CRYPTOLOGIE
TD2-codage quantique et chiffrement par blocs

Exercice 1 : Codage quantique

Alice et Bob décide de communiquer en utilisant un chiffrement à clé privée, pour cela ils décident d'utiliser le protocole quantique de génération/transmission de clé. Ils se mettent d'accord sur la conversion bit polarisation suivante :

Polarisation	–	|	/	\
Bit	0	1	0	1

1. **Génération et transmission de la clé.**
   Alice génère aléatoirement une liste de 10 photons et la transmet à Bob (deuxième ligne du tableau ci-dessous). Bob la mesure avec une liste de miroirs réglés aléatoirement (troisième ligne du tableau ci-dessous).

Photon	1	2	3	4	5	6	7	8	9	10
Alice	/	–	|	\	–	\	\	|	–	|
Réglages B.	\	–	/	\	|	/	–	|	/	\
Mesures B.										

   (a) Compléter le tableau ci-dessus en donnant une liste possible de mesures pour Bob.

   (b) Bob transmet la liste de ses réglages à Alice qui en déduit la liste des photons qui ont eu un comportement déterministe ; donner cette liste.

   (c) Alice transmet cette liste à Bob et ils en déduisent tous la deux la clé de codage grâce à la correspondance bit/polarisation ; donner cette clé.

2. **Ève intervient.**
   Ève a écouté la liste de photons émise par Alice et l'a donc modifiée, les mesures de Bob sont donc modifiées. On peut lire dans le tableau ci-dessous les nouvelles mesures de Bob :

Photon	1	2	3	4	5	6	7	8	9	10
Réglages B.	\	–	/	\	|	/	–	|	/	\
Mesures B.	\	×	/	\	×	×	–	|	/	\

   (a) Les réglages de Bob n'ayant pas changé, Alice retrouve la même liste de photons à comportement déterministe que précédemment et elle transmet cette liste à Bob. D'après ses nouvelles mesures et ses réglages, Bob déduit la polarisation des photons ayant eu un comportement déterministe ; donner cette liste de polarisation.

(b) Donner la clé qu'en déduit Bob.

(c) En testant quels bits de leur clé respective Alice et Bob peuvent-ils savoir s'ils ont été écoutés ou non ?

Exercice 2 : chiffrement par blocs

1. On construit un réseau de Feistel admettant les paramètres suivant :
   - On code des blocs de longueur 6 bits.
   - L'espace des clés est $K = \{0,1\}^4$: tous les mots de 4 bits.
   - Le réseau admet deux rondes.
   - La fonction g génératrice de sous-clés génère deux sous-clés de 3 bits : $g(k) = (k_1, k_2)$ où k_1 correspond au trois premiers bits de k, k_2 à ses trois derniers.
   - La fonction f est définie de $\{0,1\}^3 \times \{0,1\}^3$ dans $\{0,1\}^3$ par $f(m_i, k_i) = m_i + k_i$ où "+" désigne l'addition bit à bit modulo 2.

   (a) Faire le schéma complet du réseau de chiffrement.

   (b) En utilisant la clé $k = 1010$, on utilise ce réseau de Feistel pour chiffrer le message $m = 100110$; calculer le message chiffré c en faisant apparaitre tous les calculs intermédiaires.

   (c) Faire le schéma complet du réseau de déchiffrement.

   (d) On reçoit le message chiffré $c' = 111000$; sachant qu'il a été chiffré par ce réseau de Feistel avec toujours la même clé $k = 1010$, retrouver le message en clair m' en faisant apparaitre tous les calculs intermédiaires.

2. On souhaite à présent chiffrer des messages de 12 bits. Pour cela on utilise un chiffrement par bloc en mode ECB basé sur le réseau de Feistel précédent.

   (a) Faire le schéma complet de chiffrement.

   (b) On souhaite chiffrer le message $M = 100110\,000101$ toujours avec la même clé $k = 1010$; déterminer le message chiffré obtenu C.

   (c) A quel test de sécurité le mode ECB échoue-t-il ? Expliquer brièvement pourquoi (on pourra donner un exemple) ce chiffrage est sensible aux attaques à textes en clairs choisis.

3. On passe à un mode de chiffrement CFB ($c_i = e_k(c_{i-1} + m_i)$).

   (a) Faire le schéma complet de chiffrement.

   (b) On souhaite chiffrer le message $M' = 011010\,110100$ avec le bloc constant $C_0 = 100110$ et toujours la même clé $k = 1010$; déterminer le message chiffré obtenu C'.

   (c) Expliquer brièvement pourquoi le mode CFB est plus efficace que le mode ECB.

EXERCICE 3 : Codage quantique

Alice et Bernard décide de communiquer en utilisant un chiffrement à clé secrète. On s'intéresse au protocole quantique de transmission de la clé. Ils se mettent d'accord sur la conversion bit polarisation suivante :

Polarisation	–	|	/	\
Bit	0	1	0	1

1. **Génération et transmission de la clé.**
   Alice génère aléatoirement une liste de 10 photons et la transmet à Bob (deuxième ligne du tableau ci-dessous). Bob la mesure avec une liste de miroirs réglés aléatoirement (troisième ligne du tableau ci-dessous).

Photon	1	2	3	4	5	6	7	8	9	10
Alice	\	|	–	|	/	–	|	\	–	\
Réglages B.	–	|	/	\	\	–	/	\	|	/
Mesures B.										

   (a) Complétez le tableau ci-dessus en donnant une liste possible de mesures pour Bob.

   (b) Bob transmet la liste de ses réglages à Alice qui en déduit la liste des photons qui ont eu un comportement déterministe ; donnez cette liste.

   (c) Alice transmet cette liste à Bob et ils en déduisent tous la deux la clé de codage grâce à la correspondance bit/polarisation ; donnez cette clé.

2. **Ève intervient.**
   Ève a écouté la liste de photons émise par Alice et l'a donc modifiée, les mesures de Bob sont donc modifiées. On peut lire dans le tableau ci-dessous les nouvelles mesures de Bob :

Photon	1	2	3	4	5	6	7	8	9	10
Réglages B.	–	|	/	\	\	–	/	\	|	/
Mesures B.	–	|	/	\	\	×	/	\	×	×

   (a) Les réglages de Bob n'ayant pas changé, Alice retrouve la même liste de photons à comportement déterministe que précédemment et elle transmet cette liste à Bob. D'après ses nouvelles mesures et ses réglages, Bob déduit la polarisation des photons ayant eu un comportement déterministe ; donnez cette liste de polarisation.

   (b) Donnez la clé qu'en déduit Bob.

   (c) En testant quels bits de leur clé respective Alice et Bob peuvent-ils savoir s'ils ont été écoutés ou non ?

EXERCICE 4 : Codage par bloc

1. **Réseau de Feistel**
   On construit un réseau de Feistel admettant les paramètres suivant :
   - On code des blocs de longueur 6 bits.
   - L'espace des clés est $K = \{0,1\}^6$: tous les mots de 6 bits.
   - Le réseau admet deux rondes.
   - La fonction g génératrice de sous-clés génère deux sous-clés de 3 bits : $g(k) = (k_1, k_2)$ où k_1 correspond aux bits impairs (le 1^{er}, le 3^{eme}, le 5^{eme}) de k, k_2 à ses bits pairs.
   - La fonction f est définie de $\{0,1\}^3 \times \{0,1\}^3$ dans $\{0,1\}^3$ par $f(m_i, k_i) = m_i + k_i$ où "+" désigne l'addition bit à bit modulo 2.

   (a) Faites le schéma complet du réseau de chiffrement.

   (b) On utilise ce réseau de Feistel avec la clé $k = 110110$ pour chiffrer le message $m = 000\,111$; calculez le message chiffré c en faisant apparaitre tous les calculs intermédiaires.

   (c) Comment modifier le schéma précédent pour obtenir celui du réseau de déchiffrement ?

   (d) Déchiffrez le message $c' = 010\,000$ pour retrouver le message en clair m' (on travaille toujours avec la clé $k = 110110$).

2. **Étude d'un mode**
   A partir d'une fonction de chiffrement F permettant de chiffrer un bloc et de sa fonction de déchiffrement G, on voudrait chiffrer un message M se décomposant en 2 blocs $M = M_1 M_2$. On utilise pour cela un mode où C_i, le i^{eme} bloc chiffré, se calcule de la façon suivante : $C_i = F(C_{i-1}) + F(M_i)$, où C_0 est un bloc constant donné et où "+" désigne l'addition bit à bit modulo 2.

   (a) Faites le schéma de chiffrement et de déchiffrement.

   (b) Sachant que F est le réseau de Feistel étudié précédemment, toujours utilisé avec la même clé $k = 110110$, chiffrez le message $M = 000\,111\ \ 001\,010$ avec le bloc $C_0 = 001\,100$.