SÉCURITE HAUT DÉBIT POUR LES SYSTÈMES EMBARQUÉS A BASE DE FPGAs

Trouver le meilleur compromis pour les systèmes embarqués, répondre à ce « besoin » grandissant qu'est la sécurité

PAR JÉRÉMIE CRENNE

Lab-STICC
UNIVERSITÉ EUROPÉENNE DE BRETAGNE
UBS Université de Bretagne-Sud
UNIVERSITY OF MASSACHUSETTS AMHERST 1863
cnrs

SÉCURITE HAUT DÉBIT POUR LES SYSTÈMES EMBARQUÉS À BASE DE FPGAs

« […] *Puis, l'on ferra des récepteurs de télévision bijoux, comme il y a des postes de TSF bijoux. Des postes de poche, grands comme une lampe électrique. Plus besoin d'acheter un journal, l'on se branchera sur l'émission d'information, ou sur l'éditorial politique, ou sur la chronique de mode, ou sur le compte rendu sportif. Voire même sur un problème de mots croisés. Et la rue présentera un singulier spectacle.* »

R. Barjavel, « La télévision, œil de demain », 1947.

Les systèmes embarqués

- ❑ Systèmes autonomes enfouis
- ❑ Spécialisés dans une tâche précise
- ❑ Limités en ressources

Contraintes

- Un coût faible
- Une surface réduite
- Une puissance de calcul minimale
- Une consommation énergétique faible
- Une robustesse importante
- … et une **SÉCURITÉ** adaptée

Sécurité

- ❑ « Vulgariser » depuis les années 80
- ❑ Organisée professionnellement (IACR, International Association for Cryptologic Research)
- ❑ Plus de 1000 papiers scientifiques publiés chaque année
- ❑ Des milliers de chercheurs
- ❑ Des dizaines de conférences internationales

CHES

FIPS 140-2 CRYPTOGRAPHY

Crypto
CONFERENCE

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH

NIST

Asiacrypt
CONFERENCE

Puce FPGA : Field Programmable Gate Array

- ❑ Réseau de blocs logiques sur puce
- ❑ Programmable
- ❑ Déployable « sur-le-champ »

Points Forts

- Usage immédiat
- Cout minimal
- Fort parallélisme
- Idéal pour le prototypage

Points Faibles

- Utilisation des ressources en silicium moins efficace
- Fréquences limitées
- Non adapté aux applications à fort volume
- Consommation élevée

Comment authentifier des données transmises à très haut-débit ?

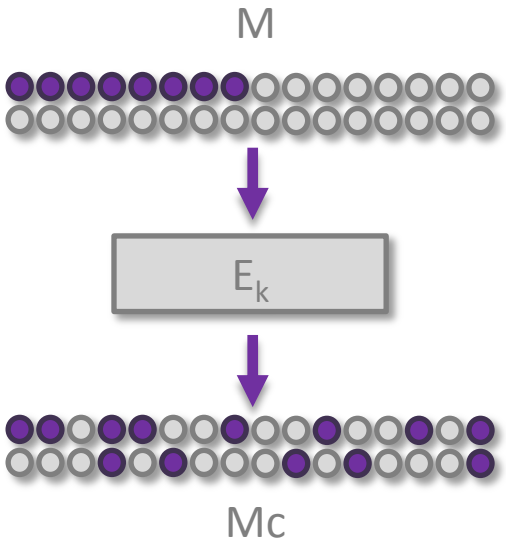
Comment utiliser intelligemment la sécurité pour limiter son impact ?

Comment stocker du matériel cryptographique de façon optimisée ?

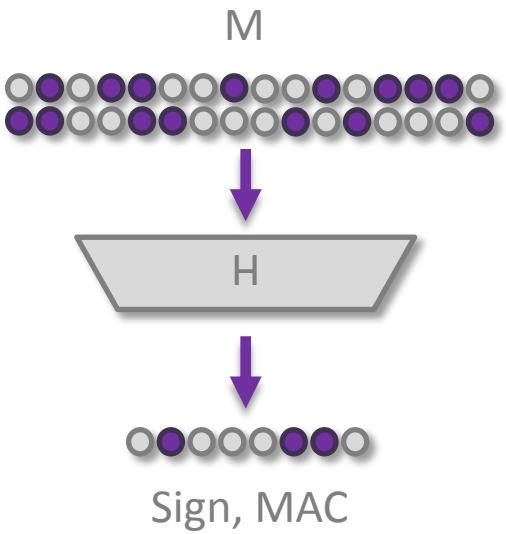
- Introduction
- **GHASH**
- **Sécurité Configurable**
- **Filtre de Bloom**
- **Conclusion**

Chiffrement

- Fonction fournissant la confidentialité
- Exemples : DES, 3DES, AES …



Hachage Cryptographique



- Fonction garantissant l'intégrité ou/et l'authentification
- Exemples : MD5, SHA, RIPEMD …

GHASH (Galois HASHing)

- ❑ Fonction de hachage cryptographique
- ❑ Permet l'authentification de message (MAC)
- ❑ Issue du mode AES-GCM [1]
- ❑ Standardisée NIST
- ❑ Intégration aux protocoles IPSec, TSL et SSH2

Points Forts

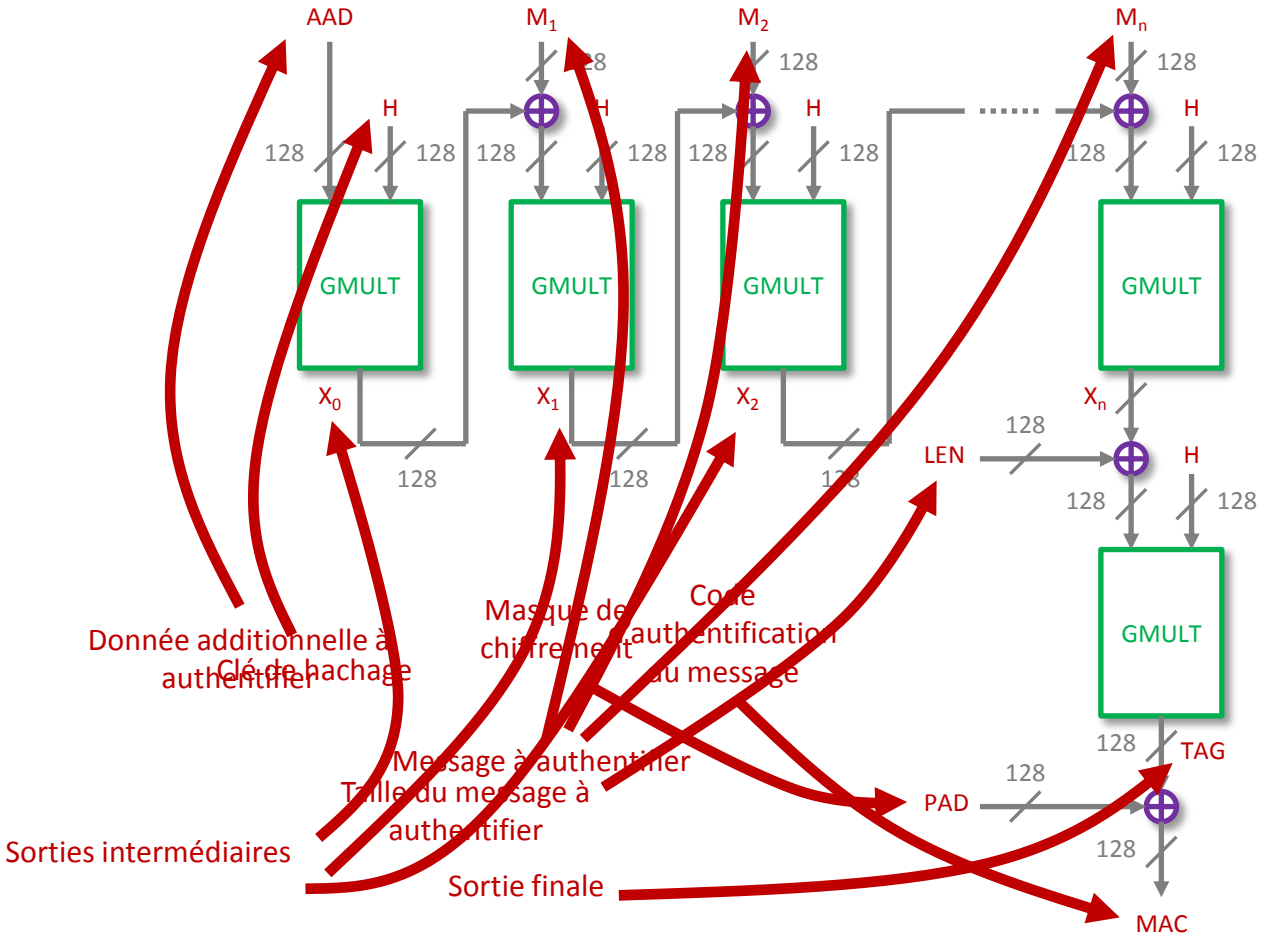
- Fonctionne en standalone (GMAC)
- Très haut débit possible
- Peut être utilisée comme fonction de hachage classique haute qualité

Points Faibles

- Surface importante …
- … ou latence élevée

[1] D. McGrew et J. Viega : The Galois/Counter Mode of Operation (GCM), 2004a. Submission to NIST Modes of Operation Process.

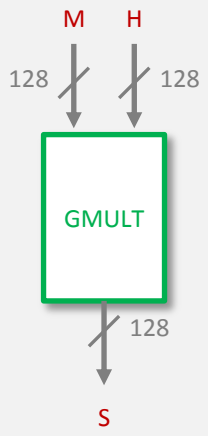
Architecture



GHASH

GMULT (Galois MULTiplication)

- Multiplication dans le corps de Galois binaire GF(2^{128})
- Utilise le polynôme irréductible $f = 1 + x + x^2 + x^7 + x^{128}$ (1)
- Suite de multiplications et de divisions de polynômes



Méthode [2]	Temps	Surface	Remarque
Parallèle	1	$O(q^2)$	-
Digit-série	q/D	$O(qD)$	D < q
Bit-série	q	$O(q)$	

q : nombre de bits pour la représentation
D : taille du digit

[1] G. Seroussi. Table of Low-Weight Binary Irreducible Polynomials. HP Labs Technical Report HPL-98-135, Computer Systems Laboratory, August, 1998.

[2] C. Paar, Implementation Options for Finite Field Arithmetic for Elliptic Curve Cryptosystems. ECC '99.

Algorithme

```
S ← 0
Pour i = 0 à 127 faire
        Si M_i = 1 alors
                S ← S ⊕ H
        Fin de si
        Si H_127 = 1 alors
                H ← décaler_à_droite ( H )
        Sinon
                H ← décaler_à_droite ( H ) ⊕ R
        Fin de si
Fin de pour
Retourner S
```

- Multiplication
- Pas de dépendance avec l'opérande M
- R est une constante

La multiplication se ramène à un « simple » ou-exclusif

H peut être représentée par une table précalculée

Exemple (1)

R

H

Non positionné (‘0’)

GHASH

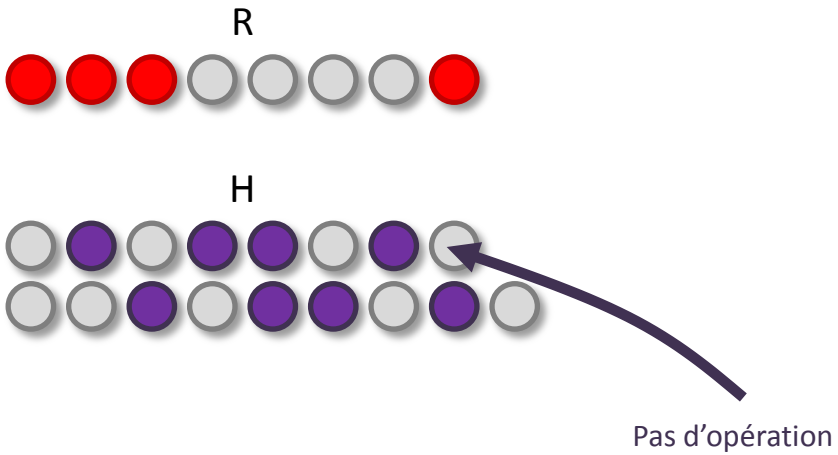
[1] exemple de génération d’une table d’un opérande de 8 bits

Exemple

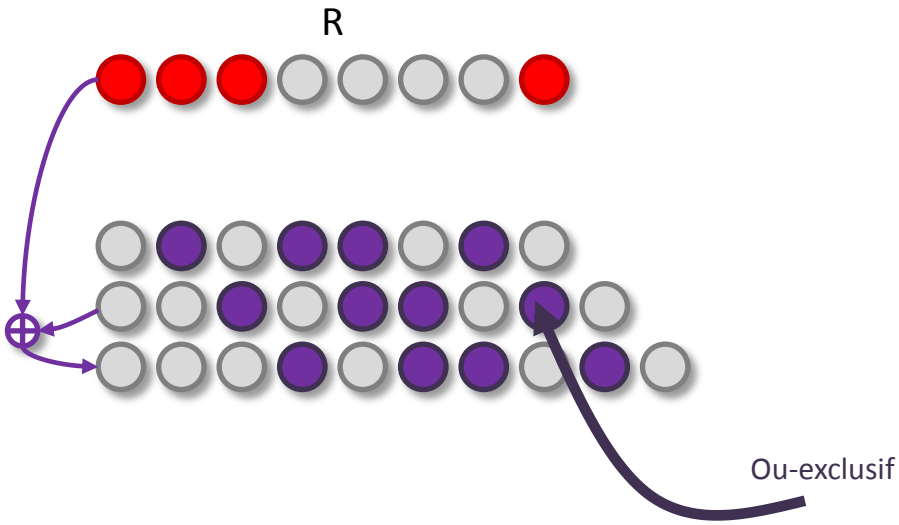
R

H

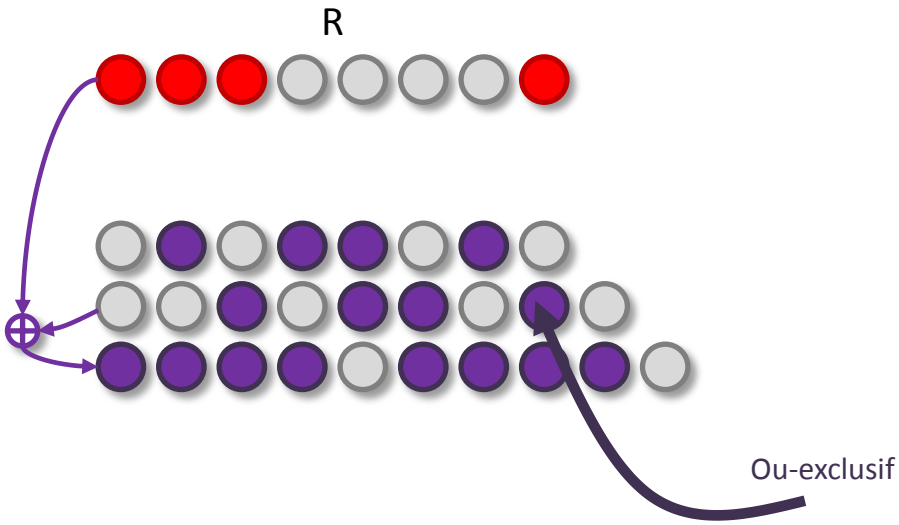
Exemple



Exemple

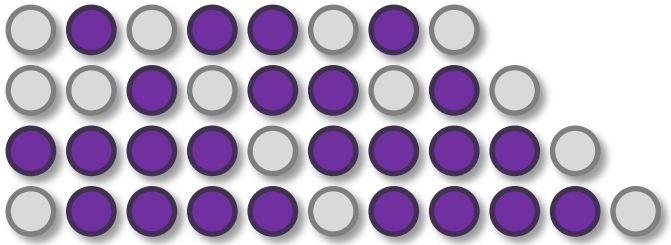


Exemple



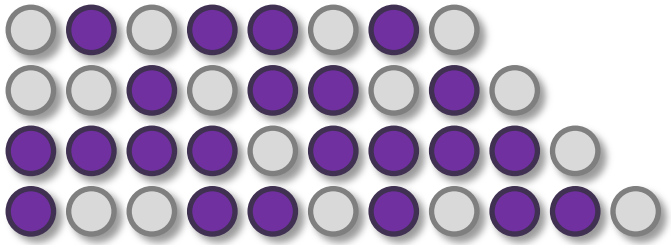
Exemple

R



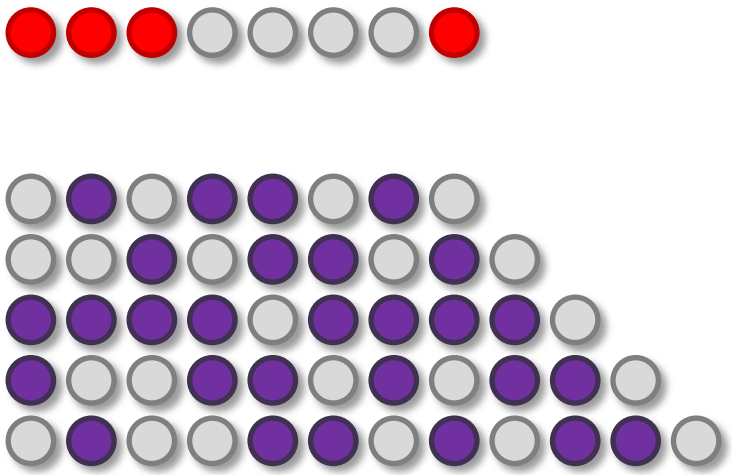
Exemple

R

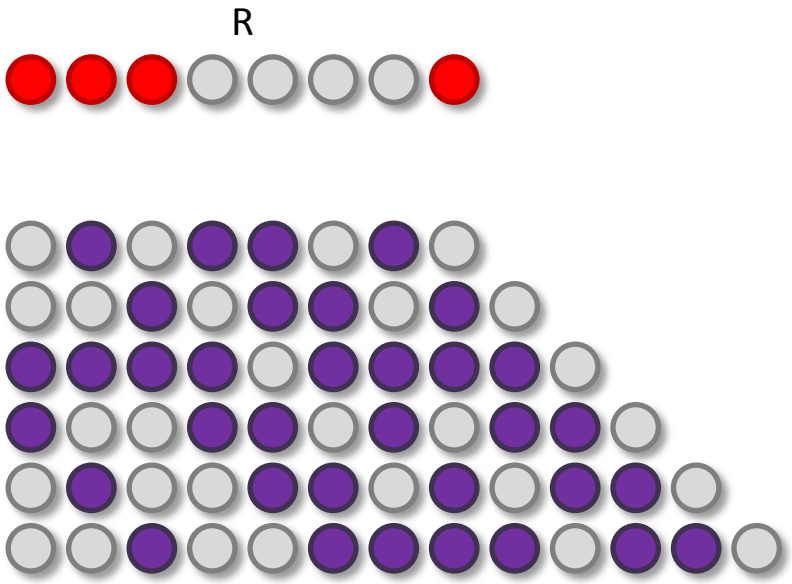


Exemple

R

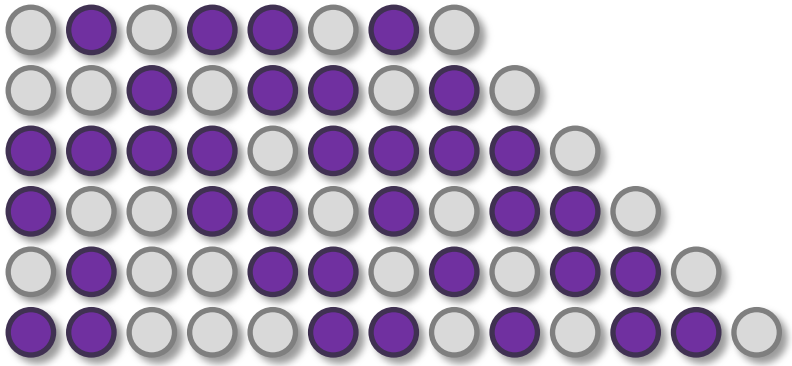


Exemple



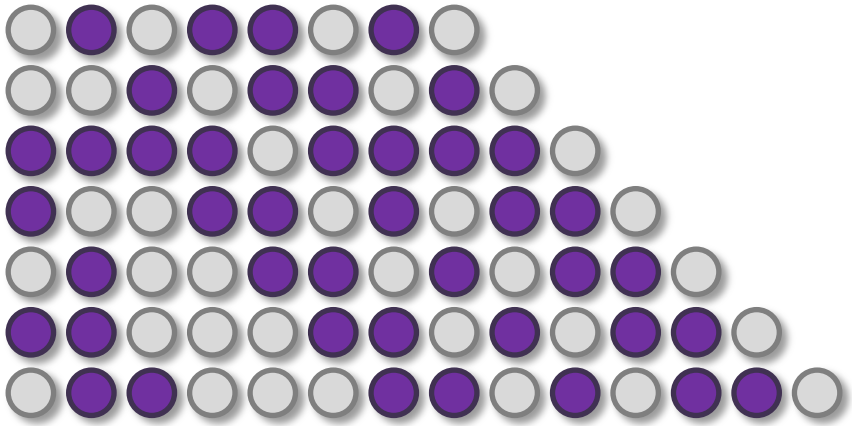
Exemple

R



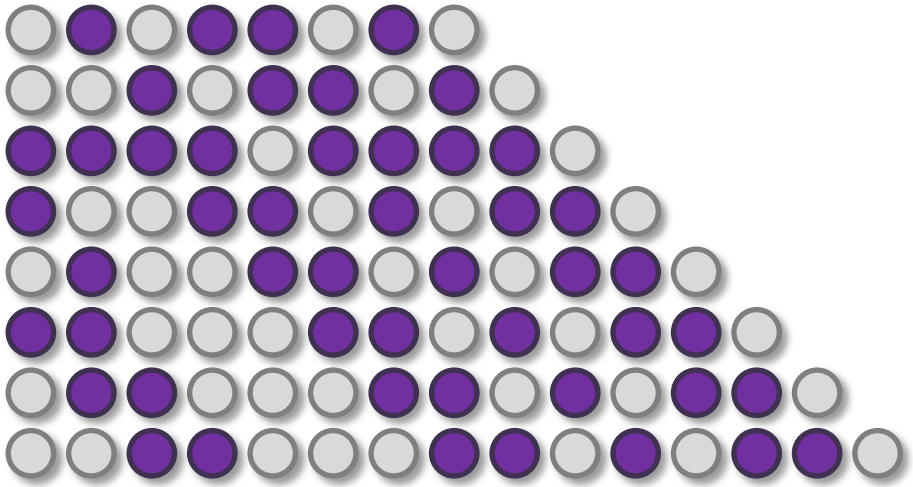
Exemple

R



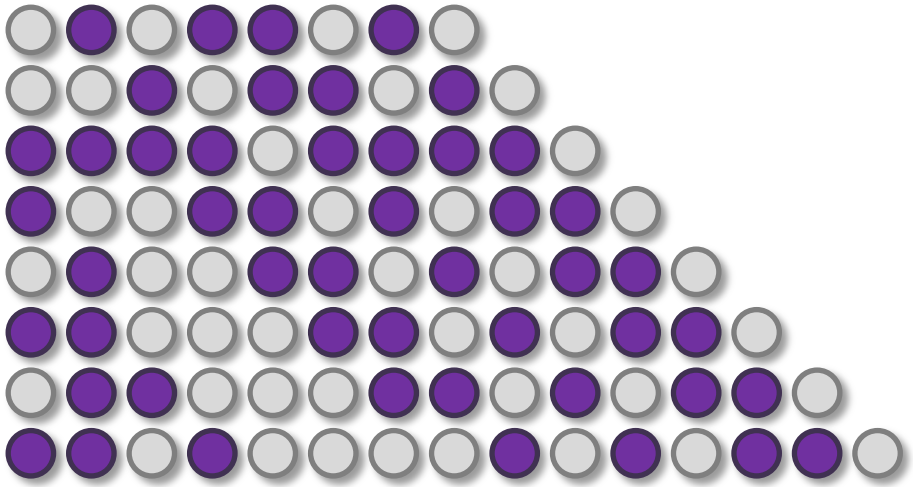
Exemple

R



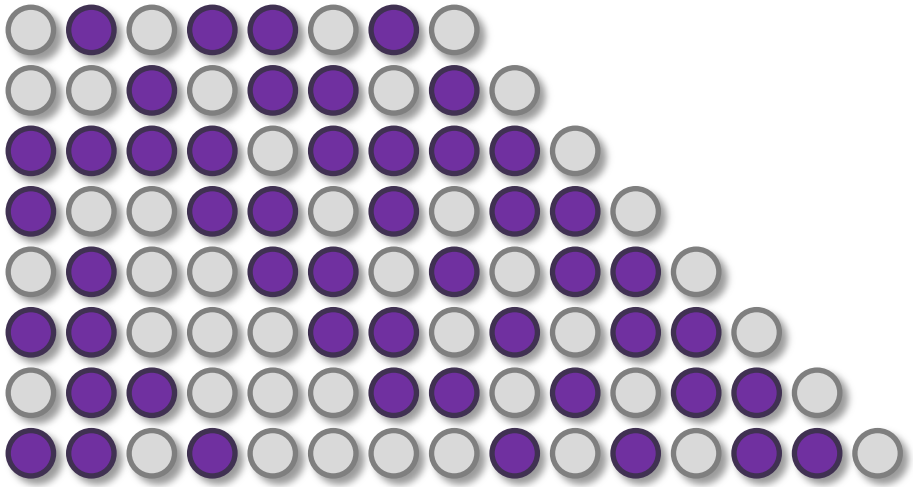
Exemple

R

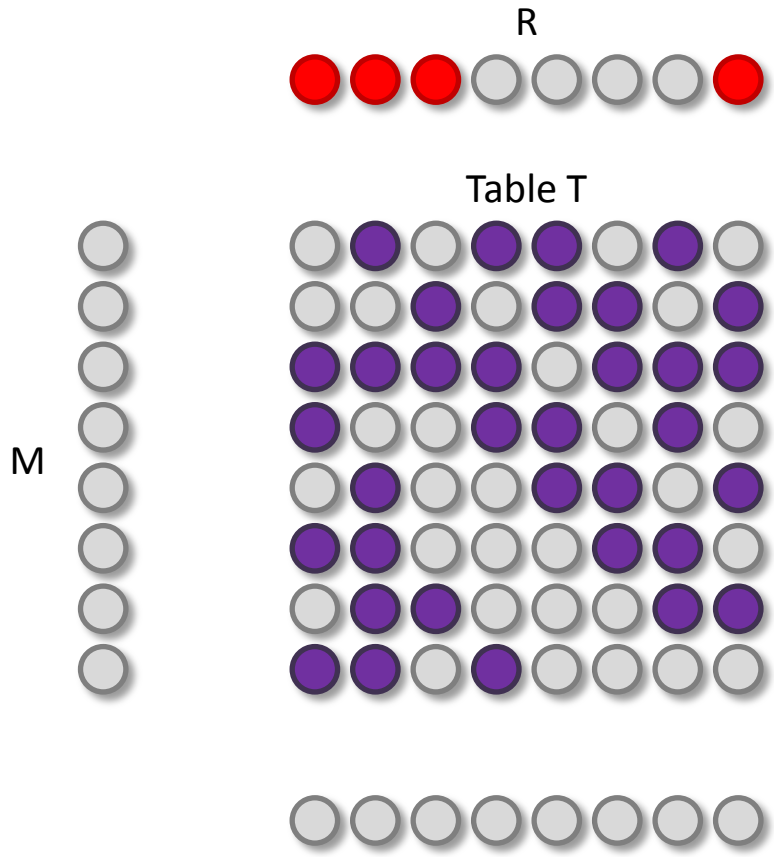


Exemple

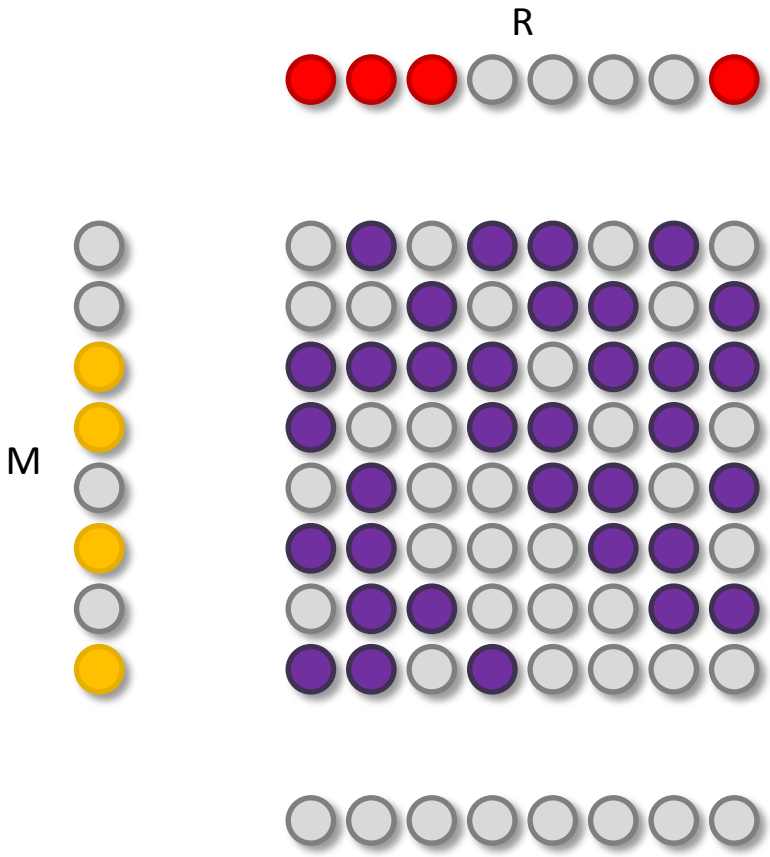
R



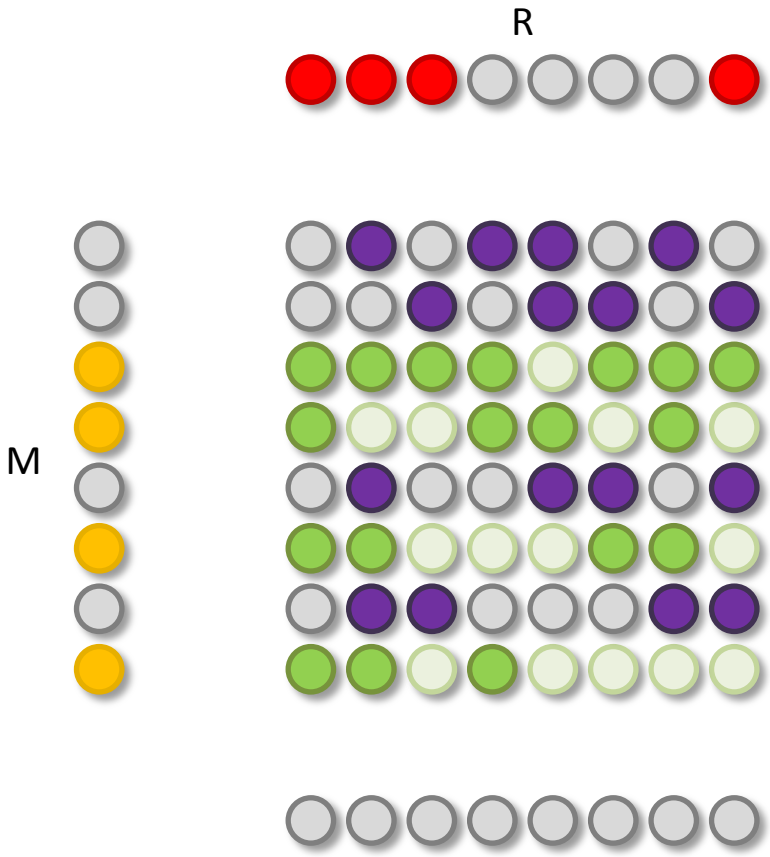
Exemple



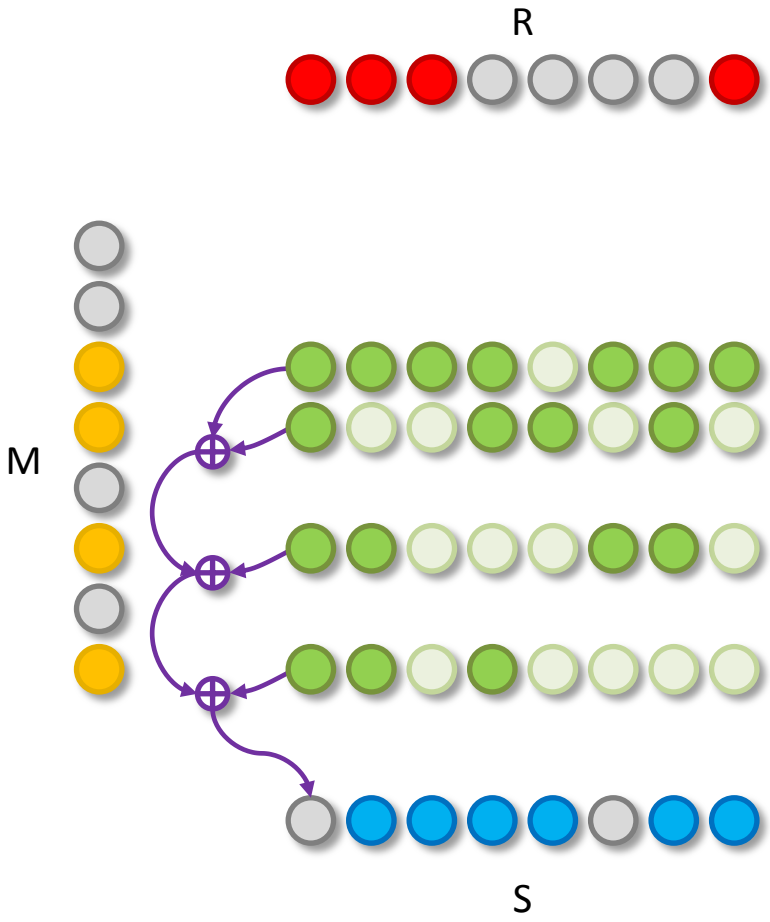
Exemple



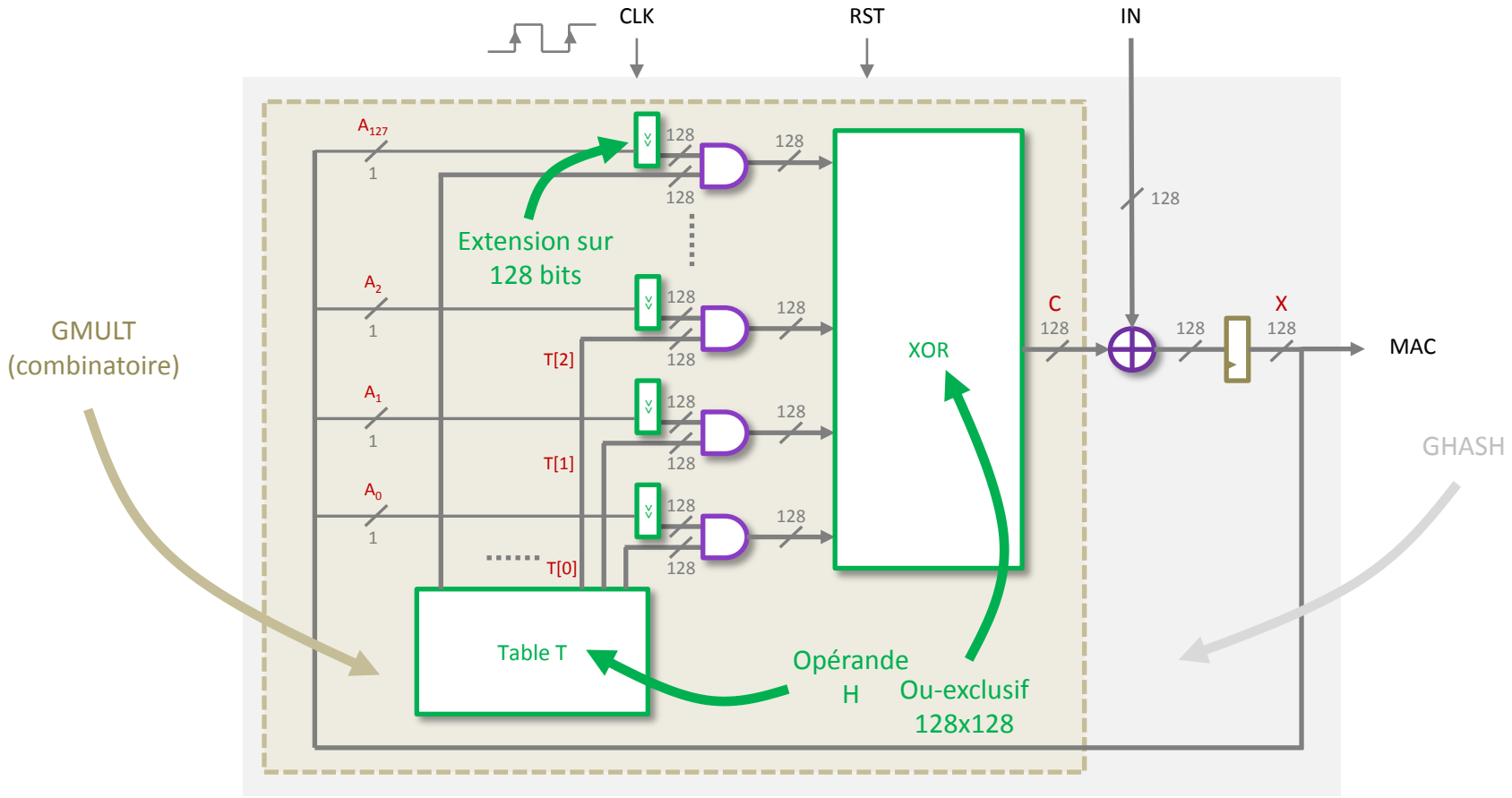
Exemple



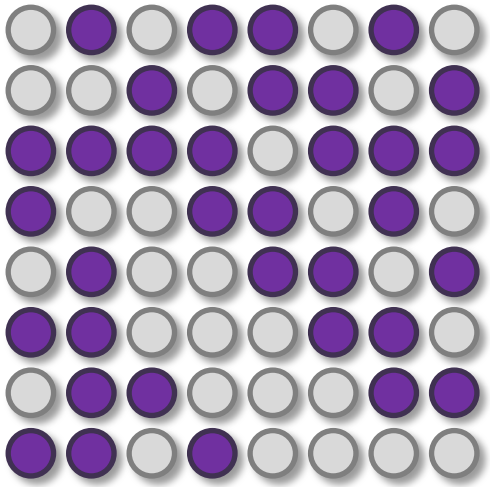
Exemple



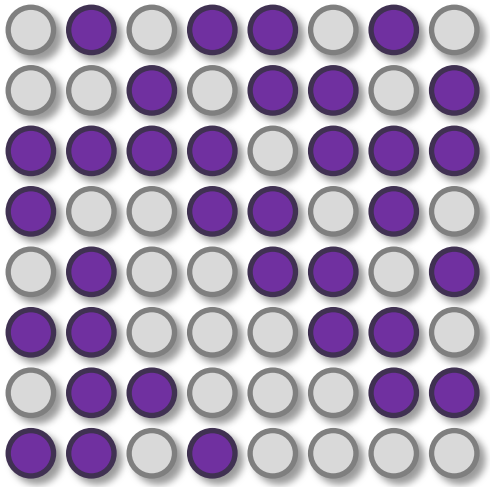
Architecture de la fonction GHASH

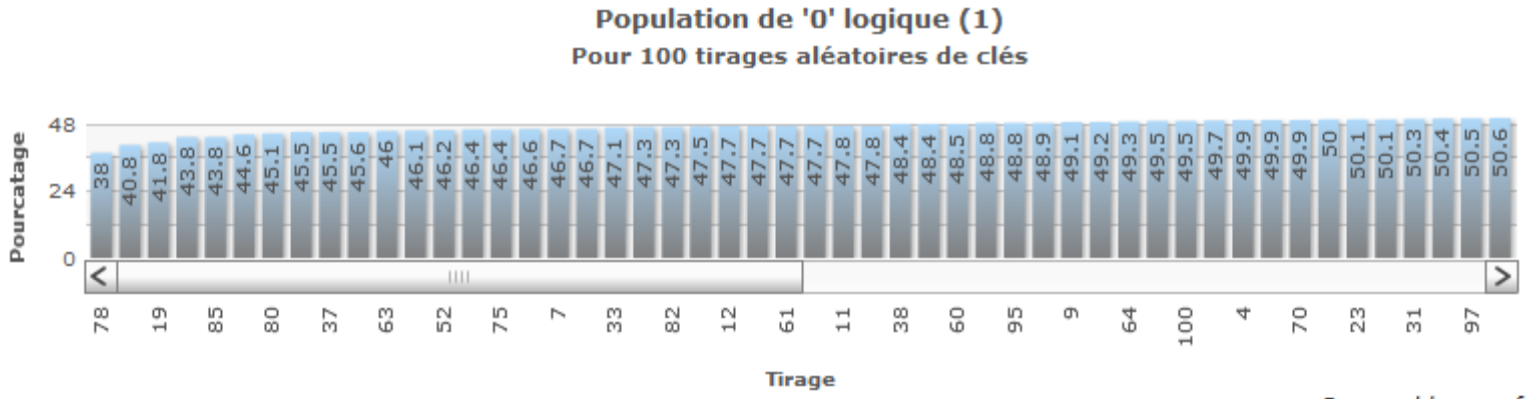


Population



Population

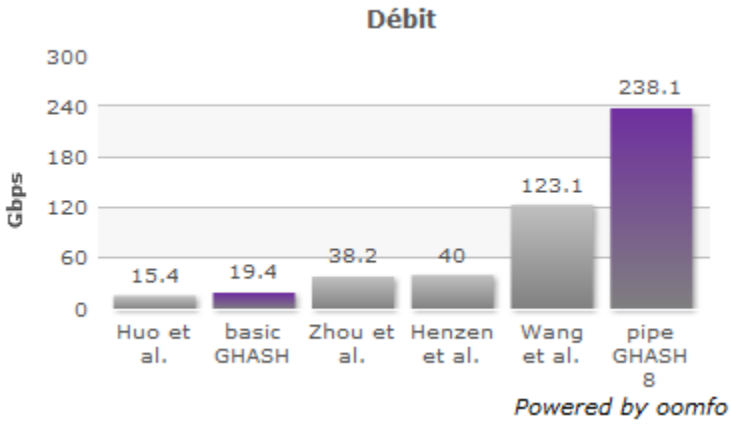


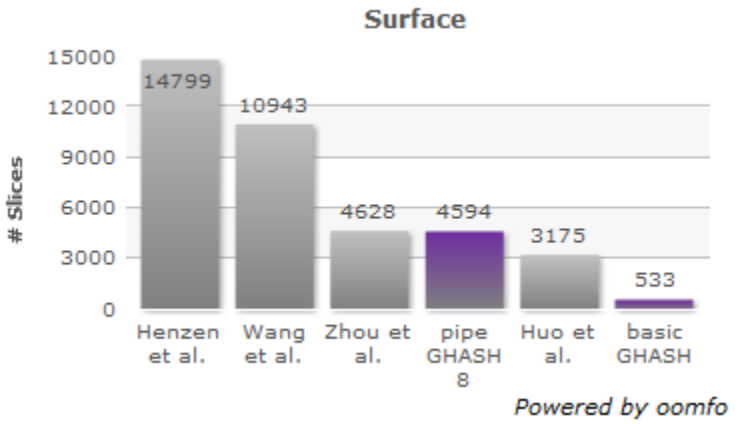


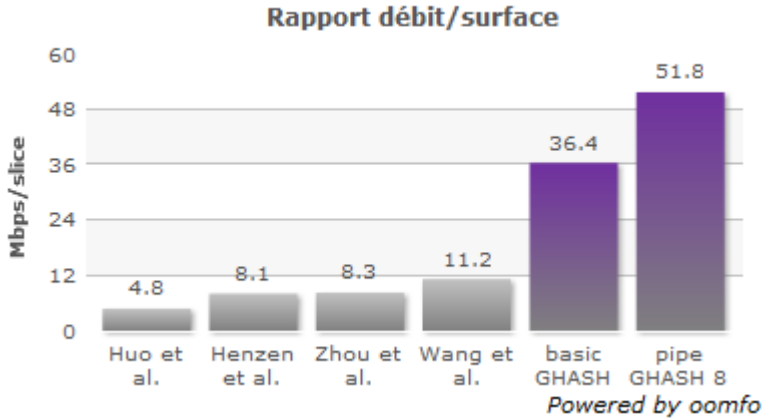
[1] population évaluée avec des clés de hachages de taille 128 bits et choisies aléatoirement par l'algorithme Mersenne twister

Résultats

Virtex-5 xc5vlx50t-31136







Conclusion

Contribution à une version optimisée de la fonction GHASH

- ❑ Architecture dédiée à clé dépendante, multi gigabits et faible surface
- ❑ Adapté pour le mode AES-GCM et pour l'authentification en standalone
- ❑ Conçu pour faciliter l'intégration de l'authentification sur des FPGAs faible-coût
- ❑ Description HDL, simulations et sources des outils disponibles gratuitement

FPT'11
CONFERENCE

IEEE

http://code.google.com/p/ghash/

- Introduction
- GHASH
- **Sécurité Configurable**
- **Filtre de Bloom**
- **Conclusion**

Sécurité configurable (1)

- ❑ Proposer une adaptabilité du niveau de sécurité
- ❑ Uniforme pour le chargement d'applications
- ❑ Programmable pour l'exécution d'applications. Trois niveaux :
  - Pas de protection
  - Confidentialité seulement
  - Confidentialité et authentification

Points Forts

- Gain en temps d'exécution
- Gain de stockage du matériel cryptographique

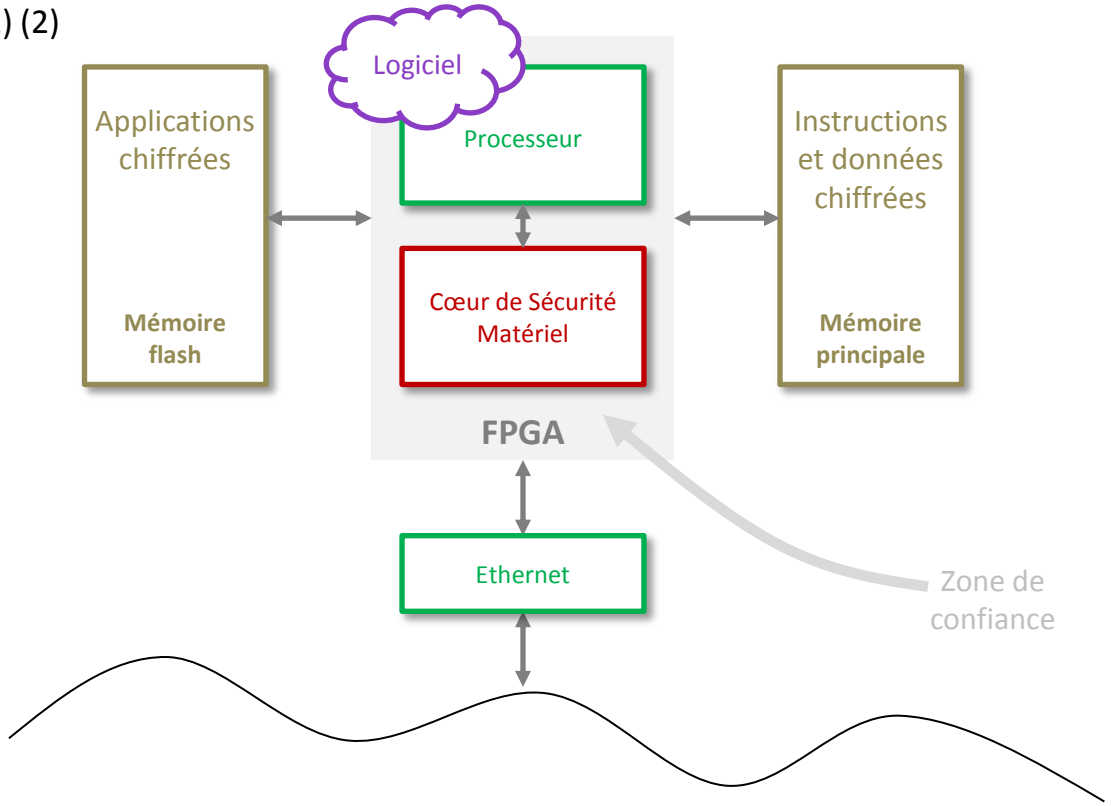
Points Faibles

- Surface pouvant être importante
- Demande au concepteur des notions de sécurité

[1] Romain Vaslin, Guy Gogniat, Jean-Philippe Diguet, Russell Tessier, Deepak Unnikrishnan et Kris Gaj : Memory security management for recongurable embedded systems. In Proceedings of the IEEE Conference on Field Programmable Technology, pages 153{160, decembre 2008.

Système embarqué

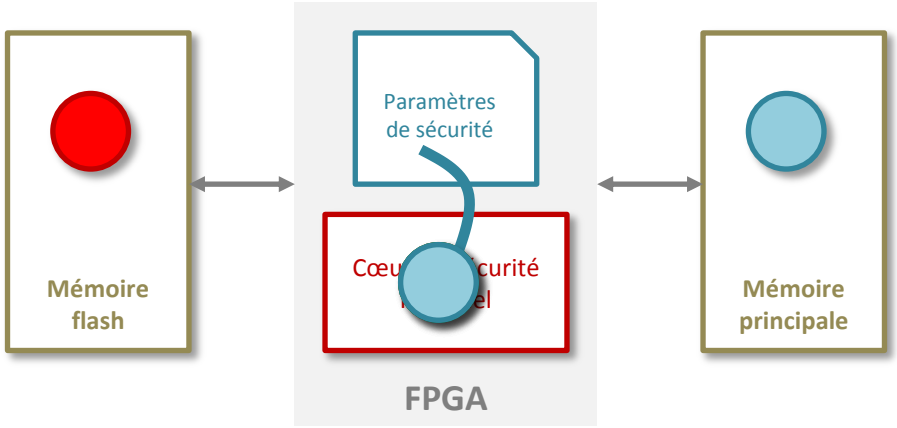
(1) (2)



[1] Kwangyoon Lee et Alex Orailoglu : Application specific non-volatile primary memory for embedded systems.

[2] Marco Pasotti, Guido De Sandre, David Iezzi, Davide Lena, Gilberto Muzzi, Marco Poles et Pier Luigi Rolandi : An application specific embeddable flash memory system for non-volatile storage of code, data and bit-streams for embedded FPGA congurations.

Politiques de sécurité



Chargement

Protection uniforme

Exécution

Protection programmable

Paramètres de sécurité

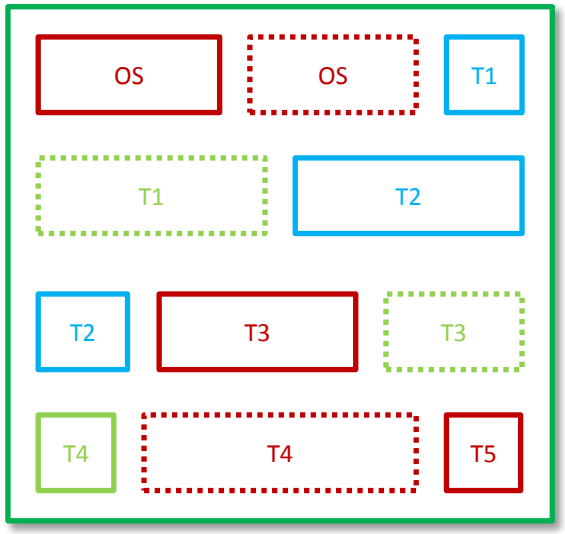
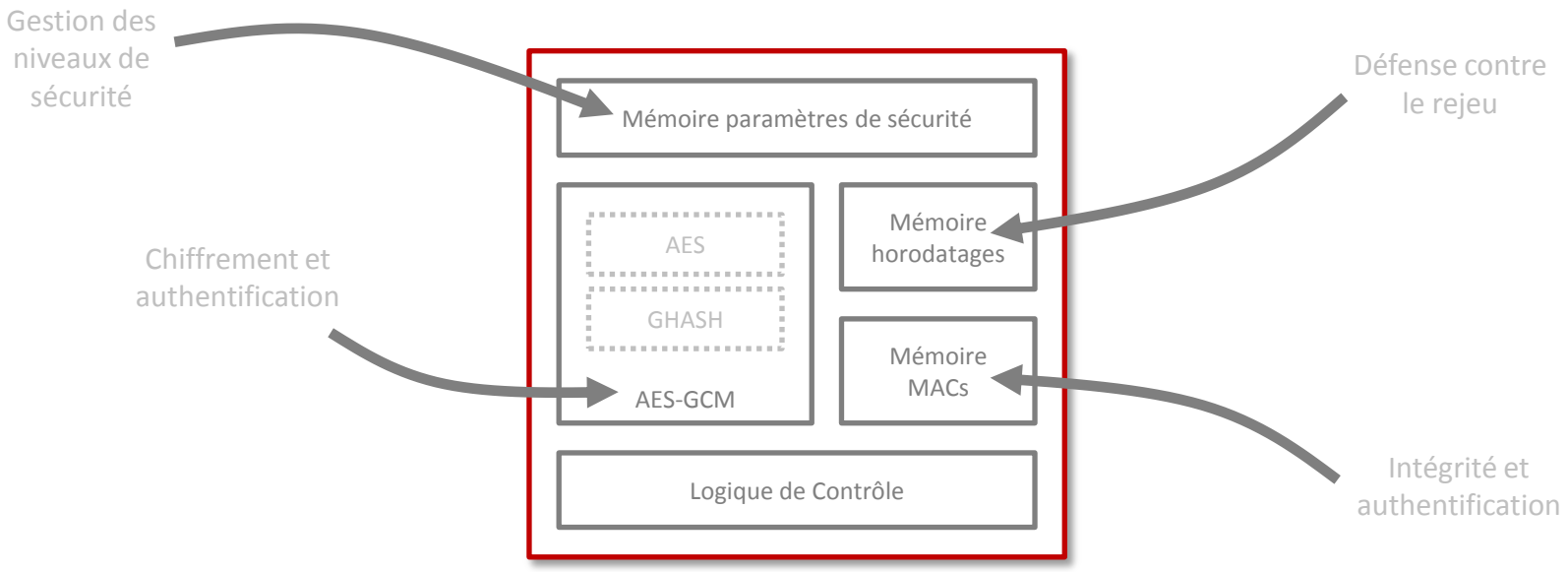


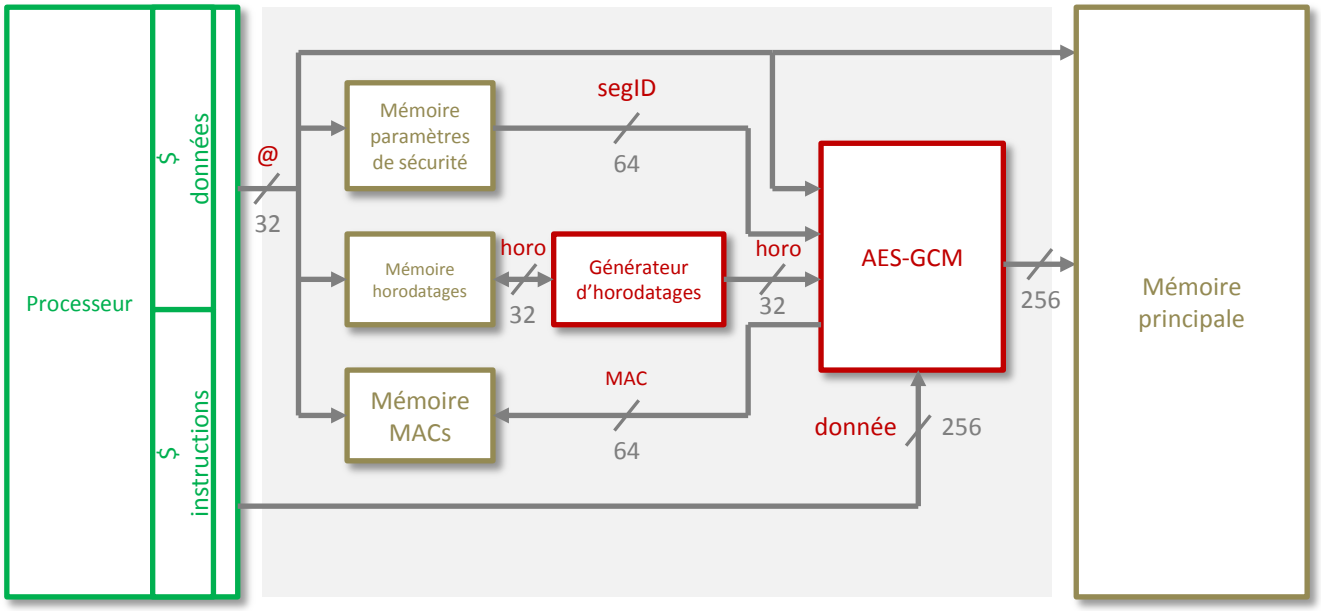
Diagramme bloc



Cœur de Sécurité Matériel

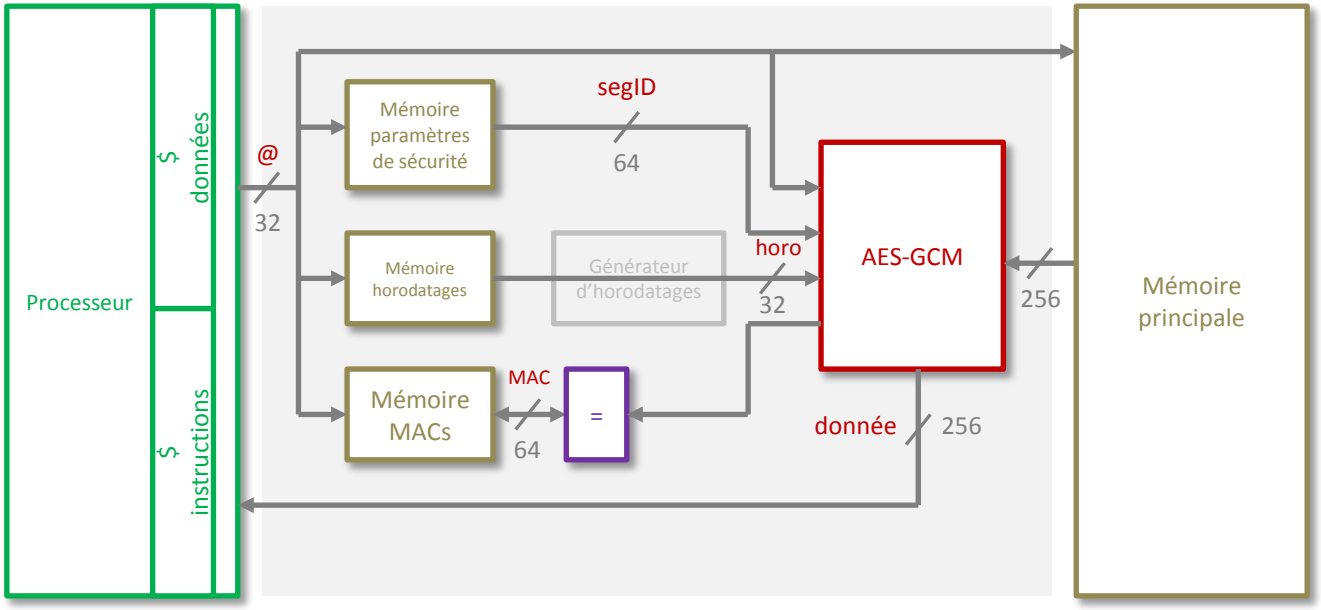
Architecture

Écriture



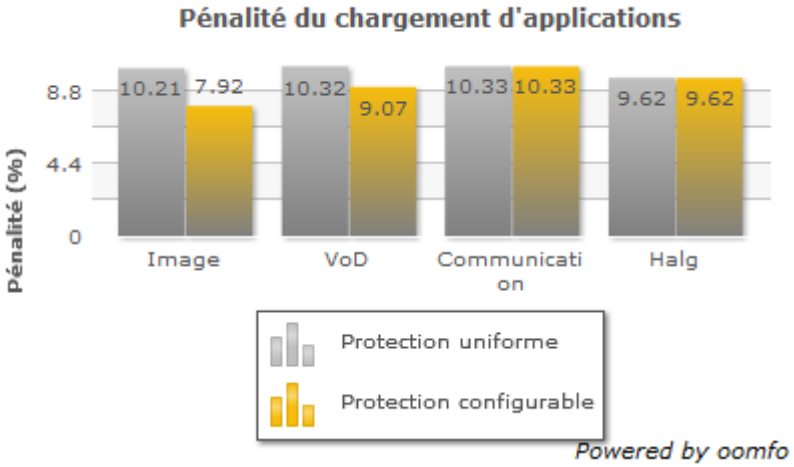
Architecture

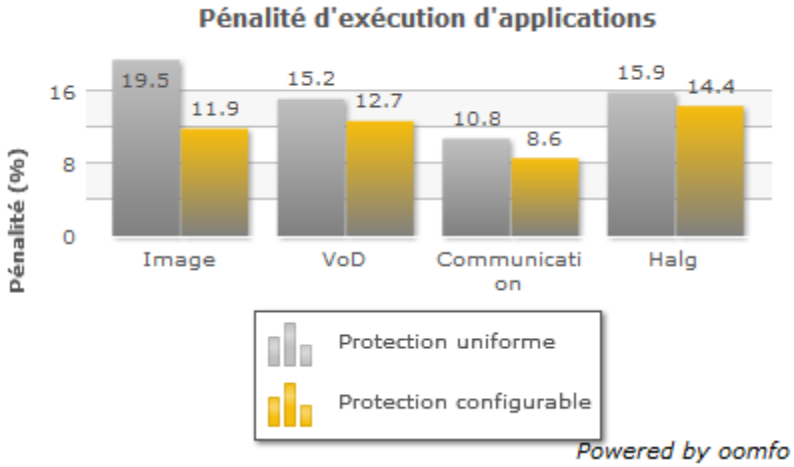
Lecture



Résultats

Spartan-6 xc6slx-45t



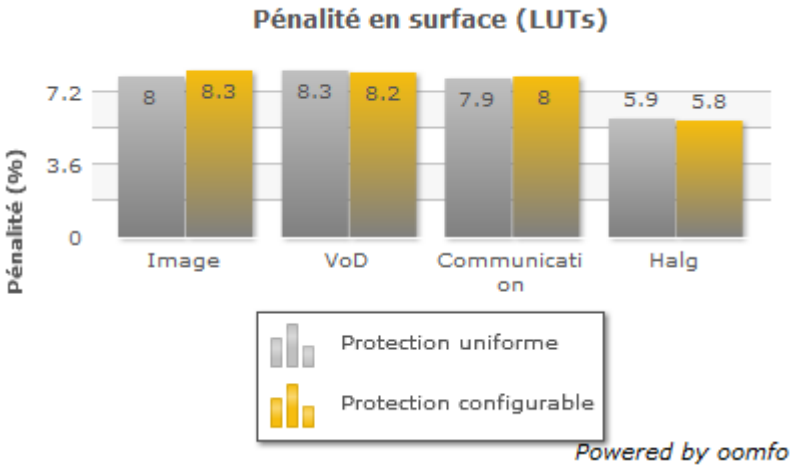


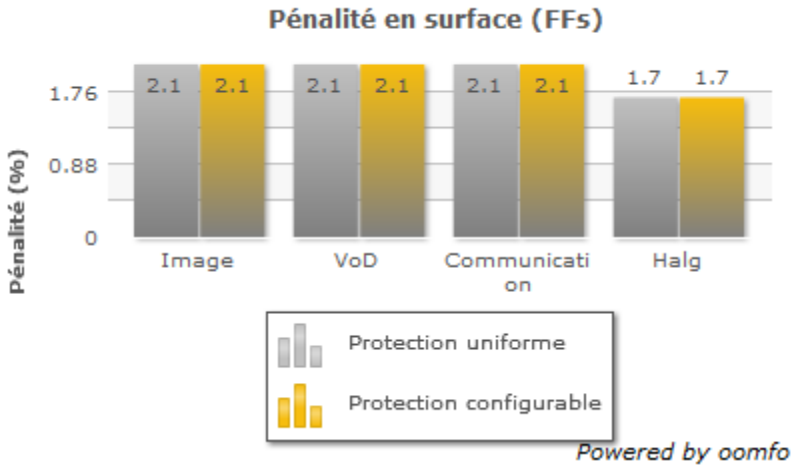
4 Applications

- Image : Morphologie
- VoD : Décodage MPEG2
- Communication : Codage/décodage Reed-Solomon
- Halg : Hachage cryptographique MD5, SHA-1 et SHA-2

Résultats

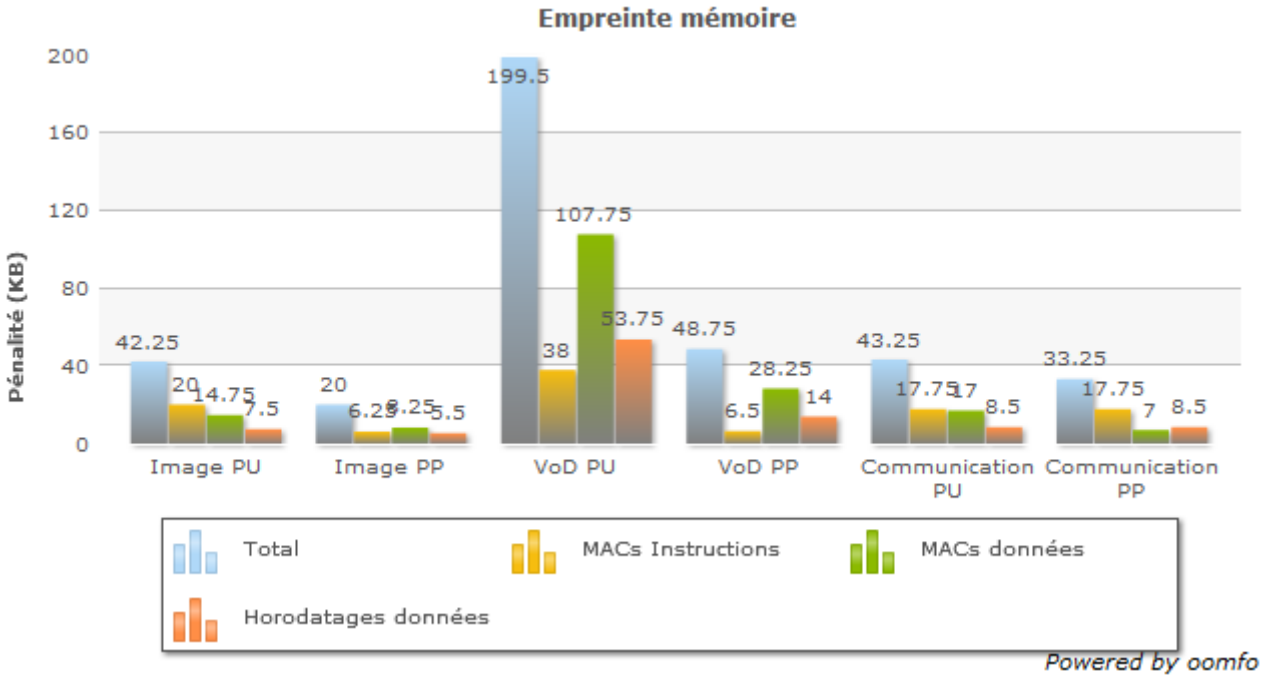
Spartan-6 xc6slx-45t





Résultats

Spartan-6 xc6slx-45t



Résultats

Comparaison

Travaux			Pénalité (%)			Sécurité			Remarque
Auteurs	Approche	Année	perf.	stock.	surf.	chiffre.	int/auth.	niveau	
Suh et al. [1]	AEGIS	2003	130	28	200	AES	SHA-1	1/2^128	-
Lie et al. [2]	XOM	2003	-	50	-	3DES	-	1/2^56	Modification de l'OS requise
Elbaz et al. [3]	PE-ICE	2006	32	33	-	AES	-	1/2^32	Stockage sur et hors puce
Yan et al. [4]	YAN-GCM	2006	8	-	-	AES	GHASH	1/2^64	Simulation uniquement
Vaslin et al.	AES-TASC AES-ICBC	2008	15-8	25	65	AES	CRC/AES diff.	1/2^64	Stockage sur puce uniquement
Crenne et al.	-	2011	15-8	25	100	AES	GHASH	1/2^64	Stockage sur puce uniquement

[1] G. Edward Suh, Dwaine Clarke, Blaise Gassend, Marten van Dijk et Srinivas Devadas : Efficient memory integrity verification and encryption for secure processors. In Proceedings of the IEEE/ACM International Symposium on Microarchitecture, pages 339-350, 2003b.
[2] David Lie, Chandramohan Thekkath et Mark Horowitz : Implementing an untrusted operating system on trusted hardware. In Proceedings of the ACM Symposium on Operating Systems Principles, pages 178-192, October 2003.
[3] Reouven Elbaz, Lionel Torres, Gilles Sassatelli, Pierre Guillemin, Michel Bardouillet et Albert Martinez : A parallelized way to provide data encryption and integrity checking on a processor-memory bus. In Proceedings of the IEEE/ACM International Design Automation Conference, pages 506-509, July 2006b.
[4] Chenyu Yan, Brian Rogers, Daniel Englender, Yan Solihin et Milos Prvulovic : Improving cost, performance, and security of memory encryption and authentication. In Proceedings of the International Symposium on Computer Architecture, pages 179-190, juillet 2006a.

Conclusion

Contribution à une approche de sécurité configurable

- ❑ Pour le chargement et l'exécution d'applications
- ❑ Flexible par sélection de différents niveaux de sécurité
- ❑ Chiffrement-authentifié approuvé NIST
- ❑ Faible coût par minimisation et réutilisation de la logique
- ❑ Limite la latence d'authentification
- ❑ Pénalités complètements évaluées en matériel

ACM Transactions on Embedded Computing Systems (TECS)

- Introduction
- GHASH
- Sécurité Configurable
- **Filtre de Bloom**
- **Conclusion**

Filtre de Bloom (1)

- Structure de donnée
  - Probabiliste
  - Compacte
- Utilisé pour tester l'appartenance d'un élément à un ensemble

Points Forts

- Représente un ensemble de façon efficace
- Fournit potentiellement un taux de compression substantiel
- Très largement paramétrique
- Des opérations filtre et inter-filtres simples

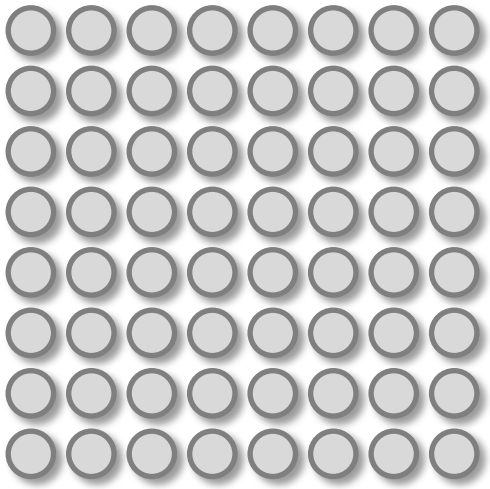
Points Faibles

- … mais d'autres complexes voire impossibles
- Introduction de propriétés non désirables
- Peut demander des ressources de calcul importantes

[1] Burton H. Bloom : Space/time trade-os in hash coding with allowable errors. Commun. ACM, 13:422{426, July 1970. ISSN 0001-0782. URL http://doi.acm.org/10.1145/362686.362692.

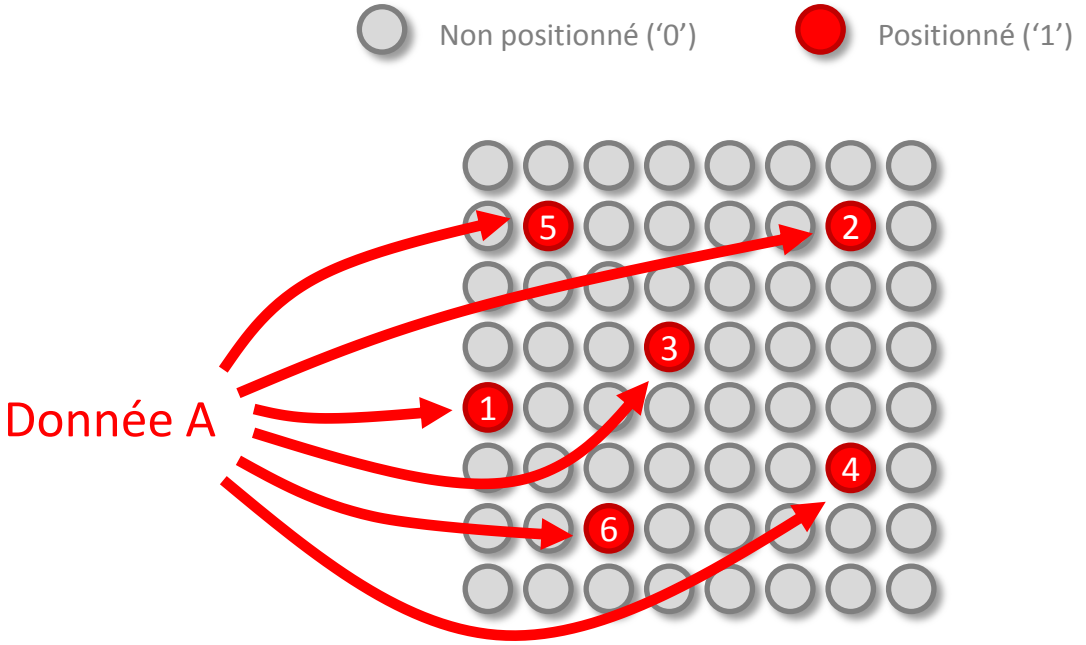
Exemple

Non positionné (‘0’)



Exemple

Programmation

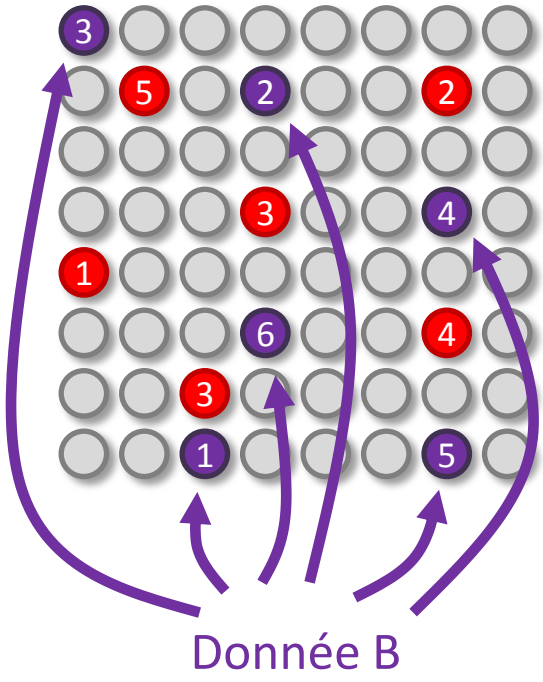


Exemple

Programmation

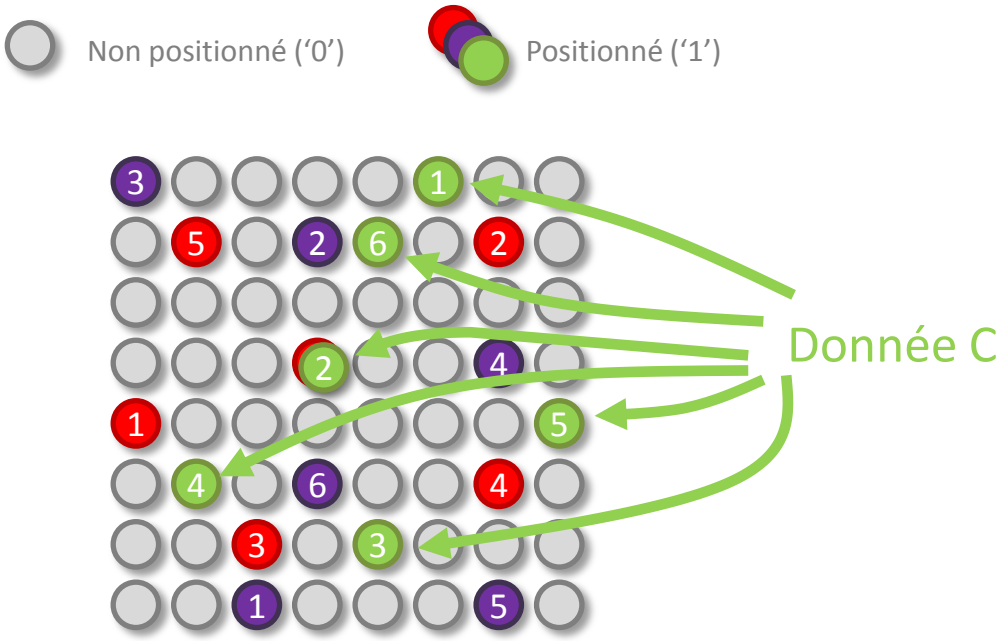
Non positionné (‘0’)

Positionné (‘1’)



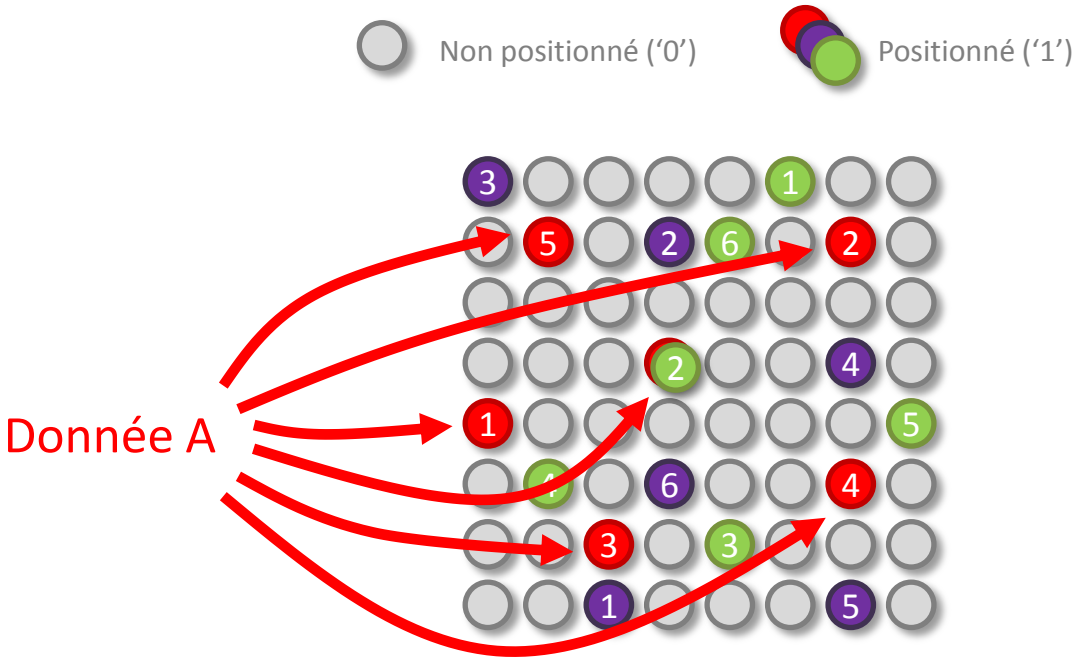
Exemple

Programmation



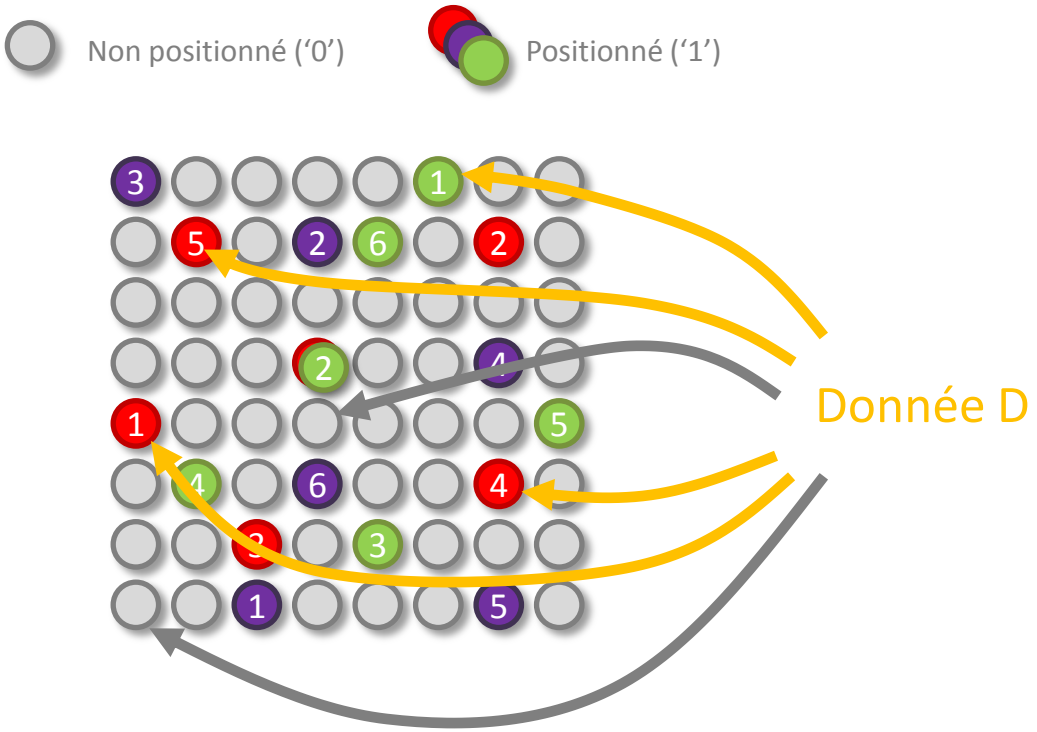
Exemple

Scrutation



Exemple

Scrutation

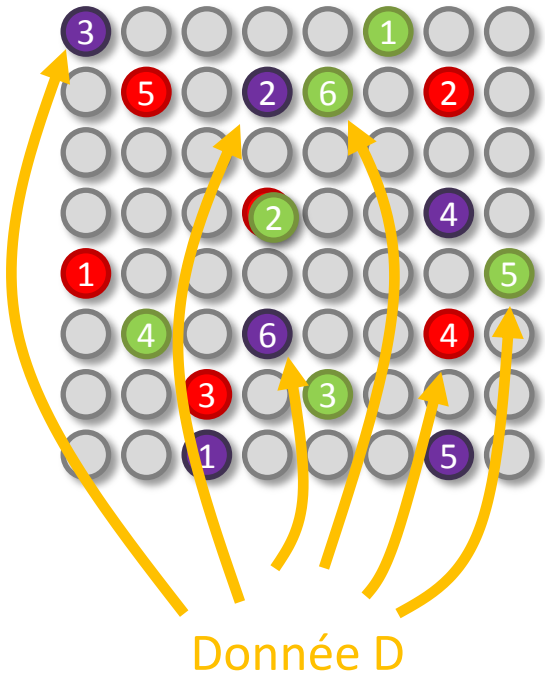


Exemple

Faux positif

Non positionné (‘0’)

Positionné (‘1’)

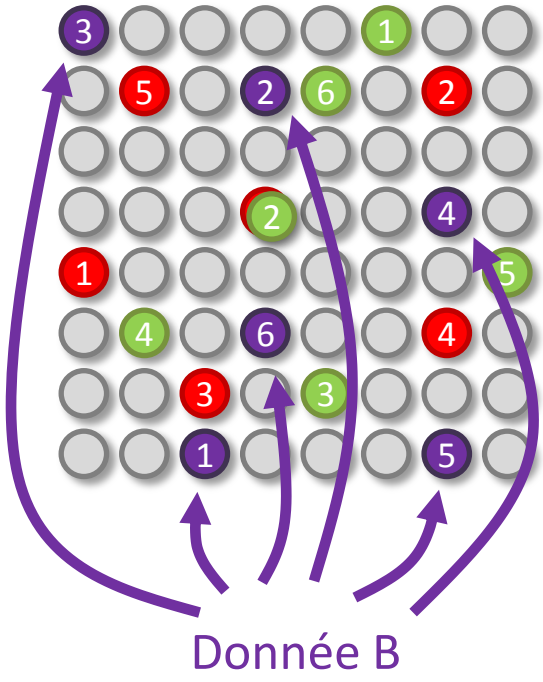


Exemple

Suppression

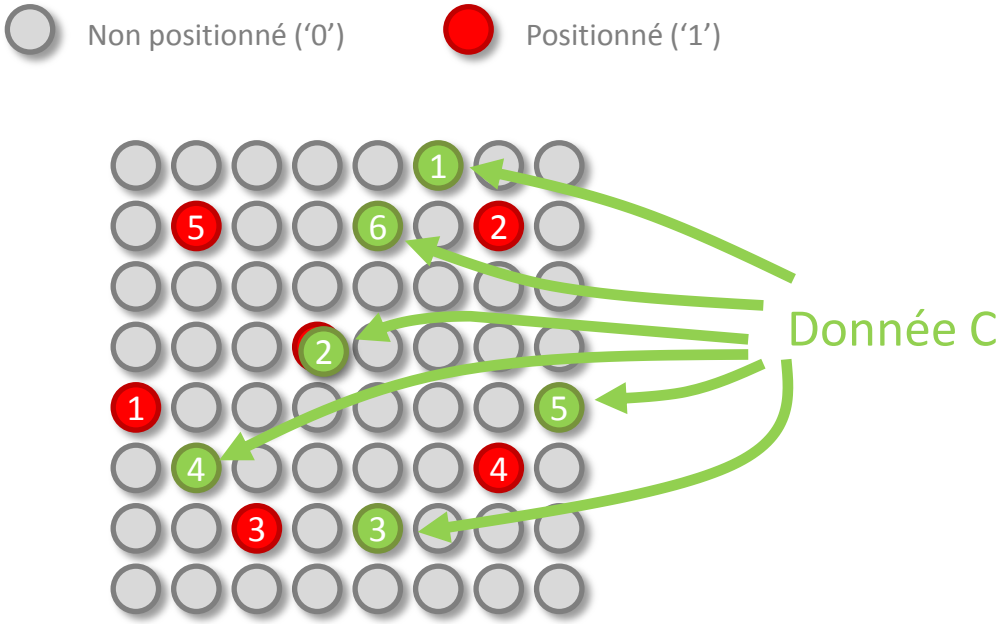
Non positionné (‘0’)

Positionné (‘1’)



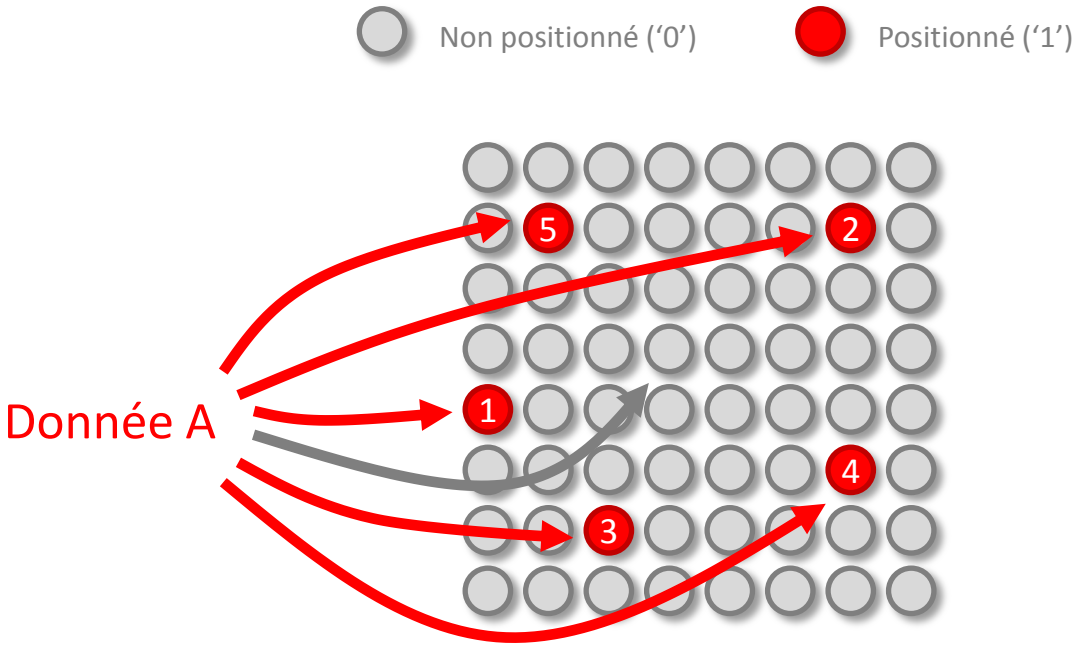
Exemple

Suppression

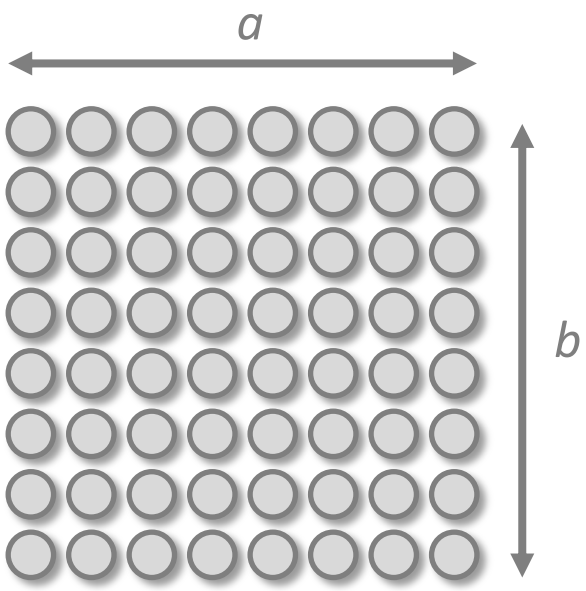


Exemple

Suppression

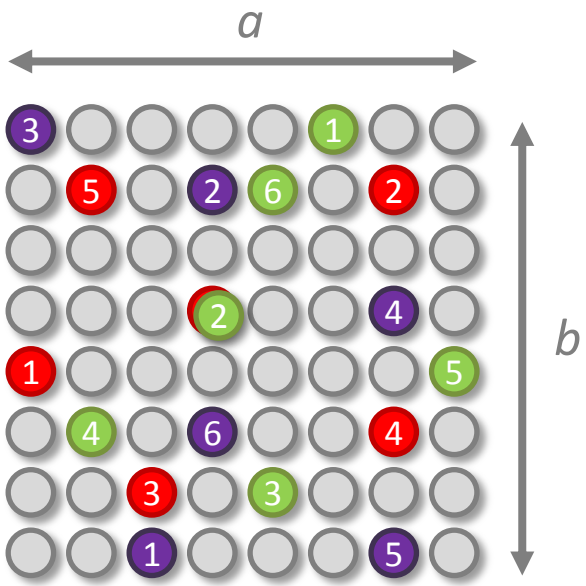


Paramètres



Taille du filtre ***m*** = *a* x *b*

Paramètres

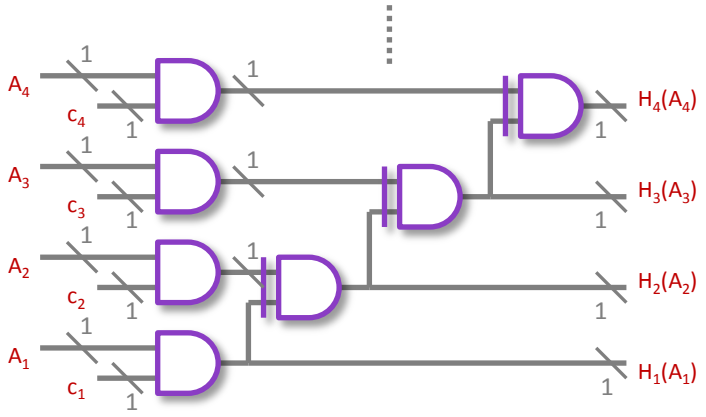


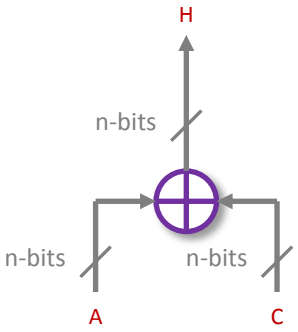
Probabilité de faux positifs ***fp***

Génération des fonctions de hachage

Hachage H3

- Fonction de hachage universelle (1)
- Délai important dépendant de la taille de la cellule



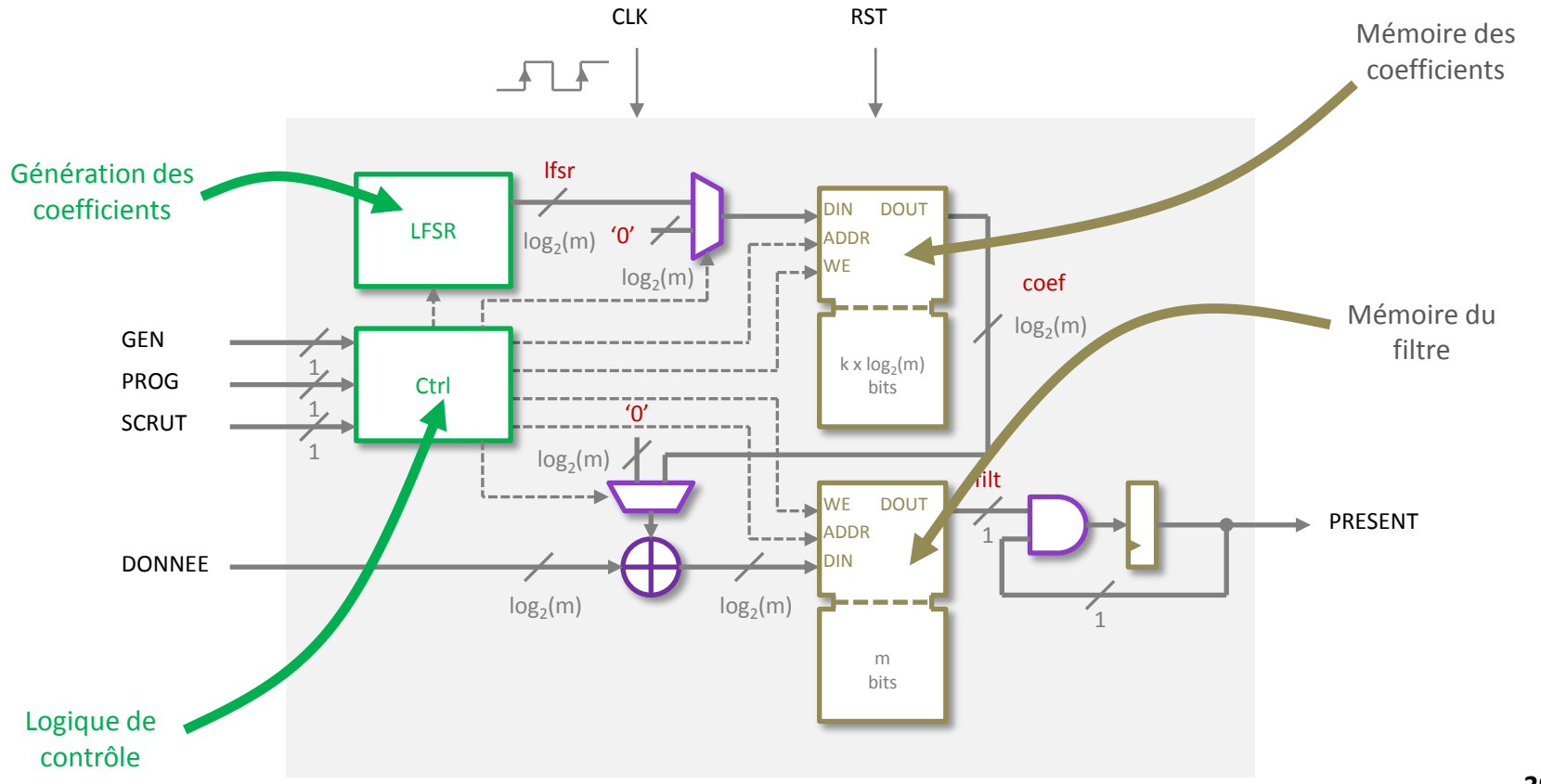


Hachage XOR

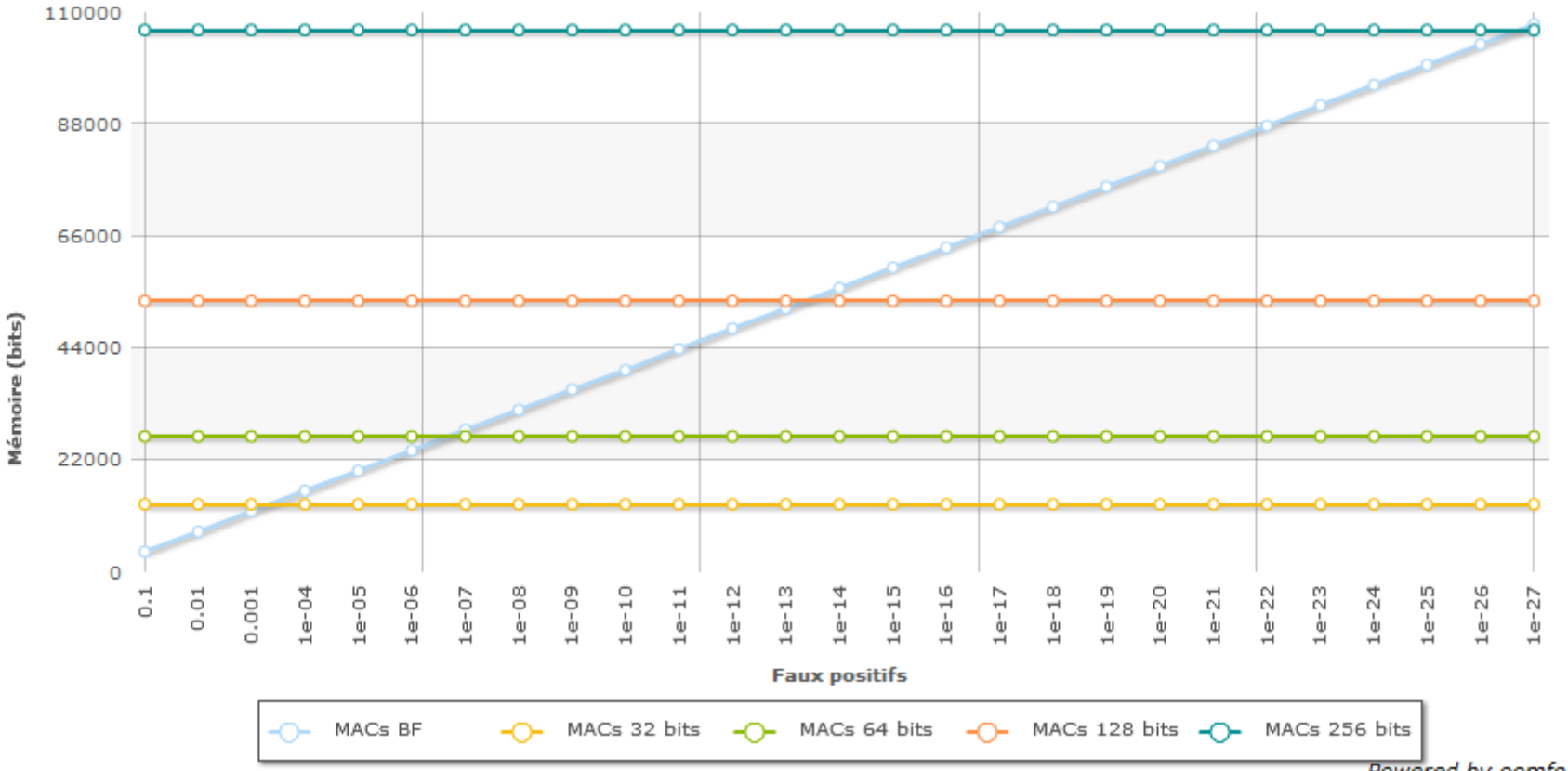
- Ne fonctionne que si la source à hacher est aléatoire (2)
- Délai minimal et indépendant de la taille de la cellule

[1] D. J. Lawrence Carter et Mark N. Wegman : Universal classes of hash functions.
[2] Michael Mitzenmacher et Salil Vadhan : Why simple hash functions work : exploiting the entropy in a data stream.

Architecture du filtre de Bloom



Application au stockage de MACs [1]



[1] Exemple issu de l'application VoD. MACs des instructions uniquement.

Conclusion

Contribution à un stockage efficace du matériel cryptographique

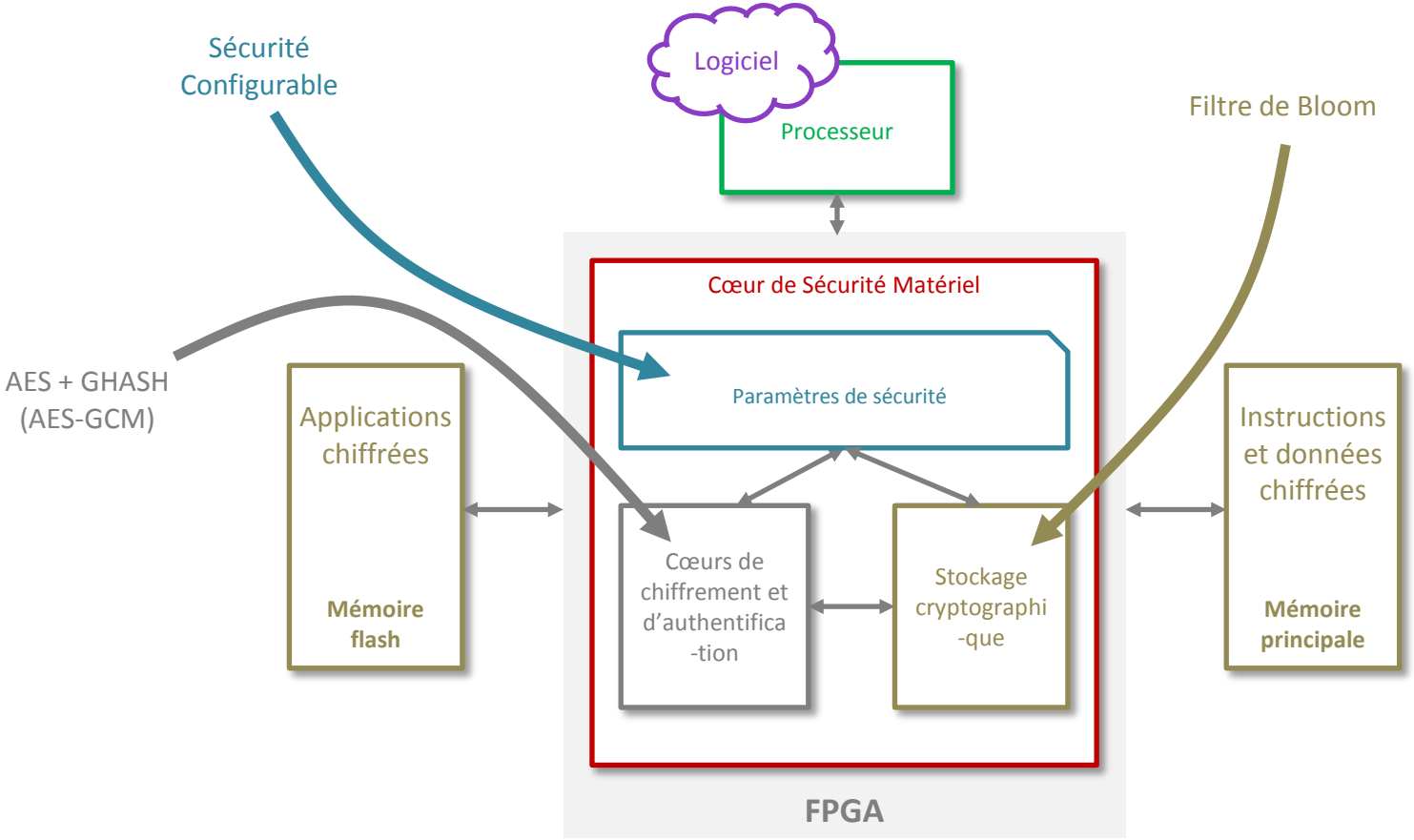
- Filtre de Bloom comme structure adéquate de compression
- Architecture conçue pour l'embarqué :
  - Fonction de hachage simplifié et logique de contrôle minimale
- Trois paramètres, *m*, *k* et *fp* pour trois approches :
  - orientée mémoire
  - orientée latence
  - orientée sécurité

- Introduction
- GHASH
- Sécurité Configurable
- Filtre de Bloom
- **Conclusion**

Trois contributions :

- à une version optimisée de la fonction GHASH
  - Brique cryptographique multi gigabits pour l'authentification
- à une approche de sécurité configurable
  - Chargement et exécution sécurisé avec différents niveaux de sécurité
- à un stockage efficace du matériel cryptographique
  - Compression originale des MACs des instructions d'une application

Synthèse


Sécurité Configurable
Logiciel
Processeur
Filtre de Bloom
Cœur de Sécurité Matériel
AES + GHASH (AES-GCM)
Applications chiffrées
Mémoire flash
Paramètres de sécurité
Cœurs de chiffrement et d'authentifica-tion
Stockage cryptographi-que
Instructions et données chiffrées
Mémoire principale
FPGA

GHASH

- Aspects dynamiques
- Évaluation pour le logiciel
- GHASH comme fonction robuste de hachage généraliste

Sécurité configurable

- Support d'autres niveaux de sécurité
- Propositions de solutions pour les technologies ASIC

Filtre de Bloom

- Support de la suppression d'élément pour le filtre de Bloom
- Évaluation l'impact des faux-positifs en conditions réelles

Publications

Revues internationales et chapitres de livre

- **J. Crenne**, R. Vaslin, G. Gogniat, J.-P. Diguet, R. Tessier and D. Unnikrishnan, **Configurable Memory Security in Embedded Systems**, *in ACM Transactions on Embedded Computer Systems (TECS)*, accepted/to appear.

- **J. Crenne**, P. Bomel, G. Gogniat, J.-P Diguet, **End-to-End Bitstreams Repository Hierarchy for FPGA Partially Reconfigurable Systems**, *in Algorithm-Architecture Matching for Signal and Image Processing*, Springer, ISBN: 978-90-481-9964-8, pp. 171-194.

Conférences internationales et workshops

- **J. Crenne**, P. Cotret, G. Gogniat, R. Tessier, and J.-P. Diguet, **Efficient Key-Dependent Message Authentication in Reconfigurable Hardware**, *in the Proceedings of the International Conference on Field-Programmable Technology (FPT'11)*, December 12-14, 2011, New Delhi, India.

- P. Cotret, **J. Crenne**, G. Gogniat, J.-P Diguet, L. Gaspar, G. Duc, **Distributed security for communications and memories in a multiprocessor architecture**, *in the Proceedings of the Reconfigurable Architecture Workshop (RAW'11)*, May 16-17, 2011 , Anchorage, Alaska, USA.

- G. Gogniat, J. Vidal, L. Ye, **J. Crenne**, S. Guillet, F. de Lamotte, J.-P Diguet, P. Bomel, **Self-reconfigurable Embedded Systems: from Modeling to Implementation**, *in the Proceedings of the International Conference on Engineering of Reconfigurable Systems and Algorithms (ERSA'10)*, July 12-15, 2010, Las Vegas, Nevada, USA.

- D. Unnikrishnan, R. Vadlamani, Y. Liao, A. Dwaraki, **J. Crenne**, L. Gao, R. Tessier, **Scalable Network Virtualization Using FPGAs**, *in the Proceedings of the International Symposium on Field-Programmable Gate Arrays (FPGA'10)*, February 21-23, 2010, Monterey, California, USA.

Publications

- **J. Crenne**, P. Bomel, G. Gogniat, J.-P Diguet, **UDP Partial Bitstreams Diffusion Through WLAN**, *in the Proceedings of the International Conference on Design and Architectures for Signal and Image Processing (DASIP'09)*, September 22-24, 2009, Sophia Antipolis, France.

- J.-P Diguet, L. Ye, Y. Eustache, **J. Crenne**, P. Bomel, G. Gogniat, J. Vidal, F. de Lamotte, **Networked Self-adaptive Systems: An Opportunity for Configuring in the Large**, *in the Proceedings of the International Conference on Engineering of Reconfigurable Systems and Algorithms (ERSA'09)*, July 13-16, 2009, Las Vegas, Nevada, USA.

- P. Bomel, **J. Crenne**, L. Ye, G. Gogniat, J.-P Diguet, **Ultra-Fast Downloading of Partial Bitstreams Through Ethernet**, *in the Proceedings of the International Conference on Architecture of Computing Systems (ARCS'09)*, March 10-13, 2009, Delft, The Netherlands.

- P. Bomel, G. Gogniat, J.-P Diguet, **J. Crenne**, **Bitstreams Repository Hierarchy for FPGA Partially Reconfigurable Systems**, *in the Proceedings of the International Symposium on Parallel and Distributed Computing (ISPDC'08)*, July 1-5, 2008, Krakow, Poland.

Conférences Nationales

- P. Cotret, **J. Crenne**, G. Gogniat, **Sécurisation des communications dans une architecture multi-processeurs**, *MAnifestation des JEunes Chercheurs en Sciences et Technologies de l'Information et de la Communication (MajecSTIC'10)*, October 14, 2010, Bordeaux, France.

www.jeremiecrenne.com

SÉCURITE HAUT DÉBIT POUR LES SYSTÈMES EMBARQUÉS À BASE DE FPGAs

R. Barjavel, « La télévision, œil de demain », 1947

SÉCURITE HAUT DÉBIT POUR LES SYSTÈMES EMBARQUÉS A BASE DE FPGAs

Trouver le meilleur compromis pour les systèmes embarqués, répondre à ce « besoin » grandissant qu'est la sécurité

PAR JÉRÉMIE CRENNE

Lab-STICC
UNIVERSITÉ EUROPÉENNE DE BRETAGNE
UBS Université de Bretagne-Sud
UNIVERSITY OF MASSACHUSETTS AMHERST 1863
cnrs