TD4 — QKD : distribution quantique de clé

1 Ordinateurs quantiques et cryptographie classique

Ex1. Rappels de crypto Le cours de cryptographie et sécurité de M1 est un peu loin. Prenons quelques minutes ensemble pour nous rafraîchir la mémoire !

- **(a)** Connaissez vous un schéma de chiffrement symétrique parfaitement sûr ?
- **(b)** D'ailleurs symétrique / asymétrique, ça marche comment déjà ? (classez AES, SHA, HMAC, RSA, DH, ECDH selon ce critère)
- **(c)** Précisez la fonction des primitives de confidentialité, de contrôle d'intégrité, d'authentification et d'échange de clé (classez les même)
- **(d)** Expliquez en détail le fonctionnement du protocole de Diffie-Hellman.
- **(e)** Discutez de la manière typique dont un protocole de communication à travers un canal non sûr combine ces différentes primitives. On pourra prendre l'exemple d'une session web et d'une connexion à travers un VPN.

Ex2 Les algorithmes de **Shor** permettent de calculer efficacement des factorisations d'entiers et des logarithmes discrets. Ils peuvent être adaptés pour calculer efficacement des logarithmes dans le cadre des courbes elliptiques. L'algorithme de **Grover** permet d'explorer plus rapidement un espace à la recherche de collisions.

- **(a)** Expliquer l'impact qu'aurait un calculateur quantique capable d'exécuter de nombreuses portes de Toffoli sur de nombreux qubits sur la sécurité des primitives de l'exercice précédent.
- **(b)** Quelles conséquence pour nos protocoles de communication à travers un canal non sûr ?
- **(c)** Supposons qu'on dispose d'un protocole sûr d'échange de clés. Comment adapter les protocoles ?

2 Le protocole BB84

Ex3. Impossibilité du clonage quantique Il n'existe pas d'opération unitaire capable de dupliquer n'importe quel état quantique.

- **(a)** Proposer un circuit quantique capable de cloner les états $|0\rangle$ et $|1\rangle$, c'est-à-dire qui réalise un opérateur C tel que $C|00\rangle = |00\rangle$ et $C|10\rangle = |11\rangle$.
- **(b)** Calculer $C(\alpha|0\rangle + \beta|1\rangle)|0\rangle$. Que peut-on conclure ?
- **(c)** Démontrer qu'en général, il n'existe pas d'opérateur unitaire C tel que $C|\alpha\rangle|0\rangle = |\alpha\rangle|\alpha\rangle$.

Ex4. Mesure et probabilités Soit un qubit est dans l'état $\alpha|a\rangle + \beta|b\rangle$ où $|a\rangle, |b\rangle$ est un base orthogonale. Lorsqu'on mesure ce qubit, on observe $|a\rangle$ avec probabilité $|\alpha|^2$ et $|b\rangle$ avec probabilité $|\beta|^2$. L'opérateur de Hadamard (la porte H) est un opérateur de changement de base entre les bases $Z = \{|0\rangle, |1\rangle\}$ (la base canonique) et $X = \{|+\rangle, |-\rangle\}$ (la base Hadamard).

- **(a)** Calculer ce qu'on observe, et avec quelle probabilité, lorsqu'on mesure en base Z les qubits $|0\rangle$, $|1\rangle$, $|+\rangle$ et $|-\rangle$. On pourra s'aider d'un circuit pour visualiser le calcul.
- **(b)** Recommencer en base X.

Pour décrire plus facilement le protocole BB84, on note $|\psi_{ij}\rangle$ avec $i, j \in \{0, 1\}$ les qubits suivants :

$$|\psi_{00}\rangle = |0\rangle \qquad |\psi_{10}\rangle = |1\rangle \qquad |\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Le protocole se déroule comme suit :

1. Alice tire une suite de $(4+\delta)n$ bits aléatoires (a_i).
2. Alice tire une suite de $(4+\delta)n$ bits aléatoires (b_i).
3. Alice construit l'état $|\psi\rangle = \bigotimes_{i=1}^{(4+\delta)n} |\psi_{a_i b_i}\rangle$ et le transmet à Bob.
4. Bob tire une suite de $(4+\delta)n$ bits aléatoires (b'_i).
5. Bob mesure les $(4+\delta)n$ qubits reçus en utilisant la base Z quand $b'_i = 0$ et la base X quand $b'_i = 1$. Il obtient (a'_i).
6. Alice et Bob échangent pour déterminer où (b_i) et (b'_i) coïncident et gardent $2n$ bits.
7. Alice sélectionne un sous-ensemble des n bits pour tester s'ils sont sur écoute.
8. Alice transmet les positions et les valeurs de cet échantillon à Bob.
9. Bob annonce les valeurs qu'il a obtenu sur l'échantillon.
10. Si Alice et Bob ne détectent pas d'écoute, ils utilisent les bits restant comme secret partagé.

Ex5 Jouons ensemble avec le protocole sur un exemple pour le comprendre.

(a) Identifier la phase quantique et la phase classique de post-traitement.

(b) Quelles hypothèses faut-il faire sur les canaux de communication entre Alice et Bob ?

(c) Montrer que si $b_i = b'_i$ alors $a'_i = a_i$ et que si $b_i \neq b'_i$ alors a'_i est indépendant de a_i.

Ex6 Eve tente une attaque frontale : elle intercepte les qubits envoyés par Alice, choisit une suite de bases (b''_i), mesure et renvoie à Bob les qubits détectés.

(a) Quelle est la probabilité, pour un qubit, que Bob découvre que la valeur du qubit est erronée ?

(b) Quel est le nombre moyen de qubits erronés détectés par Alice et Bob pour $(4+\delta)n$ qubits ?

(c) Quelle est la probabilité qu'Eve réussisse à décoder correctement un bit a_i d'Alice ?

Ex7. Attaque PNS Étudier ce qui se passe si le matériel utilisé pour mettre en œuvre le protocole est imparfait et émet plusieurs copies du même qubit à la suite au lieu d'un seul.

3 Variations

Ex8. Le protocole B92 Dans cette variante de BB84, une fois la suite (a_i) générée, Alice envoie $|0\rangle$ si $a_i = 0$ et $|+\rangle$ si $a_i = 1$. Bob génère une suite aléatoire (b'_i) et mesure comme précédemment. Il ne garde que les bits dont il est **certain** de la valeur.

(a) Expliciter cette notion de certitude.

(b) Définir proprement le protocole.

(c) Étudier le protocole comme ci-dessus.

Ex9. Le protocole SARG04 Ce protocole est une variante de BB84 qui est robuste aux attaques type PNS en utilisant le principe du protocole B92 pour la phase post-traitement de sélection des bits. Plutôt que de communiquer la suite (b_i) à Bob, Alice envoie à Bob pour chaque bit b_i une paire d'éléments : un élément de la base X et un élément de la base Z parmi lesquels figure $\psi_{a_i b_i}$. À partir de b'_i et a'_i, Bob détermine s'il est certain du qubit envoyé. Il annonce à Alice les indices des qubits dont il connaît la valeur.

(a) Expliciter les calculs effectués par Bob dans la phase de validation.

(b) Définir proprement le protocole.