Distribution quantique de clés à variables continues

Anthony Leverrier

Télécom ParisTech

20 novembre 2009

Plan

Plan

Cryptographie et distribution de clés

Cryptographie

- Alice et Bob veulent échanger des messages de manière sécurisée.
- La sécurité d'un protocole repose sur des hypothèses de complexité : certains problèmes sont supposés difficiles (factorisation, log discret ...)
- sauf si Alice et Bob partagent au préalable une clé secrète

Code de Vernam

Le scénario

- Alice veut envoyer un message M à Bob,
- Alice et Bob possèdent une clé secrète C

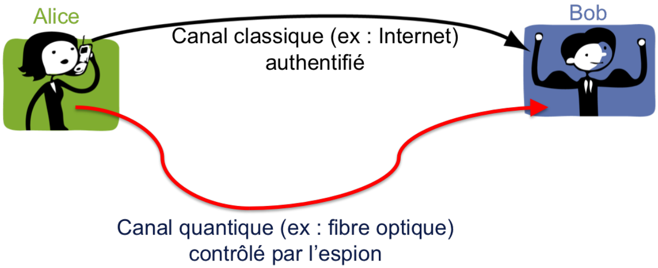
Chiffrement et déchiffrement

- Alice envoie $T = M \oplus C$ à Bob
- Bob calcule $T \oplus C = M$
- Sécurité inconditionnelle si la clé est aussi longue que le message

Problème : comment distribuer la clé initiale ?

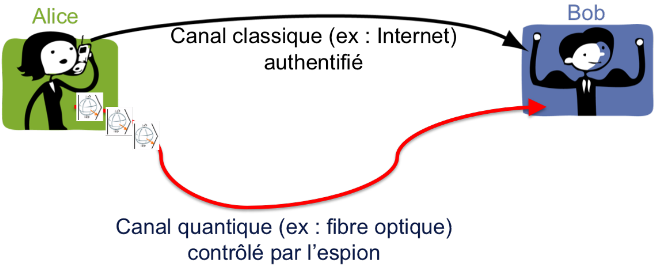
$\Rightarrow$ distribution *quantique* de clés !

Distribution quantique de clés



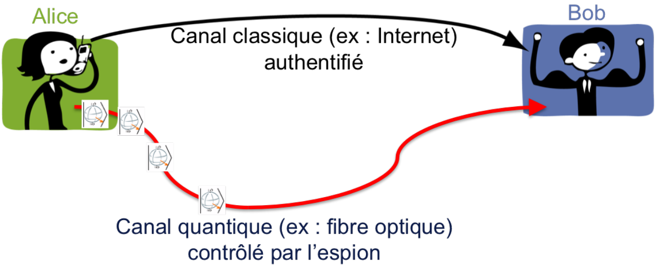
- Alice envoie des états quantiques à Bob : info mutuelle $I(A;B)$
- Si Eve acquiert de l'information sur ces états, elle les pertube :
  "bruit" $\Leftrightarrow I(B;E)$
- Si $I(A;B) > I(B;E)$, alors Alice et Bob peuvent extraire une clé de taille $K \approx I(A;B) - I(B;E)$
- Impossibilité de distribuer des clés à grande distance (centaine de km)

Distribution quantique de clés



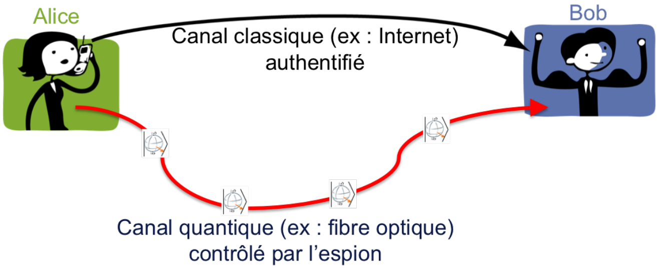
- Alice envoie des états quantiques à Bob : info mutuelle $I(A; B)$
- Si Eve acquiert de l'information sur ces états, elle les pertube :
  "bruit" $\Leftrightarrow I(B; E)$
- Si $I(A; B) > I(B; E)$, alors Alice et Bob peuvent extraire une clé de taille $K \approx I(A; B) - I(B; E)$
- Impossibilité de distribuer des clés à grande distance (centaine de km)

Distribution quantique de clés



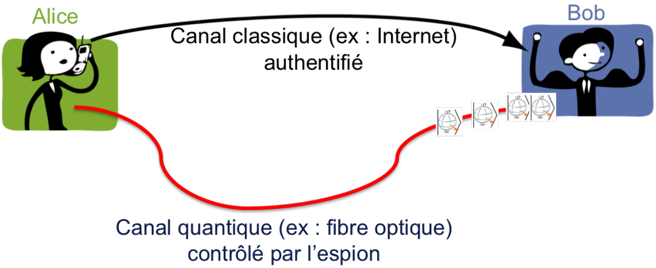
- Alice envoie des états quantiques à Bob : info mutuelle $I(A;B)$
- Si Eve acquiert de l'information sur ces états, elle les pertube :
  "bruit" $\Leftrightarrow I(B;E)$
- Si $I(A;B) > I(B;E)$, alors Alice et Bob peuvent extraire une clé de taille $K \approx I(A;B) - I(B;E)$
- Impossibilité de distribuer des clés à grande distance (centaine de km)

Distribution quantique de clés



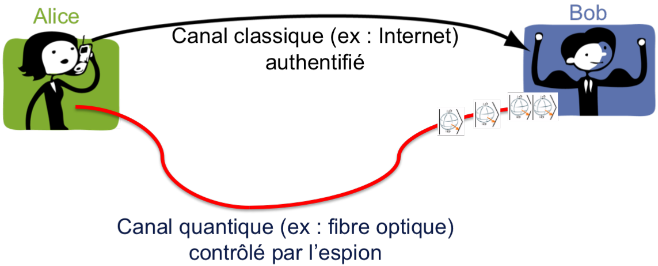
- Alice envoie des états quantiques à Bob : info mutuelle $I(A;B)$
- Si Eve acquiert de l'information sur ces états, elle les pertube :
  "bruit" $\Leftrightarrow I(B;E)$
- Si $I(A;B) > I(B;E)$, alors Alice et Bob peuvent extraire une clé de taille $K \approx I(A;B) - I(B;E)$
- Impossibilité de distribuer des clés à grande distance (centaine de km)

Distribution quantique de clés



- Alice envoie des états quantiques à Bob : info mutuelle $I(A; B)$
- Si Eve acquiert de l'information sur ces états, elle les pertube :
  "bruit" $\Leftrightarrow I(B; E)$
- Si $I(A; B) > I(B; E)$, alors Alice et Bob peuvent extraire une clé de taille $K \approx I(A; B) - I(B; E)$
- Impossibilité de distribuer des clés à grande distance (centaine de km)

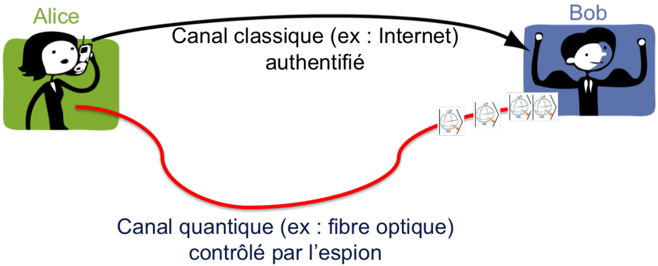
Distribution quantique de clés



- Alice envoie des états quantiques à Bob : info mutuelle $I(A; B)$
- Si Eve acquiert de l'information sur ces états, elle les pertube :

  "bruit" $\Leftrightarrow I(B; E)$
- Si $I(A; B) > I(B; E)$, alors Alice et Bob peuvent extraire une clé de taille $K \approx I(A; B) - I(B; E)$
- Impossibilité de distribuer des clés à grande distance (centaine de km)

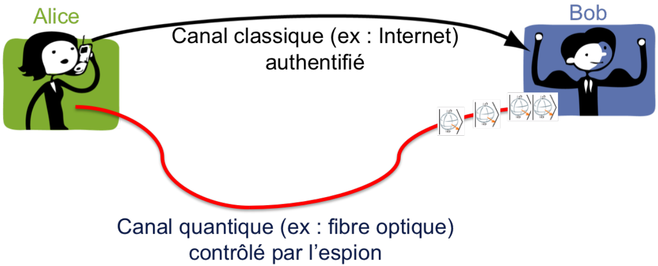
Distribution quantique de clés



- Alice envoie des états quantiques à Bob : info mutuelle $I(A;B)$
- Si Eve acquiert de l'information sur ces états, elle les pertube :

  "bruit" $\Leftrightarrow I(B;E)$
- Si $I(A;B) > I(B;E)$, alors Alice et Bob peuvent extraire une clé de taille $K \approx I(A;B) - I(B;E)$
- Impossibilité de distribuer des clés à grande distance (centaine de km)

Distribution quantique de clés

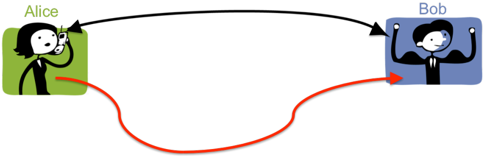


- Alice envoie des états quantiques à Bob : info mutuelle $I(A;B)$
- Si Eve acquiert de l'information sur ces états, elle les pertube :
  "bruit" $\Leftrightarrow I(B;E)$
- Si $I(A;B) > I(B;E)$, alors Alice et Bob peuvent extraire une clé de taille $K \approx I(A;B) - I(B;E)$
- Impossibilité de distribuer des clés à grande distance (centaine de km)

Distribution quantique de clés
les 3 étapes

Echange quantique (+ mesures)

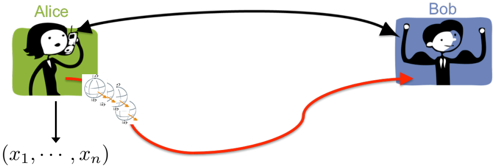
Alice et Bob obtiennent deux chaînes classiques X et Y corrélées, l'information de l'espion est représentée par ρ_E
$\rightarrow$ caractérise le protocole



Distribution quantique de clés
les 3 étapes

Echange quantique (+ mesures)

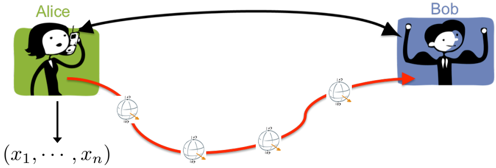
Alice et Bob obtiennent deux chaînes classiques X et Y corrélées, l'information de l'espion est représentée par ρ_E
$\rightarrow$ caractérise le protocole



Distribution quantique de clés
les 3 étapes

Echange quantique (+ mesures)

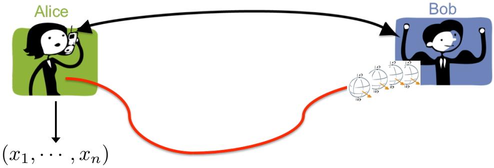
Alice et Bob obtiennent deux chaînes classiques X et Y corrélées, l'information de l'espion est représentée par ρ_E
$\rightarrow$ caractérise le protocole



Distribution quantique de clés
les 3 étapes

Echange quantique (+ mesures)

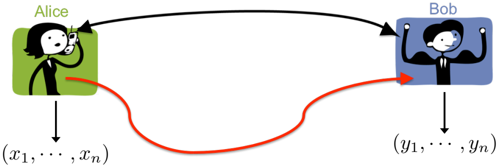
Alice et Bob obtiennent deux chaînes classiques X et Y corrélées, l'information de l'espion est représentée par ρ_E
$\rightarrow$ caractérise le protocole



Distribution quantique de clés
les 3 étapes

Echange quantique (+ mesures)

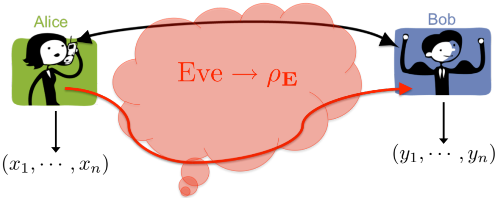
Alice et Bob obtiennent deux chaînes classiques X et Y corrélées, l'information de l'espion est représentée par ρ_E
$\rightarrow$ caractérise le protocole



Distribution quantique de clés
les 3 étapes

Echange quantique (+ mesures)

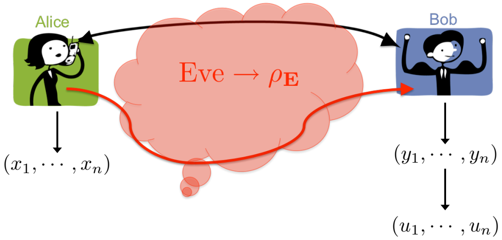
Alice et Bob obtiennent deux chaînes classiques X et Y corrélées, l'information de l'espion est représentée par ρ_E
$\rightarrow$ caractérise le protocole



Distribution quantique de clés
les 3 étapes

Réconciliation (inverse)

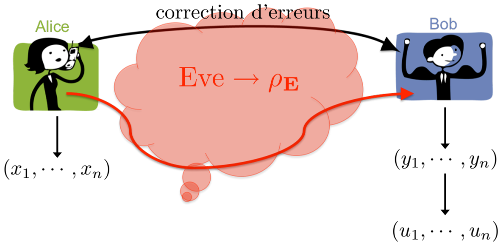
X, $Y+$ correction d'erreurs : Alice et Bob se mettent d'accord sur une chaîne commune U (partiellement connue de l'espion)
$\rightarrow \pm$ difficile suivant la nature de X et Y.



Distribution quantique de clés
les 3 étapes

Réconciliation (inverse)

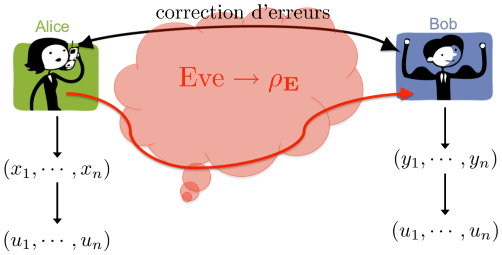
X, $Y+$ correction d'erreurs : Alice et Bob se mettent d'accord sur une chaîne commune U (partiellement connue de l'espion)
$\rightarrow \pm$ difficile suivant la nature de X et Y.



Distribution quantique de clés
les 3 étapes

Réconciliation (inverse)

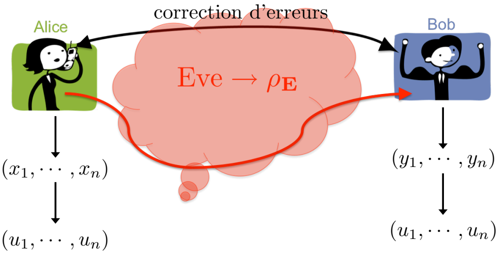
X, $Y+$ correction d'erreurs : Alice et Bob se mettent d'accord sur une chaîne commune U (partiellement connue de l'espion)
$\rightarrow \pm$ difficile suivant la nature de X et Y.



Distribution quantique de clés
les 3 étapes

Amplification de confidentialité

Alice et Bob appliquent une fonction de hachage *g* à *U*
$\longrightarrow$ clé aléatoire, inconnue d'Eve
Le bruit réduit la taille de la clé, pas sa sécurité !



$$C \equiv (c_1, \cdots, c_K) = g(u_1, \cdots, u_n)$$

Plan

Variables continues ou discrètes ?

Variables discrètes

- protocoles les plus courants
- information encodée par ex. sur la polarisation d'un photon
- Bob mesure avec des compteurs de photons

Variables continues (depuis 2000)

- information encodée dans l'espace des phases : quadratures d'états cohérents (composantes cartésiennes du champ EM quantifié)
- Bob mesure **une** quadrature avec une détection homodyne
- résultats de mesure continus

Avantages des variables continues

- pas besoin de produire ou détecter de photons uniques
- n'utilise que des composants télécom standards

Variables continues ou discrètes ?

Variables discrètes

- protocoles les plus courants
- information encodée par ex. sur la polarisation d'un photon
- Bob mesure avec des compteurs de photons

Variables continues (depuis 2000)

- information encodée dans l'espace des phases : quadratures d'états cohérents (composantes cartésiennes du champ EM quantifié)
- Bob mesure **une** quadrature avec une détection homodyne
- résultats de mesure continus

Avantages des variables continues

- pas besoin de produire ou détecter de photons uniques
- n'utilise que des composants télécom standards

Variables continues ou discrètes ?

Variables discrètes

- protocoles les plus courants
- information encodée par ex. sur la polarisation d'un photon
- Bob mesure avec des compteurs de photons

Variables continues (depuis 2000)

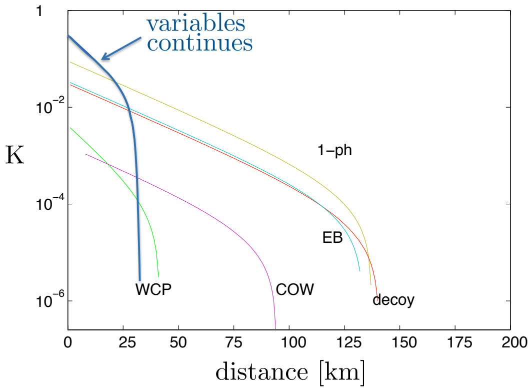
- information encodée dans l'espace des phases : quadratures d'états cohérents (composantes cartésiennes du champ EM quantifié)
- Bob mesure **une** quadrature avec une détection homodyne
- résultats de mesure continus

Avantages des variables continues

- pas besoin de produire ou détecter de photons uniques
- n'utilise que des composants télécom standards

Variables continues ou discrètes ?

mais ... portée apparemment limitée



V. Scarani et al, Rev. Mod. Phys. **81**, 1301 (2009)

Variables continues ou discrètes ?

	Var. discrètes	**Var. continues**
Support de l'information	polarisation de photons uniques	quadratures d'états cohérents
Détection	comptage de photons	détection homodyne $\rightarrow$ interférométrie
Performances	longues distances (100-200 km)	Taux important ... à courtes distances (30 km)
Principale limitation	technologique (détecteurs)	algorithmique (réconciliation)

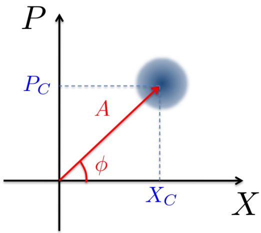
Objectif initial de la thèse : résoudre ce problème !

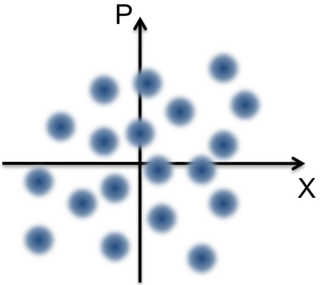
Plan

Variables continues : le protocole à modulation gaussienne

Alice envoie *n* états cohérents avec une modulation gaussienne.

$$\Delta X \Delta P \geq 1$$



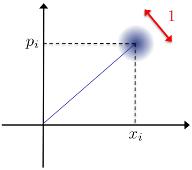


Pour chaque état, Bob mesure aléatoirement l'une des 2 quadratures.

Variables continues : le protocole à modulation gaussienne

Modèle du canal gaussien

- état initial centré en (x_i, p_i), variance 1
- transmission T
  $\rightarrow$ centré en $(\sqrt{T}x_i, \sqrt{T}p_i)$,
- excès de bruit ξ
  $\rightarrow$ variance finale $1 + T\xi$



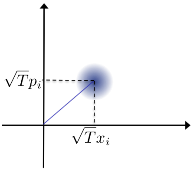
Bob mesure une quadrature et obtient y_i

- $x_i \sim \mathcal{N}(0, V_A)$
- $y_i = \sqrt{T}x_i + z_i$ avec $z_i \sim \mathcal{N}(0, 1 + T\xi)$

Variables continues : le protocole à modulation gaussienne

Modèle du canal gaussien

- état initial centré en (x_i, p_i), variance 1
- transmission T
  $\rightarrow$ centré en $(\sqrt{T}x_i, \sqrt{T}p_i)$,
- excès de bruit ξ
  $\rightarrow$ variance finale $1 + T\xi$



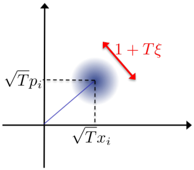
Bob mesure une quadrature et obtient y_i

- $x_i \sim \mathcal{N}(0, V_A)$
- $y_i = \sqrt{T}x_i + z_i$ avec $z_i \sim \mathcal{N}(0, 1 + T\xi)$

Variables continues : le protocole à modulation gaussienne

Modèle du canal gaussien

- état initial centré en (x_i, p_i), variance 1
- transmission T
  $\rightarrow$ centré en $(\sqrt{T}x_i, \sqrt{T}p_i)$,
- excès de bruit ξ
  $\rightarrow$ variance finale $1 + T\xi$



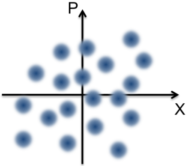
Bob mesure une quadrature et obtient y_i

- $x_i \sim \mathcal{N}(0, V_A)$
- $y_i = \sqrt{T}x_i + z_i$ avec $z_i \sim \mathcal{N}(0, 1 + T\xi)$

Variables continues : le protocole à modulation gaussienne

Modèle du canal gaussien

- état initial centré en (x_i, p_i), variance 1
- transmission T
  $\rightarrow$ centré en $(\sqrt{T}x_i, \sqrt{T}p_i)$,
- excès de bruit ξ
  $\rightarrow$ variance finale $1 + T\xi$



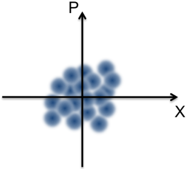
Bob mesure une quadrature et obtient y_i

- $x_i \sim \mathcal{N}(0, V_A)$
- $y_i = \sqrt{T}x_i + z_i$ avec $z_i \sim \mathcal{N}(0, 1 + T\xi)$

Variables continues : le protocole à modulation gaussienne

Modèle du canal gaussien

- état initial centré en (x_i, p_i), variance 1
- transmission T
  $\rightarrow$ centré en $(\sqrt{T}x_i, \sqrt{T}p_i)$,
- excès de bruit ξ
  $\rightarrow$ variance finale $1 + T\xi$



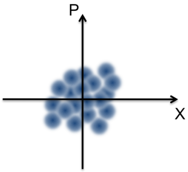
Bob mesure une quadrature et obtient y_i

- $x_i \sim \mathcal{N}(0, V_A)$
- $y_i = \sqrt{T}x_i + z_i$ avec $z_i \sim \mathcal{N}(0, 1 + T\xi)$

Variables continues : le protocole à modulation gaussienne

Modèle du canal gaussien

- état initial centré en (x_i, p_i), variance 1
- transmission T
  $\rightarrow$ centré en $(\sqrt{T}x_i, \sqrt{T}p_i)$,
- excès de bruit ξ
  $\rightarrow$ variance finale $1 + T\xi$



Bob mesure une quadrature et obtient y_i

- $x_i \sim \mathcal{N}(0, V_A)$
- $y_i = \sqrt{T}x_i + z_i$ avec $z_i \sim \mathcal{N}(0, 1 + T\xi)$

Taux secret $K = I(A;B) - I(B;E)$

Dépend des attaques considérées

- générales : l'espion est limité uniquement par la MQ
- collectives : l'espion agit de la même façon pour chaque impulsion
  $\rightarrow$ raisonnables : optimales pour la plupart des protocoles
  $\rightarrow$ beaucoup plus faciles à étudier

Dépend d'hypothèses

- réconciliation parfaite ou imparfaite
- limite asymptotique, ou effets de taille finie

Dépend de l'implémentation

problème des canaux cachés :
est-ce que l'implémentation correspond bien au modèle théorique ?

Taux secret $K = I(A;B) - I(B;E)$

Dépend des attaques considérées

- générales : l'espion est limité uniquement par la MQ
- collectives : l'espion agit de la même façon pour chaque impulsion
  $\longrightarrow$ raisonnables : optimales pour la plupart des protocoles
  $\longrightarrow$ beaucoup plus faciles à étudier

Dépend d'hypothèses

- réconciliation parfaite ou imparfaite
- limite asymptotique, ou effets de taille finie

Dépend de l'implémentation

problème des canaux cachés :
est-ce que l'implémentation correspond bien au modèle théorique ?

Taux secret $K = I(A;B) - I(B;E)$

Dépend des attaques considérées

- générales : l'espion est limité uniquement par la MQ
- collectives : l'espion agit de la même façon pour chaque impulsion
  $\longrightarrow$ raisonnables : optimales pour la plupart des protocoles
  $\longrightarrow$ beaucoup plus faciles à étudier

Dépend d'hypothèses

- réconciliation parfaite ou imparfaite
- limite asymptotique, ou effets de taille finie

Dépend de l'implémentation

problème des canaux cachés :
est-ce que l'implémentation correspond bien au modèle théorique ?

Plan

Le problème de la réconciliation

Taux théorique : $K_{\text{th}} = I(A;B) - \chi(B;E)$

- $I(A;B) = \frac{1}{2}\log_2(1+\mathrm{SNR})$ (pour un canal gaussien)
- $\mathrm{SNR} = \frac{TV_A}{1+T\xi}$
- $\chi(B;E)$: généralise $I(B;E)$ si Eve fait des mesures quantiques collectives

$K_{\text{th}} > 0$ pour toute transmission T (à ξ faible)

En pratique : $K_{\text{prat}} = \beta I(A;B) - \chi(B;E)$

- réconciliation imparfaite : Alice et Bob n'extraient que $\beta I(A;B)$
- $\beta =$ efficacité de réconciliation (< 1)
- K_{prat} s'annule à distance finie : 30 à 50 km

Réconciliation de variables gaussiennes

Y vecteur gaussien : $y_i = \sqrt{T}\, x_i + z_i$

Idée 1 : discrétiser y_i (Réconciliation par tranches)

$$\hat{y}_i = u_{i_1} u_{i_2} u_{i_3} u_{i_4}$$

Bob envoie de la redondance à Alice : syndromes de codes LDPC

$\Rightarrow$ fonctionne bien à SNR élevé

$\Rightarrow$ fonctionne mal à faible SNR (brise la symétrie gaussienne)

Réconciliation de variables gaussiennes

Y vecteur gaussien : $y_i = \sqrt{T}\, x_i + z_i$

Idée 1 : discrétiser y_i (Réconciliation par tranches)

$$\hat{y}_i = u_{i_1} u_{i_2} u_{i_3} u_{i_4}$$

Bob envoie de la redondance à Alice : syndromes de codes LDPC
$\Rightarrow$ fonctionne bien à SNR élevé
$\Rightarrow$ fonctionne mal à faible SNR (brise la symétrie gaussienne)

Idée 2 : utiliser le signe de y_i

$u_i = \text{signe}(y_i)$,
Bob envoie $|y_i|$ (+ syndrome de code LDPC) à Alice
$\Rightarrow$ fonctionne mal à SNR élevé ($\beta I(A;B) < 1$)
$\Rightarrow$ ne fonctionne pas très bien à faible SNR (mais respecte la symétrie)

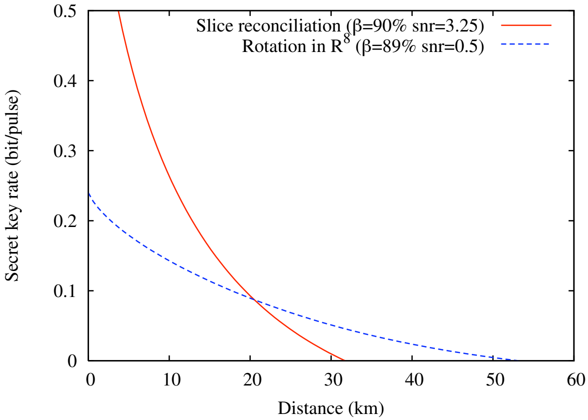
Réconciliation de variables gaussiennes

Y vecteur gaussien : $y_i = \sqrt{T}\, x_i + z_i$

Nouvelle idée : généralisation multidimensionnelle

- $Y/||Y||$ est uniformément réparti sur $\mathcal{S}^{n-1}$
- $U \in \{-1/\sqrt{n}, 1/\sqrt{n}\}^n$, Bob envoie UY^{-1} à Alice
- construction de UY^{-1} possible uniquement en dimensions $1, 2, 4$ et 8
- dim 8 fonctionne assez bien à faible SNR

Réconciliation de variables gaussiennes



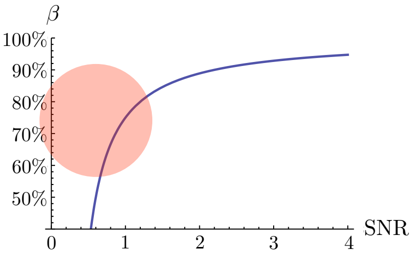
portée 30 km → 50 km avec le même hardware !

A. Leverrier, *et al*, Phys. Rev. A **77**, 042325 (2008)

Réconciliation de variables gaussiennes

Problème

Pour augmenter la portée, il faut travailler à faible SNR.
Tous les protocoles de réconciliation connus sont mauvais dans ce régime.



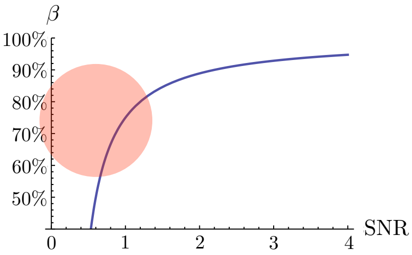
Solution

Abandonner la modulation gaussienne !

Réconciliation de variables gaussiennes

Problème

Pour augmenter la portée, il faut travailler à faible SNR.
Tous les protocoles de réconciliation connus sont mauvais dans ce régime.

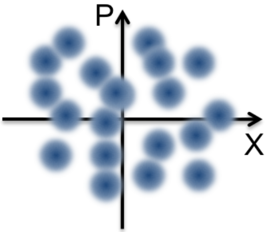


Solution

Abandonner la modulation gaussienne !

Plan

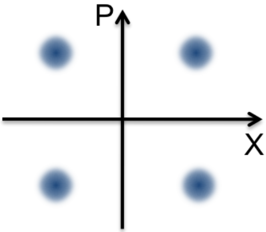
Modulation quaternaire



Nouveau protocole

- Alice n'utilise que 4 états pour encoder de l'information.
- $y_i = \sqrt{T} x_i + z_i$ avec $x_i = \pm A$
  $\Rightarrow$ problème de codage de canal très étudié : bons codes LDPC
  $\Rightarrow$ réconciliation à (très) faible SNR facile : $u_i =$ signe (y_i)

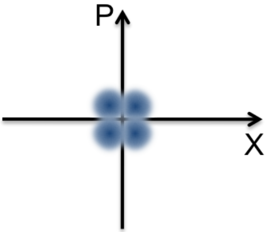
Modulation quaternaire



Nouveau protocole

- Alice n'utilise que 4 états pour encoder de l'information.
- $y_i = \sqrt{T} x_i + z_i$ avec $x_i = \pm A$
  $\Rightarrow$ problème de codage de canal très étudié : bons codes LDPC
  $\Rightarrow$ réconciliation à (très) faible SNR facile : $u_i = \text{signe}\,(y_i)$

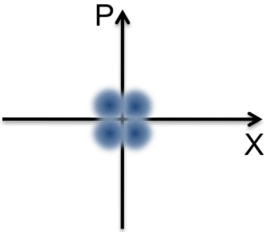
Modulation quaternaire



Nouveau protocole

- Alice n'utilise que 4 états pour encoder de l'information.
- $y_i = \sqrt{T} x_i + z_i$ avec $x_i = \pm A$
  $\Rightarrow$ problème de codage de canal très étudié : bons codes LDPC
  $\Rightarrow$ réconciliation à (très) faible SNR facile : $u_i =$ signe (y_i)

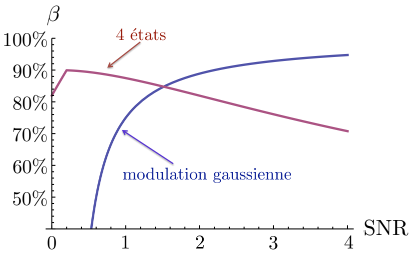
Modulation quaternaire



Nouveau protocole

- Alice n'utilise que 4 états pour encoder de l'information.
- $y_i = \sqrt{T} x_i + z_i$ avec $x_i = \pm A$
  $\Rightarrow$ problème de codage de canal très étudié : bons codes LDPC
  $\Rightarrow$ réconciliation à (très) faible SNR facile : $u_i = \text{signe}\,(y_i)$

Modulation quaternaire



Performances du nouveau protocole

- Rappel : $K = \beta I(A;B) - \chi(B;E)$
- le protocole à 4 états résout le problème de $\beta I(A;B)$
- problème : que dire de $\chi(B;E)$?

Sécurité : comment calculer $\chi(B;E)$?

2 versions équivalentes du protocole

Protocole *Prépare et mesure*

- utilisé en pratique
- Alice prépare des états cohérents et les envoie à Bob
- pas facile de calculer $\chi(B;E)$ dans ce scénario

Protocole intriqué équivalent (“purification” du protocole P&M)

- il existe un protocole où Alice prépare des états intriqués $|\psi\rangle_{A,B_0}$
- elle mesure une moitié et envoie la seconde moitié à Bob
- par ex, pour le protocole à modulation gaussienne, $|\psi\rangle_{A,B_0}$ est un état EPR, et Alice procède à une mesure hétérodyne.

Sécurité : comment calculer $\chi(B; E)$?

Le problème

- protocole intriqué : Alice et Bob partagent un état ρ_{AB}
- il existe f telle que $\chi(B; E) = f(\rho_{AB})$
- on ne connaît pas bien ρ_{AB} (dimension infinie)
- on ne sait pas calculer f en général (problème d'optimisation trop compliqué)

Miracle : optimalité gaussienne
(M. Wolf, *et al* 2005, R. Garcia-Patron & N.J. Cerf 2006)

- ρ_{AB}^G : état gaussien avec même matrice de covariance que ρ_{AB}
- théorème : $f(\rho_{AB}) \leq f(\rho_{AB}^G)$
- on sait calculer f pour les états gaussiens
- on mesure facilement la matrice de covariance de ρ_{AB}
  $\Rightarrow$ 2 paramètres à évaluer : T et ξ

Sécurité : comment calculer $\chi(B;E)$?

Le problème

- protocole intriqué : Alice et Bob partagent un état ρ_{AB}
- il existe f telle que $\chi(B;E) = f(\rho_{AB})$
- on ne connaît pas bien ρ_{AB} (dimension infinie)
- on ne sait pas calculer f en général (problème d'optimisation trop compliqué)

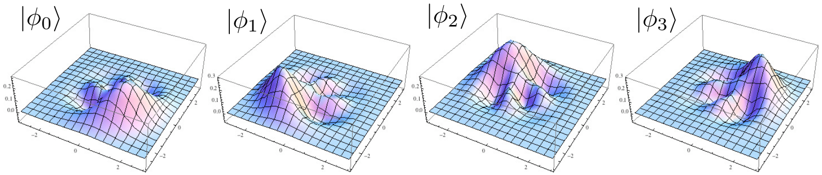
Miracle : optimalité gaussienne (M. Wolf, *et al* 2005, R. Garcia-Patron & N.J. Cerf 2006)

- ρ_{AB}^G : état gaussien avec même matrice de covariance que ρ_{AB}
- théorème : $f(\rho_{AB}) \leq f(\rho_{AB}^G)$
- on sait calculer f pour les états gaussiens
- on mesure facilement la matrice de covariance de ρ_{AB}
  $\Rightarrow$ 2 paramètres à évaluer : T et ξ

Modulation quaternaire

Protocole intriqué à 4 états

- $|\psi\rangle_{AB_0} = \frac{1}{2}\left(|\phi_0\rangle_A|\alpha_0\rangle_{B_0} + |\phi_1\rangle_A|\alpha_1\rangle_{B_0} + |\phi_2\rangle_A|\alpha_2\rangle_{B_0} + |\phi_3\rangle_A|\alpha_3\rangle_{B_0}\right)$
- $|\alpha_0\rangle, |\alpha_1\rangle, |\alpha_2\rangle, |\alpha_3\rangle$: états cohérents
- $|\phi_0\rangle, |\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle$: états orthogonaux

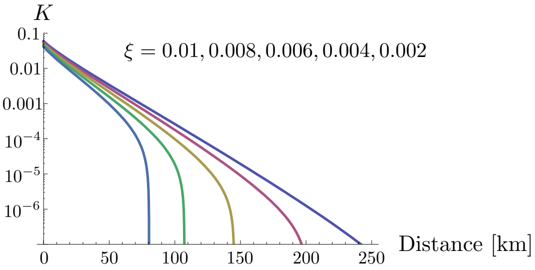


$|\psi\rangle_{AB_0}$ est quasiment gaussien à faible variance de modulation

$\chi(B;E)_4 \approx \chi(B;E)_{\text{gauss}}$ mais $\beta I(A;B)_4 \gg \beta I(A;B)_{\text{gauss}}$

$\Rightarrow K_4 \gg K_{\text{gauss}}$

Performances du nouveau protocole

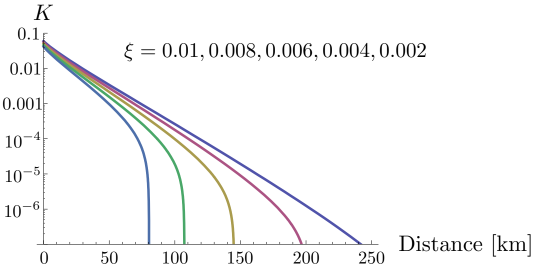


A. Leverrier & P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009)

- distribution possible à longue distance : $K \propto T$
- performances très sensibles à la qualité de l'implémentation (excès de bruit)

Attention : jusqu'ici, on a considéré uniquement les attaques collectives dans la limite asymptotique

Performances du nouveau protocole



A. Leverrier & P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009)

- distribution possible à longue distance : $K \propto T$
- performances très sensibles à la qualité de l'implémentation (excès de bruit)

Attention : jusqu'ici, on a considéré uniquement les attaques collectives dans la limite asymptotique

Plan

Problème des tailles finies

Taux secret non asymptotique (contre les attaques collectives)

$$k = \frac{n}{N}\left(\beta I(A;B) - \chi_{\text{EP}}(B;E) - \Delta(n)\right)$$

$$\text{taille du bloc } N \text{ dont} \begin{cases} n & \text{pour la distillation de clé} \\ N-n & \text{pour l'estimation de paramètres} \end{cases}$$

- $\chi_{\text{EP}}(B;E) =$ "estimation" de $\chi(B;E)$
- $\Delta(n) \to 0$ pour $n \to \infty$ (indépendant du protocole)

Principal problème : estimation du canal quantique

- estimation dans le pire des cas
  $\Rightarrow$ pires paramètres T et ξ compatibles avec les données sauf avec proba $1-\epsilon$ ($\epsilon = 10^{-10}$ par ex.)
- hypothèse : modèle gaussien

Problème des tailles finies

Taux secret non asymptotique (contre les attaques collectives)

$$k = \frac{n}{N}\left(\beta I(A;B) - \chi_{\mathrm{EP}}(B;E) - \Delta(n)\right)$$

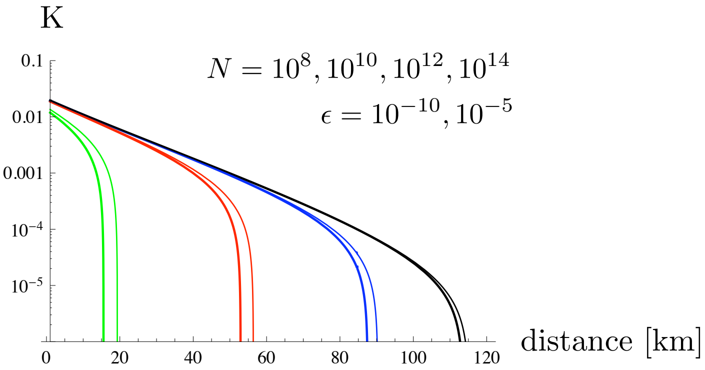
$$\text{taille du bloc } N \text{ dont } \begin{cases} n & \text{pour la distillation de clé} \\ N-n & \text{pour l'estimation de paramètres} \end{cases}$$

- $\chi_{\mathrm{EP}}(B;E) =$ "estimation" de $\chi(B;E)$
- $\Delta(n) \to 0$ pour $n \to \infty$ (indépendant du protocole)

Principal problème : estimation du canal quantique

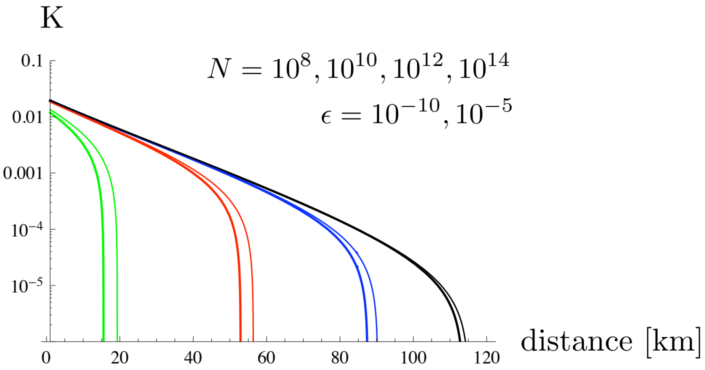
- estimation dans le pire des cas
  $\Rightarrow$ pires paramètres T et ξ compatibles avec les données sauf avec proba $1-\epsilon$ ($\epsilon = 10^{-10}$ par ex.)
- hypothèse : modèle gaussien

Problème des tailles finies



il faut des blocs très longs ($N \geq 10^8$) !

Problème des tailles finies



il faut des blocs très longs ($N \geq 10^8$) !

Plan

Attaques générales

Le problème

- protocole intriqué : $\rho_{AB}^{(n)} \in (\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$
- $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$ est beaucoup trop gros !
- attaque collective : $\rho_{AB}^{(n)} = \int p(\sigma)\, \sigma_{AB}^{\otimes n} \mathrm{d}\sigma$ avec $\sigma_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ (état i.i.d.)

Attaques générales

Le problème

- protocole intriqué : $\rho_{AB}^{(n)} \in (\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$
- $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$ est beaucoup trop gros !
- attaque collective : $\rho_{AB}^{(n)} = \int p(\sigma)\, \sigma_{AB}^{\otimes n} \mathrm{d}\sigma$ avec $\sigma_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ (état i.i.d.)

Stratégie

- on utilise les symétries du protocole pour réduire la taille de l'espace pertinent
- ensuite, théorème de de Finetti [1], ou technique de postsélection [2] pour montrer que les attaques collectives sont optimales asymptotiquement :

$$\text{état symétrique} \approx \text{état i.i.d.}$$

[1] R. Renner, Nature Physics (2007)
[2] M.Christandl, R. König, R. Renner, PRL (2009)

Attaques générales

Le problème

- protocole intriqué : $\rho_{AB}^{(n)} \in (\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$
- $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$ est beaucoup trop gros !
- attaque collective : $\rho_{AB}^{(n)} = \int p(\sigma)\, \sigma_{AB}^{\otimes n} \mathrm{d}\sigma$ avec $\sigma_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ (état i.i.d.)

Symétrie habituelle

- protocole invariant par une permutation des impulsions
- protocoles à variables continues : ça fonctionne aussi (R. Renner & J.I. Cirac, PRL, 2009)
- bornes non optimales pour les tailles finies ?
- nouvelle symétrie pour les protocoles à variables continues ?

Nouvelle symétrie dans l'espace des phases

Nouvelle symétrie (A. Leverrier, *et al*, New J. Phys. 11, 115009, 2009)

- $p(RX, RY) = p(X, Y)$ pour tout $R \in O(n)$
- le protocole est invariant si Alice et Bob appliquent des opérations gaussiennes passives conjuguées à leurs n modes respectifs
- la caractérisation des états bipartites avec cette invariance n'est pas très simple ... on ne peut pas encore conclure

Résultats partiels (A. Leverrier & N.J. Cerf, Phys. Rev. A, **80**, 010102, 2009)

- cas monopartite : étude des états invariants par transformation gaussienne passive
- mélanges d'états de Fock généralisés à n modes
- théorème de de Finetti : ces états tendent vers des états thermiques multimodes quand on trace suffisamment de modes

Plan

Conclusion et perspectives

Amélioration des performances des protocoles à variables continues

- protocole à modulation gaussienne : nouvelle technique de réconciliation optimale : portée 30 km $\rightarrow$ 50 km
- nouveau protocole à 4 états : portée > 100 km
  $\Rightarrow$ **bonne alternative aux variables discrètes**

Preuves de sécurité

- analyse des effets de taille finie
- étude de nouvelles symétries dans l'espace des phases

Conclusion et perspectives

Amélioration des performances des protocoles à variables continues

- protocole à modulation gaussienne : nouvelle technique de réconciliation optimale : portée 30 km $\rightarrow$ 50 km
- nouveau protocole à 4 états : portée > 100 km
  $\Rightarrow$ **bonne alternative aux variables discrètes**

Preuves de sécurité

- analyse des effets de taille finie
- étude de nouvelles symétries dans l'espace des phases