Université de Rennes I
UFR Mathématiques

Master de Cryptographie
Année universitaire 2017–2018

Introduction à la cryptographie quantique

Examen du 19 décembre 2017

Durée de l'épreuve : 2 heures
À rédiger directement sur le sujet (et à continuer sur une feuille libre le cas échéant). Tous les documents sont autorisés ; les calculatrices, les téléphones portables, les tablettes et les ordinateurs sont interdits.
Les résultats d'une question, même non démontrés, peuvent être utilisés aux questions suivantes

Nom et prénom:

QUELQUES INDICATIONS

Exercice 1 [Le protocole B92 de communication quantique d'une clé de cryptage (Bennett 1992)] Alice et Bernard se mettent (publiquement) d'accord sur deux vecteurs $|\beta_0\rangle$ et $|\beta_1\rangle$ de norme 1 dans $\mathbb{H} = \mathbb{C}^2$ qui ne sont ni orthogonaux ni colinéaires et sur un entier $N = \mathcal{O}(4n)$, où n est la taille du la clé qu'ils veulent échanger.

Alice utilisera $|\beta_0\rangle$ pour coder le bit classique 0 et $|\beta_1\rangle$ pour le bit 1 selon la procédure suivante :

Aux instants $k = 1, \dots, N$, elle
— génère une variable aléatoire a uniformément distribuée dans $\{0,1\}$,
— prépare un photon dans un état

$$|\psi\rangle = \begin{cases} |\beta_0\rangle & \text{si } a = 0 \\ |\beta_1\rangle & \text{si } a = 1 \end{cases}$$

qu'elle envoi aussitôt à Bernard,
— stocke chez-elle, en lieu sûr, les valeurs successives de a.

Bernard dispose de deux effets $B_0 = I - |\beta_0\rangle\langle\beta_0|$ et $B_1 = I - |\beta_1\rangle\langle\beta_1|$ et effectue des mesures selon la procédure suivante :

À la réception de chaque photon envoyé par Alice, il
— génère une variable aléatoire b uniformément distribuée dans $\{0,1\}$,
— note la valeur R la réponse (dans $\{0,1\}$) à la question « l'effet B_b prend-il la valeur 1 » ?
— stocke chez lui en lieu sûr les valeurs successives de b et de R,
— à l'instant N, il envoi à Alice par le canal classique les instants pour lesquels R vaut 1 (mais aucune information sur l'effet qu'il a mesuré).

Le but de l'exercice est de montrer qu'aux instants k où $R_k = 1$, on a $\mathbb{P}(b_k = 1 - a_k) = 1$.

1. Vérifier que les effets B_c, pour $c = 0, 1$, sont des opérateurs positifs.

Pour tout $|\psi\rangle \in \mathbb{H}$, on a $\langle\psi|B_c\psi\rangle = \langle\psi|\psi\rangle - |\langle\psi|\beta_c\rangle|^2$. Or, par l'inégalité de Buniakowski-Cauchy-Schwarz, on a aussi que $|\langle\psi|\beta_c\rangle| \leq \|\psi\|\|\beta_c\| = \|\psi\|$. Donc $\langle\psi|\psi\rangle - |\langle\psi|\beta_c\rangle|^2 \geq 0$, ce qui prouve la positivité de l'opérateur.

2. Montrer que pour chaque $c = 0,1$, l'effet B_c est un projecteur qui projette sur le sous-espace orthogonal au vecteur $|\beta_c\rangle$, i.e. $B_c = |\beta_c^\perp\rangle\langle\beta_c^\perp|$, où $|\beta_c^\perp\rangle$ désigne le vecteur unité orthogonal à $|\beta_c\rangle$.

   On calcule

$$B_c^2 = (I - |\beta_c\rangle\langle\beta_c|)^2 = I + \langle\beta_c|\beta_c\rangle|\beta_c\rangle\langle\beta_c| - 2|\beta_c\rangle\langle\beta_c| = I - |\beta_c\rangle\langle\beta_c| = B_c$$

   ce que établit le caractère projectif de B_c. En utilisant l'identité $I = |\beta_c\rangle\langle\beta_c| + |\beta_c^\perp\rangle\langle\beta_c^\perp|$, on conclut que $B_c = |\beta_c^\perp\rangle\langle\beta_c^\perp|$.

3. Déterminer $\mathrm{spec}(B_c)$ pour $c \in \{0,1\}$.

   Puisque B_c est un projecteur, son spectre est $\{0,1\}$.

4. Calculer, en indiquant explicitement les résultats non nuls,

$$\begin{aligned}
B_0|\beta_0\rangle &= \langle\beta_0^\perp|\beta_0\rangle|\beta_0^\perp\rangle = 0\\
B_1|\beta_0\rangle &= \langle\beta_1^\perp|\beta_0\rangle|\beta_1^\perp\rangle \neq 0\\
B_0|\beta_1\rangle &= \langle\beta_0^\perp|\beta_1\rangle|\beta_0^\perp\rangle \neq 0\\
B_1|\beta_1\rangle &= \langle\beta_1^\perp|\beta_1\rangle|\beta_1^\perp\rangle = 0.
\end{aligned}$$

5. En conclure que $\mathbb{P}_{\beta_a}(B_b = 1) = 1 - |\langle\beta_a|\beta_b\rangle|^2$.

   Puisque $\mathrm{spec}(B_b) = \{0,1\}$ — par ce qui a été établi en question 3 — on a

$$\mathbb{P}_{\beta_a}(B_b = 1) = \mathbb{E}_{\beta_a}(B_b) = \langle\beta_a|B_b\beta_a\rangle = |\langle\beta_a|\beta_b^\perp\rangle|^2 = 1 - |\langle\beta_a|\beta_b\rangle|^2.$$

6. Résumer dans le tableau ci-dessous vos résultats dans le cas où $|\beta_0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ et $|\beta_1\rangle = \begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$ et expliquer le principe du protocole.

a	$\|\psi\rangle$	b	$\langle\psi\|B_b\psi\rangle$
0	$\|\beta_0\rangle$	0	0
0	$\|\beta_0\rangle$	1	$\frac{1}{2}$
1	$\|\beta_1\rangle$	0	$\frac{1}{2}$
1	$\|\beta_1\rangle$	1	0

   Lorsque $\langle\psi|B_b\psi\rangle = \frac{1}{2}$, on sait que $\mathbb{P}(B_b = 1) = \frac{1}{2}$. Mais, si la réponse est $R = 1$, on connaît avec **certitude** que $b = 1 - a$ a été choisi. On aura donc coïncidence de b_k avec $1 - a_k$ aux instants k pour lesquels $R_k = 1$ ce qui arrive à $\mathcal{O}(N/2)$ d'entre eux. On continue comme pour le protocole BB84 pour distiller une clé sur $N/4$ instants.

Exercice 2 [Le paradoxe GHZ (Greenberger, Horne et Zeilinger 1989)]

1. Soient $X_a, X_b, X_c, Y_a, Y_b, Y_c$ six variables aléatoires (classiques), définies sur le même espace de probabilité $(\Omega, \mathscr{F}, \mathbb{P})$ à valeurs dans $\{-1,1\}$. La loi $\mathbb{P}$ est **arbitraire**, i.e. les variables aléatoires peuvent être indépendantes ou pas, symétriques ou pas, dégénérées ou pas. Noter W_0, W_1, W_2, W_3 les variables aléatoires

$$W_0 := X_a X_b X_c; W_1 := X_a Y_b Y_c; W_2 := Y_a X_b Y_c \text{ et } W_3 := Y_a Y_b X_c,$$

définies aussi sur $(\Omega, \mathscr{F}, \mathbb{P})$ et à valeurs aussi dans $\{-1,1\}$. Monter que

$$\mathbb{P}(W_0 = 1, W_1 = -1, W_2 = -1, W_3 = -1) = 0.$$

Supposons qu'il existe $\omega \in \Omega$ tel que la proposition

$$[W_1(\omega) = -1] \wedge [W_2(\omega) = -1] \wedge [W_3(\omega) = -1]$$

soit vraie. Mais alors pour cet ω, en effectuant le produit $\prod_{i=1}^3 W_i$, on aura $[W_1(\omega)W_2(\omega)W_3(\omega) = -1]$. Par ailleurs, en explicitant les expressions des W_i et en observant que $Y_a^2 = Y_b^2 = Y_c^2 = 1$, on arrive à la contradiction

$$-1 = W_1(\omega)W_2(\omega)W_3(\omega) = X_a(\omega)X_b(\omega)X_c(\omega) = 1.$$

Par conséquent,

$$\{X_a X_b X_c = 1, X_a Y_b Y_c = -1, Y_a X_b Y_c = -1, Y_a Y_b X_c = -1\} = \emptyset.$$

2. Dorénavant, on note $\mathscr{H} = \mathbb{C}^2$ et

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

les **matrices de Pauli** dans la base canonique $\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$. Montrer que $\mathsf{spec}(\sigma_1) = \mathsf{spec}(\sigma_2) = \mathsf{spec}(\sigma_3) = \{-1,1\}$.

On calcule les polynômes caractéristiques et on constate que, pour tout $i = 1,2,3$, on a

$$\chi_i(\lambda) := \det(\sigma_i - \lambda I) = \lambda^2 - 1.$$

3. On note $|+\rangle$ et $|-\rangle$ les vecteurs propres associés respectivement aux valeurs propres $+1$ et -1 de σ_3. On a donc $\sigma_3|s\rangle = s|s\rangle$ pour $s \in \mathbb{S} := \{+,-\}$; autrement dit, $|+\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $|-\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Calculer, pour $s \in \mathbb{S}$,

$$\sigma_1|s\rangle = |-s\rangle$$
$$\sigma_2|s\rangle = is|-s\rangle.$$

4. Soit $|\Psi\rangle = \frac{1}{\sqrt{2}}(|{+}{+}{+}\rangle + |{-}{-}{-}\rangle) \in \mathbb{H} := \mathscr{H}^{\otimes 3}$. Montrer que $|\Psi\rangle$ est un vecteur propre pour les operateurs W_i, $i = 0,\dots,3$, agissant sur $\mathbb{H}$, où

$$\begin{aligned} W_0 &:= \sigma_1 \otimes \sigma_1 \otimes \sigma_1 |\Psi\rangle = |\Psi\rangle. \\ W_1 &:= \sigma_1 \otimes \sigma_2 \otimes \sigma_2 |\Psi\rangle = -|\Psi\rangle \\ W_2 &:= \sigma_2 \otimes \sigma_1 \otimes \sigma_2 |\Psi\rangle = -|\Psi\rangle \\ W_3 &:= \sigma_2 \otimes \sigma_2 \otimes \sigma_1 |\Psi\rangle = -|\Psi\rangle \end{aligned}$$

5. Que peut-on conclure sur les probabilités que $\mathbb{P}_\Psi(W_i = 1)$ pour $i = 0,\dots,3$ et sur l'état du système après que chaque question soit posée ?

   Étant donné que $|\Psi\rangle$ est un vecteur propre pour chaque W_i, on conclut que $\mathbb{P}_\Psi(W_i = w_i) = 1$ pour w_i la valeur propre de W_i. Par ailleurs, l'état du système après avoir posé la question « $W_i = w_i$ » ? reste inchangé $|\Psi\rangle$.

6. Montrer que $\sigma_1\sigma_2 = -\sigma_2\sigma_1$.

   Il suffit de vérifier l'égalité en effectuant les multiplications des représentations matricielles de σ_1, σ_2 dans la base canonique :

$$\sigma_1\sigma_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = -\sigma_2\sigma_1.$$

7. Pour A, B, C et D des opérateurs agissant sur $\mathscr{H}$, montrer que $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$.

   Soit $(\varepsilon_0 \otimes \varepsilon_0, \varepsilon_0 \otimes \varepsilon_1, \varepsilon_0 \otimes \varepsilon_0, \varepsilon_1 \otimes \varepsilon_1)$ la base canonique de $\mathscr{H}^{\otimes 2}$. On a, pour tout $i, j, k, l = 0, 1$,

$$\langle \varepsilon_i\varepsilon_j | (A \otimes B)(C \otimes D)\varepsilon_k\varepsilon_l \rangle = \langle \varepsilon_i\varepsilon_j | (A \otimes B)(C\varepsilon_k)(D\varepsilon_l) \rangle = \langle \varepsilon_i\varepsilon_j | (AC\varepsilon_k)(BD\varepsilon_l) \rangle.$$

8. Commenter pourquoi les résultats établis dans les questions précédentes sont paradoxaux s'ils sont interprétés classiquement. (Il est rappelé que $\sigma_1^2 = \sigma_2^2 = I$).

   Les matrices $X := \sigma_1$ et $Y := \sigma_2$ ont un spectre $\{-1, 1\}$, elles sont donc les analogues quantiques des variables aléatoires à valeurs dans $\{-1, 1\}$. Les résultats établis en question 4 signifient que

$$\mathbb{P}_\Psi(W_0W_1W_2W_3 = (-)^3) = 1.$$

   Ceci n'est pas en contradiction avec les formes explicites de W_i car, à cause de l'anticommutatiivité des σ_1, σ_2 on a

$$\begin{aligned} W_1W_2W_3 &= (\sigma_1 \otimes \sigma_2 \otimes \sigma_2)(\sigma_2 \otimes \sigma_1 \otimes \sigma_2)(\sigma_2 \otimes \sigma_2 \otimes \sigma_1) \\ &= \sigma_1\sigma_2^2 \otimes \sigma_2\sigma_1\sigma_2 \otimes \sigma_2^2\sigma_1 = \sigma_1 \otimes (-\sigma_1) \otimes \sigma_1 = -W_0, \end{aligned}$$

   mais il est en contradiction flagrante avec le cas classique. Contrairement aux inégalités de Bell, nous sommes en présence d'une violation **maximale** de la prédiction classique (la probabilité passe de la valeur 0 à la valeur 1). Ce phénomène est connu sous le nom de paradoxe GHZ.

La correction sera mise en ligne peu de temps après la fin de l'examen.