Cryptographie quantique, intrication et violations du réalisme local pour les systèmes tridimensionnels

AMBLARD Zoé

Journées Codage et Cryptographie 2014

24 mars 2014

Plan de la présentation

Introduction

La sécurité de la cryptographie quantique ne repose pas sur la difficulté supposée d'un problème mathématique comme la factorisation des entiers ou la résolution du logarithme discret, mais sur des lois physiques.

Introduction

La sécurité de la cryptographie quantique ne repose pas sur la difficulté supposée d'un problème mathématique comme la factorisation des entiers ou la résolution du logarithme discret, mais sur des lois physiques.

Objectifs de cette présentation :

- Résumer les protocoles Ekert91 pour deux qubits intriqués et 3DEB pour deux qutrits intriqués.
- Présenter notre nouveau protocole h3DEB pour deux qutrits intriqués.
- Conclure sur l'apport de h3DEB en matière de sécurité et de résistance au bruit.

Plan de la présentation

Du bit au qubit

Un qubit A s'écrit comme superposition du bit 0 et du bit 1 :

$$\alpha |0\rangle + \beta |1\rangle$$

En le mesurant, on obtient :

- 0 avec une probabilité $P(A = 0) = |\alpha|^2$
- 1 avec une probabilité $P(A = 1) = |\beta|^2$

pour $|\alpha|^2 + |\beta|^2 = 1$.

Du bit au qubit

Un qubit A s'écrit comme superposition du bit 0 et du bit 1 :

$$\alpha |0\rangle + \beta |1\rangle$$

En le mesurant, on obtient :

- 0 avec une probabilité $P(A = 0) = |\alpha|^2$
- 1 avec une probabilité $P(A = 1) = |\beta|^2$

pour $|\alpha|^2 + |\beta|^2 = 1$.

Issues d'une mesure

On associe les issues 1 et -1 à un bit :
$1 = (-1)^0 \rightarrow$ bit 0
$-1 = (-1)^1 \rightarrow$ bit 1

Paire de qubits intriqués

Soient deux qubits A et B dans l'état de Bell

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

En mesurant le qubit A, on obtient soit 0 soit 1 avec une probabilité $\frac{1}{2}$.

Si on obtient b l'état est projeté vers $|bb\rangle$:

- $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rightarrow$ on obtient 0 pour A $\rightarrow |00\rangle \rightarrow$ on obtient 0 pour B
- $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rightarrow$ on obtient 1 pour A $\rightarrow |11\rangle \rightarrow$ on obtient 1 pour B

En mesurant A puis B, on obtient toujours des résultats corrélés à 100%.
Ces deux qubits sont dits intriqués.

Protocole Ekert 91

C'est un protocole de partage de clé.

Une source produit des paires de qubits intriqués dans l'état de Bell $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ et distribue un qubit de chaque paire à Alice et l'autre à Bob. Ils mesurent leurs qubits selon quatre bases chacun.

Protocole Ekert 91

C'est un protocole de partage de clé.

Une source produit des paires de qubits intriqués dans l'état de Bell $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ et distribue un qubit de chaque paire à Alice et l'autre à Bob. Ils mesurent leurs qubits selon quatre bases chacun.

- Pour chaque qubit reçu, ils choisissent une base au hasard et mesurent l'état de leur qubit.
- Ils révèlent sur un canal classique authentifié les bases utilisées.

  Mêmes bases choisies $\rightarrow$ résultats corrélés à 100% $\rightarrow$ même bit obtenu

  Bases différentes choisies $\rightarrow$ test du viol d'une inégalité de Bell
- Si aucune perturbation n'a été détectée, les résultats corrélés permettent de constituer une clé commune.

Résumé de Ekert91

On peut résumer ces différents cas par un tableau :

	B_0	B_1	B_2	B_3
A_0	k	c_1		c_1
A_1	c_2	k	c_2	
A_2		c_1	k	c_1
A_3	c_2		c_2	k

$k \rightarrow$ issues corrélées pour la clé

c_1 (ou c_2) $\rightarrow$ quatre valeurs servant à vérifier le viol d'une inégalité de Bell

Viol de l'inégalité CHSH en physique classique

Alice et Bob réalisent des mesures sur deux qubits A et B.
Alice choisit entre A_1 et A_2, et Bob entre B_1 et B_2.

$$T := A_1B_1 + A_1B_2 + A_2B_1 - A_2B_2$$

A_iB_j = produit des issues obtenues pour A_i et B_j choisis.

Chaque A_i et B_j donne 1 ou $-1 \rightarrow$ 16 combinaisons possibles.

Viol de l'inégalité CHSH en physique classique

Alice et Bob réalisent des mesures sur deux qubits A et B.
Alice choisit entre A_1 et A_2, et Bob entre B_1 et B_2.

$$T := A_1B_1 + A_1B_2 + A_2B_1 - A_2B_2$$

A_iB_j = produit des issues obtenues pour A_i et B_j choisis.

Chaque A_i et B_j donne 1 ou $-1 \rightarrow 16$ combinaisons possibles.

En physique classique, T vaut toujours -2 ou 2 et son espérance mathématique vérifie :

$$-2 \leqslant E(T) \leqslant 2$$
$$\text{avec } E(T) = E(A_1B_1) + E(A_1B_2) + E(A_2B_1) - E(A_2B_2).$$

C'est l'inégalité CHSH qui fait partie des inégalités de Bell.

Viol de CHSH par les qubits intriqués

Pour deux qubits intriqués, les mesures devraient vérifier $|E(T)| \leqslant 2$.

Or la quantité T expérimentale vérifie :

$$|E(T)| \leqslant 2\sqrt{2}$$

Cette borne $2\sqrt{2}$ est en particulier atteinte par les états de Bell, dits aussi "états maximalement intriqués".

Lien entre le facteur de viol et la résistance au bruit

Le facteur de viol v est égal au quotient de la valeur quantique avec la borne classique. Il est maximal pour les états de Bell :

$$v = \frac{2\sqrt{2}}{2} = \sqrt{2}$$

Un protocole est résistant au bruit jusqu'à un certain seuil $F = 1 - \frac{1}{v}$.

Pour les états de Bell, ce seuil est $F = 1 - \frac{1}{\sqrt{2}} \simeq 0.293$

Plan de la présentation

Qutrits et inégalité CHSH-3

Un qutrit A s'écrit comme superposition des trits $0, 1$ et 2 :

$$\alpha\,|0\rangle + \beta\,|1\rangle + \gamma\,|2\rangle$$

avec les probabilités respectives $|\alpha|^2, |\beta|^2$ et $|\gamma|^2$ pour $|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$.

Une mesure donne trois issues $1, \omega, \omega^2$, avec ω une racine troisième primitive de l'unité.

Qutrits et inégalité CHSH-3

Un qutrit A s'écrit comme superposition des trits $0, 1$ et 2 :

$$\alpha\,|0\rangle + \beta\,|1\rangle + \gamma\,|2\rangle$$

avec les probabilités respectives $|\alpha|^2, |\beta|^2$ et $|\gamma|^2$ pour $|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$.

Une mesure donne trois issues $1, \omega, \omega^2$, avec ω une racine troisième primitive de l'unité.

L'inégalité CHSH-3 s'exprime

$$S \leqslant 2$$

avec

$$\begin{aligned} S = \mathrm{Re}\Big(E(A_1B_1) + E(A_1B_2) - E(A_2B_1) + E(A_2B_2)\Big) \\ + \tfrac{1}{\sqrt{3}}\mathrm{Im}\Big(E(A_1B_1) - E(A_1B_2) - E(A_2B_1) + E(A_2B_2)\Big). \end{aligned}$$

Bases optimales et viol de CHSH-3

Les bases permettant d'obtenir les meilleurs violations de CHSH-3 sont les quatre "bases optimales" (deux pour chaque partie).

Avec ces bases et l'état maximalement intriqué $\frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$, on obtient :

$$v = (6 + 4\sqrt{3})/9 \simeq 1.436$$

Cette valeur correspond à un seuil de bruit $F \simeq 0.304$ supérieur à celui obtenu dans le cas des qubits, où $F \simeq 0.293$.

Protocole 3DEB

Une source produit une paire de qutrits intriqués dans l'état de Bell $\frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$.
Alice et Bob récupèrent un qutrit et disposent de quatre bases chacun pour effectuer leurs mesures.

Protocole 3DEB

Une source produit une paire de qutrits intriqués dans l'état de Bell $\frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$.
Alice et Bob récupèrent un qutrit et disposent de quatre bases chacun pour effectuer leurs mesures.

1. Pour chaque qutrit reçu, Alice choisit une base au hasard et effectue une mesure ; Bob fait de même.
2. Ils révèlent sur un canal classique authentifié les bases utilisées.

   Mêmes bases choisies $\rightarrow$ résultats corrélés à 100% $\rightarrow$ même trit obtenu

   Bases différentes choisies $\rightarrow$ deux tests du viol de CHSH-3
3. Si aucune perturbation n'a été détectée, les résultats corrélés permettent de constituer une clé commune.

Schéma du protocole 3DEB

Ces différents cas peuvent se résumer par un tableau :

	B_0	B_1	B_2	B_3
A_0	k	c_1		c_1
A_1	c_2	k	c_2	
A_2		c_1	k	c_1
A_3	c_2		c_2	k

Pour notre état de Bell, ce protocole permet d'atteindre un viol de CHSH-3 égal à $v_{3DEB} \simeq 1.436$, ce qui correspond à un seuil de bruit $F_{3DEB} \simeq 0.304$.

Nous avons souhaité améliorer ce seuil de bruit en construisant un nouveau protocole nommé h3DEB.

Une nouvelle inégalité à la place de CHSH-3

Remplacer CHSH-3 par une nouvelle inégalité nous a permis d'obtenir une meilleure résistance au bruit que 3DEB.

Nous proposons d'utiliser l'inégalité de Bell homogène [1] appelée hCHSH-3 :

$$-2\mathrm{Re}(T_1) \leqslant 9$$

avec

$$\begin{aligned} T_1 = {} & (4\omega+2)E(A_1^2B_1^2) + (\omega-1)E(A_1^2B_1B_2) + (4\omega-1)E(A_1^2B_2^2) \\ & - (2\omega+1)E(A_1A_2B_1^2) + (\omega-1)E(A_1A_2B_1B_2) + (\omega+2)E(A_1A_2B_2^2) \\ & + (\omega+5)E(A_2^2B_1^2) + (\omega-1)E(A_2^2B_1B_2) - (2\omega+4)E(A_2^2B_2^2). \end{aligned}$$

1. *A complete set of multidimensional Bell inequalities*, François Arnault

Protocole h3DEB

Une source produit une paire de qutrits intriqués dans l'état de Bell $\frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$.

Alice et Bob récupèrent un qutrit et disposent de six bases chacun pour effectuer leurs mesures.

Protocole h3DEB

Une source produit une paire de qutrits intriqués dans l'état de Bell $\frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$.
Alice et Bob récupèrent un qutrit et disposent de six bases chacun pour effectuer leurs mesures.

1. Pour chaque qutrit reçu, Alice choisit une base au hasard et effectue une mesure ; Bob fait de même.
2. Ils révèlent sur un canal classique authentifié les bases utilisées.

   Mêmes bases choisies $\rightarrow$ résultats corrélés à 100% $\rightarrow$ même trit obtenu

   Bases différentes choisies $\rightarrow$ deux tests du viol de hCHSH-3
3. Si aucune perturbation n'a été détectée, les résultats corrélés permettent de constituer une clé commune.

Schéma du protocole h3DEB

Ces différents cas peuvent se résumer par un tableau :

	B_{00}	B_{02}	B_{22}	B_{11}	B_{13}	B_{33}
A_{00}	k			c_1	c_1	c_1
A_{02}		k		c_1	c_1	c_1
A_{22}			k	c_1	c_1	c_1
A_{11}	c_2	c_2	c_2	k		
A_{13}	c_2	c_2	c_2		k	
A_{33}	c_2	c_2	c_2			k

Ce protocole fait intervenir des mesures produit d'autres mesures :

$$A_{ij} = A_i Aj$$

Le facteur de violation vaut ici $v_{h3DEB} \simeq 1.693$ et permet d'atteindre un seuil de bruit $F_{h3DEB} \simeq 0.409$ supérieur à celui de 3DEB, où $F_{3DEB} \simeq 0.304$

Produit de deux mesures

Une mesure A_i est expérimentalement réalisée par un tritter et un détecteur.

En physique quantique, on ne peut pas obtenir un résultat de mesure pour $A_{ij} = A_i Aj$ en mesurant A_i et Aj séparéments avec leurs tritters et détecteurs respectifs.

Cette mesure peut en revanche s'effectuer avec un tritter et un détecteur dédiés.

Plan de la présentation

Conclusion sur l'amélioration apportée par notre protocole

Dans le cadre du protocole 3DEB, l'état de Bell $\frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$ permet d'obtenir une violation de CHSH-3 égale à $v_{3DEB} \simeq 1.436$, ce qui correspond à un niveau de bruit $F_{3DEB} \simeq 0.304$.

Conclusion sur l'amélioration apportée par notre protocole

Dans le cadre du protocole 3DEB, l'état de Bell $\frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$ permet d'obtenir une violation de CHSH-3 égale à $v_{3DEB} \simeq 1.436$, ce qui correspond à un niveau de bruit $F_{3DEB} \simeq 0.304$.

Notre but était d'améliorer la résistance au bruit de ce protocole. Grâce à l'utilisation de l'inégalité homogène hCHSH-3 au lieu de CHSH-3, on atteint un facteur de viol $v_{h3DEB} \simeq 1.693$, ce qui correspond à un seuil de résistance au bruit $F_{h3DEB} \simeq 0.409$.

Merci de votre attention !