

Réconciliation de variables gaussiennes corrélées dans le cadre de protocoles de cryptographie quantique

A. Leverrier¹ R. Alléaume¹ J. Boutros² G. Zémor³
P. Grangier⁴

¹Télécom ParisTech

²Texas A&M at Qatar

³Institut de Mathématiques de Bordeaux

⁴Institut d'Optique

Journées "Codage et Cryptographie" 2008

1 Réconciliation de variables corrélées

- Cryptographie quantique
- Réconciliation : le cas discret
- Vers une généralisation au cas continu

2 Réconciliation dans \mathbb{R}^n

- Réconciliation multidimensionnelle
- Comment décrire un cube contenant X ?

3 Rotations sur S^1 , S^3 et S^7

- Existence
- Codage/Décodage
- Indépendance

Protocole de distribution quantique de clés

Distribution quantique

- En réalité, la "cryptographie quantique" est un moyen de *distribuer une clé secrète à deux parties éloignées, Alice et Bob.*
- Cette clé peut ensuite être utilisée pour un protocole de cryptographie classique, par exemple *le code de Vernam.*

Sécurité "inconditionnelle" basée sur la mécanique quantique

- **non clonage** : $(\forall |\phi\rangle) \quad |\phi\rangle \rightarrow |\phi\rangle |\phi\rangle$ est impossible
- **principe d'incertitude** de Heisenberg : mesurer un état quantique le perturbe

Les grandes étapes du protocole

Protocole purement quantique

A la fin de cette partie (échange d'états quantiques et mesure), Alice et Bob possèdent **deux variables aléatoires corrélées, X et Y** . Eve, obtient une variable aléatoire (quantique) Z corrélée à X et Y .

Réconciliation

Alice et Bob se mettent d'accord sur une variable identique U .

Amplification de confidentialité

Alice et Bob choisissent une fonction de compression aléatoire g (fonction de hachage). Le secret est $g(U)$.

Taux secret

Généralisation quantique de Csiszar-Körner

$$K = I(X; Y) - S(X; Z)$$

Physique quantique : on connaît $S(X; Z)$

- $I(X; Y)$: information mutuelle (de Shannon) entre X et Y
- $S(X; Z)$: information quantique entre X et l'état quantique Z .

Remarques

- S possède certaines des propriétés de I .
- Etude de $S(A; B)$: *théorie de l'information quantique*

Taux secret : effet de la réconciliation

Protocole (réconciliation unidirectionnelle)

- Alice choisit une variable aléatoire binaire U .
- Elle envoie de l'information α à Bob sur un canal public authentifié.
- Bob "décode" U à partir de Y et α .

Taux secret après la réconciliation

$$K_{\text{réel}} = H(U) - S(U; Z, \alpha)$$

Réconciliation imparfaite

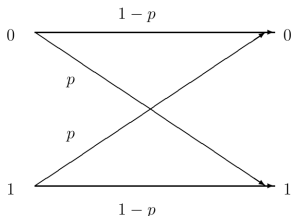
$$K_{\text{réel}} = \beta I(X; Y) - S(X; Z) \quad (\beta < 1)$$

Similarités avec le codage de canal

Réconciliation = codage de canal avec source aléatoire

$X, Y \sim \mathcal{U}(\mathbb{F}_2^n)$ avec $X \oplus Y \sim \mathcal{B}(p)^{\otimes n}$

→ canal BSC avec une source aléatoire $X_i \sim (\mathbb{F}_2)$.



Décodage par syndrome

Codage de canal classique

On envoie $X \in \mathcal{C}$, un code linéaire, de matrice de parité H .

Réconciliation binaire

- $X \in \mathcal{C}_S$, un coset de \mathcal{C} .
- Alice envoie le syndrome $S = HX$ de X à Bob
- Bob décode $Y \oplus S$.

Résumé

- $U = X \oplus S$
- $\alpha = S$
- U et α sont indépendants $\Rightarrow K \geq H(U) - S(X; Z)$

Spécificités du cas continu

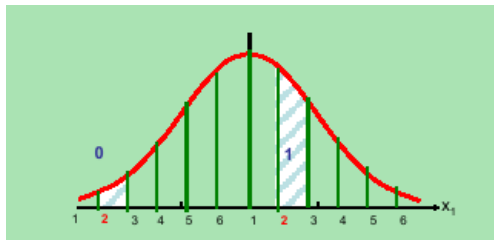
Modèle gaussien

- $X \sim \mathcal{N}(0, 1)^{\otimes n}$
- $Y = X + W$ avec $W \sim \mathcal{N}(0, \sigma^2)^{\otimes n}$
- $\text{SNR} = \frac{1}{\sigma^2}$ et $I(X; Y) = \frac{n}{2} \log_2(1 + \text{SNR})$

Crypto quantique

- on travaille à faible SNR \rightarrow 1 bit/symbole
- information acquise par l'espion ? Il suffit que U et α soient indépendants

Réconciliation par tranches

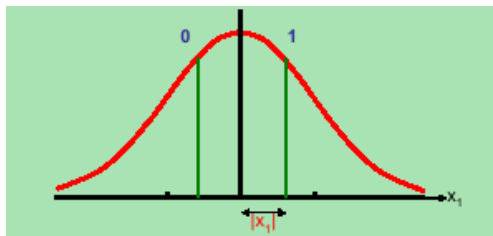


- Alice quantifie X et indique le n° de "tranche" à Bob
- $U = \hat{X}$ et $\alpha = \text{n° de tranche}$

Résumé

- 0 et 1 faciles à distinguer
- canal conditionnel peu "sympathique" : trouver un code spécifique ?

Codage dans le signe de la variable



- Alice envoie $|X|$ à Bob
- $U = \text{sgn}(X)$ et $\alpha = |X|$

Résumé

- Stratégie simple qui ne donne pas d'information à l'espion
- 0 et 1 pas toujours simples à distinguer

Réconciliation multidimensionnelle

Distribution gaussienne

Si $X \sim \mathcal{N}(0, 1)^{\otimes n}$ alors $\frac{X}{\|X\|} \sim \mathcal{U}(S^{n-1})$

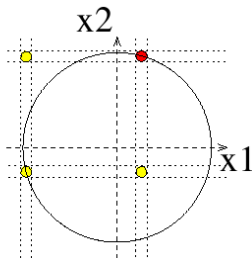
Conséquence

L'espace pertinent est S^{n-1} .

On utilise des codes sphériques.

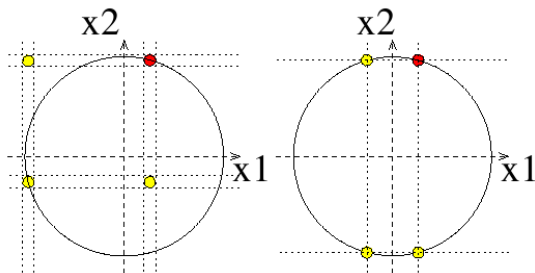
Réconciliation pour deux variables successives

- réconciliation par tranches



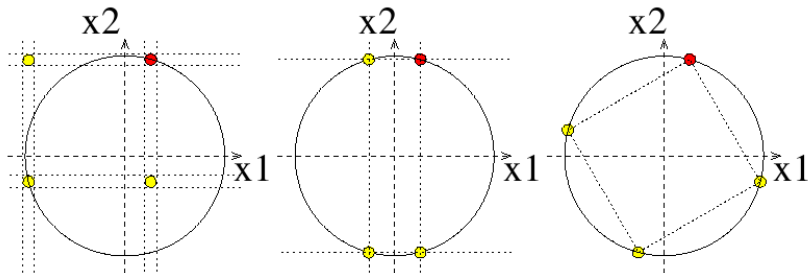
Réconciliation pour deux variables successives

- réconciliation par tranches
- codage dans le signe



Réconciliation pour deux variables successives

- réconciliation par tranches
- codage dans le signe
- **alternative proposée**



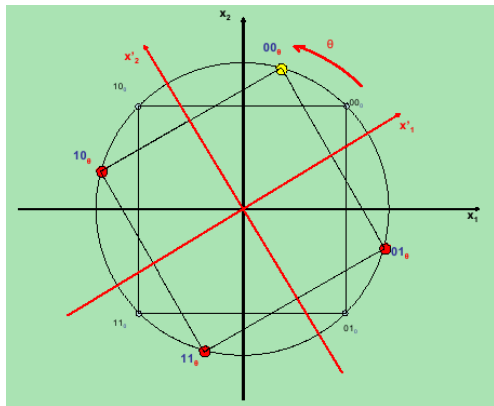
Avantages du code cubique

- 0 et 1 bien séparés : modulation apparente = loi de $\chi(n)$
- en augmentant la dimension du cube, on se rapproche d'une modulation BPSK
- permet d'utiliser les bons codes binaires (LDPC ou turbo codes)

Mais ...

Comment décrire un cube dont X donné est un des sommets ?

Comment décrire un cube dans \mathbb{R}^n ?



Un cube peut être décrit par une transformation orthogonale.

Comment décrire un cube dans \mathbb{R}^n ?

On veut une transformation qui envoie $X \in S^{n-1}$ sur $U \in \{-\frac{1}{\sqrt{n}}, \frac{1}{\sqrt{n}}\}^n$.

Première idée

- réflexion par rapport à l'hyperplan médiateur de X et U
- description simple : $\alpha = \frac{X-U}{\|X-U\|}$
- mais révèle de l'information pour $n > 2$: $p(U = u_i | \alpha) \neq \frac{1}{2^n}$

Deuxième solution ?

- transformation aléatoire de $O(n)$
- \rightarrow ne révèle pas d'information sur U
- générer une transformation aléatoire est complexe pour $n \sim 10^5 - 10^6$

Fonction déterministe \Rightarrow dimensions 1, 2, 4 et 8

Théorème

S'il existe une application continue :

$$\begin{aligned} M : S^{n-1} \times S^{n-1} &\longrightarrow O_n \\ (X, U) &\longmapsto M(X, U) \end{aligned}$$

telle que $M(X, U) \cdot X = U$ pour tous $X, U \in S^{n-1}$, alors $n = 1, 2, 4$ ou 8 .

Théorème (Adams, 1962)

Les seules sphères S^{n-1} pour lesquelles on puisse construire n champs de vecteurs indépendants sont les sphères $S^0 = \{-1, 1\}$, S^1 , S^3 et S^7 .

\mathbb{R}^2

- On peut identifier \mathcal{S}^1 avec $U(1)$
- En particulier, une rotation de \mathbb{R}^2 correspond à une multiplication par $z \in \mathbb{C}$ avec $|z| = 1$.
- $M(X, U) = U.X^{-1}$

\mathbb{R}^4 et \mathbb{R}^8

- Les sphères unités \mathcal{S}^3 et \mathcal{S}^7 peuvent s'identifier aux unités des *quaternions* et des *octonions*.
- Les quaternions et les octonions forment une *algèbre de division*. Ce sont les seules algèbres de division sur \mathbb{R} (avec \mathbb{R} et \mathbb{C}).
- $M(X, U) = U.X^{-1}$

Représentation matricielle de \mathbb{C} , \mathbb{H} , \mathbb{O}

Pour $n \in \{1, 2, 4, 8\}$, il existe une famille (non unique) de n matrices orthogonales $\mathcal{A}_n = (A_1, \dots, A_n)$ de $\mathbb{R}^{n \times n}$ telle que :

- $A_1 = \mathbb{I}_n$
- pour $i, j > 1$, $\{A_i, A_j\} = -2\delta_{i,j}\mathbb{I}_n$

Famille \mathcal{A}_2

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Familles de matrices orthogonales

Pour $n \in \{1, 2, 4, 8\}$, il existe une famille (non unique) de n matrices orthogonales $\mathcal{A}_n = (A_1, \dots, A_n)$ de $\mathbb{R}^{n \times n}$ telle que :

- $A_1 = \mathbb{I}_n$
- pour $i, j > 1$, $\{A_i, A_j\} = -2\delta_{i,j}\mathbb{I}_n$

\mathcal{A}_4

$$A_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix},$$
$$A_3 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, A_4 = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Codage

- Alice choisit U aléatoirement dans \mathbb{F}_2^n
- Calcul de α :
- $\alpha_i(X, U) = (A_i \cdot X | U)$

Décodage

- Bob calcule son estimateur \hat{U} de U :
- $\hat{U} = \sum_{i=1}^n \alpha_i A_i Y$
- on a : $\hat{U} = U + W'$ et donc $I(U; \hat{U}) = I(X; Y)$

Pas de perte d'information vers l'espion

$$\begin{aligned} f_U : \mathbb{R}^n &\longrightarrow \mathbb{R}^n \\ X &\longmapsto f_U(X) = \alpha \text{ with } \alpha_j = (U|A_jX) \end{aligned}$$

a un jacobien constant sur \mathcal{S}^{n-1} .

Conséquences

Comme $X \sim \mathcal{U}(\mathcal{S}^{n-1})$ et $U \sim \mathcal{U}(\mathbb{F}_2^{n-1})$,
on en déduit que :

- U et α sont indépendants.
- $p(U|Z, \alpha) = p(X|Z)$
- $K \geq H(U) - S(X; Z)$.

Résumé

- La réconciliation est un problème de codage de canal avec source aléatoire.
- Effectuer un “changement de coordonnées” pour se ramener à un codage de canal classique
- La généralisation de l'utilisation des codes "coset" pour les variables continues n'est possible que pour les dimensions 2, 4 et 8.