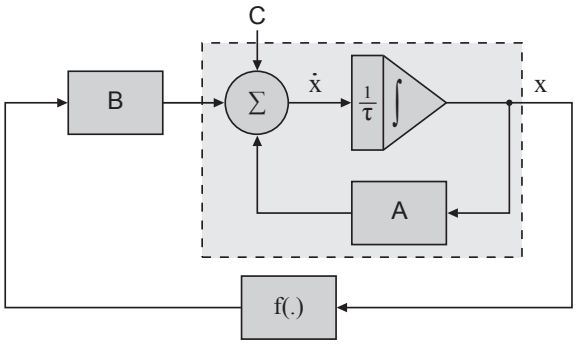


Fig. III.4 – *Schéma bloc d'un générateur de chaos autonome à temps continu [127].*

Le tableau III.2 rassemble un échantillon des générateurs de chaos en temps continu autonomes ayant été proposés dans la littérature [127]. Les fonctions non-linéaires sat, u_+, u_-, sgn et $hyst$ sont définies dans le tableau de l'annexe B. Les conditions sur (P) garantissant un comportement chaotique sont décrites dans les références citées en première colonne. Pour tous les cas répertoriés dans le tableau III.2, la matrice C est identiquement nulle et τ correspond à la matrice identité. Le tableau III.2 révèle un fait bien connu : pour générer du chaos, un système autonome doit présenter au minimum trois degrés de liberté [138]. Notons que dans le cas de l'oscillateur 4D, l'effet hystérésis induit un état additionnel [139]. Ce critère constitue une des principales différences entre les systèmes à temps continu et ceux à temps discret. En effet, dans ces derniers, une seule variable d'état suffit à générer du chaos.

L'implémentation d'un oscillateur chaotique nécessite d'adapter les équations d'état du système aux opérateurs électroniques. Si la majorité des générateurs proposés dans la littérature ont fait l'objet de dé-

Nom / Référence(s)	Paramètres		
	A	B	$f(\cdot)$
Chua [140, 141, 142, 143] [127, 126, 144]	$\begin{bmatrix} -c & a & 0 \\ 1 & -1 & 1 \\ 0 & -b & 0 \end{bmatrix}$	$\begin{bmatrix} -d \\ 0 \\ 0 \end{bmatrix}$	$f_1(X) = sat(x_1, L)$
Chua modifié [126]	$\begin{bmatrix} a & -1 & c \\ 1 & -b & 0 \\ e & 0 & -e \end{bmatrix}$	$\begin{bmatrix} 0 \\ 0 \\ -d \end{bmatrix}$	$f_1(X) = u_+(x_3 - L) - u_-(x_3 + L)$
Colpitts [145]	$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & a \\ c & c & b \end{bmatrix}$	$\begin{bmatrix} d \\ 0 \\ 0 \end{bmatrix}$	$f_1(X) = u_+(x_2 - L)$
Double-Scroll-like [146, 147, 148]	$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -a & -a & -a \end{bmatrix}$	$\begin{bmatrix} 0 \\ 0 \\ a \end{bmatrix}$	$f_1(X) = sgn(x_1)$
n-Scroll [149, 150, 151, 148]	$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -a & -b & -c \end{bmatrix}$	$\begin{bmatrix} 0 \\ 0 \\ d \end{bmatrix}$	$f_1(X)$: voir [149, 150, 151, 148].
Lorentz [152]	$\begin{bmatrix} -a & a & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -b \end{bmatrix}$	$\begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$	$f_1(X) = (c - x_3) \cdot x_1$ $f_2(X) = x_1 \cdot x_2$
Lorentz modifié [126]	$\begin{bmatrix} -a & a & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -b \end{bmatrix}$	$\begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$	$f_1(X) = (c - x_3) \cdot sgn(x_1)$ $f_2(X) = \lvert x_1 \rvert$
4D à hystérésis [139, 153]	$\begin{bmatrix} 0 & 1 \\ -b & -a \end{bmatrix}$	$\begin{bmatrix} d & 0 \\ 0 & c \end{bmatrix}$	$f_1(X) = hyst(x_1, L)$ $f_2(X) = hyst(x_2, L)$

Tab. III.2 – *Catalogue non-exhaustif d'oscillateurs chaotiques autonomes à temps continu [127].*

monstrateurs à composants discrets, en revanche, peu d'entre eux a été implémenté sous la forme de circuits intégrés monolithiques. D'après le paragraphe précédent, pour générer du chaos, un circuit autonome sans effet mémoire doit contenir au minimum [128] : un éléments non linéaire, une résistance active et trois éléments réactifs. Les fonctions linaires par morceaux (PWL pour « *Picewise-Linear* ») apparaissent comme les plus adaptées à l'implémentation monolithique de champs de vecteurs non-linéaires [138]. En effet, la fonction « interrupteur » est l'unique opérateur primitif nécessaire à leurs synthèses. De plus, elles peuvent être réalisées avec une précision relativement importante. En ce qui concerne les éléments réactifs, l'intégration des inductances ne peut être envisagée que pour des fréquences de l'ordre du gigahertz. De fait, les primitives dynamiques reposent généralement sur des capacités. Dans ce cas, les tensions incarnent les variables d'état et les courants sont les vecteurs de leur évolution. En particulier, l'utilisation combinée d'amplificateurs à transconductance et de capacités (techniques Gm-C) autorise une conversion directe des équations différentielles en circuits intégrés monolithiques. Qui plus est, les techniques Gm-C reposent uniquement sur des capacités à la masse. Par conséquent, elles ne sont pas affectées par les effets parasites associés au plateau inférieur des capacités intégrées. Enfin, les techniques Gm-C permettent de réaliser des circuits ne comportant, à l'échelle des cellules analogiques élémentaires (OTA, CCII, etc.), que des nœuds hautes impédances. Ils peuvent donc être alimentés de façon asymétrique et ce, sans faire appel à une masse virtuelle (cf. figure III.10).

Dans le cadre d'une application sécuritaire, la robustesse du système est également un critère important. La précision des cellules analogiques est intrinsèquement limitée par de nombreux défauts. Par conséquent, le modèle mathématique doit présenter une sensibilité limitée aux déviations de ses paramètres. En termes de dynamique, le système doit s'inscrire dans les plages de fonctionnement linéaire des cellules analogiques. Toutefois, la largeur des bassins d'attraction doit être supérieure à l'amplitude des perturbations électroniques, de sorte que ces dernières n'ont qu'une influence limitée sur le comportement de l'oscillateur. Dans le cas contraire, le système risque soit de diverger, soit de converger vers un cycle limite (solution périodique) ou un point fixe. Enfin, afin de limiter la distortion, la bande passante des cellules analogiques doit impérativement englober la majorité du spectre théorique des signaux chaotiques.

III.3.3.3.c Générateurs chaotiques en temps continu non-autonomes

Les oscillateurs chaotiques en temps continu non-autonomes sont caractérisés par la présence d'un signal d'excitation ($e(t)$) dans le jeu d'équations différentielles non-linéaires les décrivant. En particulier, ce signal d'excitation peut engendrer un comportement chaotique dans un oscillateur régi par un système non-linéaire du second ordre [154]. En pratique, l'excitation $e(t)$ se présente généralement sous la forme d'un signal périodique généré au moyen d'un oscillateur reposant, quant à lui, sur un système autonome à au moins deux degrés de liberté (cadre en pointillé). Dans ce cas, le système non-autonome est équivalent à un système autonome de degré supérieur ou égal à quatre [154].

La majorité des oscillateurs chaotiques non-autonomes proposée dans la littérature exploitent un signal d'excitation sinusoïdal [155, 156, 157]. De par les composants entrant dans leur composition (inductance, ampoule au néon, etc.), aucun de ces circuits n'est véritablement adapté à une intégration sur silicium. En revanche, la méthode d'excitation par impulsion présentée plus récemment dans [154] permet de transfor-

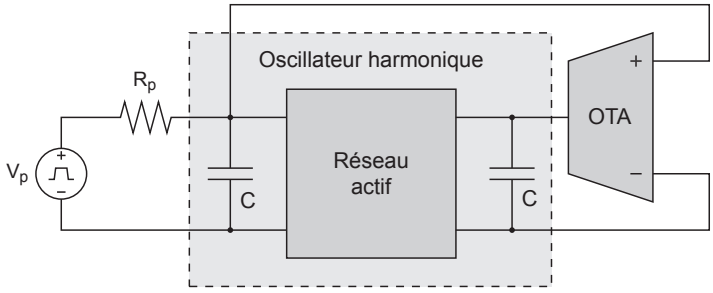


Fig. III.5 – *Générateur chaotique en temps continu non-autonome à excitation pulsée [154].*

mer tout oscillateur sinusoïdal à deux capacités en un oscillateur chaotique non-autonome (cf. figure III.5). Dans cette approche, le signal d'horloge périodique utilisé comme source d'excitation est converti en un train d'impulsions chaotique. Ainsi, cette technique permet de générer un signal d'horloge chaotique tout en offrant une implémentation monolithique. Cependant, elle ne permet pas de contrôler avec précision les caractéristiques de la plage de variation fréquentielle (largeur, uniformité, etc.).

III.3.4 Conclusion

Bien qu'un grand nombre de générateurs aient été proposés dans la littérature, aucun d'entre eux ne permet d'atteindre simultanément l'ensemble des objectifs fixés par le cahier des charges. Néanmoins, comme nous le verrons à la section suivante, certains des principes exposés peuvent servir de base à l'élaboration d'une solution sur mesure.

III.4 Générateur proposé

III.4.1 Introduction

Le générateur proposé repose sur la polarisation d'un oscillateur par un courant aléatoire en escalier. L'amplitude de ses marches varie de manière aléatoire sur un intervalle continu, uniformément distribué et à largeur ajustable. La largeur temporelle de ses marches varie de façon pseudo-aléatoire sur un intervalle continu à valeur moyenne paramétrable. Le signal d'horloge ainsi généré présente des sauts de fréquence intervenant à des instants aléatoires entre des fréquences elles-même aléatoires.

III.4.2 Principe

Le schéma-bloc du générateur proposé est représenté sur la figure III.6. Il comporte six cellules : un oscillateur chaotique (CO pour « *Chaotic Oscillator* »), un détecteur de front (ED pour « *Edge Detector* »), un générateur de signal triangulaire (TG « *pour Triangle-wave Generator* »), un échantillonneur-bloqueur (S&H pour « *Sample-and-Hold* »), un convertisseur tension-courant (VCC pour « *Voltage-to-Current Converter* ») et un oscillateur en anneau (RO pour « *Ring Oscillator* »). Les signaux de sortie de ces différents cellules, ainsi qu'un signal interne de l'oscillateur chaotique (V_X), sont illustrés sur le chronogramme de la figure III.8.

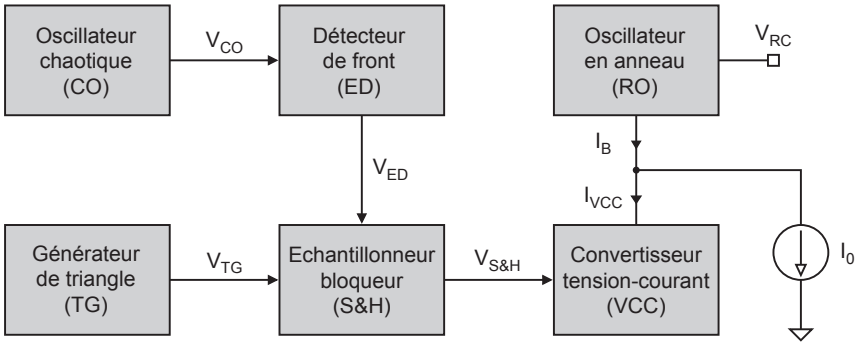


Fig. III.6 – *Schéma-bloc du générateur proposé.*

L'oscillateur chaotique (CO) génère un attracteur étrange de type « *double-scroll* ». Le *double-scroll* présente deux bassins d'attraction occupés chacun par une spirale de type Rössler. Dans une représentation de type portrait de phase (cf. figure III.7), le passage d'une trajectoire de l'attracteur par le plan séparant les deux bassins d'attractions correspond, dans une représentation temporelle (cf. figure III.8), au passage du signal $V_X(t)$ par sa valeur moyenne. Le signal de sortie de l'oscillateur chaotique (V_{CO}) est engendré par seuillage du signal $V_X(t)$. Ainsi, chaque transition de l'attracteur se traduit par une inversion du signal $V_{CO}(t)$. Chaque transition de $V_{CO}(t)$ (montante ou descendante) engendre une courte impulsion en sortie du détecteur de front (ED). A chaque impulsion de $V_{ED}(t)$, l'échantillonneur-bloqueur (S&H) transmet la valeur instantanée du signal triangulaire (V_{TG}) vers sa sortie, puis il la maintient jusqu'à l'arrivée de l'impulsion suivante. La tension ainsi générée ($V_{S\&H}$) est convertie en un courant à valeur moyenne nulle (I_{VCC}) auquel est additionné un courant constant (I_0). Le signal résultant ($I_B(t)$) est utilisé pour piloter l'oscillateur contrôlé en courant (RO). Ainsi, la fréquence moyenne du signal d'horloge (V_{RC}) est fixée par I_0, tandis que la largeur de sa plage de variation fréquentielle dépend de l'amplitude du courant de modulation ($I_{VCC}(t)$). Cette dissociation permet de fixer précisément les caractéristiques de $V_{RC}(t)$.

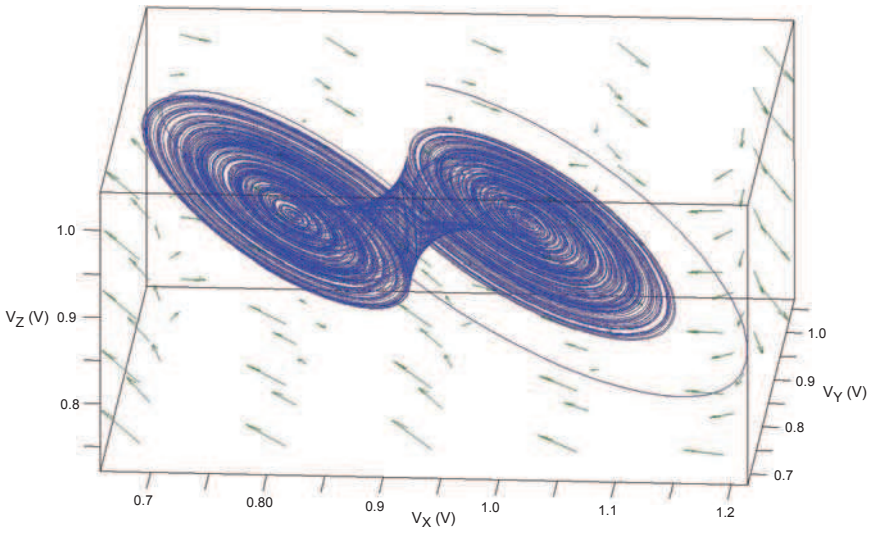


Fig. III.7 – *Portrait de phase de l'attracteur étrange.*

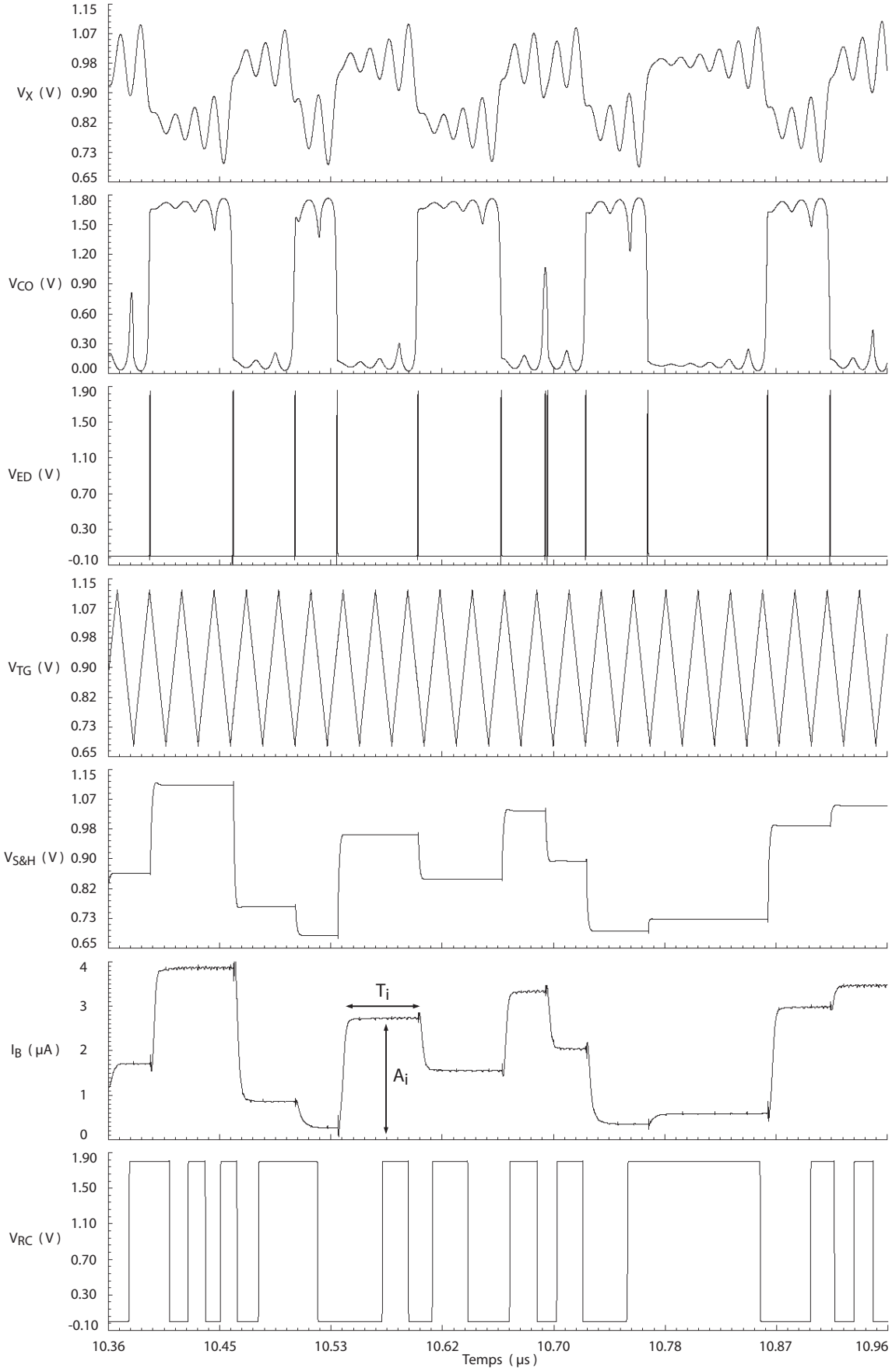


Fig. III.8 – *Chronogramme des signaux du générateur proposé.*

La fréquence du signal d'horloge généré par l'oscillateur en anneau (V_{RC}) est directement proportionnelle à l'amplitude de son courant de polarisation (I_B). Soient A_i et T_i l'amplitude et la durée du palier i de $I_B(t)$. La fréquence (f_i) et la durée de l'état stable i de l'oscillateur sont respectivement proportionnelles aux paramètres A_i et T_i du palier i correspondant. Les séquences $A = \{A_i\}_{i\geq 0}$ et $T = \{T_i\}_{i\geq 0}$ pouvant être considérées comme aléatoires, le signal $V_{RC}(t)$ présente des sauts de fréquence intervenant à des instants aléatoires entre des fréquences elles-même aléatoires.

La séquence T est définie comme la différence des instants successifs où la trajectoire de phase de l'oscillateur chaotique traverse le plan central séparant ses deux bassins d'attraction. Par conséquent, cette séquence est pseudo-aléatoire, non prédictible, non périodique et définie sur un intervalle continu. Les conditions initiales du système chaotique dépendent d'un grand nombre de paramètres physiques (température, bruit, etc.). Puisque les trajectoires de phase sont très sensibles aux conditions initiales, les séquences ainsi générées peuvent être considérées comme décorrelées. Enfin, la pulsation propre de l'oscillateur est facilement ajustable. Par conséquent, la moyenne arithmétique de T l'est également. En définitive, les délais entre les sauts de fréquences décrivent une séquence pseudo-aléatoire, non prédictible et non-périodique, qui prend ses valeurs dans un intervalle continu à valeur moyenne paramétrable.

La séquence A est générée par échantillonnage d'un signal triangulaire indépendant (V_{TG}) aux instants où la trajectoire de phase de l'oscillateur chaotique traverse le plan central séparant ses deux bassins d'attraction. Un signal triangulaire est uniformément distribué sur sa dynamique. En effet, une rampe constitutive de ce dernier peut être assimilée à la fonction de répartition d'une variable aléatoire suivant une loi uniforme. Par conséquent, l'échantillonnage aléatoire de ce signal donne, pour un nombre d'échantillons suffisamment grand, un ensemble de valeurs équiréparties sur un intervalle continu. En outre, le signal triangulaire et le signal chaotique sont issus de deux sources indépendantes, il est par conséquent légitime de les considérer comme mutuellement décorrélées. De plus, la fréquence du signal triangulaire est prise plus de deux fois supérieure à la fréquence moyenne d'échantillonage, ce qui a pour conséquence d'augmenter l'influence du bruit phase. Cette démarche augmente nécessairement l'entropie du flux. Par ailleurs, l'amplitude du signal triangulaire est ajustable. En définitive, la fréquence du signal d'horloge décrit une séquence aléatoire, qui prend ses valeurs dans une plage continue, uniformément distribuée et à largeur paramétrable.

III.4.3 Description des cellules

III.4.3.1 Vue d'ensemble

Le circuit du générateur d'horloge aléatoire est schématisé sur la figure III.9. Par rapport au schéma de principe de la figure III.6, cette implémentation fait intervenir des cellules supplémentaires. Le bloc de polarisation (RCG_B) assure la distribution des courants de polarisation à partir du courant de référence externe (I_b). Le décaleur de tension (LV_to_HV) permet de rehausser le signal de sortie de l'oscillateur en anneau (RO) du niveau V_{DD} au niveau V_{PS} (cf. figure II.44). Le suiveur de tension (VF), l'OTA et la capacité MOS ne sont autres que les cellules constitutives du convertisseur tension-courant (VCC). Enfin, les deux inverseurs situés à gauche propagent le signal d'activation (PD) vers les différentes cellules du générateur.

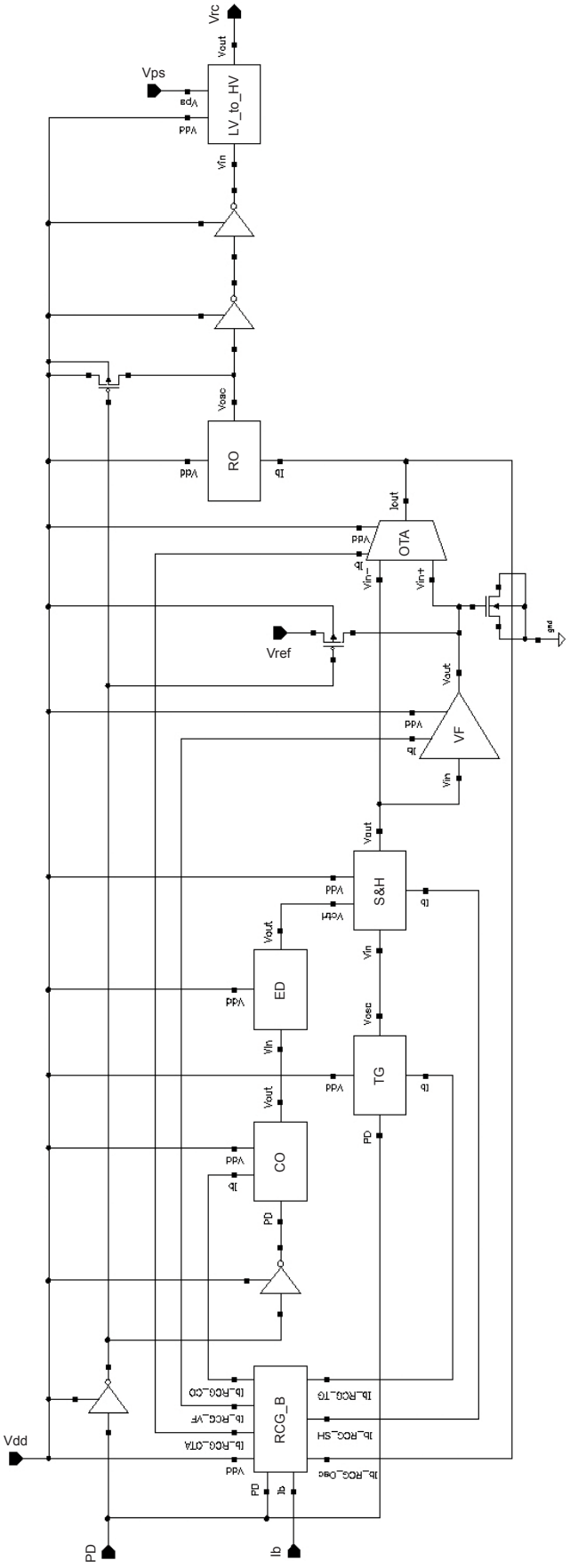


Fig. III.9 – *Circuit du générateur proposé.*

III.4.3.2 Oscillateur chaotique

III.4.3.2.a Modélisation du circuit

Une partie non négligeable des générateurs de nombres aléatoires proposés récemment dans la littérature reposent sur un oscillateur chaotique de type *double-scroll* [158, 159, 160]. De fait, cette catégorie de systèmes chaotiques a fait l'objet de nombreuses implémentations électroniques. Cependant, à notre connaissance, seule celle proposée en 2003 par Radwan et al. [147] est véritablement adapté à nos contraintes technologiques (cf. figure III.10). En effet, sa topologie gm-C permet d'aboutir à la réalisation d'un circuit monolithique en technologie CMOS.

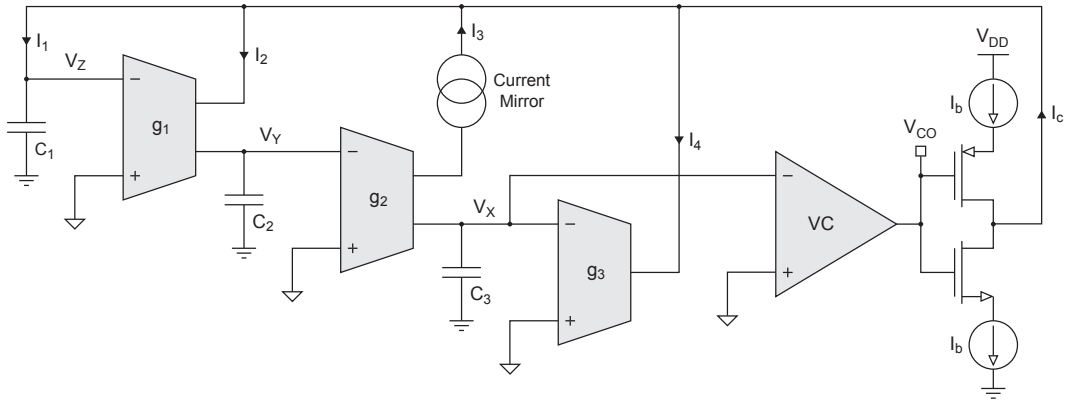


Fig. III.10 – *Schéma-bloc de l'oscillateur chaotique (CO) [147].*

Le schéma-bloc proposé dans [147] est représenté sur la figure III.10. Il est constitué d'une chaîne de trois intégrateurs gm-C, d'un miroir de courant (CM pour « *Current Mirror* »), d'un comparateur de tension (VC pour « *Voltage Comparator* »), de deux interrupteurs complémentés et de deux sources de courant (I_b). Chaque intégrateur repose sur une capacité C_i et une transconductance g_i. Le courant de polarisation I_b est délivré par une référence de courant externe. On suppose que le circuit est alimenté de façon asymétrique et que les tensions de polarisation des noeuds V_X, V_Y et V_Z sont égales à $V_{DD}/2$. Dans ce cas, la loi de Kirchhoff relative aux noeuds permet d'écrire :

$$I_1 = -I_2 + I_3 - I_4 + I_c \tag{III.4}$$

où I_c est donnée par :

$$I_c = \begin{cases} I_b & \text{si} \quad V_X \geq \frac{V_{DD}}{2} \\ -I_b & \text{si} \quad V_X < \frac{V_{DD}}{2} \end{cases} \tag{III.5}$$

avec

$$I_4 = g_3 \cdot \left(V_X - \frac{V_{DD}}{2}\right) \tag{III.6}$$

$$I_3 = g_2 \cdot \left(V_Y - \frac{V_{DD}}{2}\right) = -C_3 \cdot \frac{dV_X}{dt} \tag{III.7}$$

$$I_2 = g_1 \cdot \left(V_Z - \frac{V_{DD}}{2}\right) = -C_2 \cdot \frac{dV_Y}{dt} = \frac{C_2 \cdot C_3}{g_2} \cdot \frac{d^2V_X}{dt^2} \tag{III.8}$$

$$I_1 = C_1 \cdot \frac{dV_Z}{dt} = \frac{C_1 \cdot C_2 \cdot C_3}{g_1 \cdot g_2} \cdot \frac{d^3V_X}{dt^3} \tag{III.9}$$

En substituant les expressions III.6, III.7, III.8 et III.4 dans la relation III.9, puis en opérant le changement de variables linéaire définie par :

$$\begin{cases} V_x = V_X - \frac{V_{DD}}{2} \\ V_y = V_Y - \frac{V_{DD}}{2} \\ V_z = V_Z - \frac{V_{DD}}{2} \end{cases} \tag{III.10}$$

on aboutit a :

$$\frac{C_1 \cdot C_2 \cdot C_3}{g_1 \cdot g_2} \cdot \frac{d^3V_x}{dt^3} = -\frac{C_2 \cdot C_3}{g_2} \cdot \frac{d^2V_x}{dt^2} - C_3 \cdot \frac{dV_x}{dt} - g_3 \cdot V_x + I_c \tag{III.11}$$

Soient a une constante, V_b une tension de polarisation et sgn la fonction signe (cf. annexe B). Si l'on suppose que $g_1 = g_2 = g_3 = g$, que $C_2 = C_3 = C$, que $C_1 = C/a$ et que $I_c = g \cdot V_b \cdot sgn(V_x)$, alors l'expression III.11 peut se réécrire sous la forme :

$$\frac{d^3V_x}{dt^3} = -a \cdot \left(\frac{g}{C}\right) \cdot \frac{d^2V_x}{dt^2} - a \cdot \left(\frac{g}{C}\right)^2 \cdot \frac{dV_x}{dt} - a \cdot \left(\frac{g}{C}\right)^3 \cdot V_x + a \cdot V_b \cdot \left(\frac{g}{C}\right)^3 \cdot sgn(V_x) \tag{III.12}$$

Par suite, le comportement du circuit de la figure III.10 est entièrement décrit par le système (P) composé de l'équation différentielle III.12 et d'un jeu de conditions initiales :

$$(P) \begin{cases} \frac{d^3V_x}{dt^3} + a \cdot \left(\frac{g}{C}\right) \cdot \frac{d^2V_x}{dt^2} + a \cdot \left(\frac{g}{C}\right)^2 \cdot \frac{dV_x}{dt} + a \cdot \left(\frac{g}{C}\right)^3 \cdot V_x = a \cdot V_b \cdot \left(\frac{g}{C}\right)^3 \cdot sgn(V_x) \\ \\ V_x(0) = V_{x_0} \qquad \frac{d}{dt}V_x(0) = -\frac{g}{C} \cdot V_y(0) \qquad \frac{d^2}{dt^2}V_x(0) = \left(\frac{g}{C}\right)^2 \cdot V_z(0) \end{cases} \tag{III.13}$$

Afin d'établir les propriétés mathématiques du système (P), il convient de l'adimensionner. Pour ce faire, on opère un changement de variable linéaire et on définit un nouvel opérateur de dérivation temporelle :

$$x := \frac{V_x}{V_b}, \qquad [\dot{\ }] := \frac{C}{g}\frac{d}{dt}[\ ] \tag{III.14}$$

Dans ce cas, le problème (P) d'inconnue $x(t)$ s'écrit :

$$(P) \begin{cases} V_b \left(\frac{g}{C}\right)^3 \dddot{x} + aV_b \left(\frac{g}{C}\right)^3 \ddot{x} + aV_b \left(\frac{g}{C}\right)^3 \dot{x} + aV_b \left(\frac{g}{C}\right)^3 x = aV_b \left(\frac{g}{C}\right)^3 sgn(V_x) \\ \\ x(0) = \frac{V_{x_0}}{V_b} \qquad \dot{x}(0) = -\frac{V_{y_0}}{V_b} \qquad \ddot{x}(0) = \frac{V_{z_0}}{V_b} \end{cases} \tag{III.15}$$

où $V_{y_0} = V_y(0)$ et $V_{z_0} = V_z(0)$. En constatant que le terme $V_b\,(g/c)^3$ est un facteur commun non nul et en redéfinissant les conditions initiales par $x_0 = V_x/V_b$, $y_0 = -V_y/V_b$ et $z_0 = V_z/V_b$, il est possible d'exprimer le problème (P) sous sa forme adimensionnée (P_a) :

$$(P_a)\begin{cases} \dddot{x} + a\cdot\ddot{x} + a\cdot\dot{x} + a\cdot x = a\cdot sgn(x) \\ x(0) = x_0 \qquad \dot{x}(0) = y_0 \qquad \ddot{x}(0) = z_0 \end{cases} \tag{III.16}$$

Il s'agit d'un problème de Cauchy reposant sur une équation différentielle non-linéaire du troisième ordre, non-homogène et à coefficients constants. Le coefficient réel a agit comme un paramètre de contrôle; de lui dépend la stabilité des solutions du problème. Si $a > 0$, tous les coefficients sont positifs; le problème (P_a) est elliptique. Si $a < 0$, le coefficient associé à la dérivée troisième est positif tandis que les autres coefficients sont négatifs; le problème (P_a) devient parabolique. Notons que pour $a = 0$, la solution est non bornée. Quoiqu'il en soit, seul le cas $a > 0$ correspond à une solution physiquement réalisable [82].

Le changement de variable canonique :

$$\begin{cases} x := x \\ y := \dot{x} \\ z := \dot{y} = \ddot{x} \end{cases} \tag{III.17}$$

permet de ramener l'étude de l'équation différentielle de (P_a) à celle, équivalente, d'un système dynamique autonome de trois équations différentielles non-linéaires du premier ordre couplées :

$$(P_a)\begin{cases} \dot{x} = y \\ \dot{y} = z \\ \dot{z} = -a\cdot x - a\cdot y - a\cdot z + a\cdot sgn(x) \end{cases} \tag{III.18}$$

Soient X, $\dot{X}$ et X_o trois vecteurs de $\mathbb{R}^3$ tels que :

$$X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}, \quad \dot{X} = \begin{bmatrix} \dot{x} \\ \dot{y} \\ \dot{z} \end{bmatrix}, \quad X_0 = \begin{bmatrix} x_0 \\ y_0 \\ z_0 \end{bmatrix} \tag{III.19}$$

Soient A la matrice carrée d'ordre 3, B le vecteur de $\mathbb{R}^3$ et $f(X)$ le champ de vecteurs non-linéaires de $\mathbb{R}^3$ définis par :

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -a & -a & -a \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0 \\ -a \end{bmatrix}, \quad f(X) = sgn(x) \tag{III.20}$$

La forme vectorielle du problème (P_a) est donnée par :

$$(P_a)\begin{cases} \dot{X} = A\cdot X + B\cdot f(X) \\ X_0 \end{cases} \tag{III.21}$$

On retombe bien sur l'équation d'état d'un système chaotique en temps-continu autonome de type *double-scroll* (cf. équation III.21 et ligne 5 du tableau III.2).

III.4.3.2.b Caractérisation du système

Les simulations numériques présentées dans cette section ont été réalisées par Fabien Chaillan [82]. Elles ont été calculées sous Matlab (The Mathworks), en utilisant la méthode de Runge-Kutta d'ordre 4.

Comportement du système (P_a) au voisinage de ses points fixes

Afin de prendre en compte l'aspect fini du gain du comparateur VC, on crée le champ de vecteurs $f_\epsilon(X)$ à partir de $f(X)$ en remplaçant la fonction sgn par la fonction non-linéaire η_ϵ définie pour tout $x \in \mathbb{R}$ telle que :

$$f_\epsilon(X) := \begin{bmatrix} \eta_\epsilon(x) \\ 0 \\ 0 \end{bmatrix}, \quad \eta_\epsilon(x) := \begin{cases} -1 & \text{si} \quad x < -\epsilon \\ \dfrac{x}{\epsilon} & \text{si} \quad x \in [-\epsilon,\epsilon[\\ 1 & \text{si} \quad x \geq \epsilon \end{cases} \tag{III.22}$$

Intuitivement, l'application η_ϵ est définie de la sorte car :

$$\lim_{\epsilon \to 0} \eta_\epsilon(x) = sgn(x) \tag{III.23}$$

Soit $F_a(X)$ l'application définissant le champ de vecteurs de $\mathbb{R}^3$ dans $\mathbb{R}^3$ telle que :

$$F_a(X) := A \cdot X + B \cdot f_\epsilon(X) \tag{III.24}$$

Le scalaire a est le paramètre de contrôle du champ de $F_a(X)$. Pour tout réel a et tout $X \in \mathbb{R}^3$, l'application $F_a(X)$ est continue sur $\mathbb{R}^3$. De plus, on démontre que $div\,[F_a(x)] = -a$. Or, la divergence renseigne sur la propriété du champ de vecteurs à contracter ou non les volumes. Ainsi, si $a < 0$, le champs de vecteur $F_a(X)$ est dissipatif, alors que si $a > 0$, $F_a(X)$ est conservatif. Dans le contexte de cette étude, le cas $a \leq 0$ ne présente pas d'intérêt.

Les points fixes d'un système sont les états pour lesquels son champ de vecteurs s'annule. Les points fixes de (P_a) sont donc solutions de $F_a(X) = 0$. Ainsi, on démontre que (P_a) présente trois points fixes p_{-1}, p_0 et p_1, indépendants de a et de coordonnées dans l'espace des phases [82] :

$$p_{-1} = \begin{bmatrix} -1 \\ 0 \\ 0 \end{bmatrix}, \quad p_0 = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \quad p_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \tag{III.25}$$

Nous allons étudier le comportement du système au voisinage de ses points fixes. Qualitativement, un point fixe est dit stable si les trajectoires débutant dans son voisinage y restent indéfiniment. Dans le cas contraire, le point fixe est dit instable. Soit p un point fixe du système (P_a). Afin d'étudier le comportement de (P_a) au voisinage de p, on linéarise l'équation d'état du système autour de p [128] :

$$\begin{aligned} \dot{p} + \dot{\delta_X} &= F_a(p + \delta_X) \\ &\cong F_a(p) + J_{F_a}(p) \cdot \delta_X \end{aligned} \tag{III.26}$$

où δ_X est un vecteur de $\mathbb{R}^3$ représentant une perturbation autour du point p et $J_{F_a}(p)$ la matrice jacobienne 3×3 de l'application $F_a(X)$ calculée au point p :

$$\delta_X := \begin{bmatrix} \delta_x - p_x \\ \delta_y - p_y \\ \delta_z - p_z \end{bmatrix}, \quad J_{F_a}(p) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -a\left(1 - \frac{\prod_\epsilon(x)}{\epsilon}\right) & -a & -a \end{bmatrix} \tag{III.27}$$

où $\prod_\epsilon(x)$ est la fonction non-linéaire définie en annexe B. En retranchant $F_a(p)$ de part et d'autre de l'égalité III.26, on obtient :

$$\dot{\delta_X} = J_{F_a}(p) \cdot \delta_X \tag{III.28}$$

Cette relation décrit, en approximation du premier ordre, la dynamique du système (P_a) au voisinage de p. En d'autres termes, elle régit le circuit équivalent petit signal au point de polarisation p. Par suite, l'intégration du système linéarisé (P_a^l) :

$$(P_a^l) \begin{cases} \dot{\delta_X} = J_{F_a}(p) \cdot \delta_X \\ \delta_{X_0} \end{cases} \tag{III.29}$$

conduit à la solution :

$$\delta_X(t) = e^{J_{F_a}(p)t} \cdot \delta_{X_0} \tag{III.30}$$

Si $J_{F_a}(p)$ est diagonalisable, la résolvante $e^{J_{F_a}(p)t}$ du problème est une matrice telle que :

$$e^{J_{F_a}(p)t} = \Lambda e^{Dt} \Lambda^{-1} \tag{III.31}$$

où D est la matrice diagonale contenant les valeurs propres de $J_{F_a}(p)$ et Λ la matrice de passage de la base associée à $J_{F_a}(p)$ vers la base associée à D. La matrice Λ a pour colonne les vecteurs propres de $J_{F_a}(p)$. De plus, si A est diagonalisable avec des valeurs propres de multiplicité 1, alors la solution $\delta_X(t)$ s'écrit, dans la base orthogonale $\{V_i\}_{i=1\ldots3}$ formée des vecteurs propres de $J_{F_a}(p)$:

$$\delta_X(t) = \beta_1 e^{\lambda_1 t} V_1 + \beta_2 e^{\lambda_2 t} V_2 + \beta_2 e^{\lambda_2 t} V_2 \tag{III.32}$$

où $(\beta_1; \beta_2; \beta_3)$ sont des vecteurs de R_*^3 dépendant de a et de δ_{X_0}. Autrement dit, la solution est une combinaison linéaire d'exponentielles complexes pour lesquelles :

$$\left| e^{\lambda_j t} \right| = \left| e^{[Re(\lambda_j) + i \cdot Im(\lambda_j)]t} \right| < e^{Re(\lambda_j)}, \quad \forall j \in \{1, \ldots, 3\} \tag{III.33}$$

Ainsi, lorsque p est un point d'équilibre du système, les valeurs propres du système linéarisé autour de p renseignent sur la stabilité du système au voisinage de p [128]. Dans une direction donnée, la perturbation initiale δ_{X_0} s'amortie, stagne ou s'amplifie au cours du temps selon que la partie réelle de la valeur propre de $J_{F_a}(p)$ correspondant à cette direction est respectivement négative, nulle ou positive. Par définition, les valeurs propres de $J_{F_a}(p)$ sont les racines λ de l'équation caractéristique :

$$det\left[J_{F_a}(p) - \lambda \cdot I\right] = 0 \tag{III.34}$$

où I est la matrice identité. Ainsi, si aucune des valeurs propres de $J_{F_a}(p)$ n'a de partie réelle positive et, si celles dont la partie réelle est nulle sont des zéros simples de III.34, alors le point d'équilibre p

est stable. Si de plus, les parties réelles de toutes les valeurs propres sont strictement négatives, le point d'équilibre est asymptotiquement stable. On parle alors de « puits », car toutes les trajectoires proches de ce point convergent vers lui. Si l'une des valeurs propres possède une partie réelle positive, le point est instable. Enfin, si toutes les valeurs propres ont une partie réelle positive, le point est généralement qualifié de « source ».

En remarquant que $J_{F_a}(p_{-1}) = J_{F_a}(p_1) = A$, l'étude des points fixes p_{-1} et p_1 de $((P_a))$ peut être menée conjointement. Par définition, les valeurs propres de A sont solutions de :

$$det\,(A - \lambda \cdot I) = 0 \;\Leftrightarrow\; \lambda^3 + a \cdot \lambda^2 + a \cdot \lambda + a = 0 \tag{III.35}$$

La résolution de ce polynôme de degré trois permet de démontrer que, pour tout $a \neq 0$, la matrice A présente trois valeurs propres : une réelle et deux complexes conjuguées ($\lambda_1 \in \mathbb{R}$, $\lambda_2 \in \mathbb{C} = \alpha + i\omega$ et $\lambda_3 \in \mathbb{C} = \overline{\lambda_2}$) [82]. Leurs expressions sont données en annexe C.1. Les vecteurs propres associés permettent d'avoir une indication sur la direction du flot au voisinage des points fixes. Dans le cas des points p_{-1} et p_1, les vecteurs propres V_1, V_2 et V_3 respectivement associés aux valeurs propres λ_1, λ_2 et λ_3 sont déterminés, $\forall j \in \{1, \ldots, 3\}$, par la relation d'équivalence :

$$\begin{aligned} [V_j \text{ vecteur propre de } A] \quad &\Leftrightarrow \quad [V_j \in Ker\,(A - \lambda \cdot I)] \\ &\Leftrightarrow \quad [V_j \text{ solution de } (A - \lambda \cdot I)\,X = 0,\ \forall X \neq 0] \end{aligned} \tag{III.36}$$

Or, pour tout $X \neq 0$ de l'espace des phases :

$$(A - \lambda \cdot I)\,X = 0 \;\Leftrightarrow\; \begin{cases} y = \lambda_j \cdot x \\ z = \lambda_j \cdot y = \lambda_j^2 \cdot x \\ -\underbrace{\left(a + a \cdot \lambda_j + a \cdot \lambda_j^2 + \lambda_j^3\right)}_{=0} x = 0 \end{cases} \tag{III.37}$$

car λ_j est naturellement solution du polynôme caractéristique. Les solutions de cette équation sont de la forme $\mathbb{R}\left[1; \lambda_j; \lambda_j^2\right]$. Ainsi, les vecteurs propres regroupés en colonne constituent la matrice de passage Λ :

$$\Lambda \;=\; \begin{bmatrix} | & | & | \\ V_1 & V_2 & V_3 \\ | & | & | \end{bmatrix} \;=\; \begin{bmatrix} 1 & 1 & 1 \\ \lambda_1 & \lambda_2 & \lambda_3 \\ \lambda_1^2 & \lambda_2^2 & \lambda_3^2 \end{bmatrix} \tag{III.38}$$

A la valeur propre λ_1 correspond le vecteur propre V_1, et aux valeurs propres complexes conjuguées λ_2 et λ_3 correspond le plan engendré par les vecteurs $Re(V_2)$ et $Im(V_2)$.

Enfin, l'inversion de la matrice Λ permet, via la relation III.32, de déterminer, pour une condition initiale δ_{X_0}, la solution $\delta_X(t)$ du système linéarisé autour des points fixes $p_{\pm 1}$. Son expression est donnée dans l'annexe C.1.

Les courbes représentatives des applications qui à tout $a \in \mathbb{R}$ font correspondre les parties réelles et imaginaires des valeurs propres $\{\lambda_i\}_{i=1\cdots3}$ de A sont tracées sur la figure III.11.

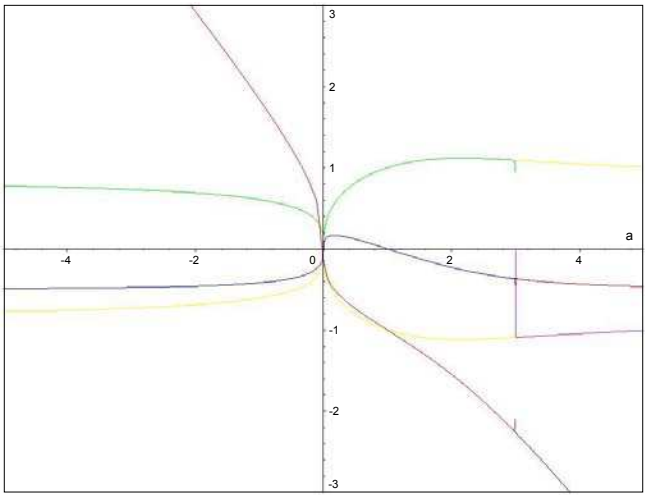


Fig. III.11 – *Courbes représentatives des parties réelles et imaginaires des valeurs propres de A en fonction de a : $\lambda_1(a)$ (rouge), $Re\,[\lambda_2(a)]$ (bleu), $Im\,[\lambda_2(a)]$ (vert), $Im\,[\lambda_3(a)]$ (jaune si $a < 3$, magenta sinon) [82].*

Comme le montre la figure III.11, la position relative des racines change aux points $a = 0$ et $a = 3$:

- Si $a < 0$, alors $\lambda_1 > 0$ et $Re\,[\lambda_2(a)] < 0$ avec $|\lambda_1| > |\lambda_2|$, par conséquent, les points fixes sont conjointement instables. De fait, dans cette zone, les volumes sont en extension (si $a < 0$, $div\,[F_a(X)] > 0$).
- Si $a \in]0; 1[$, alors $\lambda_1 < 0$ et $Re\,[\lambda_2(a)] > 0$, par conséquent, les points fixes sont des points selles de type II instables. Le cas $a = 0.7$ est représenté sur la figure III.12.

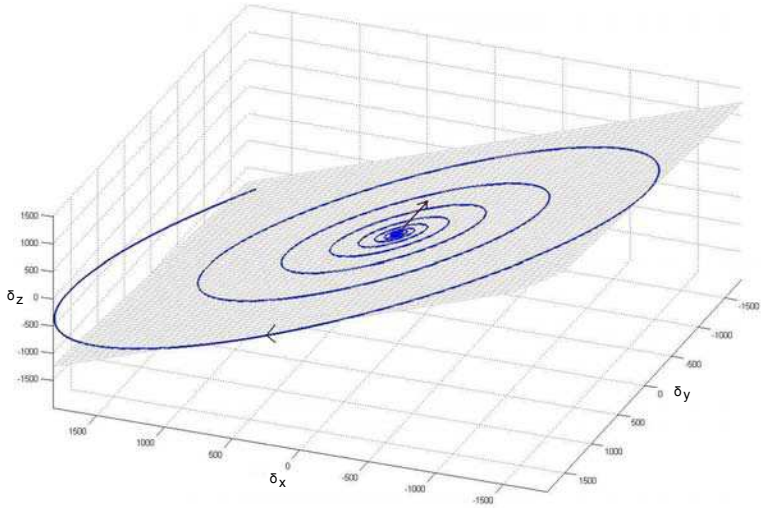


Fig. III.12 – *Portrait de phase du système linéarisé (P_a^l) au voisinage de $p_{\pm1}$ pour $a = 0.7$ [82].*

∞ Si $a = 1$, alors $\lambda_1 < 0$ et $[\lambda_2(a)] = 0$. Dans ce cas, les trajectoires tendent à s'enrouler autour d'un cycle limite qui est un cercle de centre $p_{\pm 1}$ (cf. figure III.13).

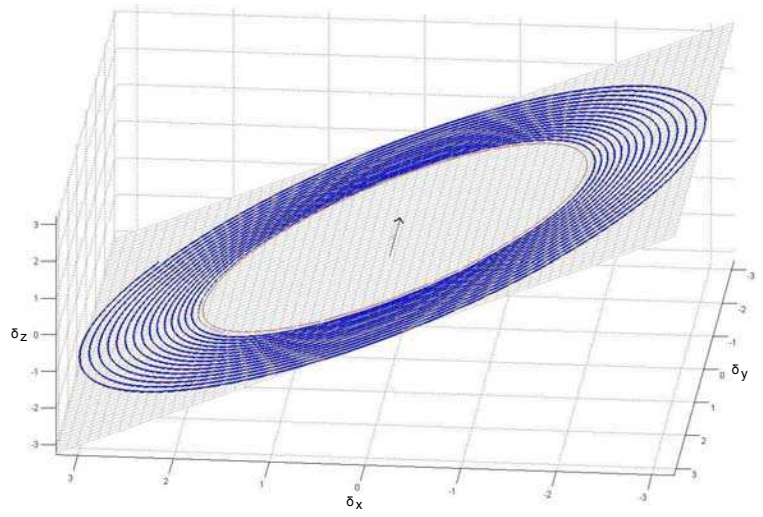


Fig. III.13 – *Portrait de phase du système linéarisé* (P_a^l) *au voisinage de* $p_{\pm 1}$ *pour* $a = 1$ *[82].*

∞ Si $a \in]1; 3]$, alors $\lambda_1 < 0$ et $Re\,[\lambda_2(a)] < 0$ avec $|\lambda_1| > |\lambda_2|$. Les deux valeurs propres sont à parties réelles négatives, par conséquent, les points fixes sont des attracteurs stables : ils attirent asymptotiquement les trajectoires. Le cas $a = 2$ est représenté sur la figure III.14.

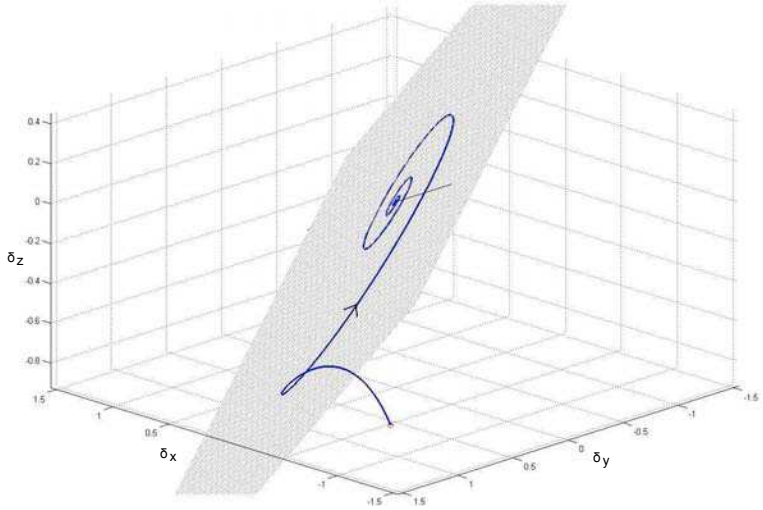


Fig. III.14 – *Portrait de phase du système linéarisé* (P_a^l) *au voisinage de* $p_{\pm 1}$ *pour* $a = 2$ *[82].*

∞ Enfin, si $a > 3$, alors $\lambda_1 < 0$ et $Re\,[\lambda_2(a)] < 0$ avec $|\lambda_1| < |\lambda_2|$. Par conséquent, le comportement est identique au cas précédent. Le cas $a = 4$ est illustré sur la figure III.15.

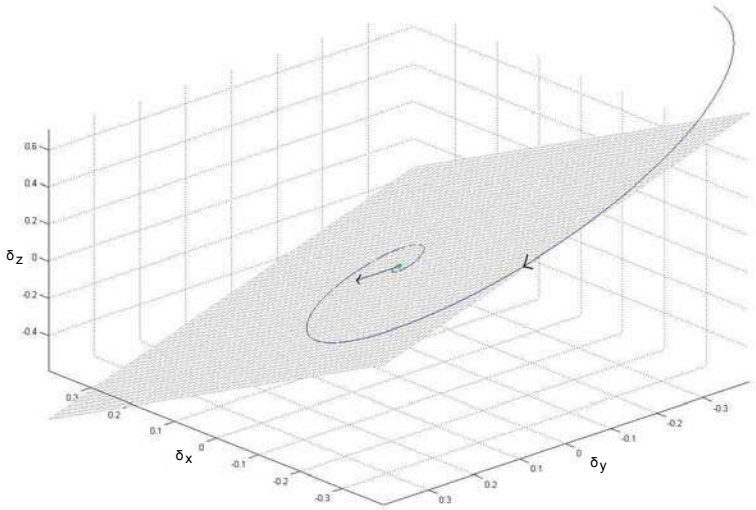


Fig. III.15 – *Portrait de phase du système linéarisé* (P_a^l) *au voisinage de* $p_{\pm 1}$ *pour* $a = 4$ *[82].*

Pour tout point fixe $X = [x,y,z]^T$ de l'espace des phases tel que $|x| < \epsilon$, la matrice Jacobienne de $F_a(X)$ évaluée au point p_0 s'écrit :

$$J_{F_a}(P_0) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -a\left(1-\frac{1}{\epsilon}\right) & -a & -a \end{bmatrix} = A_\epsilon \tag{III.39}$$

Les valeurs propres de A_ϵ sont solutions de :

$$\lambda^3 + a \cdot \lambda^2 + a \cdot \lambda + a\left(1 - \frac{1}{\epsilon}\right) = 0 \tag{III.40}$$

Par résolution de ce polynôme du troisième degré, on démontre que pour tout $a \neq 0$, la matrice A_ϵ présente trois valeurs propres : une réelle et deux complexes conjuguées ($\lambda_1 \in \mathbb{R}$, $\lambda_2 \in \mathbb{C} = \alpha + i\omega$ et $\lambda_3 \in \mathbb{C} = \overline{\lambda_2}$) [82]. Leurs expressions sont données en annexe C.2. Les courbes représentatives des applications qui à tout $a \in \mathbb{R}$ font correspondre les parties réelles et imaginaires des valeurs propres $\{\lambda_i\}_{i=1\cdots 3}$ de A_ϵ sont tracées sur la figure III.16 pour $\epsilon = 0.1$.

La figure III.16 permet d'affirmer que pour tout $a \in]0;3[$, la valeur propre réelle est strictement positive, tandis que la partie réelle des valeurs propres complexes est négative avec $|\lambda_1| > |\alpha|$. De plus, la partie imaginaire des valeurs propres complexes ne s'annule pas. Par conséquent, le point d'équilibre p_0 est un point selle de type I instable.

En conclusion, l'étude locale du problème (P_a) a permis d'établir que, pour $a \in]0;1[$, le système dynamique présente simultanément trois point fixes hyperboliques instables : deux points selle de type II en p_{-1} et p_1 et un point selle de type I en p_0. De plus, cet intervalle est le seul sur lequel le système vérifie la première hypothèse du théorème de Shil'nikov [161] (i.e., $|\lambda_1| > |\alpha|$), condition sine qua non d'un comportement chaotique.

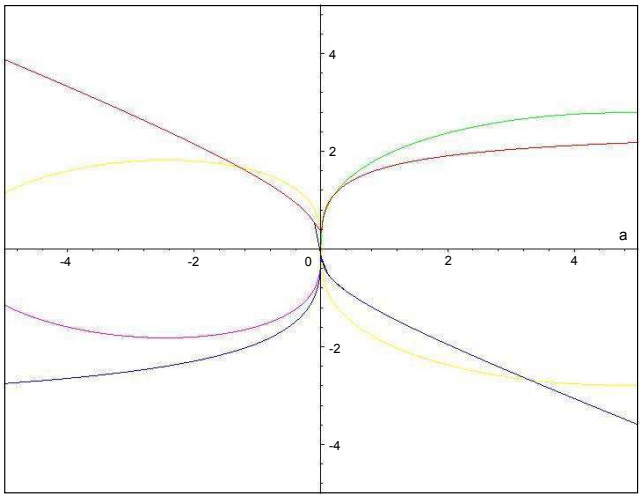


Fig. III.16 – *Parties réelles et imaginaires des valeurs propres de A_ϵ pour $\epsilon = 0.1$: $\lambda_1(a)$ (rouge), $Re\,[\lambda_2(a)]$ (bleu), $Im\,[\lambda_2(a)]$ (vert), $Im\,[\lambda_3(a)]$ (jaune si $a < 0$, magenta sinon) [82].*

Mise en évidence du chaos dans le système (P_a)

Le diagramme de bifurcation du système (P_a) permet de déterminer empiriquement l'intervalle du paramètre de contrôle a menant à un comportement chaotique. Il s'agit d'une représentation graphique en dimension deux où les valeurs du paramètre de contrôle sont portées en abscisse et une valeur caractérisant l'état du système en régime stationnaire est portée en ordonnée. Le principe algorithmique est le suivant :

- Le paramètre de contrôle a est discrétisé sur l'intervalle $a \in]0;3]$ avec le plus petit pas Δ_a possible (i.e., autorisé par la puissance de calcul disponible).
- Pour chaque valeur de a, on effectue N calculs de trajectoires, issus d'autant de conditions initiales, jusqu'à un temps où le régime stationnaire est suffisamment installé. N'est retenu que la partie de la trajectoire pour laquelle $t > t_p$, temps à partir duquel le régime permanent est supposé atteint.
- La valeur moyenne de la première composante de chacune des N sous-trajectoires est calculée puis portée en ordonnée.

Ce processus a été appliqué au problème (P_a) pour des trajectoires de 600 échantillons présentant un pas de discrétisation de 0.05 et $N = 50$. Compte tenu de la puissance de calcul disponible au moment de cette étude, ces valeurs offrent un bon compromis entre précision et temps de simulation. Le diagramme résultant est représenté sur les figures III.17 et III.18 pour, respectivement, $a \in]0;3]$ et $a \in]0;1]$.

Les comportements observés sont analogues à ceux rencontrés lors de l'étude locale du système. En effet, trois tendances se dégagent :

- Si $a \in]0;0.4]$, les trajectoires divergent rapidement. Le cas $a = 0.3$ est illustré sur la figure III.19.
- Si $a \in]0.4;0.99]$, la répartition des valeurs est désordonnée autour des trois points fixes, tout en restant borné; le système évolue de façon chaotique. Le cas $a = 0.5$ apparaît sur la figure III.20.

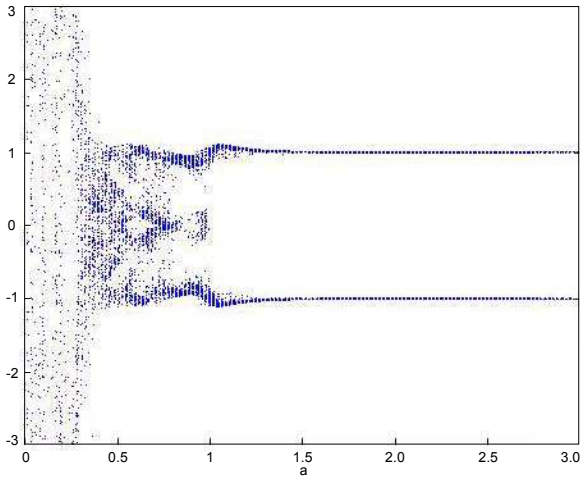


Fig. III.17 – *Diagramme de bifurcation du système* (P_a) *pour* $a \in]0;3]$ *[82].*

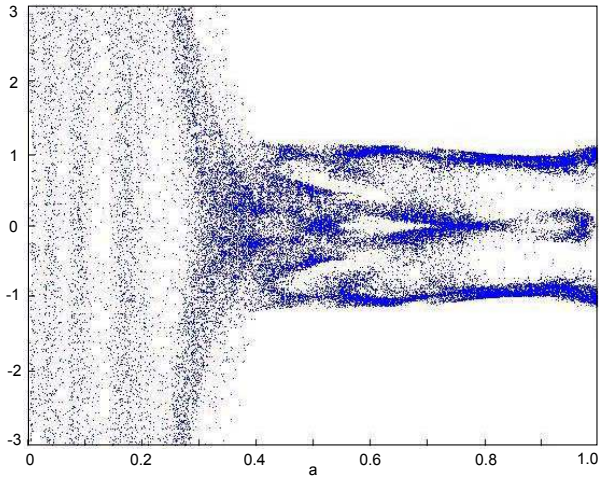


Fig. III.18 – *Diagramme de bifurcation du système* (P_a) *pour* $a \in]0;1]$ *[82].*

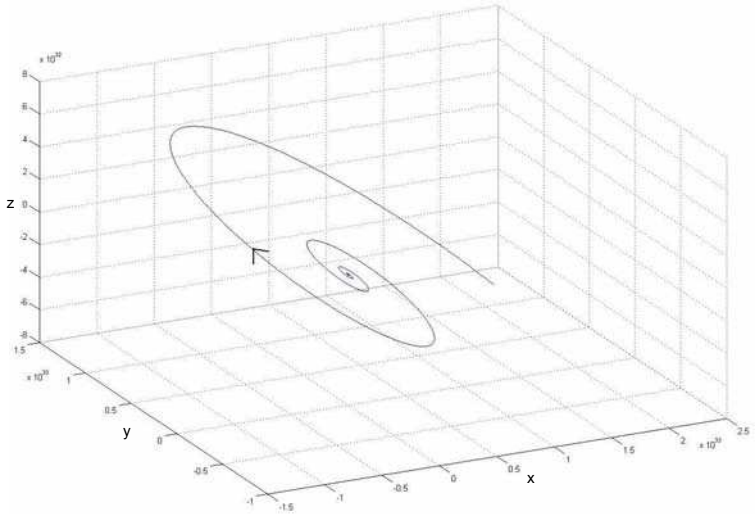


Fig. III.19 – *Portrait de phase du système* (P_a) *pour* $a = 0.3$ *[82].*

∞ Enfin, si $a > 1$, les trajectoires convergent systématiquement vers la première coordonnée des points fixes $p_{\pm 1}$ (i.e., $x = \pm 1$). Deux trajectoires réalisées pour $a = 1.1$ sont illustrées sur la figure III.21.

Ainsi, le système (P_a) présente un comportement chaotique lorsque a appartient à l'intervalle $[0.4; 0.99[$. Cette plage de valeur est légèrement plus large que celle annoncée dans la littérature électronicienne [126], à savoir : $[0.48; 0.98]$. Cet écart s'explique par les différences existantes entre résolution numérique et simulation électrique [82]. Dans l'implémentation proposée par Radwan & al., le paramètre a correspond à un ratio de taille de capacités [147]. Pour limiter l'influence des déviations du procédé de fabrication, il est préférable de fixer a au centre de la plage chaotique. Le milieu de la plage déterminée numériquement est approximativement égal à 0.7.

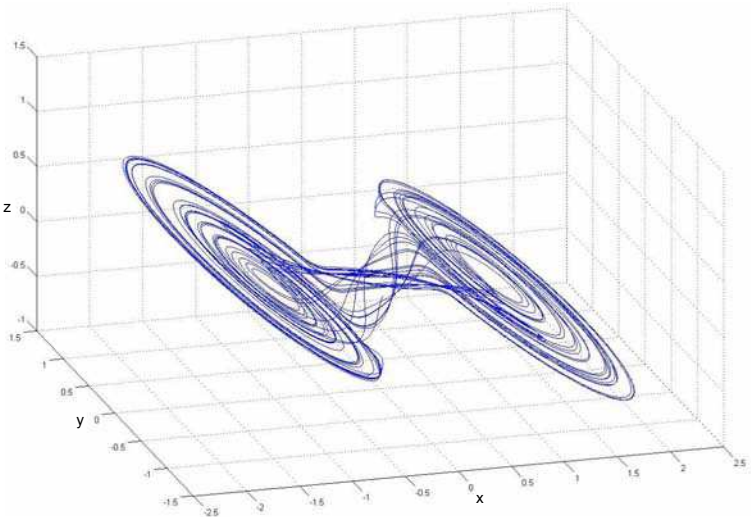


Fig. III.20 – *Portrait de phase du système* (P_a) *pour* $a = 0.5$ *[82].*

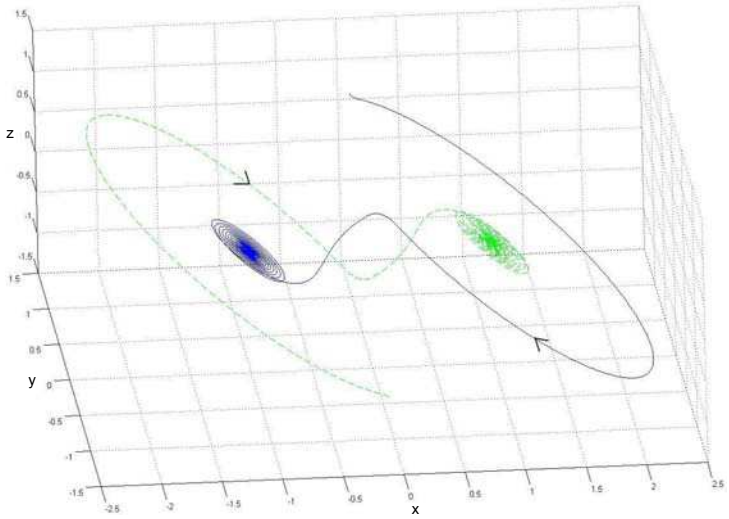


Fig. III.21 – *Portraits de phase du système* (P_a) *pour* $a = 1.1$ *[82].*

Afin de confirmer le caractère chaotique du système lorsque $a = 0.7$, nous allons étudier les exposants de Lyapunov du système pour cette valeur. Ces derniers mettent en évidence la sensibilité d'un système dynamique aux conditions initiales. Ils permettent de mesurer au cours du temps la distance séparant deux trajectoires issues de deux conditions initiales distinctes. Lorsque le système est chaotique, la distance entre chacune des trois composantes des deux trajectoires évolue de façon exponentielle. Si $d_x(0)$ est la distance entre les deux premières coordonnées des deux conditions initiales, alors, au temps fixé t_0, la distance $d_x(t_0)$ est telle qu'il existe un coefficient scalaire L_x vérifiant :

$$d_x(t_0) \cong e^{L_x t_0} d_x(0) \tag{III.41}$$

ce qui amène à définir asymptotiquement L_x et, par analogie, L_y et L_z :

$$\begin{cases} L_x & := & \lim\limits_{t\to+\infty} \dfrac{1}{t} \ln\left(\dfrac{d_x(t)}{d_x(0)}\right) \\ L_y & := & \lim\limits_{t\to+\infty} \dfrac{1}{t} \ln\left(\dfrac{d_y(t)}{d_y(0)}\right) \\ L_z & := & \lim\limits_{t\to+\infty} \dfrac{1}{t} \ln\left(\dfrac{d_z(t)}{d_z(0)}\right) \end{cases} \tag{III.42}$$

L_x, L_y et L_z sont les exposants de Lyapunov associés au problème (P_a). En particulier, si un des exposants est positif, un autre nul et le troisième négatif, alors le système évolue de manière chaotique [162]. Pour $a = 0.7$, l'estimation des exposants donne [82] : $L_x \approx 0.11$, $L_y \approx -0{,}002$ et $L_z \approx -0{,}8$. Ce triplet peut être interprété comme une signature de la forme $(+; 0; -)$, ce qui confirme le caractère chaotique du système pour cette valeur. De plus, dans ce cas, le système vérifie simultanément les deux hypothèses du théorème de Shil'nikov [82]. Par conséquent, lorsque $a = 0.7$, le système (P_a) est bien chaotique.

III.4.3.2.c Réalisation et simulation du circuit en technologie CMOS

Le circuit de l'oscillateur chaotique (CO) est représenté sur la figure III.22. Dans cette réalisation, les cellules du schéma-bloc de la figure III.10 reposent exclusivement sur des inverseurs en technologie CMOS. L'inverseur est une cellule entièrement adaptée à la réalisation des structures gm-C [163]. En effet, celui-ci présente une plage de fonctionnement *rail-to-rail* en entrée et en sortie De plus, sa transconductance est linéaire sur la quasi-totalité de sa plage de fonctionnement en entrée, ce qui n'est généralement pas le cas des OTA. En contrepartie, un inverseur est auto-polarisé, par conséquent, la valeur de sa transconductance est difficilement maitrisable et son taux de réjection d'alimentation est relativement bas. Néanmoins, l'injection du bruit d'alimentation augmente nécessairement l'entropie du flux, à condition toutefois que l'oscillateur reste en mode chaotique malgré les perturbations. En contrepartie, l'utilisation d'OTA permettrait d'ajuster à la volée la fréquence d'oscillation et, de fait, faciliterait la mise en œuvre de boucles de contre-réactions. Cependant, à performances fréquentielles équivalentes, les OTA nécessitent un courant d'alimentation plus élevé et une surface plus importante.

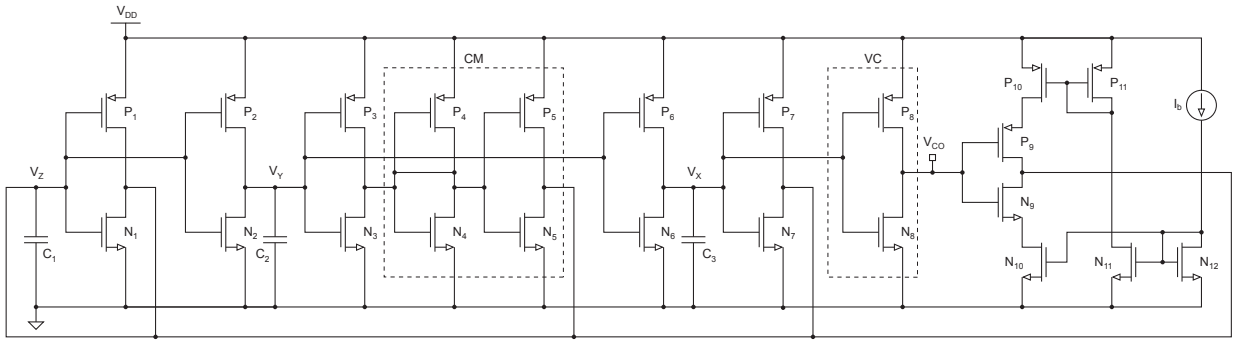


Fig. III.22 – *Circuit de l'oscillateur chaotique (CO) en technologie CMOS [147].*

Dans le circuit de la figure III.22, les inverseurs sont supposés identiques de sorte que $g_1 = g_2 = g_3 = g$. Les composants C_1, C_2 et C_3 sont des capacités MOS de type poly1-poly2, dont les dimensions sont

telles que $a = C/C_1$ avec $C_2 = C_3 = C$. Chacun des noeuds V_X, V_Y et V_Z attaque deux inverseurs. Cet équilibre permet de limiter l'influence des capacités parasites sur la valeur de a. On suppose que les transistors des inverseurs sont tous de même longueur : $L_N = L_P = L$. Pour que la tension d'autopolarisation de chaque nœud du circuit se stabilise aux milieux de la plage d'alimentation, chaque inverseur doit être dimensionné tel que :

$$\begin{aligned} I_{DS_N}|_{V_{GS}=\frac{V_{DD}}{2},V_{DS}=\frac{V_{DD}}{2}} &= I_{DS_P}|_{V_{GS}=\frac{V_{DD}}{2},V_{DS}=\frac{V_{DD}}{2}} \\ \Leftrightarrow \quad \frac{W_P}{W_N} &= \frac{\mu_N \left(\frac{V_{DD}}{2} - V_{T_N}\right)^2 \left(1 + \lambda_N \frac{V_{DD}}{2}\right)}{\mu_P \left(\frac{V_{DD}}{2} - V_{T_P}\right)^2 \left(1 + \lambda_P \frac{V_{DD}}{2}\right)} := \alpha \end{aligned} \tag{III.43}$$

Par conséquent, si l'on pose $W_N = W$, la condition d'équilibrage III.43 impose de prendre $W_P = \alpha \cdot W$. Par suite, la transconductance d'un inverseur est donnée par :

$$g = gm_N + gm_P \cong C_{ox} \cdot \frac{W}{L} \left[\mu_N \cdot \left(\frac{V_{DD}}{2} - V_{T_N}\right) + \alpha \cdot \mu_P \left(\frac{V_{DD}}{2} - V_{T_P}\right)\right] \tag{III.44}$$

Lorsque l'oscillateur fonctionne en mode sinusoïdal, la pulsation des oscillations (ω_0) est égale à g/C. En mode chaotique, le spectre fréquentiel s'étale autour de ω_0 [146]. Ainsi, la donnée de ω_0 permet de fixer le rapport g/C. On détermine ensuite g et C par le biais d'un compromis entre consommation, surface et fiabilité. A pulsation fixée, une diminution de C permet de réduire la surface et la consommation du circuit. Cependant, elle se traduit également par une augmentation de la sensibilité du paramètre a aux capacités parasites et aux déviations du procédé de fabrication. Enfin, la donnée des paramètres technologiques permet, via les relations III.43 et III.44, de déterminer W_N puis W_P. Les bassins d'attraction sont centrés sur les points fixes p_{-1} et p_1. D'après les changements de variables III.10 et III.14, leurs coordonnées respectives dans le plan $(V_X; V_Y)$ sont $(V_{DD}/2 - V_b; V_{DD}/2)$ et $(V_{DD}/2 + V_b; V_{DD}/2)$ ou $V_b = I_b/g$. Concernant les transistors des miroirs véhiculant I_b, leurs dimensions font l'objet d'un compromis appariement/surface.

Paramètre	Valeur		Unité
	STM $0.18\ \mu m$	AMS $0.35\ \mu m$	
$L := (L_i)_{i\in\{1,\ldots,9\}}$	0.36	0.7	μm
$L_{N_{10}}, L_{N_{11}}, L_{P_{10}}, L_{P_{11}}, L_{P_{12}}$	2	2	μm
$W := (W_{N_i})_{i\in\{1,\ldots,9\}}$	1	1.2	μm
$\alpha \cdot W := (W_{P_i})_{i\in\{1,\ldots,9\}}$	2.4	3.2	μm
$W_{N_{10}}, W_{N_{11}}, W_{N_{12}}$	10	40	μm
$W_{P_{10}}, W_{P_{11}}$	30	40	μm
C_1	1	0.75	pF
$C := C_2 = C_3$	0.7	0.5	pF
I_b	24	80	μA

Tab. III.3 – *Dimensions des éléments constitutifs de l'oscillateur chaotique (CO).*

L'oscillateur chaotique de la figure III.22 a été simulé avec les paramètres technologiques des procédés STM CMOS $0.18\ \mu m$ et AMS CMOS $0.35\ \mu m$. Dans les deux cas, le circuit a été dimensionné de sorte que a soit proche de 0.7 et que la fréquence du signal V_{CO} (f_{co}) soit supérieure à $10\ MHz$ (cf. tableau III.3). Puisque le détecteur de front (ED) déclenche sur fronts montants et descendants (cf. figure III.8), cette valeur de f_{co} est suffisante pour atteindre la fréquence de rafraîchissement f_j spécifiée par le cahier des charges (i.e. $20\ MHz$, cf. tableau III.1). Afin de limiter l'influence des perturbations (bruit d'alimentation, bruit substrat, etc.), la dynamique de l'attracteur doit représenter une fraction importante de la plage d'alimentation. Les valeurs rassemblées dans les tableaux , II.3 et III.3 permettent, via la relation III.44, d'évaluer les caractéristiques des oscillateurs. Ainsi, pour la technologie STM, on obtient $g \approx 280\ \mu S$, $V_b \approx 86\ mV$ et $f_0 = \omega_0 (2\pi)^{-1} \approx 45.4\ MHz$, tandis qu'en technologie AMS, les calculs donnent $g \approx 285\ \mu S$, $V_b \approx 280\ mV$ et $f_0 \approx 63.2\ MHz$.

Les portraits de phase obtenues sous Virtuoso sont représentés sur les figures III.23 (technologie STM) et III.24 (technologie AMS). Comme prévu, les attracteurs sont centrés au milieu de la plage d'alimentation. La position relative des bassins d'attraction permet de déterminer les valeurs simulées de V_b. Dans les deux cas, les valeurs simulées sont proches des valeurs théoriques établies précédemment (erreur relative $< 6\%$).

Les caractéristiques simulées de l'oscillateur chaotique sont rassemblées dans le tableau III.4. Dans la technologie STM, la fréquence moyenne $\overline{f_{co}}$ du signal V_{CO} atteint $20.8\ MHz$, la dynamique de l'attracteur suivant V_X s'étend sur presque $400\ mV$ et la consommation totale du circuit reste inférieure à $0.49\ mW$ ($270\ \mu A$ sous $1.8\ V$). Dans la technologie AMS, la fréquence moyenne $\overline{f_{co}}$ est approximativement égale à $15.3\ MHz$, l'amplitude pic-pic maximum de V_X est d'environ $1.2\ V$ et la consommation atteint $2.95\ mW$ ($894\ \mu A$ sous $3.3\ V$). En définitive, la technologie STM permet d'atteindre un meilleur rapport performance-consommation.

Paramètre	Valeur		Unité
	STM $0.18\ \mu m$	AMS $0.35\ \mu m$	
Valeur moyenne de f_{co}.	20.8	15.3	MHz
Variation maximum de $\overline{f_{co}}$ en PVT.	15	19	$\%$
Amplitude pic-pic maximum de V_X	0.4	1.2	V
Consommation moyenne.	0.49	2.95	mW
Temps de démarrage.	< 120	< 50	ns

Tab. III.4 – *Caractéristiques simulées de l'oscillateur chaotique (CO).*

Afin de vérifier la robustesse du mode chaotique au bruit d'alimentation, la génération de l'attracteur a été simulée pour deux types de signaux V_{DD} : le signal $V_{DD}(t)$ bruité par l'activité de la charge sous $V_{PS} = 5\ V$ (cf. figure III.25) et, plus extrême, un signal $V_{DD}(t)$ impulsionnel périodique de fréquence $10\ MHz$ et d'amplitude $300\ mV$ comprise entre $1.5\ V$ et $1.8\ V$ (cf. figure III.26). Les portraits de phases résultants sont représentés, respectivement, sur les figures III.25 et III.26. Dans les deux cas, l'attracteur se translate au rythme des variations de V_{DD}, sans que les perturbations n'endiguent sa formation. En revanche, au-delà d'une certaine amplitude du signal impulsionnel ($\approx 360\ mV$), l'oscillateur quitte le mode chaotique pour un cycle limite (cf. § III.4.3.2.b). Néanmoins, une carte à puce est généralement désactivée par son système de surveillance bien avant que ce seuil ne soit atteint.

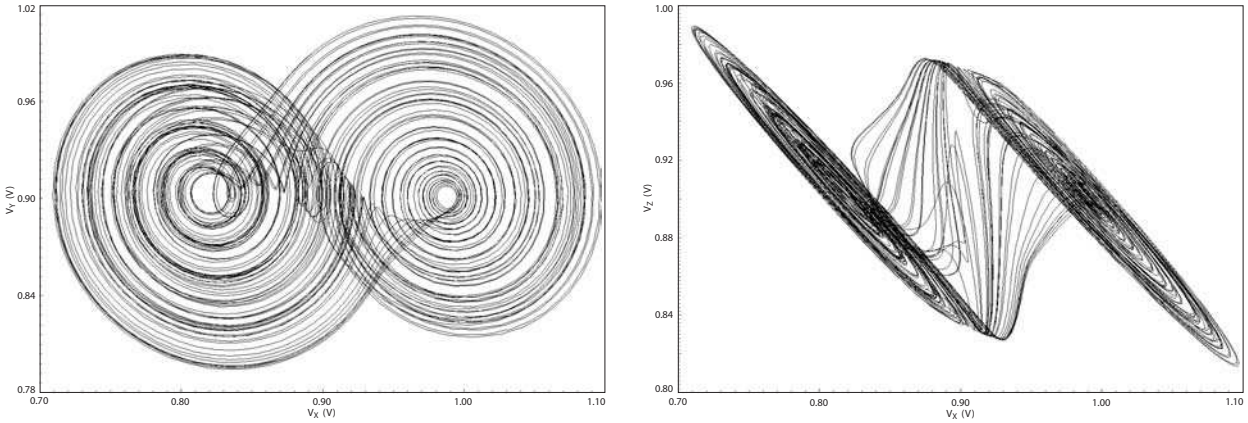


Fig. III.23 – *Projections sur les plans (V_X;V_Y) et (V_X;V_Z) de la simulation en technologie STM ($a \approx 0.7$).*

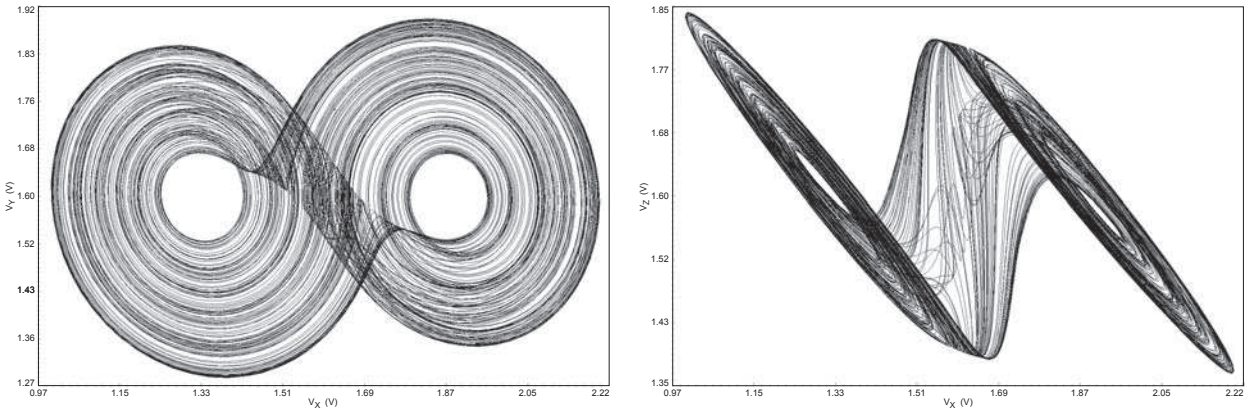


Fig. III.24 – *Projections sur les plans (V_X;V_Y) et (V_X;V_Y) de la simulation en technologie AMS ($a \approx 0.67$).*

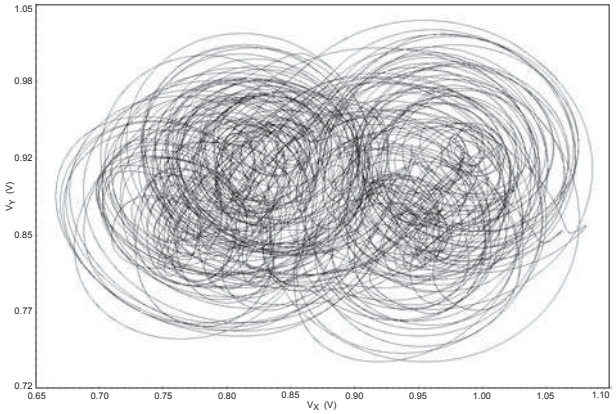


Fig. III.25 – *Portrait de phase V_Y=$f(V_X)$ obtenu via un signal d'alimentation bruité (STM, $a = 0.7$).*

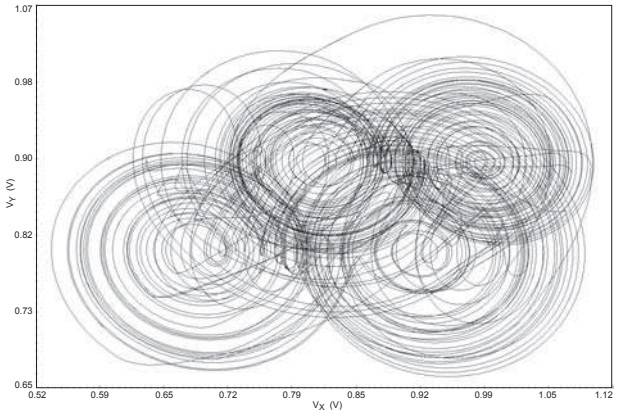


Fig. III.26 – *Portrait de phase V_Y=$f(V_X)$ obtenu via une alimentation impulsionnelle (STM, $a = 0.7$).*

III.4.3.2.d Dessin des masques en technologie AMS $0.35\ \mu m$

A notre connaissance, le circuit présenté au paragraphe précédent n'a jamais été fabriqué sous la forme d'un circuit intégré monolithique. Or, de toutes les cellules constitutives du générateur proposé, l'oscillateur chaotique est de loin le plus sensible aux variations des paramètres technologiques. Afin de valider expérimentalement les résultats obtenus en simulation, nous avons conçu un prototype en technologie AMS CMOS $0.35\ \mu m$. Ce dernier a été réalisé dans le cadre d'une opération multi-projets menée au sein du laboratoire d'accueil. Il a été fabriqué par l'intermédiaire du service CMP, sous la référence A35C6_4-L2MP_PROTO. Le dessin des masque (fichier GDSII) a été réalisé sous l'environnement Layout-XL de la plateforme Cadence Virtuoso. La vérification du *layout* (DRC, extraction et LVS) a été effectuée à l'aide des outils Assura et Diva. Enfin, le circuit rétro-annoté a été simulé avec Spectre (simulations post-*layout*).

Le schéma-bloc du circuit de test est représenté sur la figure III.27. Il est constitué d'un oscillateur chaotique (CO), de trois suiveurs de tension analogiques (VF), de deux *buffers* (Buf_0 et Buf_1) et d'une référence de courant compensée en température (Iref). Le rôle des suiveurs et des *buffers* est de transmettre les signaux V_X, V_Y, V_Z et V_{CO} vers des plots métalliques (les « *pads* ») destinés à accueillir les micropointes d'un banc de mesure. Pour se faire, leur bande passante doit englober la majorité du spectre des signaux chaotiques et leur capacité parasite d'entrée doit rester négligeable devant C. La référence de courant repose sur le circuit de la figure II.51 (cf. § II.5.2.4). Elle délivre les courants de polarisation destinés à l'oscillateur chaotique (I_b) et aux suiveurs. Enfin, le bit de contrôle (PD pour (« *Power Down* ») permet d'activer l'oscillateur chaotique lorsque le courant I_b a atteint son régime permanent.

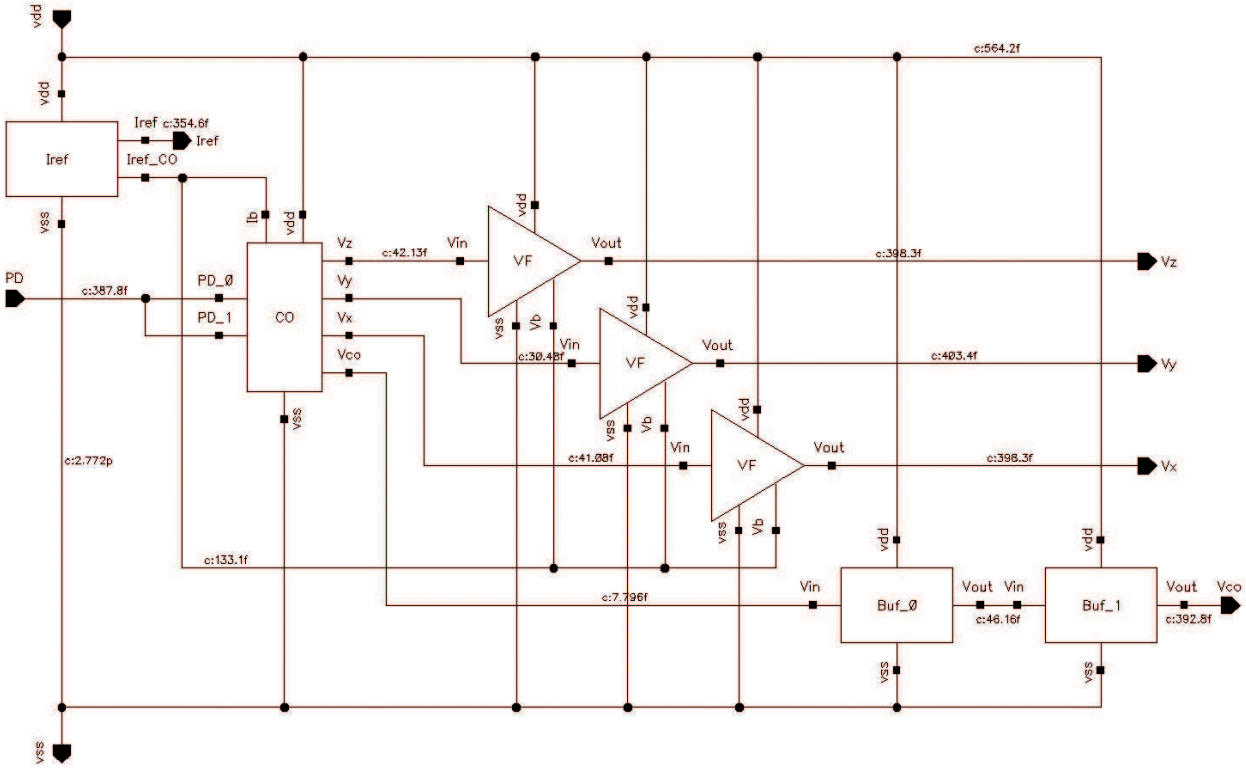


Fig. III.27 – *Schéma-bloc du circuit de test.*

Les vues schéma et *layout* des cellules du circuit de test sont représentées sur les figures suivantes. Les valeurs des capacités parasites extraites ont été retro-annotées sur les vues schémas (« *back-annotation* » : lettre « c » suivie de la valeur de la capacité parasite associée au nœud correspondant). Chaque *layout* est dessiné suivant des règles visant, d'une part, à maximiser la fiabilité et les performances et d'autre part, à minimiser la sensibilité aux déviations locales et globales du procédé de fabrication :

- ∞ Les composants requérant un appariement précis sont découpés en éléments unitaires identiques, de sorte que les variations globales aient des répercutions identiques sur chacun d'entre eux [118].
- ∞ Afin de limiter l'influence des fluctuations locales, les dimensions des éléments unitaires sont prises grandes par rapport aux tailles minimales de la technologie .
- ∞ Un élément compact subit des déviations plus uniformes en tout point de sa structure. Pour cette raison, l'aspect ratio des éléments unitaires est pris aussi faible que possible (i.e., proche de l'unité). Pour les transistors, une méthode consiste à replier le dispositif par multiplication du nombre de grilles (structure en « peigne »). En plus de réduire la surface totale du composant, cette technique permet de minimiser les capacités parasites C_{DB} et C_{SB}.
- ∞ Les longueurs des pistes de polysilicium sont réduites au minimum afin de limiter les résistances séries, de minimiser la taille des capacités parasites et d'empêcher l'effet d'antenne [116].
- ∞ Les éléments unitaires sont orientés dans la même direction de sorte que les porteurs présentent des mobilités identiques. En outre, si les éléments se trouvent à proximité d'une source de chaleur (transistors de puissance, etc.), ils doivent être disposés parallèlement au gradient thermique [164].
- ∞ Pour que les gradients (thermiques, de procédé de fabrication, etc.) aient un effet identique sur tous les composants, les éléments constitutifs de ces derniers sont interdigitalisés et placés à proximité les uns des autres suivant une disposition à barycentre commun (« *common centroid* ») [118].
- ∞ Si la surface l'autorise, des éléments factices (« *dummies* ») sont placés en périphérie de la matrice, afin que tous les éléments d'intérêt présentent un voisinage identique. Cette technique vise à minimiser l'impact des effets de bord [116].
- ∞ Afin de limiter les effets de couplages, les pistes métalliques sont routées à l'extérieur des zones actives. Dans la même optique, les pistes d'un niveau métallique donné sont routés perpendiculairement aux pistes des niveaux adjacents [117].
- ∞ Afin de réduire le bruit d'alimentation, des capacités de découplages sont placées à proximité des cellules bruyantes [116].
- ∞ Pour limiter le bruit substrat, chaque cellule contient une densité importante de prises substrats à faible résistance série. Cette mesure permet également limiter le risque d'effet thyristor parasite (« *latch-up* »). De plus, les cellules analogiques sensibles sont entourées d'un double anneau de garde (« *double guard-ring* ») et placées à distance des cellules bruyantes (blocs digitaux, convertisseurs à capacités commutées, etc.) [116].
- ∞ Enfin, afin d'augmenter la fiabilité, les contacts et les vias sont doublés, et la largeur des pistes est prise systématiquement supérieure aux minima fixés par le DRM [117].

Le circuit de test de l'oscillateur chaotique est représenté sur la figure III.28. Il repose sur le circuit étudié au § III.4.3.2.c (cf. figure III.22), auquel ont été ajoutés des transistors d'activation commandés par les bits PD_0 et PD_1. Les dimensions de ses éléments constitutifs sont rassemblées dans le tableau III.3. Le *layout* correspondant est représenté sur les figures III.29 et III.30.

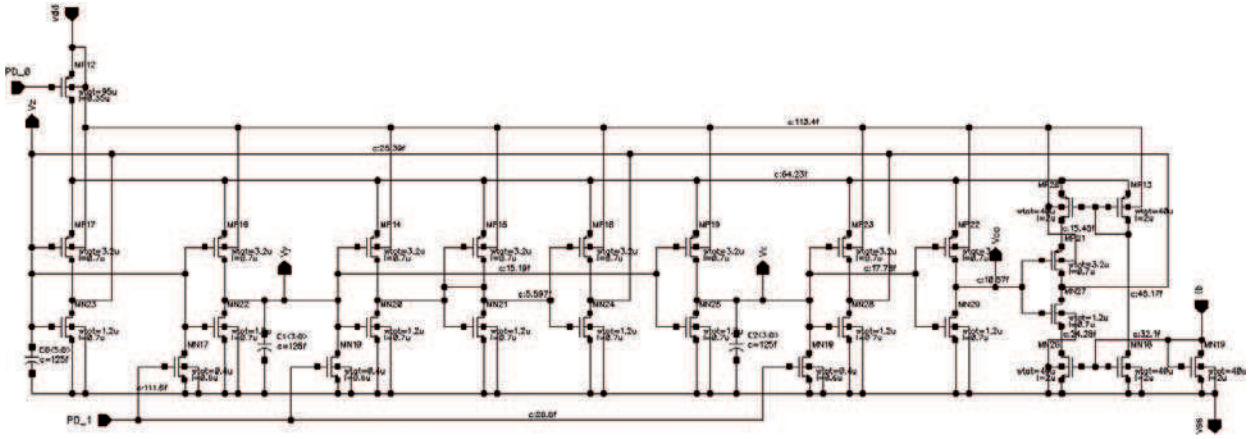


Fig. III.28 – *Circuit de l'oscillateur chaotique (CO) en technologie AMS* $0.35\ \mu m$.

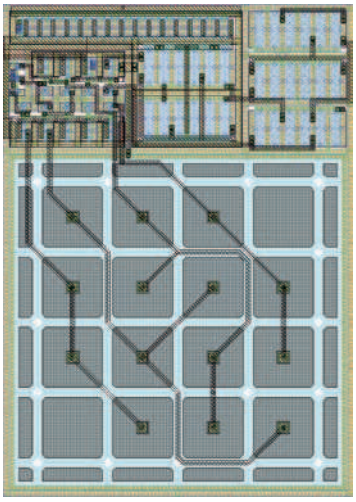


Fig. III.29 – *Layout de l'oscillateur chaotique (CO) en technologie AMS (*$69\ \mu m \times 97\ \mu m$*).*

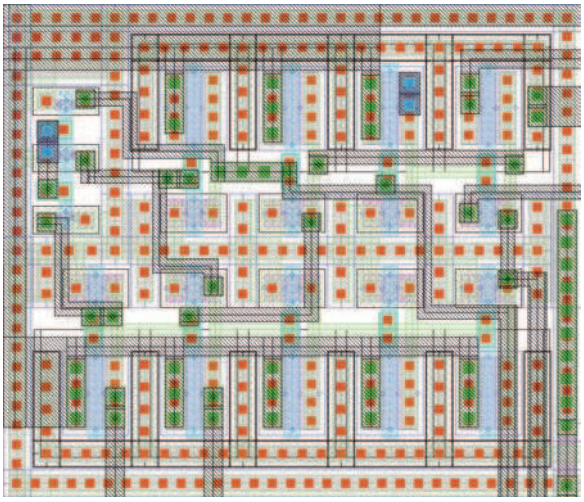


Fig. III.30 – *Zoom sur la partie supérieure gauche du layout la figure III.29 (*$25.3\ \mu m \times 21.6\ \mu m$*).*

Les capacités C_1, C_2 et C_3 sont divisées en capacités poly1-poly2 identiques de $125\ pF$. Ces dernières sont disposées suivant une matrice *common centroid* carrée et compacte. Afin de limiter les effets de bord, les plateaux des capacités présentent des angles de $45°$ [164]. De plus, pour que chaque capacité présente un voisinage similaire, des *dummies* ont été placés en position $(1;4)$ et $(4;1)$, ainsi qu'en périphérie de la matrice. En ce qui concerne les transistors des miroirs, ils sont interdigitalisés et disposés de sorte à présenter un barycentre commun (cf. partie supérieure droite de la figure III.29). Enfin, les inverseurs des étages gm-C sont regroupés sur deux lignes de façon à minimiser la dispersion des transconductances (cf. figure III.30). Les dimensions de l'oscillateur chaotique sont de $69\ \mu m$ sur $97\ \mu m$.

Les vues schéma et *layout* du suiveur de tension sont représentées sur la figure III.31. Dans ces deux vues, la position relative des transistors est identique. A nouveau, un soin particulier a été apporté au dessin des dispositifs. Par exemple, les transistors des miroirs sont interdigitalisés suivant une matrice *common centroid*. De plus, la structure « *cross-quad* » de la paire différentielle permet d'améliorer le *matching* tout en minimisant la capacité parasite d'entrée [116]. Le *layout* du suiveur mesure $28\ \mu m$ sur $42\ \mu m$.

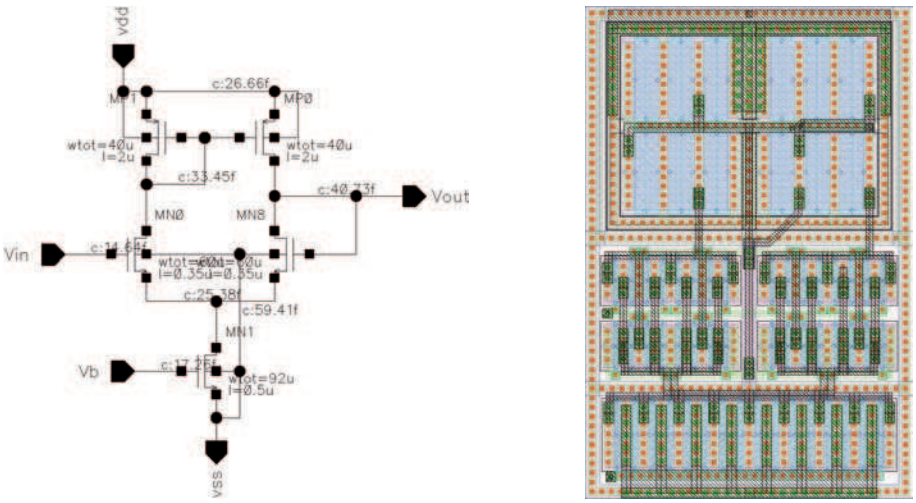


Fig. III.31 – *Schéma et layout du suiveur de tension (VF) en technologie AMS* $0.35\ \mu m$ *(*$28\ \mu m \times 42\ \mu m$*).*

Les vues schéma et *layout* des cellules Buf_0 et Buf_1 sont représentées, respectivement, sur les figures III.32 et III.33. Dans les deux cas, la forte densité de prises substrats permet d'absorber les courants de commutations et par voie de conséquence, de réduire l'injection de bruit et les risques de *latch-up*. Les cellules Buf_0 et Buf_1 mesurent, respectivement, $25\ \mu m$ sur $14\ \mu m$ et $28\ \mu m$ sur $15\ \mu m$.

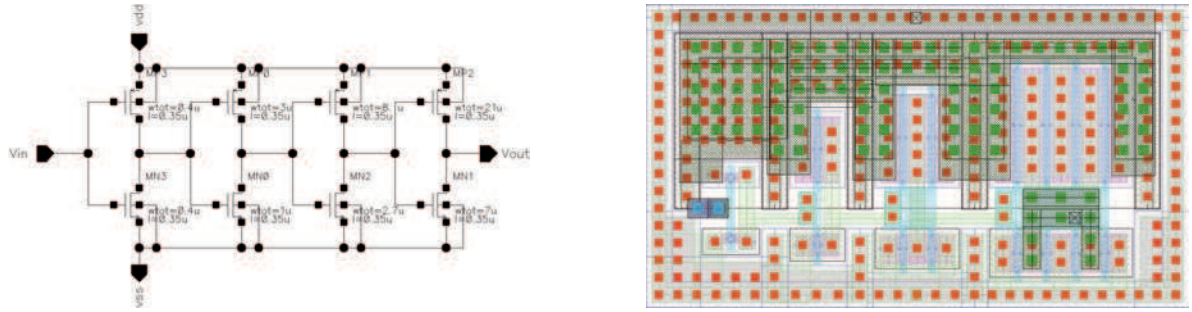


Fig. III.32 – *Schéma et layout du premier buffer (Buf_0) en technologie AMS* $0.35\ \mu m$ *(*$25\ \mu m \times 14\ \mu m$*).*

Le schéma et le *layout* de la référence de courant sont représentés sur la figure III.34. Cette cellule comporte deux sorties : une sortie de test connectée directement à un *pad* ($Iref = 2\ \mu A$) et une sortie destinée à l'oscillateur chaotique ($Iref\_CO = I_b = 80\ \mu A$). Afin d'obtenir un LVS sans erreur, le transistor PMOS factice du *layout* a été reporté dans la vue schéma ($MP0$). Les dimensions de la cellule sont de $64\ \mu m$ sur $52\ \mu m$.

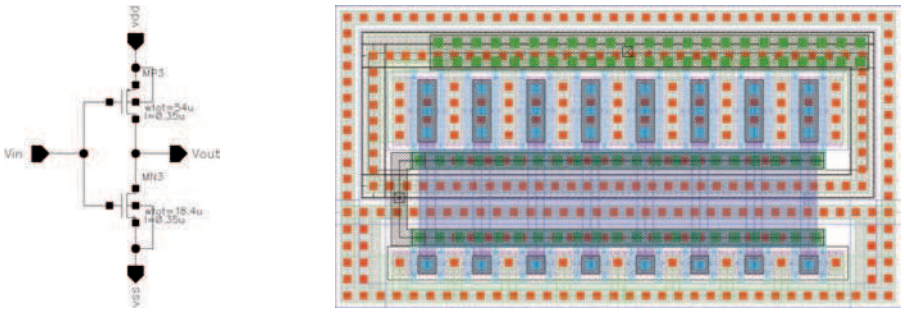


Fig. III.33 – *Schéma et layout du second buffer (Buf_1) en technologie AMS* 0.35 μm *(*28 $\mu m \times$ 15 μm*).*

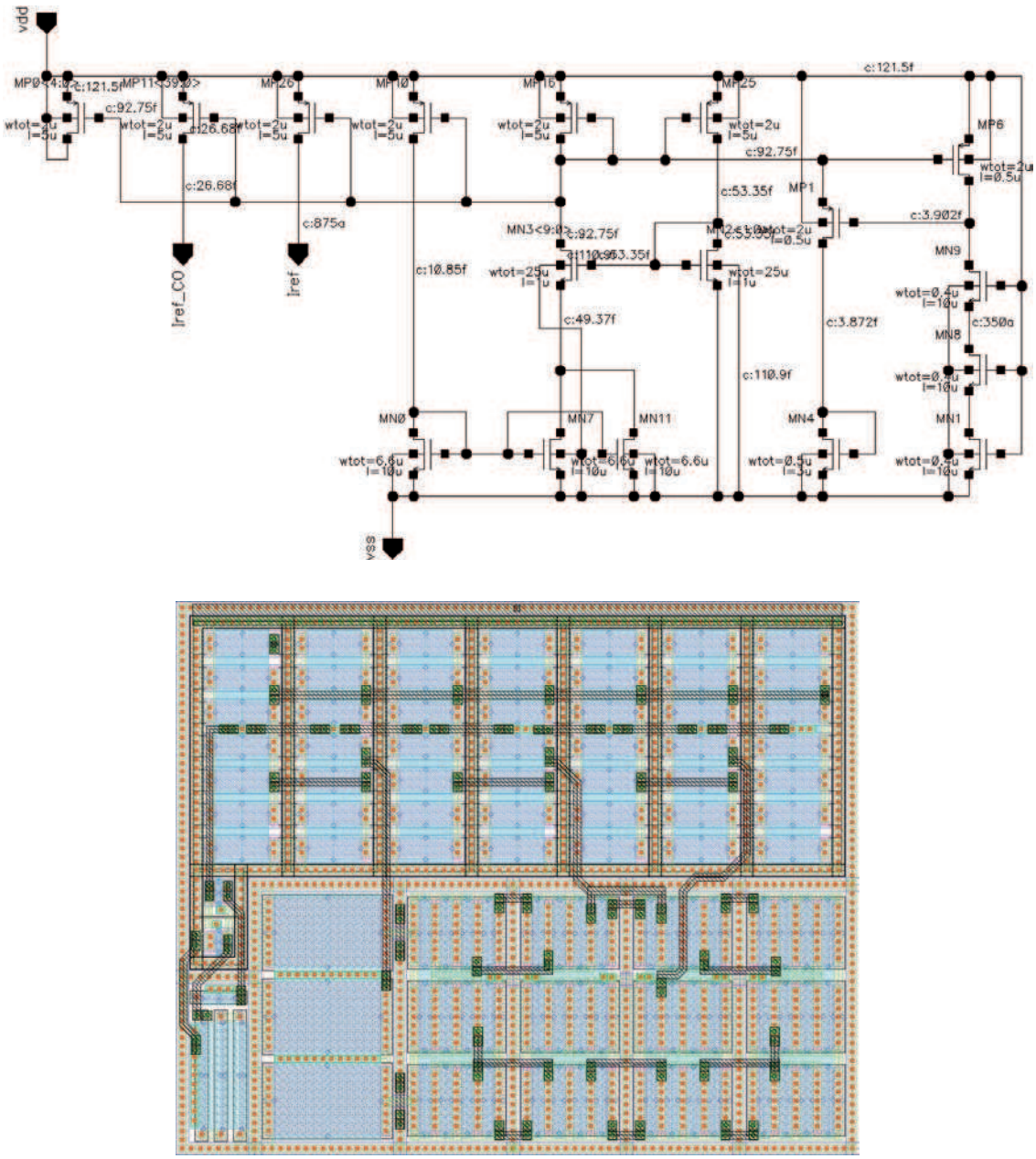


Fig. III.34 – *Schéma et layout de la référence de courant (Iref) en technologie AMS (*64 $\mu m \times$ 52 μm*).*

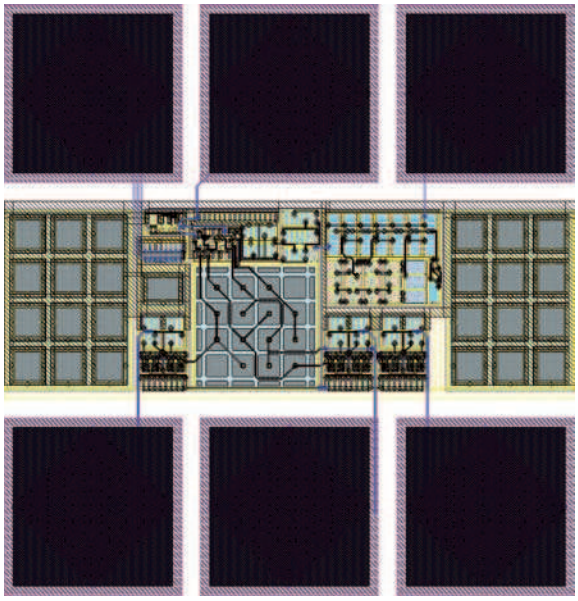


Fig. III.35 – *Layout du circuit de test en technologie AMS* $0.35\ \mu m$ *(*$305\ \mu m \times 315\ \mu m$*).*

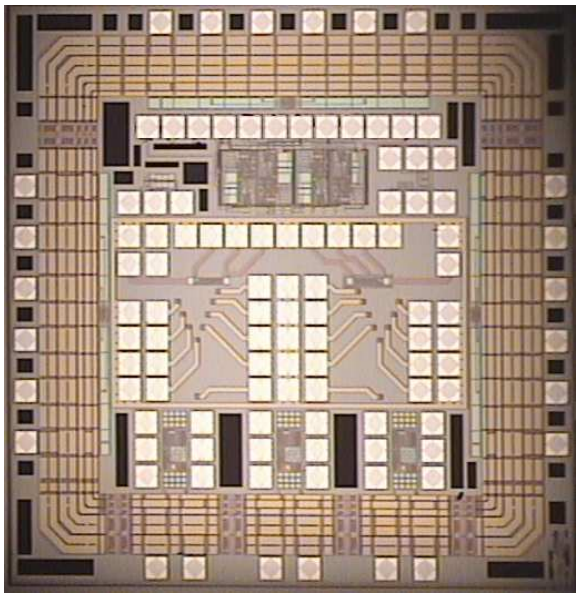


Fig. III.36 – *Photographie du circuit multi-projets en technologie AMS* $0.35\ \mu m$ *(*$4\ mm^2$*).*

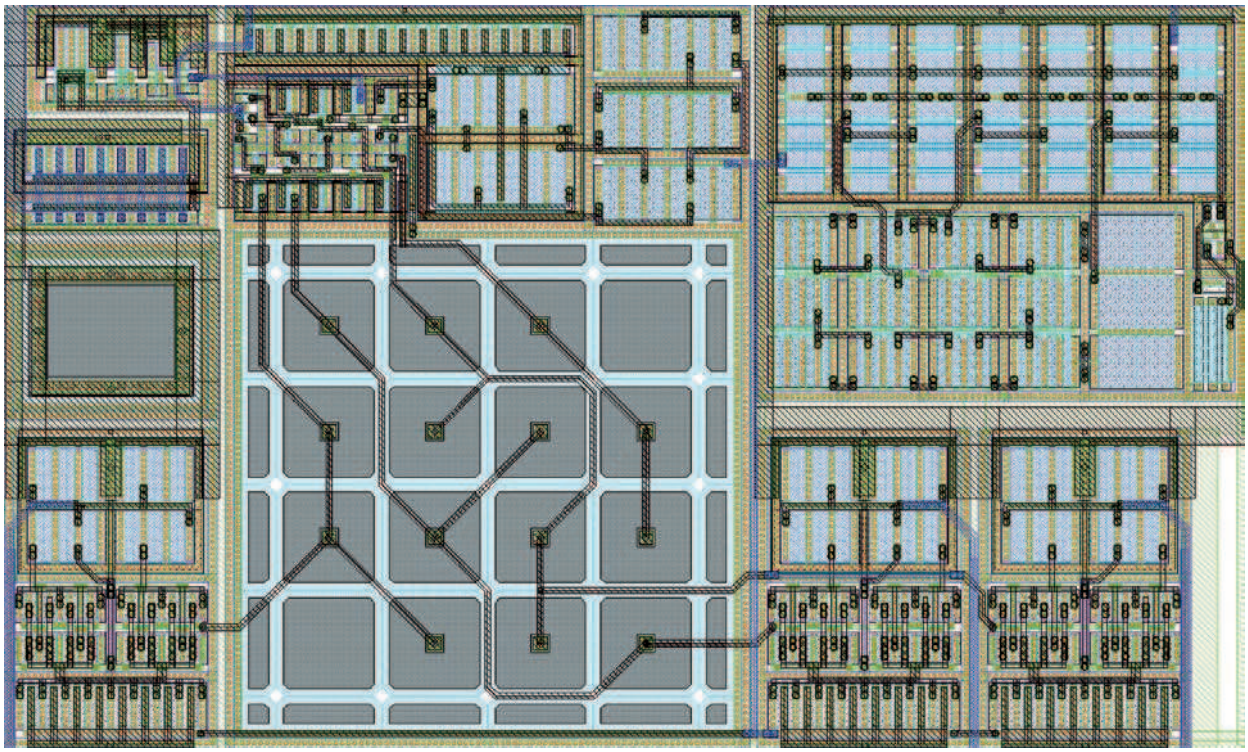


Fig. III.37 – *Agrandissement de la partie centrale du layout de la figure III.35 (*$163\ \mu m \times 97\ \mu m$*).*

Le *layout* du circuit de test est représenté sur les figures III.35 (vue d'ensemble) et III.37 (agrandissement de la partie centrale). La vue globale comporte six *pads* issues des bibliothèques . Ces carrés métalliques de $90\ \mu m$ de côté sont connectés, respectivement, à : V_{CO}, PD, I_{ref}, V_Z, V_Y et V_X (de gauche à droite et de haut en bas). Des capacités de découplage occupent les espaces latéraux laissés libres par la disposition des *pads*. Au final, l'ensemble du *layout* mesure $305\ \mu m$ sur $315\ \mu m$, soit moins de $0.1\ mm^2$.

Une photographie du circuit multi-projets est représentée sur la figure III.36. Les dimensions extérieures du *padframe* sont de $2\ mm$ sur $2\ mm$. L'espace alloué à cette étude correspond au quart inférieur de la surface intérieure au *padframe*. La largeur disponible nous a permis d'implémenter trois versions différentes de l'oscillateur chaotique : le module de droite correspond à la version décrite précédemment ($a \approx 0.67$, cf. figure III.37), le module central fait intervenir la capacité factice $(1;4)$ ($a \approx 0.57$), tandis que le module de gauche exploite les capacités factices $(1;4)$ et $(4;1)$ ($a = 0.5$). Pour chaque version, les rails d'alimentation V_{dd} et V_{ss} sont connectés, respectivement, aux *pads* gauche et droit inclus dans la partie du « *padframe* » localisée sous le module correspondant.

III.4.3.2.e Mesures expérimentales

Le prototype de la figure III.36 à été fabriqué à vingt exemplaires. Ce lot a été divisé équitablement entre les trois équipes du L2MP ayant participé au projet. Nos six exemplaires ont été testés sous pointes, dans le laboratoire de caractérisation électrique du L2MP situé au sein de l'ISEN-Toulon. Sur les dix-huit modules de test (trois par *testchip*), les mesures du courant I_{ref} ont donné, à l'ambiante, un ensemble de valeurs comprises entre $1.63\ \mu A$ et $1.82\ \mu A$, au lieu des $2\ \mu A$ escomptés. Cet écart inexpliqué s'accompagne, entre autre, d'une sous-alimentation des suiveurs de tension (VF); le courant de polarisation étant trop faible, le suiveur n'est pas en mesure de piloter la charge (i.e., l'ensemble *pad*, pointe, câble coaxial et oscilloscope) avec une bande passante et un *slew rate* adaptés aux signaux chaotiques. La polarisation des suiveurs par l'intermédiaire d'un *pad* supplémentaire aurait permis d'éviter ce problème. Néanmoins, le circuit présentant le courant I_{ref} le moins faible (i.e. $1.82\ \mu A$) permet tout de même de mettre en évidence le comportement chaotique de l'oscillateur. Les signaux générés par ce module central ($a \approx 0.57$) ont été mesurés à l'aide d'un oscilloscope numérique, puis traités sous Origin. Les courbes ainsi obtenues sont représentées sur les figures III.38 et III.39.

La courbe expérimentale de $V_X(t)$ est représentée sur la figure III.38. La dynamique du signal expérimental est nettement inférieure à celle de son homologue simulé, ce qui tend à renforcer l'hypothèse de sous-polarisation des suiveurs. Néanmoins, malgré la distortion résultante, l'allure et les caractéristiques du signal sont proches de celles obtenues en simulation post-*layout* (cf. figure III.8). Notamment, la valeur moyenne du signal mesuré est inférieure de seulement $100\ mV$ à celle du signal simulé. De plus, la fréquence expérimentale du signal $V_{CO}(t)$ est approximativement égale à $12.1\ MHz$, ce qui correspond à erreur relative de 8% par rapport à la fréquence obtenue en simulation ($13.2\ MHz$).

Le portrait de phase associant les valeurs mesurées de V_X et V_Y est représenté sur la figure III.39. La distortion et l'atténuation des signaux engendrent, a priori, une déformation importante de l'attracteur.

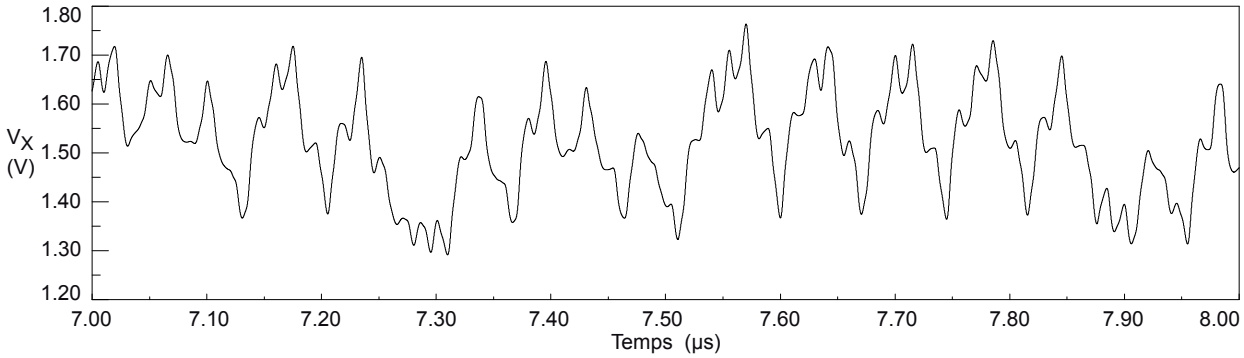


Fig. III.38 – *Représentation temporelle du signal $V_X(t)$ mesuré à l'oscilloscope numérique ($a \approx 0.57$).*

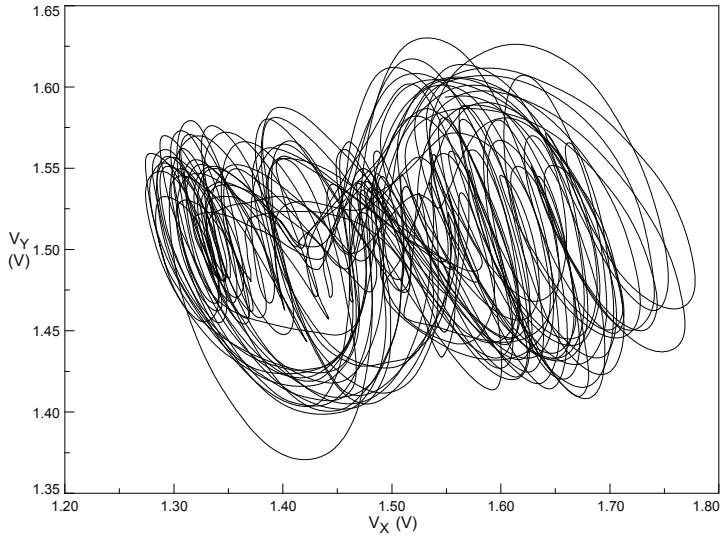


Fig. III.39 – *Portrait de phase $V_Y = f(V_X)$ mesuré à l'oscilloscope numérique ($a \approx 0.57$).*

Néanmoins, la trajectoire occupe principalement deux zones et passe aléatoirement d'une zone à l'autre en transitant par le centre. Ce comportement est analogue à celui observé en simulation (cf. figure III.24).

III.4.3.3 Détecteur de front

Le détecteur de front est schématisé sur la figure III.40. Il comporte deux voies complémentaires : la voie supérieure qui détecte les fronts montants du signal V_{CO} et la voie inférieure qui détecte ses fronts descendants.

Une voie de détection est constituée d'une porte NAND dont les deux entrées sont connectées au signal observé via des chaînes de délais présentant des temps de propagation différents. Ainsi, un front montant ou descendant du signal V_{CO} déclenche une courte impulsion en sortie de la porte NAND correspondante. La durée de cette impulsion est égale à la différence entre les délais de propagation. Les signaux des deux voies sont ensuite additionnés par l'intermédiaire d'une troisième porte NAND. Dans l'implémentation proposée, la largeur moyenne des impulsions vaut approximativement $0.5\ ns$. Lorsque la cellule est sollicitée à une fréquence moyenne de $20\ MHz$, elle consomme moins de $6\ \mu A$.

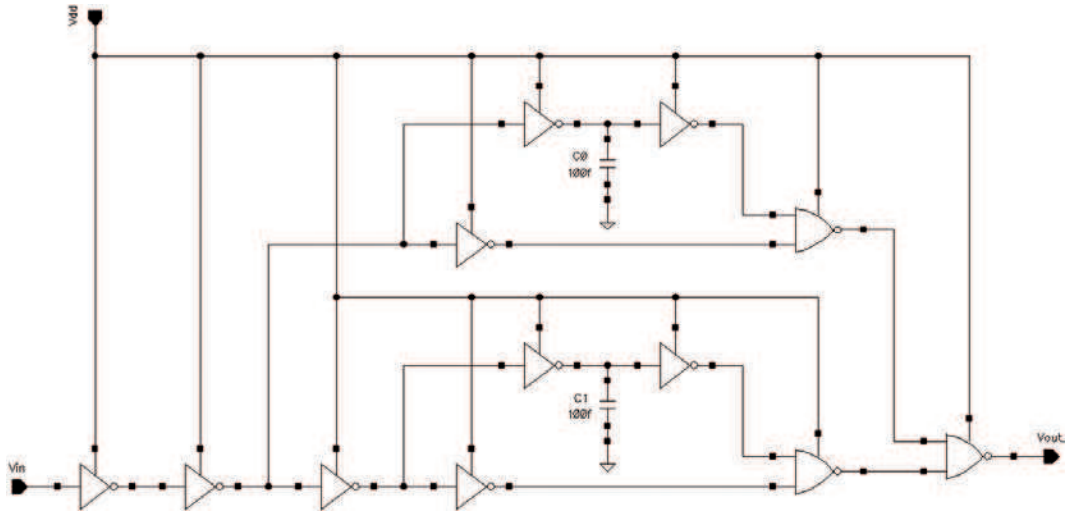


Fig. III.40 – *Schéma du détecteur de front (ED).*

III.4.3.4 Générateur de triangle

Une approche en mode courant permettrait de supprimer le convertisseur tension-courant (VCC). Cependant, la synthèse d'un courant triangulaire requiert un effet inductif dont l'intégration présente de nombreuses contraintes (cf. § II.4.3.2). Le mode tension proposé permet de contourner cette difficulté.

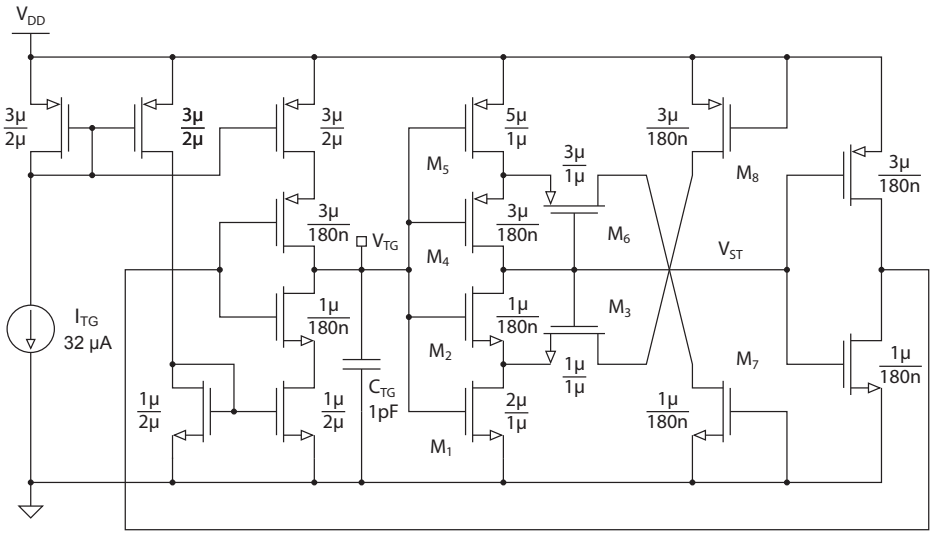


Fig. III.41 – *Schéma du générateur de triangle (TG) [104].*

Le générateur de tension triangulaire repose sur le circuit proposé dans [104] (cf. figure III.41). Par rapport au circuit original, celui de la figure III.41 comporte deux transistors supplémentaires (M_7 et M_8). Le rôle de ces dispositifs est de limiter les tensions aux bornes des dispositifs NMOS (M_1, M_3, M_5 et M_6), de sorte à réduire les mécanismes de dégradations. Le signal V_{TG} est généré par charge et décharge d'une capacité (C_{TG}) à courant constant (I_{TG}). Les transitions entre charges et décharges sont amorcées

par des déclencheurs de Schmitt (« *Schmitt triggers* »). Ainsi, les seuils de déclenchement des *triggers* déterminent l'amplitude du signal triangulaire. La tension de commutation haute (V_{HS}) est la valeur de V_{TG} pour laquelle les transistors M_1 et M_2 commencent à s'ouvrir :

$$V_{HS} = V_{T_{N_2}} + V_{DS_1} \tag{III.45}$$

Lorsque M_2 commence à s'ouvrir, la tension de sortie du *trigger* (V_{ST}) diminue ce qui a pour effet de fermer M_3 et d'accélérer la décroissance de V_{ST}. Cette contre-réaction positive permet de définir précisément la tension de commutation. Lorsque la relation III.45 est vérifiée, les courants circulant dans M_1 et M_3 sont quasiment identiques [104] :

$$I_{DS_1} = I_{DS_3} \quad \Leftrightarrow \quad \frac{\beta_1}{2} \cdot \left(V_{HS} - V_{T_{N_1}}\right)^2 = \frac{\beta_3}{2} \cdot \left(V_{DD} - V_{DS_1} - V_{T_{N_3}}\right)^2 \tag{III.46}$$

Puisque M_1 et M_3 présentent la même tension substrat-source, on peut considérer que $V_{T_{N_1}} = V_{T_{N_3}} = V_{T_N}$. Dans ce cas, la combinaison des relations III.45 et III.46 donne :

$$V_{HS} = \frac{V_{DD} + \sqrt{\frac{\beta_1}{\beta_3}} \cdot V_{T_N}}{1 + \sqrt{\frac{\beta_1}{\beta_3}}} \tag{III.47}$$

Un raisonnement identique, mené pour la tension de commutation basse (V_{LS}), aboutit à :

$$V_{LS} = \frac{\frac{\beta_5}{\beta_6} \cdot (V_{DD} - V_{T_P})}{1 + \sqrt{\frac{\beta_5}{\beta_6}}} \tag{III.48}$$

Soient t_c et t_d les temps de charge et de décharge de C_{TG}. Comme souhaité, la fréquence du signal V_{TG} (f_{tg}) est directement proportionnelle à I_{TG} :

$$f_{tg} = \frac{1}{t_c + t_d} = \frac{I_{TG}}{2 \cdot C_{TG} \cdot (V_{HS} - V_{LS})} \tag{III.49}$$

Dans l'implémentation proposée, l'amplitude de V_{TG} est fixée à $400\ mV$ (cf. figure III.8). La capacité C_{TG} est prise relativement grande ($1\ pF$) de sorte à limiter l'influence des déviations en procédé de fabrication et des injections de charges associées à la fermeture des interrupteurs. D'après la relation III.49, un courant I_{TG} de $32\ \mu A$ doit permettre d'atteindre la fréquence seuil fixée au § III.4.2 ($f_{tg} \geq 2 \cdot \overline{f_{rc}} = 40\ MHz$). Ce résultat a été confirmé en simulation. Dans ces conditions, la consommation de la cellule est inférieure à $110\ \mu A$.

III.4.3.5 Echantillonneur-bloqueur

L'échantillonneur-bloqueur comporte deux canaux (S&H$_A$ et S&H$_B$) fonctionnant en alternance (cf. figure III.42). Le signal impulsionnel V_{ED} est d'abord converti en deux signaux d'horloge complémentés non-recouvrants (V_{clk} et V_{nclk}). Le signal V_{clk} pilote la cellule S&H$_A$, tandis que le signal V_{nclk} pilote la cellule S&H$_B$. Ainsi, lorsqu'une cellule échantillonne le signal V_{TG}, la seconde transmet à la sortie ($V_{S\&H}$) la valeur bloquée lors de la phase précédente. Les rôles sont inversés à chaque impulsion du signal V_{ED}. Lorsque l'attracteur entame une transition sans l'achever, deux impulsions rapprochées apparaissent sur V_{ED}. Afin de filtrer la seconde, le convertisseur est ralenti par des chaînes de retard à inverseurs.

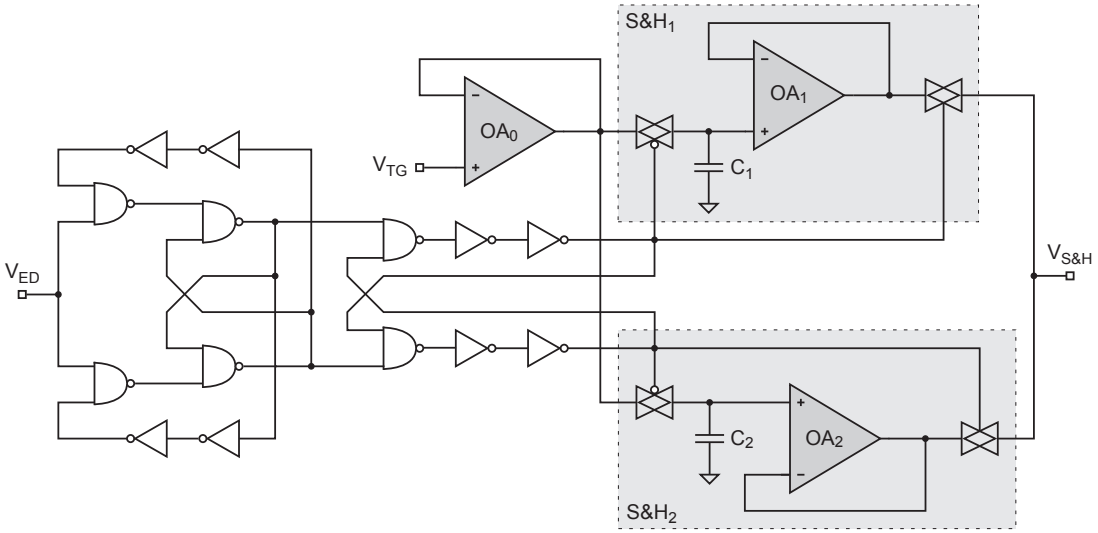


Fig. III.42 – *Schéma de l'échantillonneur-bloqueur (S&H).*

En minimisant l'injection de charge et la transmission du signal d'horloge, des échantillonneurs-bloqueurs différentiels en boucle fermée permettraient d'améliorer la précision d'échantillonnage [78, 104, 111]. Toutefois, la précision des échantillonneurs simples de la figure III.42 (ici 2%) est suffisante dans le cadre de l'application visée. Lorsqu'il est rafraîchi à une fréquence moyenne de $20\ MHz$, le circuit consomme approximativement $130\ \mu A$.

III.4.3.6 Convertisseur tension-courant

Le convertisseur tension-courant est schématisé sur la figure III.43. Il fait intervenir l'OTA de la figure III.44. Celui-ci est attaqué, d'une part, par le signal $V_{S\&H}$ sur son entrée inverseuse et, d'autre part, par la valeur moyenne du signal $V_{S\&H}$ sur son entrée non-inverseuse. Cette dernière est obtenue par l'intermédiaire d'un suiveur de tension chargé par une capacité MOS de $1.4\ pF$ (C_{VCC}) et polarisé par un courant de $10\ nA$. Afin d'accélérer la phase de démarrage, la capacité C_{VCC} est préchargée à $900\ mV$ par l'intermédiaire d'un transistor PMOS connecté à V_{ref} et piloté via $\overline{PD}$ (cf. figure III.9).

Certaines techniques de linéarisation permettent d'augmenter significativement la largeur de la plage de fonctionnement linéaire d'une paire différentielle (paire différentielle couplée-croisée, dégénération de la source, polarisation adaptative, etc.) [165]. Néanmoins, l'OTA simple de la figure III.44 permet d'atteindre une plage de fonctionnement linéaire adaptée à la dynamique du signal triangulaire. Lorsque la valeur moyenne de I_{VCC} est fixée à $2\ \mu A$, le convertisseur consomme moins de $5\ \mu A$.

III.4.3.7 Bloc de polarisation

Le bloc de polarisation est représenté sur la figure III.45. Une fois activé via PD, il assure la distribution des courants de polarisation. Ces courants sont des multiples ou sous-multiples du courant I_{ref} délivré par le générateur de références (RG).

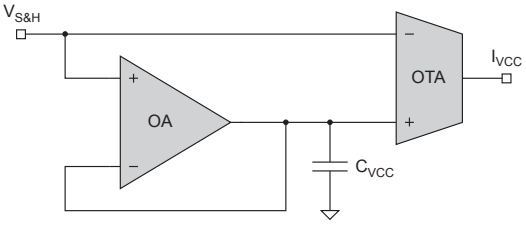


Fig. III.43 – *Schéma du convertisseur tension-courant (VCC).*

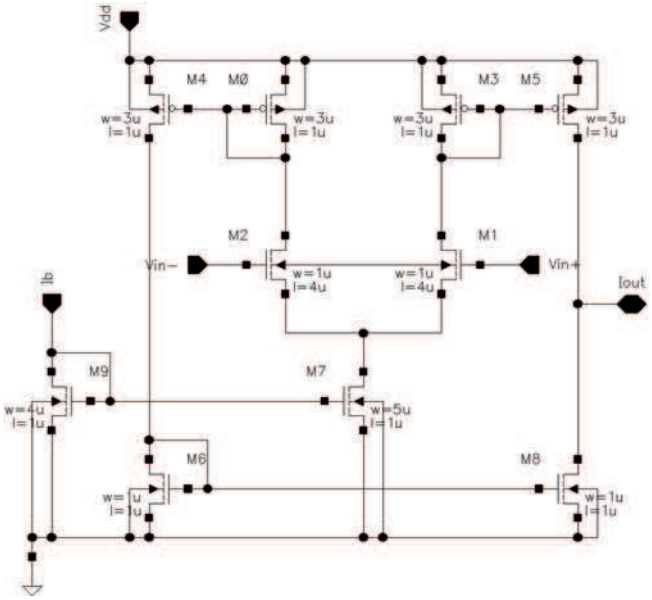


Fig. III.44 – *Schéma de l'OTA intégré au convertisseur tension-courant (VCC).*

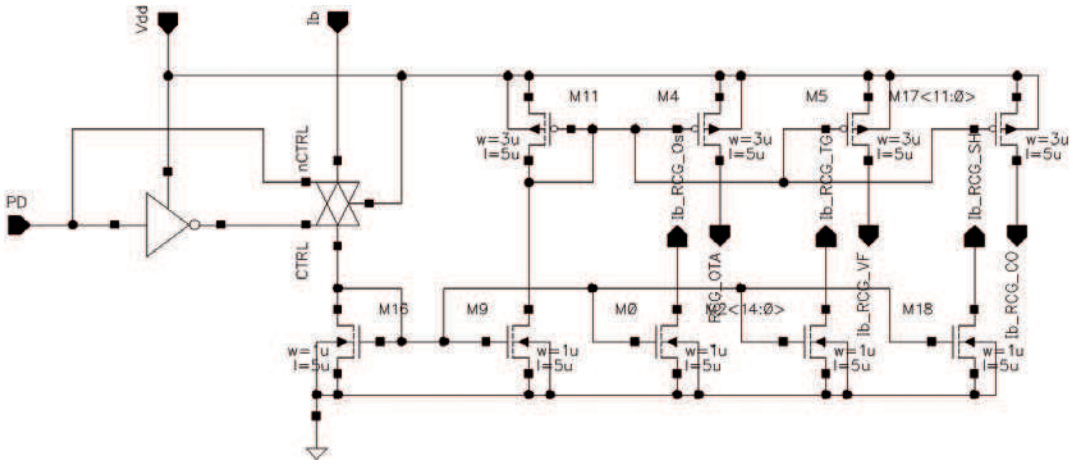


Fig. III.45 – *Schéma du circuit de polarisation (RCG_B).*

III.4.3.8 Oscillateur en anneau

La dernière cellule du générateur d'horloge aléatoire est un oscillateur en anneau contrôlé en courant (cf. figure III.46). Cette structure à cinq étages d'inverseurs sous-alimentés en courant (« *current-starved* ») est issue de [104]. La fréquence du signal de sortie (V_{RO}) est donnée par [104] :

$$f_{RO} = \frac{I_B}{5 \cdot C_L \cdot V_{DD}} \tag{III.50}$$

où I_B est le courant de polarisation et C_L, la capacité de charge vue par chaque inverseur. Cette dernière est égale à la somme des capacités d'entrée (C_{in}) et de sortie (C_{out}) d'un inverseur [104] :

$$C_L = \underbrace{C'_{ox} \cdot (W_P \cdot L_P + W_N \cdot L_N)}_{C_{out}} + \underbrace{\frac{3}{2} \cdot C'_{ox} \cdot (W_P \cdot L_P + W_N \cdot L_N)}_{C_{in}} \tag{III.51}$$

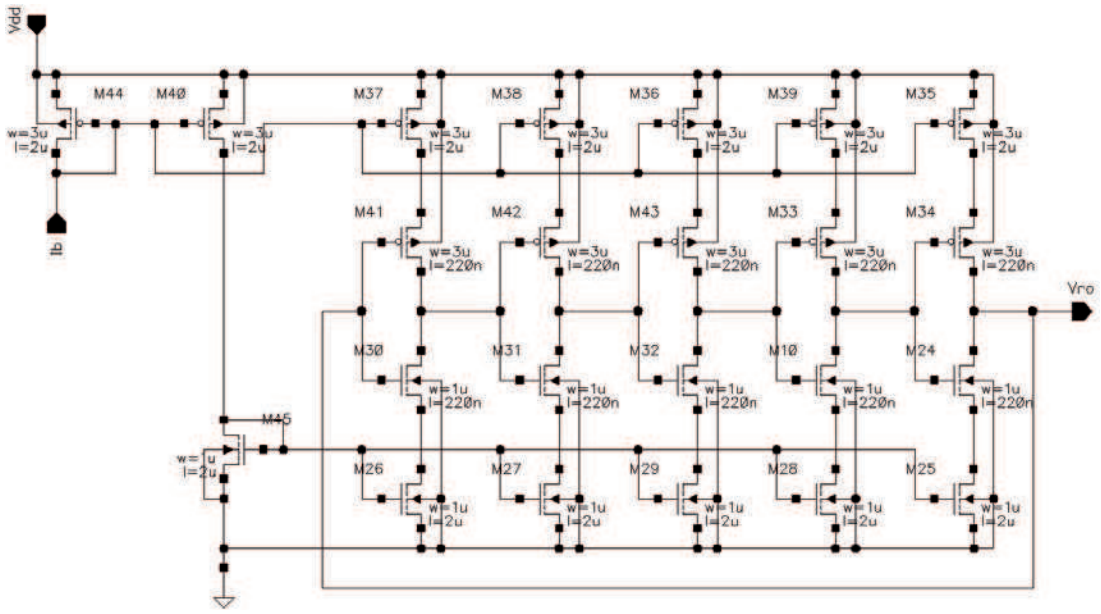


Fig. III.46 – *Schéma de l'oscillateur en anneau (RO).*

Dans le circuit présenté, f_{RO} est approximativement égal à 20 MHz pour $I_B = 2\ \mu A$. A cette fréquence, la consommation moyenne de l'oscillateur reste inférieure à 12 μA. Les deux inverseurs placés en sortie de l'oscillateur (cf. figure III.9) contribuent à la mise en forme du signal V_{RC}.

III.4.4 Résultats

III.4.5 Caractéristiques du générateur

Les caractéristiques simulées du générateur d'horloge aléatoire sont rassemblées dans le tableau III.5. Conformément aux spécifications du cahier des charges, la plage de variation fréquentielle du signal V_{RC} (f_{rc}) est centrée autour de 20 MHz et s'étend symétriquement sur plus de 30 MHz. Pour des variations cumulées du procédé de fabrication (3σ), de la tension d'alimentation (1.8 V $\pm 10\%$) et de la température (-40 à 125 °C), la valeur moyenne de f_{rc} varie d'au maximum 16%. Cette valeur est supérieure au seuil spécifiée par le cahier des charges (cf. tableau III.1). Cependant, si nécessaire, elle peut être largement améliorée par l'introduction de boucles de régulation. Le temps de démarrage du générateur est de l'ordre de 0.2 μs. Lorsqu'il est actif, le circuit consomme moins de 1 mW (530 μA sous 1.8 V), tandis qu'en mode veille, sa consommation chute à 3 μW. Enfin, la surface estimée du circuit est d'approximativement 0.01 mm^2.

III.4.6 Répartition des valeurs de $V_{S\&H}$

Un histogramme du signal $V_{S\&H}$ est représenté sur la figure III.47. Il a été réalisé à partir d'une simulation transitoire de 2 ms. La fréquence d'échantillonnage étant supérieure à 20 MHz, le signal résultant comporte plus de 4.10^4 paliers. Si l'on fait abstraction des effets de bord, le nombre d'occurrences par classe est quasiment constant. Par conséquent, la séquence A peut être considérée comme uniformément distribuée sur la dynamique du signal triangulaire.

Paramètre		Symbole	Valeur	Unité
Fréquence moyenne typique de V_{RC}.		$\overline{f_{rc}}$	20.6	MHz
Largeur de la plage de variation fréquentielle.		Δf_{rc}	31.3	MHz
Déviation maximum de f_{rc} en PVT.		-	16	$\%$
Temps de démarrage.		-	0.2	μs
Consommation.	En fonctionnement.	-	0.95	mW
	En veille.	-	3	μW
Surface estimée.		-	0.01	mm^2

Tab. III.5 – *Caractéristiques simulées du générateur d'horloge aléatoire.*

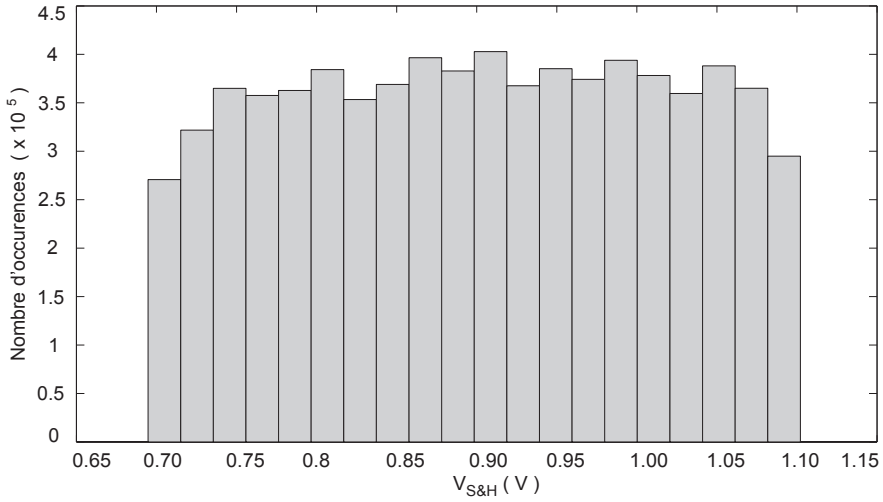


Fig. III.47 – *Histogramme du signal ($V_{S\&H}$) réalisé à partir d'une simulation transitoire de* $2\ ms$.

III.4.7 Caractérisation statistique du flux de sortie

III.4.7.1 Introduction

Publié en Décembre 2002 par le National Institute of Standards and Technology (NIST), le Federal Information Processing Standard (FIPS) 140-2 établit les spécifications sécuritaires des modules cryptographiques [166]. En particulier, les flux aléatoires doivent satisfaire à une série de cinq tests statistiques : le test monobit, le test duobit, le test du poker, le test des trous et des blocs et le test d'autocorrélation (cf. § III.4.7.2). Afin de soumettre le générateur proposé à ces tests, le signal analogique V_{RC} doit être préalablement converti en un flux binaire. A cet effet, une simulation transitoire de $2\ ms$ du signal V_{RC} a été échantillonnée à une fréquence constante de $5\ MHz$. Les $N_S = 10044$ valeurs ainsi recueillies permettent de construire la séquence $\{S_i\}_{i=1...N_S}$ suivant l'oracle valeur moyenne; si un échantillon à une valeur supérieure à la valeur moyenne, alors il génère un 1, dans le cas contraire, il génère un 0.

III.4.7.2 Définition des tests statistiques

III.4.7.2.a Test monobit

Le test monobit consiste à comparer le nombre de 1 et de 0 présents dans la séquence étudiée. Si N_1 est le nombre de 1 et N_0 le nombre de 0, alors la statistique X_1 définie par :

$$X_1 := \frac{(N_0 - N_1)^2}{N_s} \tag{III.52}$$

est la réalisation d'une variable aléatoire $\mathbf{X}_1$ qui suit une loi du χ^2 à 1 degré de liberté :

$$\mathbf{X}_1 \hookrightarrow \chi^2(1) \tag{III.53}$$

Le seuil d'acceptation à 90% de X_1 est égal à :

$$\chi_1^s := \chi_{0.9}^2(1) \approx 2.702 \tag{III.54}$$

III.4.7.2.b Test duobit

Le test duobit vise à vérifier que les symboles 00, 01, 10 et 11 sont présents dans la séquence en proportions identiques. Soit N_{00}, N_{01}, N_{10} et N_{11}, leurs nombres d'occurrences respectifs, et X_2 la statistique définie par :

$$X_2 := \frac{4}{N_s - 1} \cdot \left(N_{00}^2 + N_{01}^2 + N_{10}^2 + N_{11}^2\right) - \frac{2}{N_s} \cdot \left(N_0^2 + N_1^2\right) + 1 \tag{III.55}$$

Cette dernière est la réalisation d'une variable aléatoire $\mathbf{X}_2$ qui suit une loi du χ^2 à 2 degrés de liberté :

$$\mathbf{X}_2 \hookrightarrow \chi^2(2) \tag{III.56}$$

Le seuil d'acceptation à 90% de X_2 est égale à :

$$\chi_2^s := \chi_{0.9}^2(2) \approx 4.607 \tag{III.57}$$

III.4.7.2.c Test du poker

Le test du poker permet de vérifier que toutes les sous-séquences binaires possibles de longueurs $M_s < N_s$ apparaissent en proportions identiques dans la séquence totale. M_s est défini comme le plus grand entier vérifiant :

$$\left\lfloor \frac{N_s}{M_s} \right\rfloor \geq 5 \cdot \left(2^{M_s}\right) \tag{III.58}$$

Si $K_3 = \lfloor N_s/M_s \rfloor$, alors la suite $\{S_i\}_{i=1\ldots N_S}$ peut être découpée en K_3 blocs de longueur M_s. Il existe 2^{M_s} façons d'écrire un bloc binaire de taille M_s. Soit N_i le nombre d'occurrences associées à la $i^{\text{ème}}$

possibilité. Pour une séquence de longueur M_s, le test du poker est un succès si N_i est invariant quel que soit $i \in \{1,...,2^{M_s}\}$. La statistique correspondante est définie par :

$$X_3 := -K_3 + \frac{2^{M_s}}{K_3} \cdot \sum_{i=1}^{2^{M_s}} N_i^2 \tag{III.59}$$

Celle-ci est la réalisation d'une variable aléatoire $\mathbf{X}_3$ qui suit une loi du χ^2 à $2^{M_s} - 1$ degrés de liberté :

$$\mathbf{X}_3 \hookrightarrow \chi^2(2^{M_s} - 1) \tag{III.60}$$

Le seuil d'acceptation à 90% de X_3 est donné par :

$$\chi_3^s := \chi_{0.9}^2(2^{M_s} - 1) \tag{III.61}$$

III.4.7.2.d Test des trous et des blocs

Le test des trous et des blocs (« *blocks and gaps test* ») consiste à vérifier que les *blocks* (sous-suites de 0) et les *gaps* (sous-suites de 1) de différentes longueurs interviennent dans des proportions identiques. Si j est la longueur de la sous-suite, alors le nombre théorique d'occurrences de cette sous-suite est :

$$e_j = \frac{N_s - j + 3}{2^{j+2}} \tag{III.62}$$

Ainsi, si K_4 est l'entier vérifiant :

$$K_4 = \underset{j=1...N_s}{argmax} \left[e_j \geq 5 \right] \tag{III.63}$$

et si, pour tout $j \in \{1,...,K_4\}$, B_j et G_j sont, respectivement, le nombre de blocs de 1 et de 0 de taille j, alors la statistique X_4 définie par :

$$X_4 := \sum_{j=1}^{K_4} \frac{(B_j - e_j)^2}{e_j} + \sum_{j=1}^{K_4} \frac{(G_j - e_j)^2}{e_j} \tag{III.64}$$

est la réalisation d'une variable aléatoire $\mathbf{X}_4$ qui suit une loi du χ^2 à $2 \cdot K_4 - 2$ degrés de liberté :

$$\mathbf{X}_4 \hookrightarrow \chi^2(2 \cdot K_4 - 2) \tag{III.65}$$

Le seuil d'acceptation à 90% de X_4 est donné par :

$$\chi_4^s := \chi_{0.9}^2(2 \cdot K_4 - 2) \tag{III.66}$$

III.4.7.2.e Test d'autocorrélation

Le test d'autocorrélation est un test de redondance cyclique permettant de vérifier l'absence de corrélations trop importantes dans le flux étudié. Soit $A(d)$ l'autocorrélation définie par :

$$A(d) := \sum_{i=0}^{N_s-d} S_i \oplus S_{i+d} \qquad \forall d \in \left\{1,..., \left\lfloor \frac{N_s}{2} \right\rfloor \right\} \tag{III.67}$$

où le symbole $\oplus$ désigne l'opérateur XOR. La statique X_5, construite à partir de $A(d)$, est définie par :

$$X_5 := \frac{2 \cdot A(d) - N_s + d}{\sqrt{N_s - d}} \tag{III.68}$$

Elle est la réalisation d'un vecteur aléatoire $\mathbf{X}_5$ de dimension $\lfloor N_s/2 \rfloor$ qui suit une loi normale :

$$\mathbf{X}_5 \hookrightarrow \mathcal{N}(\vec{0}, Id_{\lfloor \frac{N_s}{2} \rfloor}) \tag{III.69}$$

où Id est la fonction identité. Une approche qualitative consiste à vérifier que plus de 99% des valeurs sont contenues dans l'intervalle $[-3; 3]$.

III.4.7.3 Résultats

La suite $\{S_i\}_{i=1...N_S}$ extraite du signal d'horloge $V_{RC}(t)$ a été soumise aux cinq tests statistiques :

- ∞ Pour le test monobit, on obtient $N_0 = 5065$ zéros et $N_1 = 4979$ uns. Ainsi, $X_1 = 0.736$.
- ∞ En ce qui concerne le test duobit, on obtient : $N_{00} = 2573$, $N_{01} = 2491$, $N_{10} = 2491$, $N_{11} = 2488$. Par conséquent, $X_2 = 1.234$.
- ∞ Pour le test du Poker, $M_s = 7$ et le flux est divisible en $K_3 = 1434$ morceaux. Le nombre d'occurrences de chacun des $2^{M_s} = 128$ mots possibles est donné à la figure III.48. On obtient $X_3 = 138.954$.

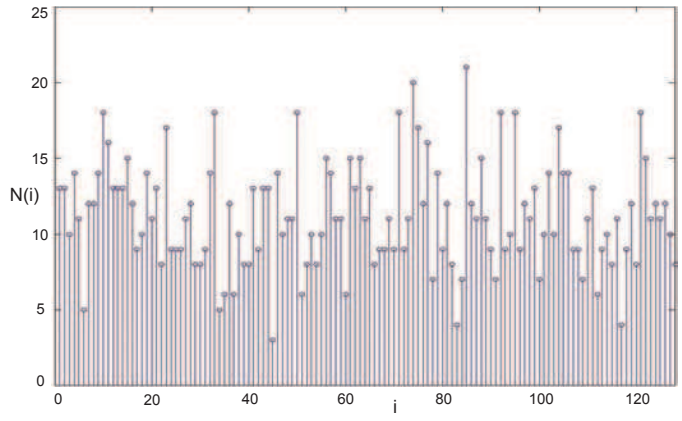


Fig. III.48 – *Nombre $N(i)$ d'occurrences associées à chaque mot binaire de pendant décimal i [82].*

∞ Dans le cadre des test des trous et des blocs, la taille maximum des sous-suites est $K_4 = 9$. Les proportions idéales (traits pleins) et expérimentales (cercles rouges et carrés verts) des trous et des blocs sont illustrées sur la figure III.49. On obtient $X_4 = 22.855$.

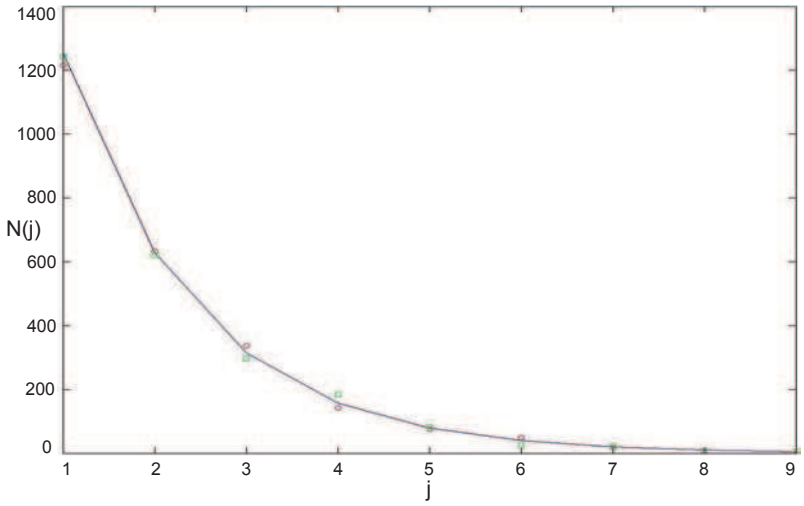


Fig. III.49 – *Nombres théoriques (trait plein) et expérimentaux $N(j)$ d'occurrences des trous (○) et blocs (□) de longueur j [82].*

∞ Enfin, le test d'autocorrélation est effectué sur 5022 points. Le résultat est représenté sur la figure III.50. Sauf exceptions ponctuelles, les valeurs sont contenues dans l'intervalle de confiance $[-3; 3]$.

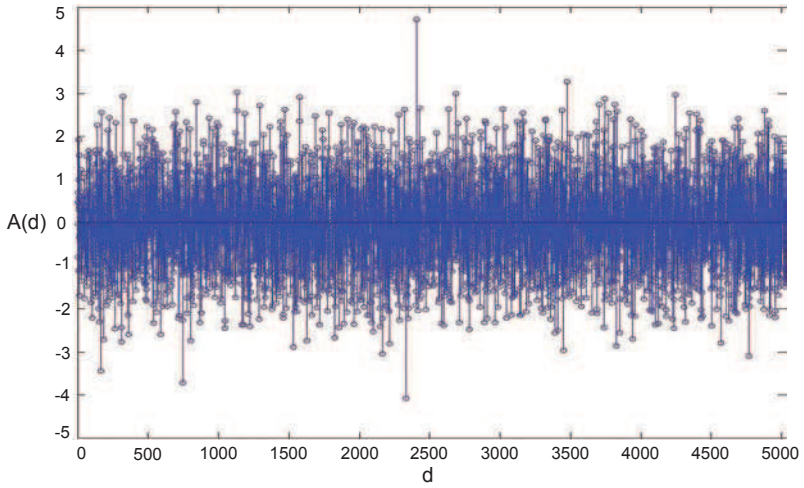


Fig. III.50 – *Autocorrélation binaire $A(d)$ de la suite $\{S_i\}_{i=1...N_S}$ pour des décalages d positifs [82].*

Le tableau III.6 confronte ces résultats aux seuils d'acceptations définis précédemment. Il apparaît que les statistiques X_1, X_2, X_3 et X_4 sont en dessous de leur seuil à 90%, et que 99% des valeurs de X_5 appar-

tiennent à l'intervalle $[-3;3]$. Par conséquent, la suite $\{S_i\}_{i=1...N_S}$ peut être considérée comme aléatoire au sens de la norme FIPS 140-2.

Statistique	$\chi^2_{0.9}$	Score
X_1	2.702	0.736
X_2	4.607	1.234
X_3	147.83	138.954
X_4	21.057	20.855
X_5	99% des valeurs $\in [-3;3]$	oui

Tab. III.6 – *Résultats des tests statistiques effectués sur* $\{S_i\}_{i=1...N_S}$ *[82]*

.

III.5 Conclusion

Le générateur d'horloge aléatoire proposé dans ce troisième et dernier chapitre a été développé spécifiquement pour répondre aux besoins du système d'alimentation présenté au second chapitre. Il offre un compromis adéquat entre performances et consommation, tout en respectant les contraintes technologiques des cartes à puces. Son architecture repose entre autre, sur un oscillateur chaotique de type *double-scroll*. Ce dernier a été fabriqué avec succès en technologie AMS CMOS $0.35\ \mu m$. Le générateur a été simulé à partir des paramètres du procédé CMOS $0.18\ \mu m$ fourni par STMicroelectronics. Pour une plage de variation fréquentielle de $30\ MHz$ centrée sur $20\ MHz$, le circuit consomme moins de $1\ mW$ et sa surface est estimée à $0.01\ mm^2$. Par ailleurs, il peut être utilisé directement pour générer un flux binaire aléatoire de $5\ Mb/s$ conforme à la norme FIPS 140-2. Le générateur proposé a fait l'objet d'un brevet mondial et d'un article en conférence internationale (cf. annexe D).

Conclusion

L'objectif de cette étude était de concevoir et de réaliser un système d'alimentation destiné à protéger les cartes à puce contre les attaques par analyse en courant. Une fois intégré au microcontrôleur de la carte, ce système devait être capable, d'une part, de réguler la tension d'alimentation interne du microcontrôleur à partir de la tension d'alimentation externe fournie par le lecteur et, d'autre part, de décorréler le courant d'alimentation externe du courant d'alimentation interne, le tout, en respectant les contraintes technologiques imposées par les normes associées au support. Enfin, le système proposé devait être implémenté suivant un procédé CMOS $0.18\ \mu m$ de la société STMicroelectronics.

Le premier chapitre met en évidence la nécessité de concevoir de nouvelles protections contre les attaques par analyse du courant consommé. A titre d'introduction, nous avons détaillé une partie des ressources cryptographiques embarquées par les cartes à puce et leur utilisation dans les procédures d'authentification courantes. Nous avons ensuite décrit les différents canaux cachés résultant de l'implémentation électronique des cryptosystèmes, en mettant l'accent sur le canal visé par cette étude : le courant d'alimentation. Nous avons alors exposé les différentes catégories d'attaques basées sur ce dernier. En particulier, l'analyse des attaques de type SPA et DPA a permis de mettre en évidence la nécessité de détruire les corrélations existantes entre le signal de consommation et les données manipulées. Enfin, nous avons expliqué en quoi les contre-mesures actuelles tendent à dégrader les caractéristiques des microcontrôleurs sans vraiment pérenniser leur sécurité.

Le second chapitre propose un nouveau convertisseur de tension DC-DC sur puce dédié à la protection des microcontrôleurs encartables contre les attaques par analyse du courant d'alimentation. Après un bref rappel du vocabulaire lié à la régulation, nous avons décrit le cahier des charges élaboré par la division DSA de la société STMicroelectronics. Nous avons ensuite passé en revue les différents types de convertisseurs proposées dans la littérature. Pris individuellement, aucun d'entre eux ne permet d'atteindre simultanément tous les objectifs fixés par le cahier des charges. En effet, comme nous l'avons vu, les régulateurs linéaires séries n'offrent aucune protection contre les attaques par analyse du courant, les régulateurs linéaires à dérivation engendrent une surconsommation trop élevée et les convertisseurs à éléments commutés requièrent une surface trop importante. Cependant, l'utilisation conjointe de plusieurs de ces solutions, par le biais d'une architecture adéquate, a permis de répondre à nos attentes. En particulier, nous avons constaté que la majeure partie des informations est généralement véhiculée par une faible proportion du courant total. De ce constat est né le principe du convertisseur proposé : en traitant séparément les composantes AC et DC du courant de consommation, notre architecture bi-canal permet d'atteindre un compromis approprié entre régulation, rendement et sécurité, tout en respectant les contraintes de surface du support. La topologie pré-

sentée a été simulé en utilisant Eldo avec les paramètres MM9 d'un procédé CMOS $0.18\ \mu m$ fournies par STMicroelectronics. Les résultats des simulations ont permis de vérifier la qualité de la régulation, la stabilité du système et l'efficacité du masquage. En outre, la reconfiguration dynamique du système en fonction de l'amplitude de la tension d'alimentation externe permet d'atteindre, en toute circonstance, un rendement en puissance supérieur ou égal à celui d'un régulateur linéaire classique. La surface totale du circuit a été estimée à $0.8\ mm^2$, ce qui est plus de cinq fois inférieur à la surface qu'aurait nécessité un circuit reposant uniquement sur des capacités commutées. Le convertisseur proposé a fait l'objet de deux brevets mondiaux et de deux articles en conférences internationales (cf. annexe D).

Le système proposé au second chapitre comprend un générateur d'horloge aléatoire. La conception et la réalisation de ce dernier font l'objet du troisième et dernier chapitre. Dans un état de l'art préliminaire, nous avons vu en quoi les générateurs existants ne répondent pas entièrement à nos attentes. Une solution a néanmoins retenu notre intention : dans son générateur de nombres aléatoires, Intel emploie un oscillateur piloté par un signal de contrôle analogique aléatoire. Cependant, ce signal est engendré par amplification d'un bruit thermique, ce qui occasionne une consommation importante. Afin d'adapter cette solution à notre budget énergétique, nous avons proposé un nouveau générateur de signal analogique aléatoire. Ce dernier repose sur l'échantillonnage aléatoire d'un signal triangulaire afin d'obtenir un signal de contrôle uniformément distribué. En outre, notre générateur exploite un oscillateur chaotique comme source d'entropie. Une étude bibliographique des circuits chaotiques a orienté notre choix vers l'implémentation proposée par Radwan & Al. [147]. L'analyse mathématique et numérique du système non-linéaire décrivant cet oscillateur a ensuite permis de déterminer les valeurs du paramètre de contrôle engendrant un comportement chaotique. Enfin, le générateur a été simulé avec la technologie CMOS $0.18\ \mu m$. Les résultats des simulations ont confirmé l'équirépartition du signal de contrôle. Pour une plage de variation fréquentielle de $30\ MHz$ centrée sur $20\ MHz$, le circuit consomme moins de $1\ mW$ et sa surface a été estimée à $0.01\ mm^2$. Enfin, afin d'évaluer le caractère aléatoire du signal d'horloge ainsi généré, un flux binaire extrait de ce dernier a été soumis à une série de tests statistiques. En définitive, notre circuit permettrait de produire un flux aléatoire de $5\ Mbit/s$ conforme à la norme FIPS 140-2 [166]. Le générateur proposé a fait l'objet d'un brevet mondial et d'un article en conférence internationale (cf. annexe D).

Au début de cette thèse, la division DSA de STMicroelectronics avait planifié la fabrication de plusieurs véhicules de test en technologie CMOS $0.18\ \mu m$. Malheureusement, suite à des difficultés conjoncturelles, aucun de ces *testchips* n'a vu le jour. Il ne nous a donc pas été possible de vérifier expérimentalement les performances du convertisseur proposé. En particulier, il aurait été souhaitable d'évaluer le temps nécessaire à la réalisation d'une attaque DPA sur un microcontrôleur de carte à puce alimenté par ce dernier. Nous aurions ainsi pu comparer l'efficacité de notre solution à celle des contre-mesures présentées dans la littérature. Néanmoins, dans le cadre d'une opération multi-projets menée au sein du laboratoire L2MP, l'oscillateur chaotique a été fabriqué via le service CMP, dans la technologie AMS C35B4 fournie par le CNFM. Malgré une distorsion importante attribuée à la sous-polarisation des suiveurs, les mesures ont confirmé les résultats des simulations post-*layout*.

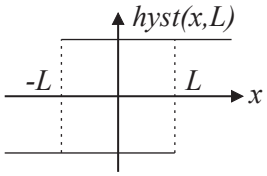
Annexe

A - Spécifications des cartes à puce

Standard	Classe	V_{cc}	f_c	I_{cc} maximum
ISO/IEC 7816-3	Class A	5 V $\pm$ 10%	1 à 5 MHz	60 mA à 5 MHz
	Class B	3 V $\pm$ 10%	1 à 5 MHz	50 mA à 4 MHz
	Class C	1.8 V $\pm$ 10%	1 à 5 MHz	30 mA à 4 MHz
EMV 2000	-	5 V	1 à 5 MHz	50 mA
GSM 11.11	5 V SIM	5 V $\pm$ 10%	1 à 5 MHz	10 mA à 5 MHz 200 μA à 1 MHz (veille) 200 μA (horloge arrêtée)
GSM 11.12	3 V SIM	3 V $\pm$ 10%	1 à 5 MHz	6 mA à 3.3 V et 5 MHz 200 μA à 1 MHz (veille) 100 μA (horloge arrêtée)
GSM 11.18	1.8 V SIM	1.8 V $\pm$ 10%	1 à 5 MHz	4 mA à 1.8 V et 5 MHz 200 μA à 1 MHz (veille) 100 μA (horloge arrêtée)
ETSI TS 102.221	Class A	5 V $\pm$ 10%	1 à 5 MHz	10 mA à 5 MHz 200 μA à 1 MHz (veille) 60 mA à 5 MHz (spécial)
	Class B	3 V $\pm$ 10%	1 à 5 MHz	7.5 mA à 5 MHz 6 mA à 4 MHz 200 μA à 1 MHz (veille) 50 mA à 5 MHz (spécial)
	Class C	1.8 V $\pm$ 10%	1 à 5 MHz	5 mA à 5 MHz 4 mA à 4 MHz 200 μA à 1 MHz (veille) 30 mA à 5 MHz (spécial)

Tab. A.1 – *Caractéristiques électriques des cartes à puce (principaux standards).*

B - Définition des fonctions non-linéaires

Nom	Définition	Dérivation
Heaviside	$H(x) = \begin{cases} 1 & \text{si} \quad x > 0 \\ 0 & \text{si} \quad x < 0 \end{cases}$	Triviale.
Hystérésis symétrique		Triviale.
Opérateur d'extension concave	$u_+(x) = \begin{cases} x & \text{si} \quad x > 0 \\ 0 & \text{si} \quad x < 0 \end{cases}$	Triviale.
Opérateur d'extension convexe	$u_+(x) = \begin{cases} 0 & \text{si} \quad x > 0 \\ x & \text{si} \quad x < 0 \end{cases}$	Triviale.
Valeur absolue	$\lvert x \rvert = \begin{cases} x & \text{si} \quad x > 0 \\ -x & \text{si} \quad x < 0 \end{cases}$	$\frac{d\lvert x \rvert}{dx} = u_+(x) - u_-(x)$
Signe	$sgn(x) = \begin{cases} 1 & \text{si} \quad x > 0 \\ 0 & \text{si} \quad x = 0 \\ -1 & \text{si} \quad x < 0 \end{cases}$	$sgn'(x) = H(x) - H(-x)$
Saturation symétrique	$sat(x,L) = \begin{cases} -L & \text{si} \quad x < -L \\ x & \text{si} \quad \lvert x \rvert < L \\ L & \text{si} \quad x > L \end{cases}$	$sat'(x,L) = \frac{\lvert x+L \rvert - \lvert x-L \rvert}{2}$
Fonction porte modifiée	$\prod_\epsilon(x) = \begin{cases} 1 & \text{si} \ x \in]-\epsilon; -\epsilon] \\ 0 & \text{sinon} \end{cases}$	Triviale.

Tab. B.1 – *Définitions des fonctions non-linéaires utilisées au chapitre III [127].*

C - Solutions du système linéarisé (P_a^l)

C.1 - Caractérisation des points fixes p_{-1} et p_1

La matrice A possède trois valeurs propres [82] : $\lambda_1 \in \mathbb{R}$, $\lambda_2 \in \mathbb{C} = \alpha + i\omega$ et $\lambda_3 \in \mathbb{C} = \overline{\lambda_2}$. Leurs expressions dépendent de a [82] :

∞ si $a = 0$:

$$\lambda_1 = \lambda_2 = \lambda_3 = 0 \tag{C.70}$$

∞ si $a = 3$:

$$\left\{ \begin{array}{l} \lambda_1 = -1 - \sqrt[3]{2} \\ \lambda_2 = -1 - \sqrt[3]{2} \cdot e^{i\frac{\pi}{3}} \\ \lambda_3 = -1 - \sqrt[3]{2} \cdot e^{-i\frac{\pi}{3}} \end{array} \right. \Rightarrow \left\{ \begin{array}{l} \lambda_1 \approx -2.26 \\ Re(\lambda_2) = -1 + \frac{\sqrt[3]{2}}{2} \approx -0.37 \\ Im(\lambda_2) = -1 + \frac{\sqrt[3]{2}\sqrt{3}}{2} \approx 1.09 \end{array} \right. \tag{C.71}$$

∞ si $a < 3$:

$$\left\{ \begin{array}{l} \lambda_1 = R(a) + \dfrac{a\,(a-3)}{9R(a)} - \dfrac{a}{3} \\ \lambda_2 = -\dfrac{1}{2}\left[R(a) + \dfrac{a\,(a-3)}{9R(a)}\right] + i\dfrac{\sqrt{3}}{2}\left[R(a) - \dfrac{a\,(a-3)}{9R(a)}\right] - \dfrac{a}{3} \\ \lambda_3 = -\dfrac{1}{2}\left[R(a) + \dfrac{a\,(a-3)}{9R(a)}\right] - i\dfrac{\sqrt{3}}{2}\left[R(a) - \dfrac{a\,(a-3)}{9R(a)}\right] - \dfrac{a}{3} \end{array} \right. \tag{C.72}$$

avec

$$R(a) := \frac{1}{6}\sqrt[3]{-8a^3 + 36a^2 - 108a + 12\sqrt{9a^4 - 42a^3 + 81a^2}} \tag{C.73}$$

∞ si $a > 3$:

$$\left\{ \begin{array}{l} \lambda_1 = \dfrac{1}{2}\left[R(a) + \dfrac{a\,(a-3)}{9R(a)}\right] + i\dfrac{\sqrt{3}}{2}\left[R(a) - \dfrac{a\,(a-3)}{9R(a)}\right] - \dfrac{a}{3} \\ \lambda_2 = -R(a) - \dfrac{a\,(a-3)}{9R(a)} - \dfrac{a}{3} \\ \lambda_3 = \dfrac{1}{2}\left[R(a) + \dfrac{a\,(a-3)}{9R(a)}\right] - i\dfrac{\sqrt{3}}{2}\left[R(a) - \dfrac{a\,(a-3)}{9R(a)}\right] - \dfrac{a}{3} \end{array} \right. \tag{C.74}$$

Par suite, l'inversion de la matrice de passage III.38 permet, via la relation III.32, de déterminer, pour la condition initiale δ_{X_0}, la solution du système linéarisé autour de p_{-1} et p_1 [82] :

$$\left\{ \begin{array}{rcl} \delta_x(t) & = & \beta_1 e^{\lambda_1 t} + e^{\alpha t}\left[\beta_2 cos\,(\omega t) + \beta_3 sin\,(\omega t)\right] \\ \delta_y(t) & = & \beta_1\lambda_1 e^{\lambda_1 t} + e^{\alpha t}\left[(\beta_2\alpha + \beta_3\omega)\,cos\,(\omega t) + (\beta_3\alpha - \beta_2\omega)\,sin\,(\omega t)\right] \\ \delta_z(t) & = & \beta_1\lambda_1^2 e^{\lambda_1 t} + e^{\alpha t}\left[\left(\beta_2\alpha^2 + 2\beta_3\alpha\omega - \beta_2\omega^2\right)cos\,(\omega t) + \left(\beta_3\alpha^2 - 2\beta_2\alpha\omega - \beta_3\omega^2\right)sin\,(\omega t)\right] \end{array} \right. \tag{C.75}$$

avec

$$\left\{ \begin{array}{rcl} \beta_1 & = & \dfrac{\left(\alpha^2 + \omega^2\right)\delta_{x_0} - 2\alpha\delta_{y_0} + \delta_{z_0}}{(\lambda_1 - \alpha)^2 + \omega^2} \\ \beta_2 & = & \dfrac{\lambda_1\left(\lambda_1 - 2\alpha\right)\delta_{x_0} + 2\alpha\delta_{y_0} - \delta_{z_0}}{(\lambda_1 - \alpha)^2 + \omega^2} \\ \beta_3 & = & \dfrac{\lambda_1\left(\alpha^2 - \omega^2 - \lambda_1\alpha\right)\delta_{x_0} + \left(\omega^2 - \alpha^2 + \lambda_1^2\right)\delta_{y_0} + (\alpha - \lambda_1)\,\delta_{z_0}}{\omega\left[(\lambda_1 - \alpha)^2 + \omega^2\right]} \end{array} \right. \tag{C.76}$$

La physionomie de la solution C.75 confirme le rôle prépondérant des valeurs propres sur la dynamique du système.

C.2 - Caractérisation du point fixe p_0

La matrice A_ϵ possède trois valeurs propres [82] : $\lambda_1 \in \mathbb{R}$, $\lambda_2 \in \mathbb{C} = \alpha + i\omega$ et $\lambda_3 \in \mathbb{C} = \overline{\lambda_2}$. Leurs expressions dépendent de a [82] :

∞ si $a = 0$:

$$\lambda_1 = \lambda_2 = \lambda_3 = 0 \tag{C.77}$$

∞ si $a = 3$:

$$\left\{\begin{array}{l} \lambda_1 = -1 - \sqrt[3]{\dfrac{3}{\epsilon} - 2} \\ \lambda_2 = -1 + \sqrt[3]{\dfrac{3}{\epsilon} - 2} \cdot e^{i\frac{2\pi}{3}} \\ \lambda_3 = -1 - \sqrt[3]{\dfrac{3}{\epsilon} - 2} \cdot e^{-i\frac{2\pi}{3}} \end{array}\right. \Rightarrow \left\{\begin{array}{l} \lambda_1 = -1 - \sqrt[3]{\dfrac{3}{\epsilon} - 2} \\ Re(\lambda_2) = -1 - \dfrac{1}{2}\sqrt[3]{\dfrac{3}{\epsilon} - 2} \\ Im(\lambda_2) = \dfrac{\sqrt{3}}{2}\sqrt[3]{\dfrac{3}{\epsilon} - 2} \end{array}\right. \underset{\epsilon=0.1}{\Rightarrow} \left\{\begin{array}{l} \lambda_1 \approx 2.03 \\ Re(\lambda_2) \approx -2.52 \\ Im(\lambda_2) \approx 2.63 \end{array}\right. \tag{C.78}$$

∞ si $a \in]0; 3[$:

$$\left\{\begin{array}{l} \lambda_1 = R(a) + \dfrac{a\,(a-3)}{9R(a)} - \dfrac{a}{3} \\ \lambda_2 = -\dfrac{1}{2}\left[R(a) + \dfrac{a\,(a-3)}{9R(a)}\right] + i\dfrac{\sqrt{3}}{2}\left[R(a) - \dfrac{a\,(a-3)}{9R(a)}\right] - \dfrac{a}{3} \\ \lambda_3 = -\dfrac{1}{2}\left[R(a) + \dfrac{a\,(a-3)}{9R(a)}\right] - i\dfrac{\sqrt{3}}{2}\left[R(a) - \dfrac{a\,(a-3)}{9R(a)}\right] - \dfrac{a}{3} \end{array}\right. \tag{C.79}$$

avec

$$R(a) := \frac{\sqrt[3]{4a}}{6}\sqrt[3]{2a^2 - 9a + 27\left(1 - \frac{1}{\epsilon}\right) + 3\sqrt{3}\sqrt{\left(3 - \frac{4}{\epsilon}\right)a^2 - 2\left(7 - \frac{9}{\epsilon}\right)a + 27\left(1 - \frac{1}{\epsilon}\right)^2}} \tag{C.80}$$

Les expressions des vecteurs V_1, V_2 et V_3, des sous espaces propres associés, de la matrice Λ, de son inverse et de la solution du système linéarisé, sont, pour p_0, formellement identiques à celles établies pour $p_{\pm 1}$. Seules différent les expressions de λ_1, α et ω.

D - Valorisation

D.1 - Brevets

- V. Telandro, A. Malherbe and E. Kussener, "Secure supply of an integrated circuit", US2006176032, EP1688869 (A1), FR2881851 (A1), October 10, 2006.
- V. Telandro, A. Malherbe and E. Kussener, "Scrambling of the current signature of an integrated circuit", US2006176033, EP1688870 (A1), FR2881852 (A1), October 10, 2006.
- V. Telandro, F. Chaillan et E. Kussener, "Generator of a pseudo-random digital flow", US2006279366, EP1727276 (A1), FR2886426 (A1), December 14, 2006.

D.2 - Publications

- V. Telandro, E. Kussener, A. Malherbe and H. Barthélemy, "On-chip voltage regulator protecting against power analysis attacks", in *Proceedings of the IEEE Midwest Symposium on Circuits and Systems (MWSCAS'06)*, vol. 2, pp. 507-511, San Juan, Puerto Rico, Aug. 2006.
- V. Telandro, B. Duval, F. Chaillan and E. Kussener, "Chaos based random clock generator", in *Proceedings of the IEEE Midwest Symposium on Circuits and Systems (MWSCAS'06)*, vol. 2, pp. 2-6, San Juan, Puerto Rico, Aug. 2006.
- V. Telandro, E. Kussener and A. Malherbe, "Convertisseur de tension DC/DC bi-canal dédié à la protection des cartes à puce", in *Proceedings of the 6th Faible Tension Faible Consommation Conference (FTFC'07)*, Paris, France, May 2007.

D.3 - Poster

- V. Telandro, "On-chip Voltage Regulator Protecting Smart Cards Against Power Analysis Attacks", EDAA PhD Forum of the *Design, Automation and Test in Europe Conference (DATE'07)*, Nice, France, Apr. 2007.

Bibliographie

[1] P.-Y. Liardet, "Ingénierie cryptographique - implantations sécurisées," Ph.D. dissertation, Université de Montpellier II, 161, rue ADA - 34000 Montpellier cedex - France, July 2006. 1, 15, 20

[2] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," *Lecture Notes in Computer Science*, vol. 1109, pp. 104–113, 1996, Springer-Verlag. 1, 14

[3] R. H. Dennard, F. H. Gaensslen, H.-N. Yu, V. L. Rideout, E. Bassous, and A. R. Leblanc, "Design of ion-implanted MOSFET's with very small physical dimensions," *IEEE Journal of Solid-State Circuits*, vol. 9, no. 3, pp. 256–268, Oct. 1974. 2, 27

[4] S. Moore, R. Anderson, and M. Kuhn, "Improving smartcard security using self-timed circuit technology," in *Proceedings of the 8th IEEE International Symposium on Asynchronous Circuit And Systems (ASYN'02)*, Manchester, UK, Apr. 2002, pp. 23–58. 2, 23, 27

[5] J. Dethloff and H. Gröttrup, "Identifikanden/identifikationsschalter," German Patent DE1 945 777C3, 1982. 5

[6] *Identification cards - Physical characteristics*, International Organization for Standardization Std. ISO/IEC 7810, 1985.
URL : http://www.cyberd.co.uk/support/technotes/isocards.htm 5

[7] *Identification cards - Integrated circuit cards*, International Organization for Standardization Std. ISO/IEC 7816, 1987.
URL : http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx 5, 6

[8] C. G. Wensley, S. Gustafson, and C. R. Nelson, "Card with embedded IC and electrochemical cell," European Patent EP1 623 460, Feb. 8, 2006.
URL : http://v3.espacenet.com/textdoc?DB=EPODOC&IDX=EP1623460&F=0 5

[9] *Identification cards - Contactless integrated circuit(s) cards - Proximity cards*, International Organization for Standardization Std. ISO/IEC 14 443, 1987. 6

[10] *Identification cards - Contactless integrated circuit(s) cards - Vicinity cards*, International Organization for Standardization Std. ISO/IEC 15 693, 2001. 6

[11] *Data Encryption Standard (DES)*, NIST Std. FIPS 46-3, Oct. 1999.
URL : http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf 7, 9, 10

[12] W. Rankl and W. Effing, *Smart Card Handbook*, 3rd ed. West Sussex, England: John Wiley & Sons, 2003. 7, 8, 11

[13] B. Schneier, *Cryptographie appliquée*. Paris, France: Vuibert, Jan. 2001. 9, 10

[14] C. Tavernier, *Les cartes à puce : Guide du concepteur et du développeur*. Paris, France: Dunod, 2002. 9

[15] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.
URL : http://www.cs.ucla.edu/~jkong/research/security/shannon1949.pdf 10

[16] *American National Standard Data Encryption Algorithm*, ANSI Std. X3.92-1981, Dec. 1980. 10

[17] W. Diffie and M. Hellman, "Exhaustive cryptanalysis of the NBS data encryption standard," *Computer*, pp. 74–84, June 1977. 10, 13

[18] *Advanced Encryption Standard (AES)*, NIST Std. FIPS 197, Nov. 2001.
URL : http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf 11

[19] R. L. Rivest, A. Shamir, and L. M. Leonard, "Cryptographic communications system and method," U.S. Patent US4 405 829, Sept. 20, 1983.
URL : http://v3.espacenet.com/textdoc?DB=EPODOC&IDX=US4405829&F=0 11

[20] J.-F. Dhem and N. Feyt, "Hardware and software symbiosis helps smartcard evolution," *IEEE Micro*, vol. 21, no. 6, pp. 14–25, Dec. 2001. 11

[21] H. Bar-El, "Known atacks against smartcards," White Paper, Discretix Technologies Ltd., Aug. 2003.
URL : www.discretix.com/PDF/Known%20Attacks%20Against%20Smartcards.pdf 11

[22] R. Anderson and M. Kuhn, "Tamper resistance - a cautionary note," in *Proceedings of the 2nd USENIX Workshop on Electronic Commerce*, Oakland, CA, USA, Nov. 1996, pp. 1–11.
URL : http://www.cl.cam.ac.uk/~mgk25/tamper.pdf 12

[23] T. W. Lee and S. V. P. (eds.), *Microelectronic Failure Analysis, Desk Reference*, 5th ed. Materials Park, OH, USA: ASM International, 2004. 12

[24] S. Blythe, B. Fraboni, S. Lall, H. Ahmed, and U. de Riu, "Layout reconstruction of complex silicon chips," *IEEE Journal of Solid-State Circuits*, vol. 28, no. 2, pp. 138–145, Feb. 1993. 12

[25] O. Kömmerling and M. G. Kuhn, "Design principles for tamper-resistant smartcard processors," in *Proceedings of the USENIX Workshop on Smartcard Technology (Smartcard'99)*, Chicago, IL, USA, May 1999, pp. 9–20. 12

[26] J. O. Grabbe, "Smart cards and private currencies," *Laissez Faire City Times*, vol. 3, no. 12, 1999.
URL : http://www.aci.net/kalliste/smartcards.htm 12

[27] J. Daniel, D. Moore, and J. Walker, "Focused ion beams for microfabrication," *Engineering Science and Education Journal*, pp. 53–56, Apr. 1998. 12

[28] M. Witteman, "Advances in smartcard security," Information Security Bulletin ISB0707MW, Riscure, July 2002.
URL : http://www.riscure.com/1_general/articles/ISB0707MW.pdf 13

[29] E. Biham and A. Shamir, "Differential fault analysis of secret key cryptosystems," *Lecture Notes in Computer Science*, vol. 1294, pp. 513–525, 1997, Springer-Verlag. 14

[30] P. C. Kocher, J. Jaffe, and B. Jun, "Introduction to differential power analysis and related attacks," Cryptography Research, Inc., Tech. Rep., 1998.
URL : http://www.cryptography.com/resources/whitepapers/DPATechInfo.pdf 15, 17, 20

[31] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," *Lecture Notes in Computer Science*, vol. 1666, pp. 388–397, Aug. 1999, Springer-Verlag. 15, 17, 18, 20, 21

[32] W. V. Eck, "Electromagnetic radiation from video display units: An eavesdropping risk?" *Computers & Security*, vol. 4, pp. 269–286, 1985.
URL : http://www.uninett.no/wlan/download/emr.pdf 15

[33] K. F. Gazarek, "Cabinets for electromagnetic interference/radio-frequency interference and TEMPEST shielding," *Data Processing & Communications Security*, vol. 9, no. 6, pp. 12–13, Aug. 1985. 15

[34] J.-J. Quisquater and D. Samyde, "Electro magnetic analysis (EMA): Measures and countermeasures for smart cards," *Lecture Notes in Computer Science*, vol. 2140, pp. 200–210, 2001, Springer-Verlag. 15

[35] H. Handschuh, "Smartcard security - contactless technology security issues," Information Security Bulletin ISB0903HH, CHI Publishing Ltd., Apr. 2004.
URL : http://www.chi-publishing.com/samples/ISB0903HH.pdf 15

[36] A. Shamir and E. Tromer, "Acoustic cryptanalysis," rump session at Proceedings of Eurocrypt'2004, Interlaken, Switzerland, May 2004.
URL : http://www.wisdom.weizmann.ac.il/~tromer/acoustic/ 15

[37] A. Chandrakasan, S. Sheng, and R. Brodersen, "Low-power CMOS digital design," *IEEE Journal of Solid-State Circuits*, vol. 27, no. 4, pp. 473–484, Apr. 1992. 15

[38] D. Suzuki, M. Saeki, and T. Ichikawa, "DPA leakage models for CMOS logic circuits," *Lecture Notes in Computer Science*, no. 3659, pp. 366–382, Feb. 2005, Springer-Verlag. 15

[39] D. Suzuki, M. Saeki, and T. Ichikawa, "Random switching logic: A countermeasure against DPA based on transition probability," ePrint report 2004/346, Cryptology ePrint Archive, Dec. 2004.
URL : http://eprint.iacr.org/2004/346.pdf 15, 24

[40] M.-L. Akkar, R. Bevan, P. Dischamp, and D. Moyart, "Power analysis: What is now possible..." *Lecture Notes in Computer Science*, vol. 1976, pp. 489–502, 2000, Springer-Verlag. 16, 22

[41] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Investigations of power analysis attacks on smartcards," in *Proceedings of the USENIX Workshop on Smart-Card Technology (Smartcard 99)*, May 1999, pp. 151–162.
URL : http://www.usenix.org/events/smartcard99/full_papers/messerges/messerges.pdf 16

[42] M. Fournigault, P.-Y. Liardet, Y. Teglia, A. Trémeau, and F. Robert-Inacio, "Reverse engineering of embedded software using syntactic pattern recognition," *Lecture Notes in Computer Science*, vol. 4277, pp. 527–536, 2006, proceedings of Information Security 06. 18

[43] J. A. Muir, "Techniques of side channel cryptanalysis," Master's thesis, University of Waterloo, Ontario, Canada, July 2001. 19

[44] M.-L. Akkar, "Attaques et méthodes de protections de systèmes cryptographiques embarqués," Ph.D. dissertation, Université de Versailles Saint-Quentin-en-Yvelines, 55, avenue de Paris - 78035 Versailles cedex - France, 2004. 20

[45] P. N. Fahn and P. Rearson, "IPA: A new class of power attacks," *Lecture Notes in Computer Science*, vol. 1717, pp. 173–186, 1999, Springer-Verlag. 21

[46] T. Messerges, "Using second-order power analysis to attack DPA resistant software," *Lecture Notes in Computer Science*, vol. 1965, pp. 238–251, 2000, Springer-Verlag. 21

[47] J. Waddle and D. Wagner, "On second-order DPA-type attacks," *Lecture Notes in Computer Science*, vol. 3156, pp. 1–15, 2004, Springer-Verlag. 21

[48] M. Joye, P. Paillier, and B. Schoenmakers, "On second-order DPA-type attacks," *Lecture Notes in Computer Science*, vol. 3659, pp. 293–308, 2005, Springer-Verlag.
URL : http://www.geocities.com/MarcJoye/papers/hodpa05.pdf 21

[49] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," *Lecture Notes in Computer Science*, vol. 1666, pp. 13–28, Aug. 1999, Springer-Verlag.
URL : http://ece.gmu.edu/crypto/ches02/talks_files/Chari.ppt 22

[50] C. Clavier, J.-S. Coron, and N. Dabbous, "Differential power analysis in the presence of hardware countermeasures," *Lecture Notes in Computer Science*, vol. 1965, pp. 252–263, 2000, Springer-Verlag.
URL : www.gemplus.com/smart/rd/publications/pdf/CCD00dpa.pdf 22, 24

[51] L. Goubin, "A refined power-analysis attack on elliptic curve cryptosystems," *Lecture Notes in Computer Science*, vol. 2567, pp. 199–210, 2003, Springer-Verlag. 22

[52] T. Akishita and T. Takagi, "Zero-value point attacks on elliptic curve cryptosystem," *Lecture Notes in Computer Science*, vol. 2851, pp. 218–233, 2003, Springer-Verlag. 22

[53] V. S. Miller, "Use of elliptic curves in cryptography," *Lecture Notes in Computer Science*, vol. 218, pp. 417–426, 1986, Springer-Verlag. 22

[54] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987. 22

[55] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi., "Towards sound approaches to counteract power-analysis attacks," in *Proceedings of Advances in Cryptology (CRYPTO'99)*, Santa Barbara, CA, USA, Aug. 1999, pp. 398–412. 23, 24, 49

[56] L. Goubin and J. Patarin, "DES and differential power analysis - the duplication method," *Lecture Notes in Computer Science*, vol. 1717, pp. 158–172, 1999, Springer-Verlag. 23

[57] M.-L. Akkar and C. Giraud, "An implementation of DES and AES, secure against some attacks," *Lecture Notes in Computer Science*, vol. 2162, pp. 309–318, 2001, Springer-Verlag. 23

[58] J. Coron, "Resistance against differential power analysis for elliptic curve cryptosystems," *Lecture Notes in Computer Science*, vol. 1717, pp. 292–302, 1999, Springer-Verlag. 23

[59] S. J. M. J. C. Ha, "Randomized signed-scalar multiplication of ECC to resist power attacks," *Lecture Notes in Computer Science*, vol. 2523, pp. 551–563, 2003, Springer-Verlag. 23

[60] P.-Y. Liardet and N. Smart, "Preventing SPA/DPA in ECC systems using the jacobi form," *Lecture Notes in Computer Science*, vol. 2162, pp. 391–401, 2001, Springer-Verlag. 23

[61] N. S. D. May, H.L. Muller, "Random register renaming to foil DPA," *Lecture Notes in Computer Science*, vol. 2162, pp. 28–38, 2003, Springer-Verlag. 23

[62] M. Joye and C. Tymen, "Protections against differential analysis for elliptic curve cryptography: An algebraic approach," *Lecture Notes in Computer Science*, vol. 2162, pp. 377–390, 2001, Springer-Verlag. 23

[63] C. Karlof and D. Wagner, "Hidden markov model cryptanalysis," *Lecture Notes in Computer Science*, vol. 2779, pp. 17–34, 2003, Springer-Verlag.
URL : http://digitalassets.lib.berkeley.edu/techreports/ucb/text/CSD-03-1244.pdf 23

[64] J.-J. Quisquater and F. Koeune, "State-of-the-art regarding side channel attacks," Math RiZK and K2Crypt, Tech. Rep., Oct. 2002.
URL : http://www.cryptography.com/resources/whitepapers/DPATechInfo.pdf 23

[65] J. Fournier, S. Moore, H. Li, R. Mullins, and G. Taylor, "Security evaluation of asynchronous circuits," *Lecture Notes in Computer Science*, vol. 2779, pp. 137–141, 2003, Springer-Verlag. 23

[66] F. Gurkaynak, S. Oetiker, H. Kaeslin, N. Felber, and W. Fichtner, "Improving DPA security by using globally-asynchronous locally-synchronous systems," in *Proceedings of the 31st European Solid-State Circuits Conference (ESSCIRC 2005)*, Grenoble, France, Sept. 2005, pp. 407–410.
URL : http://www.iis.ee.ethz.ch/async/pub/esscirc2005.pdf 23

[67] G. F. Bouesse, "Contribution à la conception de circuits intégrés sécurisés : L'alternative asynchrone," Ph.D. dissertation, Institut National Polytechnique de Grenoble, 46, avenue Félix Viallet - 38031 Grenoble Cedex 1 - France, 2005. 23

[68] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," in *Proceedings of the 29th European Solid-State Circuits Conference (ESSCIRC 2002)*, Florence, Italy, Sept. 2002, pp. 403–406.
URL : http://www.ee.ucla.edu/~tiri/files/esscirc2002.pdf 24

[69] J. M. Rabaey, *Digital Integrated Circuits: A Design Perspective*, 1st ed. Upper Saddle River, NJ, USA: Prentice Hall, Dec. 1995. 24

[70] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proceedings of the Design, Automation and Test in Europe Conference (DATE 2004)*, Paris, France, Feb. 2004, pp. 246–251. 24

[71] D. Sokolov, J. Murphy, A. Bystrov, and A. Yakovlev, "Improving the security of dual-rail circuits," *Lecture Notes in Computer Science*, vol. 3156, pp. 282–297, 2004, Springer-Verlag. 24

[72] T. Popp and S. Mangard, "Masked dual-rail pre-charge logic: DPA-resistance without routing constraints," *Lecture Notes in Computer Science*, vol. 3659, pp. 172–186, 2005, Springer-Verlag.
URL : http://www.iaik.tugraz.at/research/sca-lab/publications/pdf/Popp2005MaskedDual-RailPre-Charge.pdf 24

[73] F. Mace, F.-X. Standaert, I. Hassoune, J.-D. Legat, and J.-J. Quisquater, "A dynamic current mode logic to counteract power analysis attacks," in *Proceedings of the 19th Conference on Design of Circuits and Integrated*

Systems (DCIS 2004), Nov. 2004, pp. 186–191.
URL : http://www.dice.ucl.ac.be/crypto/files/publications/pdf227.pdf 24

[74] R. G. Lyons, *Understanding Digital Signal Processing*, 1st ed. Upper Saddle River, NJ,USA: Pearson Education, Nov. 1996. 24

[75] P. Rakers, L. Connell, T. Collins, and D. Russell, "Secure contactless smartcard ASIC with DPA protection," *IEEE Journal of Solid-State Circuits*, vol. 36, no. 3, pp. 559–565, Mar. 2001. 24, 38, 57, 58

[76] A. Shamir, "Protecting smart cards from passive power analysis with detached power supplies," in *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2000)*, vol. 1965, Worcester, MA, USA, Aug. 2000, pp. 71–77. 25, 38, 66

[77] B. S. Lee, "Understanding the terms and definitions of LDO voltage regulators," Texas Instruments, Inc.," Application Report, SLVA079, Oct. 1999.
URL : http://focus.ti.com/lit/an/slva079/slva079.pdf 28

[78] P. E. Allen and D. R. Holberg, *CMOS Analog Circuit Design*, 2nd ed. New York, NY, USA: Oxford University Press, 2002. 29, 30, 31, 81, 140

[79] T. H. Lee, *The Design of CMOS Radio-Frequency Integrated Circuits*, 2nd ed. 32 Avenue of the Americas, New York, NY, USA: Cambridge University Press, 2003. 30

[80] G. A. Rincón-Mora, *Power Management ICs - A Top-Down Design Approach*, 3rd ed., 2006.
URL : http://users.ece.gatech.edu/rincon-mora/publicat/books/pmic_book/pmic_book.htm 32, 33, 66

[81] G. A. Rincón-Mora, "Current efficient, low voltage, low dropout regulators," Ph.D. dissertation, Georgia Institute of Technology, 686 Cherry Street, Atlanta, GA, USA, Nov. 1996.
URL : http://users.ece.gatech.edu/rincon-mora/publicat/books/thesis/ldo_book.pdf 34, 55

[82] F. Chaillan, "Sécurisation des smart cards par masquage de signal informationnel sur canal secondaire," Ph.D. dissertation, Université du Sud Toulon Var (USTV), BP 20132-83957 - La Garde Cedex, Dec. 2006. 34, 94, 101, 116, 117, 119, 120, 121, 122, 123, 124, 125, 126, 146, 147, 148, 155, 156

[83] M. Fournigault, "Evaluation de la sécurité d'une puce électronique par traitement d'images," Ph.D. dissertation, Université de Provence (Aix-Marseille 1), 3, place Victor-Hugo - 13331 Marseille cedex 3, Dec. 2007. 34, 94

[84] F. Rémond, "La plupart des circuits mixtes ne descendront pas sous les 0.18 μm avant longtemps," Electronic International Hebdo, Nov. 2005. 35

[85] B. J. Blalock, P. E. Allen, and G. A. Rincón-Mora, "Designing 1-V op amps using standard digital CMOS technology," *IEEE Transactions on Circuits and Systems—Part II: Analog and Digital Signal Processing*, vol. 45, no. 7, pp. 769–780, 1998.
URL : http://users.ece.gatech.edu/rincon-mora/publicat/journals/tcas98_1v_amps.pdf 36

[86] G. A. Rincón-Mora and P. E. Allen, "A low-voltage, low quiescent current, low drop-out regulator," *IEEE Journal of Solid-State Circuits*, vol. 33, no. 1, pp. 36–44, Jan. 1998.
URL : http://users.ece.gatech.edu/rincon-mora/publicat/journals/jssc98_lvldo.pdf 36, 57

[87] R. Velghe, D. Klaassen, and F. Klaassen, "MOS Model 9 (MM9)," Philips Research Laboratories, Eindhoven, The Netherlands., Tech. Rep. 37

[88] H. Barthélemy, S. Meillere, and E. Kussener, "CMOS sinusoidal oscillator based on current-controlled current conveyors," *IEE Electronics Letters*, vol. 38, no. 21, pp. 1254–1256, Oct. 2002. 37

[89] G. B. Ratanpal, R. D. Williams, and T. N. Blalock, "An on-chip signal suppression countermeasure to power analysis attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 3, pp. 179–189, Sept. 2004. 38, 56

[90] J. Dickson, "On-chip voltage generation in MNOS integrated circuits using an improved voltage multiplier technique," *IEEE Journal of Solid-State Circuits*, vol. 11, pp. 374–378, June 1976. 40, 41

[91] G. W. den Besten and B. Nauta, "Embedded 5V-to-3.3V voltage regulator for supplying digital IC's in 3.3V CMOS technology," *IEEE Journal of Solid-State Circuits*, vol. 33, no. 7, pp. 956–962, July 1998. 41, 42, 77

[92] H. J. Shin, S. Reynolds, K. R. Wrenner, T. Rajeevakumar, S. Gowda, and D. J. Pearson, "Low-dropout on-chip voltage regulator for low-power circuits," in *Proceedings of the IEEE Symposium on Low Power Electronics*, 1994, pp. 77–78. 41, 42, 76

[93] *TPS731xx : Cap-Free, NMOS, 150mA Low-Dropout Regulator with Reverse Current Protection*, SBVS034A, Texas Instruments, Sept. 2003. 42

[94] G. A. R.-M. V. Gupta and P. Raha, "Analysis and design of monolithic, high PSR, linear regulators for SOC applications," in *Proceedings of the IEEE International System on Chip (SOC) Conference*, Santa Clara, CA, USA, Sept. 2004, pp. 311–315.
URL : http://users.ece.gatech.edu/rincon-mora/publicat/journals/socc04_psr.pdf 47, 48, 53, 54, 76

[95] A. Makharia and G. A. Rincón-Mora, "Integrating power inductors onto the IC - SOC implementation of inductor multipliers for DC-DC converters," in *Proceedings of the IEEE Industrial Electronics Conference (IECON'03)*, vol. 1, Roanoke, VA, USA, Nov. 2003, pp. 556–561.
URL : http://users.ece.gatech.edu/rincon-mora/publicat/journals/iecon03_ind_mult.pdf 60

[96] G. A. Rincón-Mora and P. E. Allen, "Active capacitor multiplier in miller-compensated circuits," *IEEE Journal of Solid-State Circuits*, vol. 35, no. 1, pp. 26–32, Jan. 2000.
URL : http://users.ece.gatech.edu/rincon-mora/publicat/journals/jssc00_ldo-cx.pdf 60

[97] M. Makowski and D. Maksimović, "Performance limits of switched-capacitor DC-DC converters," in *Proceedings of the IEEE Power Electronics Specialists Conference (PESC'95)*, vol. 2, June 1995, pp. 1215–1221. 61

[98] S. C. W. C. K. Tse and M. H. L. Chow, "On lossless switched-capacitor power converters," *IEEE Transactions on Power Electronics*, vol. 10, no. 3, pp. 286–291, May 1995. 61, 62

[99] S. Zhou and G. A. Rincón-Mora, "A high efficiency, soft switching DC-DC converter with adaptive current-ripple control for portable applications," *IEEE Transactions on Circuits and Systems—Part II: Analog and Digital Signal Processing*, vol. 53, no. 4, pp. 319–323, Apr. 2006.
URL : http://users.ece.gatech.edu/rincon-mora/publicat/journals/tcasii06_adp_rip2.pdf 62

[100] *TPS605xx : HIGH EFFICIENCY, 250-mA STEP-DOWN CHARGE PUMP*, SLVS391B, Texas Instruments, Feb. 2002. 62, 65

[101] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Optimized control of the «flying»-capacitor operating voltage in «gear-box»-charge-pumps," in *Proceedings of the IEEE Power Electronics Specialist Conference (PESC'03)*, vol. 2, Acapulco, Mexico, June 2003, pp. 610–615. 62

[102] A. Shamir, "Protecting smart cards from power analysis with detached power supplies," European Patent EP1 113 386, July 4, 2001.
URL : http://v3.espacenet.com/textdoc?DB=EPODOC&IDX=EP1113386&F=0 66, 67

[103] H. Chung, B. O, and A. Ioinovici, "Switched-capacitor-based DC-to-DC converter with improved inputcurrent waveform," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS'96)*, vol. 1, Atlanta, GA, USA, May 1996, pp. 541–544. 67

[104] R. J. Baker, W. L. Harry, and D. E. Boyce, *CMOS Circuit Design, Layout and Simulation*, 2nd ed. Wiley-IEEE Press, Oct. 2004. 75, 80, 87, 138, 139, 140, 141

[105] M. G. Degrauwe, J. Rijmenants, E. A. Vittoz, and H. J. D. Man, "Adaptive biasing CMOS amplifier," *IEEE Journal of Solid-State Circuits*, vol. 17, no. 3, pp. 522–528, June 1982. 77, 78

[106] J. H. Huijsing, *Operational Amplifiers : Theory and Design*, 1st ed. P.O. Box 17, 3300, AA Dordrecht, The Netherlands: Kluwer Academics Publishers, 2001. 77

[107] K.-J. de Langen and J. H. Huijsing, *Compact Low-Voltage and High-Speed CMOS, BiCMOS and Bipolar Operational Amplifiers*, 1st ed. P.O. Box 17, 3300, AA Dordrecht, The Netherlands: Kluwer Academics Publishers, 1999. 77

[108] E. A. Vittoz and J. Fellrath, "CMOS analog integrated circuits based on weak inversion operation," *IEEE Journal of Solid-State Circuits*, vol. 12, no. 3, pp. 224–231, June 1977. 77, 83, 84

[109] Y. Nakagome, H. Tanaka, K. Takeuchi, E. Kume, Y. Watanabe, T. Kaga, Y. Kawamoto, F. Murai, R. Izawa, D. Hisamoto, T. Kisu, T. Nishida, E. Takeda, and K. Itoh, "An experimental 1.5-V 64-Mb DRAM," *IEEE Journal of Solid-State Circuits*, vol. 26, no. 4, pp. 465–472, Apr. 1991. 79

[110] R. Perigny, U.-K. Moon, and G. Temes, "Area efficient CMOS charge pump circuits," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS'01)*, vol. 1, Sydney, NSW, Australia, May 2001, pp. 492–495. 80

[111] B. Razavi, *Design of Analog CMOS Integrated Circuits*, 1st ed. Columbus, OH, USA: McGraw-Hill Science / Engineering / Math, 2000. 82, 140

[112] H. J. Oguey and D. Aebischer, "CMOS current reference without resistance," *IEEE Journal of Solid-State Circuits*, vol. 32, no. 7, pp. 1132–1135, July 1997. 83, 84, 85, 90

[113] K. C. Smith and A. S. Smith, "The current conveyor–a new circuit building block," *Proceedings of the IEEE*, vol. 56, pp. 1368–1369, Aug. 1968. 83

[114] F. Guigues and E. Kussener, "Sub-1V Oguey's current reference without resistance," in *Proceedings of the 13th IEEE International Conference on Electronics, Circuits and Systems (ICECS 2006)*, Nice, France, Dec. 2006. 84

[115] R. Gregorian, *Introduction to CMOS Op-Amps and Comparators*, 1st ed. P.O. Box 17, 3300, AA Dordrecht, The Netherlands: Kluwer Academics Publishers, 2001. 85

[116] C. Saint and J. Saint, *IC Mask Design*. Columbus, OH, USA: McGraw-Hill Science/Engineering/Math, 2002. 85, 131, 133

[117] D. Clein, *CMOS IC Layout : Concepts, Methodologies, and Tools*, 1st ed. Elsevier, 200 Wheeler road, Burlington, MA 01803, USA: Newnes, 1999. 85, 131

[118] A. Hastings, *The Art of Analog Layout*, 2nd ed. Upper Saddle River, NJ 07458, USA: Prentice Hall, Inc., 2005. 85, 131

[119] G. Bontempo, T. Signorelli, and F. Pulvirenti, "Low supply voltage, low quiescent current, ULDO linear regulator," in *Proceedings of the IEEE International Conference on Circuits and Systems (ICECS'01)*, vol. 1, Malta, Sept. 2001, pp. 409–412. 86

[120] L. Najafizadeh and I. Filanovsky, "A simple voltage reference using transistor with ztc point and PTAT current source," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS'04)*, vol. 1, Vancouver, Canada, May 2004, pp. 909–911. 90

[121] E. Kussener and H. Barthélemy, "Versatile macromodel for the power supply of submicronic CMOS microprocessors based on voltage down converter," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS'02)*, vol. 5, Scottsdale, AZ, USA, May 2002, pp. 821–824. 93, 94

[122] E. Kussener, "Conception de circuits integres de regulation intelligente pour les microprocesseurs securises (carte a puce)," Ph.D. dissertation, Université des Sciences et Technologies de Lille, 59655 Villeneuve d'Ascq Cedex - France, July 2002. 93, 94

[123] W. T. Holman, J. A. Connelly, and A. Dowlatabadi, "An integrated analog/digital random noise source," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 44, no. 6, pp. 521–528, Feb. 1997. 102, 103, 104

[124] C. S. Petrie and J. A. Connelly, "A noise-based random bit generator IC for applications in cryptography," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS'98)*, vol. 2, Monterey, CA, May 1998, pp. 197–200. 102

[125] E. Hoffman, "Random number generator," US Patent US6 061 702, 2000. 102, 105

[126] A. S. Elwakil and M. P. Kennedy, "Construction of classes of circuit independent chaotic oscillators using passive-only nonlinear devices," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 48, no. 3, pp. 289–307, Mar. 2001. 102, 107, 124

[127] M. Delgado-Restituto and A. Rodriguez-Vazquez, "Integrated chaos generators," *Proceedings of the IEEE*, vol. 90, no. 5, pp. 747–767, May 2002. 102, 105, 106, 107, 153

[128] M. P. Kennedy, "Three steps to chaos-Part I: Evolution," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 40, no. 10, pp. 640–656, Oct. 1993. 102, 108, 117, 118

[129] M. P. Kennedy, "Three steps to chaos-Part II: A chua's circuit primer," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 40, no. 10, pp. 657–674, Oct. 1993. 102

[130] T. Stojanovski and L. Kocarev, "Chaos-based random number generators-Part I: Analysis," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 48, no. 3, pp. 281–288, Mar. 2001. 102

[131] T. Stojanovski and L. Kocarev, "Chaos-based random number generators-Part II: Practical realization," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 48, no. 3, pp. 381–385, Mar. 2001. 102

[132] S. W. Golomb, *Shift Register Sequences*, 1st ed. Aegean Park Pr, 1981. 102, 103

[133] P. Horowitz and W. Hill, *The Art of Electronics*, 2nd ed. 32 Avenue of the Americas, New York, NY, USA: Cambridge University Press, 1989. 103

[134] P. Courmontagne, *Ingénierie du signal : Théorie et pratique*, 1st ed. Ellipses Marketing, Jan. 2005. 103

[135] H. Mathieu, *Physique des semiconducteurs et des composants électroniques*, 5th ed. Dunod, Apr. 2001. 104

[136] W. Holman and J. Connelly, "A pseudo-BiCMOS high gain-bandwidth low noise operational amplifier using a Darlington input stage," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS'95)*, vol. 3, Seattle, WA, USA, May 1995, pp. 1724–1727. 104

[137] M. Small and C. K. Tse, "Detecting determinism in time series: The method of surrogate data," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 50, no. 5, pp. 663–672, May 2003. 105

[138] M. Delgado-Restituto and A. Rodriguez-Vazquez, "Design consideration for integrated continous-time chaotic oscillators," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 45, no. 4, pp. 481–495, Apr. 1998. 106, 108

[139] S. Nakagawa and T. Saito, "Design and control of RC VCCS 3-D hysteresis chaos generators," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 45, no. 2, pp. 182–186, Feb. 1998. 106, 107

[140] L. Chua, M. Komuro, and T. Matsumoto, "The double scroll family," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 33, no. 11, pp. 1072–1118, Nov. 1986. 107

[141] L. Chua and G.-N. Lin, "Canonical realization of Chua's circuit family," *IEEE Transactions on Circuits and Systems*, vol. 37, no. 7, pp. 885–902, July 1990. 107

[142] J. Cruz and L. Chua, "An IC chip of Chua's circuit," *IEEE Transactions on Circuits and Systems—Part II: Analog and Digital Signal Processing*, vol. 40, no. 10, pp. 614–625, Oct. 1993. 107

[143] A. Rodriguez-Vazquez and M. Delgado-Restituto, "CMOS design of chaotic oscillators using state variables: a monolithic chua's circuit," *IEEE Transactions on Circuits and Systems—Part II: Analog and Digital Signal Processing*, vol. 40, no. 10, pp. 596–613, Oct. 1993. 107

[144] A. S. Elwakil and M. P. Kennedy, "Improved implementation of chua's chaotic oscillator using current feedback op amp," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 47, no. 1, pp. 76–79, Jan. 2000. 107

[145] M. P. Kennedy, "Chaos in Colpitts oscillator," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 41, no. 11, pp. 771–774, Nov. 1994. 107

[146] A. S. Elwakil, K. N. Salama, and M. P. Kennedy, "An equation for generating chaos and its monolithic implementation," *Int. J. of Bifurcation and Chaos*, vol. 12, no. 12, pp. 2885–2895, 2002. 107, 127

[147] A. G. Radwan, A. M. Soliman, and A.-L. El-Sedeek, "Mos realization of the double-scroll like chaotic equation," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 50, no. 2, pp. 285–288, Feb. 2003. 107, 114, 124, 126, 150

[148] J. Lü, G. Chen, X. Yu, and H. Leung, "Design and analysis of multiscroll chaotic attractors from saturated function series," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 51, no. 12, pp. 2476–2490, Dec. 2004. 107

[149] M. Yalçin, J. Suykens, and J. Vandewalle, "On the realization of n-scroll attractors," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS'99)*, vol. 5, Orlando, FL, USA, May 1999, pp. 483–486. 107

[150] M. Yalçin, S. Ozoguz, J. Suykens, and J. Vandewalle, "n-scroll chaos generators: a simple circuit model," *IEE Electronics Letters*, vol. 37, no. 3, pp. 147–148, Feb. 2001. 107

[151] K. N. Salama, S. Özoguz, and A. S. Elwakil, "Generation of n-scroll chaos using nonlinear transconductors," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS'03)*, vol. 3, Bangkok, Thailand, May 2003, pp. 176–179. 107

[152] O. Gonzales, G. Han, J. de Gyvez, and E. Sanchez-Sinencio, "Lorenz-based chaotic cryptosystem: a monolithic implementation," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 47, no. 8, pp. 1243–1247, Aug. 2000. 107

[153] J. E. Varrientos and E. Sanchez-Sinencio, "A 4-D chaotic oscillator based on differential hysteresis comparator," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 33, no. 7, pp. 542–543, Mar. 1997. 107

[154] S. Ozoguz and A. Elwakil, "On the realization of circuit-independent nonautonomous pulse-excited chaotic oscillator circuits," *IEEE Transactions on Circuits and Systems—Part II: Analog and Digital Signal Processing*, vol. 51, no. 10, pp. 552–556, Oct. 2004. 108, 109

[155] A. Azzouz, R. Duhr, and M. Hasler, "Transition to chaos in a simple nonlinear circuit driven by a sinusoidal voltage source," *IEEE Transactions on Circuits and Systems*, vol. 30, no. 12, pp. 913–914, Dec. 1983. 108

[156] M. P. Kennedy and L. O. Chua, "Van der pol and chaos," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 41, no. 11, pp. 974–980, Oct. 1986. 108

[157] K. Murali, M. Lakshmanan, and L. O. Chua, "The simplest dissipative nonautonomous chaotic circuit," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 41, no. 6, pp. 462–463, June 1994. 108

[158] A. Johansson and H. Floberg, "Random number generation by chaotic double scroll oscillator on chip," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS'99)*, vol. 5, Orlando, FL, USA, May 1999, pp. 407–409. 114

[159] M. Yalçin, J. Suykens, and J. Vandewalle, "True random bit generation from a double-scroll attractor," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 51, no. 7, pp. 1395–1404, July 2004. 114

[160] S. Ergün and S. Örg uz, "Truly random number generators based on a double-scroll attractor," in *Proceedings of the IEEE International Midwest Symposium on Circuits and Systems (MWSCAS'06)*, San Juan, Puerto Rico, USA, Aug. 2006. 114

[161] C. P. Silva, "Shil'nikov's theorem-a tutorial," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 40, no. 10, pp. 675–682, Oct. 1993. 122

[162] P. Bergé, Y. Pomeau, and C. Vidal, *L'ordre dans le chaos*. Paris, France: Hermann, Oct. 1997. 126

[163] H. Barthélemy and G. Bas, "Negative gain transductance amplifier circuit," U.S. Patent US2 006 186 966, Aug. 24, 2006. 126

[164] F. Maloberti, *Analog Design for CMOS VLSI Systems*, 1st ed. Springer, Oct. 2001. 131, 132

[165] C. Toumazou, F. Lidgey, and D. Haigh, *Analogue IC design: the current mode approach.* IEE Press, 1990. 140

[166] *Security requierements for cryptographic modules*, NIST Std. 140-2, Dec. 2002.
URL : http://csrc.nist.gov/cryptval/140-2.htm 143, 150

Index

Titre :	**Conception d'un système d'alimentation intégré dédié à la sécurisation des cartes à puce.**
Résumé :	Le courant d'alimentation d'une carte à puce présente des corrélations significatives avec les données traitées par son microcontrôleur. Les techniques de cryptanalyse dites « par analyse en courant » exploitent ces corrélations pour déterminer les clés secrètes des cryptosystèmes embarqués. Cette étude traite de la conception d'un système d'alimentation sur puce destiné à protéger les microcontrôleurs encartables contre les attaques par analyse en courant. Le nouveau système proposé permet de réguler la tension d'alimentation interne du microcontrôleur à partir de la tension d'alimentation externe fournie par le lecteur, tout en décorrélant le courant d'alimentation externe du courant d'alimentation interne. Sa surface et son rendement respectent les contraintes imposées par le support. De plus, son architecture inclut un nouveau générateur d'horloge aléatoire basé, entre autres, sur un attracteur chaotique de type « *double-scroll* ». Le système a été simulé avec Eldo et les paramètres MM9 d'un procédé CMOS $0.18\ \mu m$ standard de la société STMicroelectronics; les résultats des simulations témoignent de son efficacité. Par ailleurs, l'oscillateur chaotique a été fabriqué suivant le procédé CMOS $0.35\ \mu m$ 2P/4M du fondeur AMS; les mesures expérimentales confirment les résultats théoriques.
Mots-clés :	Carte à puce, canaux cachés, analyse en courant, convertisseur DC-DC, régulateur de tension, horloge aléatoire, générateur de chaos, oscillateur chaotique, circuit intégré, CMOS.

Title:	**Integrated power supply system design dedicated to securing smart cards.**
Abstract:	The power supply current of a smart card exhibits significant correlations with the data processed by its microcontroller. Power analysis attacks exploit these correlations to determine the secret keys of the embedded cryptosystems. This study deals with the design of an on-chip power supply system intended to protect smart card microcontrollers against power analysis attacks. The proposed system allows the microcontroller internal supply voltage to be regulated from the external supply voltage provided by the reader, while uncorrelating the external supply current from internal supply current. Its area and its efficiency respect the smart card constraints. Moreover, its architecture includes a new random clock generator based on, among other things, a double-scroll-like chaotic attractor. The system has been simulated with Eldo using the MM9 model and the parameters of a standard STMicroelectronics $0.18\ \mu m$ CMOS process; the simulation results show its efficiency. Furthermore, the chaotic oscillator has been fabricated using the AMS 2P/4M $0.35\ \mu m$ CMOS process; experimental measurements confirm the theoretical results.
Keywords:	Smart card, side channels, power analysis, DC-DC converter, voltage regulator, random clock, chaos generator, chaotic oscillator, integrated circuit, CMOS.