N^o d'ordre :30/2012 – $M/M.T$

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE D'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE "HOUARI BOUMEDINNE"

FACULTE DE MATHEMATIQUES

MEMOIRE

Présenté pour l'obtention du diplôme de MAGISTER
En : Mathématiques
Spécialité : Recherche Opérationnelle : Génie Mathématiques

Par : CHARCHALI Fella

Thème

Introduction à la cryptographie quantique et aux techniques de cryptanalyse

Soutenu publiquement le : 15/03/2012, devant le jury composé de :

BOUCHEMAKH Isma	Professeur, U.S.T.H.B	Président
BOUROUBI Sadek	Professeur, U.S.T.H.B.	Directeur de mémoire
GUERBYENNE Hafida	Maitre de Conférences A, U.S.T.H.B.	Examinatrice
SEMRI Ahmed	Maitre de Conférences A, U.S.T.H.B	Examinateur

Introduction à la cryptographie quantique et aux techniques de cryptanalyse

CHARCHALI Fella
Département de Recherche Opérationnelle
Faculté de Mathématiques,
Université des Sciences et de la Technologie Houari Boumedienne,
U.S.T.H.B.

Remerciements

Dieu soit loué.

Mes remerciements vont en premier lieu à mon Directeur du mémoire Monsieur BOUROUBI Sadek Professeur à l'U.S.T.H.B., pour m'avoir confié ce travail sur "Introduction à la cryptographie quantique et aux techniques de cryptanalyse". Je le remercie beaucoup de m'avoir soutenu par ses précieuses orientations, les nombreux conseils, sa disponibilité, ainsi que pour la confiance et la liberté qu'il m'a accordé durant la réalisation de ce mémoire.

Je remercie Madame BOUCHEMAKH Isma Professeur à l'U.S.T.H.B., pour avoir bien voulu me faire l'honneur de présider le jury de ce mémoire.

Mes sincères remerciements vont aussi à Madame GUERBYENNE Hafida Maitre de Conférences *A* à l'U.S.T.H.B., et Monsieur SEMRI Ahmed Maitre de Conférences *A* à l'U.S.T.H.B., pour avoir bien voulu me faire l'honneur d'accepter d'être examinateurs de ce travail.

J'adresse également mes remerciements aux enseignants de la graduation et la poste graduation qui ont contribué à ma formation.

Je remercie Monsieur HACHEMANE Mahmoud, Professeur au laboratoire de Physique Théorique de la Faculté de Physique à l'U.S.T.H.B., pour son aide, et sa disponibilité ainsi que les membres du laboratoire Physique des Lasers. Je remercie aussi tous les collègues de la Faculté de Mathématiques, qui m'ont soutenu, soit par leurs actes, soit par leurs encouragements. Je leur exprime ici toute ma reconnaissance.

Mille merci et toute ma gratitude ne suffisent pas pour exprimer ma reconnaissance vers mes chèrs parents, tout ce que je peux dire est Merci. Merci à ma sœur Djazia d'avoir toujours eu la confiance en moi et merci à mon frère Mohamed de m'avoir toujours donné l'encouragement et la force pour continuer à réussir.

Table des matières

Table des figures

Liste des tableaux

Introduction générale

La cryptographie joue un rôle crucial dans la vie moderne, car elle permet une communication sécurisée à travers des canaux insécurisés, même face à des adversaires puissants. La cryptographie a été utilisée pour les communications militaires et gouvernementales depuis plus de 2000 ans, mais seulement au cours des 30 dernières années, la cryptographie est venue à être utilisée dans la vie quotidienne et pour des raisons civiles. L'expansion de l'Internet à partir d'un réseau de petite échelle académique à un réseau mondial permettant des centaines de milliards de dollars d'investissement en commerce électronique, a contribué en grande partie à la disponibilité de la cryptographie.

La conception d'une multitude d'algorithmes cryptographiques sécurisés - échange de clés publiques, les signatures numériques, le chiffrement par bloc et par flot, fonctions de hachage, message de codes d'authentification - et des protocoles sécurisés qui emploient ces primitives est une réalisation remarquable. Parmi ceux qui ont été largement adoptés, la majorité est restée fondamentalement sécuritaire malgré des années de cryptanalyse intensive et font progresser la technologie informatique [3].

La cryptographie a connu un saut très important en terme de l'utilisation d'outils. Elle assure actuellement la sécurité totale des communications en se basant sur des phénomènes naturels tels que le comportement des photons et leurs propriétés ; nous parlons alors du passage du classique au quantique ; et ceci est dû au développement énorme qu'a vécu la cryptanalyse.

Le présent travail touche deux aspects du concept cryptologie et il est organisé comme suit : Après l'introduction, le premier chapitre rappelle quelques notions et généralités qui nous serons utiles tout au long du document. Un aperçu de la cryptologie est présenté dans le deuxième chapitre où nous pouvons comprendre la structure de ce domaine et faire la distinction entre ses branches. Le troisième chapitre décrit un nouveau détournement de la cryptographie, du style classique au quantique. A cette étape une explication claire de la notion de la cryptographie quantique est donnée, ce qui facilite la compréhension de son principe de fonctionnement qui peut conduire à de futures recherches et explorations. Pour remédier aux problèmes de génération et d'échange de clés utilisées pour le chiffre de Vernam, le chapitre quatre expose la création d'un protocole simulé du premier protocole quantique $BB84$, nommé $BC10$. Le chapitre cinq est sous forme d'une enquête sur la cryptanalyse engendrant une description de la notion ainsi que les différentes méthodes et techniques développées par la communauté scientifique et les amateurs du domaine. Finalement, le mémoire se clôture par une conclusion qui résume tout ce qui a été présenté antérieurement et en mettant l'accent sur les perspectives de recherche induites par les résultats obtenus.

1

Rappels et généralités

Contents

Introduction

Nous illustrons dans ce chapitre quelques concepts mathématiques qui rendent la compréhension de certains résultats cryptographiques et cryptanalytiques claire tels que l'algèbre et la théorie des nombres.

1.1 Quelques notions d'Algèbre

Une suite $(x_n)_{n\in\mathbb{N}}$ de points d'un espace métrique (E,d) est une suite de Cauchy si :

$$\forall\epsilon\in\mathbb{R}_+^*\ \exists t\in\mathbb{N}/\forall n,m\geq t,\ d(x_n,x_m)<\epsilon$$

Dans un espace métrique (E,d), toute suite convergente est une suite de Cauchy (la réciproque est fausse en général). Si toute suite de Cauchy d'un espace métrique (E,d) est convergente alors (E,d) est dit complet [23].

Un espace vectoriel normé, complet s'appelle espace de Banach.
Un espace de Hilbert H $(E,(-|-))$ est un espace de Banach dont la norme est définie à partir d'un produit scalaire sur $\mathbb{R}$ ou d'un produit hermitien sur $\mathbb{C}$ [23].
Rappelons qu'une base hilbertienne est une suite (e_n) d'éléments de H tels que [35]

1. $\forall i,\ |e_i|=1\ et\ (e_i|e_j)=0\ \forall i,\ j,\ i\neq j.$
2. L'espace vectoriel engendré par les (e_i) est dense dans H.

Pour représenter les vecteurs appartenant à l'espace de Hilbert, on introduit la notation $|.\rangle$ dite notation de Dirac [1] (bra-ket notation). Soit $\psi\in H$ (Ket-vecteur) de dimension n alors :

$$|\psi\rangle=\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix},\ \alpha_i\in\mathbb{C}.$$

Le vecteur adjoint $\langle\psi|$ (bra-vecteur) est un vecteur ligne, le conjugué [2] du vecteur $|\psi\rangle$:

$$\langle\psi|=(\overline{\alpha_1},\ldots,\overline{\alpha_n}).$$

Soit maintenant, une base hilbertienne [3] $\{|e_i\rangle,\ i=1,2,\ldots,n\}$. Tout ket $|\psi\rangle$ ou bra $\langle\psi|$ se décompose sur cette base selon [35]

$$|\psi\rangle=\sum_{i=1}^{n}\alpha_i|e_i\rangle;\ \langle\psi|=\sum_{i=1}^{n}\overline{\alpha_i}\langle e_i|, \tag{1.1}$$

avec [4] $\alpha_i=\langle e_i|\psi\rangle$ et $\overline{\alpha_i}=\langle\psi|e_i\rangle$.

Le produit scalaire Hermitien de $|\psi\rangle$ par $|\phi\rangle$ où $\phi=\begin{pmatrix}\beta_1\\ \vdots\\ \beta_n\end{pmatrix}$ est noté $\langle\psi|\phi\rangle$, et est donné par la quantité complexe suivante :

$$\langle\psi|\phi\rangle=(\overline{\alpha_1},\ldots,\overline{\alpha_n})\begin{pmatrix}\beta_1\\ \vdots\\ \beta_n\end{pmatrix}=\sum_{i=1}^{n}\overline{\alpha_i}\beta_i.$$

1. En mécanique quantique cette notion est la convention utilisée pour décrire l'aspect vectoriel des états quantiques.
2. Le complexe conjugué de Z est noté $\overline{Z}$ en mathématiques et il est noté $Z^\star$ en physique.
3. Si H est de dimension infinie alors $n=\mathbb{N}^\star$.
4. $\langle e_i|\psi\rangle$ est le coefficient de Fourier d'ordre i, $1\leq i\leq n$. La série de Fourier d'un vecteur x est la série $\sum_{i=1}^{n}\langle x,e_i\rangle e_i$ qui est une série de vecteurs de H si $n=\mathbb{N}^\star$ et une somme finie si $n<+\infty$ [37].

Il possède la symétrie hermitienne [11] :

$$\overline{\langle\phi|\psi\rangle} = \langle\psi|\phi\rangle.$$

La norme d'un vecteur $|\psi\rangle$, notée $\||\psi\rangle\|$ ou $\|\psi\|$, est définie par

$$\|\psi\| = \sqrt{\langle\psi|\psi\rangle}.$$

Le produit tensoriel de deux vecteurs $|\psi\rangle$ et $|\phi\rangle$ est donné par :

$$|\psi\rangle \otimes |\phi\rangle = |\psi\rangle|\phi\rangle = |\psi\phi\rangle.$$

Le produit externe de $|\psi\rangle$ et $|\phi\rangle$ est donné par

$$|\psi\rangle\langle\phi| = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} (\overline{\beta_1}, \ldots, \overline{\beta_n}).$$

Ce produit représente un opérateur linéaire A.

Un opérateur linéaire d'un espace vectoriel E dans un espace vectoriel F est une application $A : E \to F$ qui associe à $x \in E$, $A(x) \in F$ et qui vérifie :

$$\begin{cases} \text{A(x+y)=A(x)+A(y)}, & \forall x,\ y \in E, \\ \text{A}(\lambda x) = \lambda A(x), & \forall \lambda \in \mathbb{R},\ \forall x \in E. \end{cases}$$

En mécanique quantique, un opérateur est une application linéaire de l'espace de Hilbert dans lui-même [32], d'où :

$$\begin{array}{ccc} A : H & \to & H \\ |\psi\rangle & \to & A|\psi\rangle \end{array}$$

vérifiant $A(a|\psi\rangle + b|\psi\rangle) = aA|\psi\rangle + bA|\psi\rangle$ *avec* $a,\ b \in \mathbb{C}$. Notons que $A|\psi\rangle$ est équivalent à $|A\psi\rangle$. L'opérateur A transforme un vecteur $|\psi\rangle$ en un autre vecteur $A|\psi\rangle$. Comme nous travaillons dans **un espace de Hilbert de dimension finie**, l'opérateur A est une matrice carrée $n \times n$.

L'opérateur adjoint d'un opérateur A est définie par [35]

$$\langle\varphi|A\psi\rangle = \langle A^\dagger\varphi|\psi\rangle$$

où $A^\dagger = (\overline{A})^t$, pour tout vecteur $|\psi\rangle$ de H.

l'opérateur A est dit $\begin{cases} \textit{auto} - \textit{adjoint ou Hermitien si} & A = A^\dagger\,; \\ \textit{normal si} & AA^\dagger = A^\dagger A\,; \\ \textit{unitaire si} & AA^\dagger = A^\dagger A = I. \end{cases}$

Soit$\lambda \in \mathbb{C}$, un vecteur non nul $|\psi_\lambda\rangle$ est un vecteur propre de A si :

$$A|\psi_\lambda\rangle = \lambda|\psi_\lambda\rangle \tag{1.2}$$

λ est une valeur propre de A et $|\psi_\lambda\rangle$ le vecteur propre associé [11].

Les valeurs propres d'opérateurs hermitiens sont réelles [11]. En outre, si $|\psi_\lambda\rangle$ et $|\psi_\mu\rangle$ sont deux vecteurs propres d'un opérateur hermitien correspondants à des valeurs propres distinctes λ et μ, ils sont orthogonaux, en effet, d'une part

$$\langle\psi_\lambda|A|\psi_\mu\rangle = \langle\psi_\lambda|(A|\psi_\mu\rangle) = \mu\langle\psi_\lambda|\psi_\mu\rangle$$

d'autre part

$$\langle\psi_\lambda|A|\psi_\mu\rangle = (\langle\psi_\lambda|A)|\psi_\mu\rangle = \lambda\langle\psi_\lambda|\psi_\mu\rangle.$$

Comme $\lambda \neq \mu$ il vient $\langle\psi_\lambda|\psi_\mu\rangle = 0$.
Si le sous espace propre correspondant à la valeur propre λ_i est de dimension d_{λ_i} supérieur à 1 alors λ_i est dite dégénérée avec degré de dégénérescence d_{λ_i}. L'opérateur A possède une infinité de valeurs propres dans le cas où la dimension est infinie [11].

Soit $e_1, e_2, \ldots, e_n$ un système orthonormal fini et $V = V[e_1, e_2, \ldots, e_n]$ le sous espace vectoriel de H engendré par les e_i. Alors

$$\forall\psi \in H,\ P(|\psi\rangle) = \sum_{i=1}^{n}\langle\psi|e_i\rangle|e_i\rangle. \tag{1.3}$$

L'opérateur $P_i = |e_i\rangle\langle e_i|$ est dit l'opérateur de projection ou le projecteur sur l'état $|e_i\rangle$ [11]. La projection de $|\psi\rangle$ sur la base hilbertienne $\{|e_i\rangle,\ i = 1, 2, \ldots, n\}$ est donnée par

$$P(|\psi\rangle) = \sum_{i=1}^{n}\langle\psi|e_i\rangle|e_i\rangle \quad et \tag{1.4}$$

$$\|P(|\psi\rangle)\|^2 = \sum_{i=1}^{n}|\langle\psi|e_i\rangle|^2. \tag{1.5}$$

Par conséquent, nous avons la décomposition de l'identité [11]

$$\sum_i P_{e_i} = \sum_i |e_i\rangle\langle e_i| = I, \tag{1.6}$$

où I est l'opérateur identité.

1.2 Quelques notions de la théorie des nombres

Définition 1.1 *Le plus grand diviseur commun de deux entiers a et b, noté $PGCD(a, b)$, est le plus grand entier g tel que g divise a et b.*

Deux entiers a et b sont dits copremier si $PGCD(a, b) = 1$.

Définition 1.2 *La fonction ϕ d'Euler donne le nombre d'entiers positifs $\leq n$ premiers avec n :*

$$\phi(n) = |\{a : PGCD(a, n) = 1, a \leq n\}|$$

Si $\phi(n) = n(1 - \frac{1}{p_1^{\alpha_1}})(1 - \frac{1}{p_2^{\alpha_2}})\ldots(1 - \frac{1}{p_k^{\alpha_k}})$ est la factorisation de n en nombres premiers, alors :
- *Si n est un nombre premier alors $\phi(n) = n - 1$.*
- *Si $n = a.b$ où $a, b \in \mathbb{Z}$ copremier alors $\phi(n) = \phi(a).\phi(b)$.*
- *Si p un nombre premier et $n = p^\alpha$ alors $\phi(n) = \phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.*

L'ensemble des entiers modulo un entier positif n est noté $\mathbb{Z}/n\mathbb{Z}$ ou de manière équivalente $\mathbb{Z}_n$.
L'ensemble $\mathbb{Z}_n$ est un anneau commutatif pour tout entier positif n. De plus si n est une puissance d'un nombre premier alors $\mathbb{Z}_n$ est un corps de Galois d'ordre n [3].

L'ensemble des entiers modulo un entier positif n qui sont inversibles est noté $\mathbb{Z}_n^\times$. De façons équivalentes, c'est l'ensemble des entiers qui sont premiers avec n ce qui veut dire que $card(\mathbb{Z}_n^\times) = \phi(n)$ [3].

1.3 Quelques notions de la théorie de l'information

Chercheur de génie, Claude Shannon, a travaillé au célèbre laboratoire AT&T Bell. Il est en grande partie responsable de l'omniprésence du concept de bits en information par son application des techniques de thermodynamique (étude de la chaleur, de l'ordre et du désordre dans les systèmes physiques) à la représentation des informations.

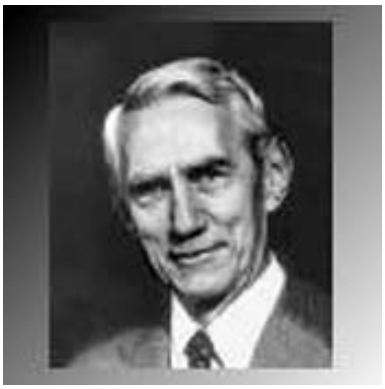


FIGURE 1.1 – Claude Shannon (1916-2001)

Shannon a mis au jour les limites de la représentation des informations en bits, car il a constaté qu'il était possible de représenter un texte de plusieurs façons différentes en anglais par l'utilisation de bits. Le génie de Shannon a été d'établir le lien entre la probabilité d'occurrence d'un terme ou d'un caractère et la " quantité d'informations " qui lui est associée [54].

Exemple 1.1 (exemple pris de [54]) Soit un texte de 3 mots "A", "B" et "C". Nous choisissons d'abord de représenter le premier mot sous la forme binaire "00", le second sous la forme "10" et le dernier sous la forme "11". La séquence "$ABCA$" devient alors "00101100" ou "$00-10-11-00$". Il a donc fallu 8 bits pour stocker les 4 mots (2 bits par mot). Shannon savait qu'il était possible d'être encore plus efficace. En effet, il a représenté le premier mot avec un seul bit : "0". La séquence "$ABCA$" devient alors "010110" ou "$0-10-11-0$", donc 6 bits pour stocker 4 mots, ce qui représentait un gain substantiel ! Shannon s'est alors demandé s'il était possible de faire mieux.

1.3.1 Entropie

La notion d'entropie due à Claude Shannon [2], introduite en 1948, est une fonction mathématique qui mesure l'incertitude sur ce que la source émet et est par conséquent, inversement proportionnelle à la quantité moyenne d'information contenue ou délivrée.

En télécommunication, plus l'émetteur (qui constitue la source d'information) émet d'informations différentes, plus l'entropie est grande et vice versa. Et plus le récepteur reçoit d'informations sur le message transmis plus l'entropie vis-à-vis ce message décroit. La définition de l'entropie d'une source selon Shannon est telle que, plus la source est redondante, moins elle contient d'information. En absence de contraintes particulières, l'entropie est maximale pour une source dont tous les symboles sont équiprobables.

Soit X une variable aléatoire qui prend ses valeurs dans $\{x_1, x_2, \ldots, x_n\}$ avec la probabilité $P(X = x_i) = p_i$, où $0 \leq p_i \leq 1$ pour tout $i, 1 \leq i \leq n$, et où $\sum_{i=1}^{n} p_i = 1$.

L'entropie de X est une mesure de la quantité moyenne d'informations fournies par une observation de X [16]. D'une manière équivalente, c'est l'incertitude à propos du résultat avant une

observation de X. L'entropie est aussi utile pour approcher le nombre moyen de bits nécessaires pour coder les éléments de X.

Définition 1.3 *[16] L'entropie ou incertitude de X est définie comme étant*

$$H(X) = -\sum_{i=1}^{n} p_i \log_2 p_i.$$

– **Entropie d'une variable aléatoire à deux issues [27] :**
Considérons le jet d'une pièce de monnaie. Soient p la probabilité d'obtenir pile et $q = 1 - p$ la probabilité d'obtenir face. Alors l'entropie du jet s'écrit $H = -p \log_2 p - q \log_2 q$.

De manière similaire nous pouvons écrire :

$$H = -[p \log_2 p + (1-p) \log_2 (1-p)] = -[p \log_2 \frac{p}{(1-p)} + \log_2 (1-p)].$$

Nous pouvons alors étudier la variation de H en fonction de p.

$$\frac{dH(p)}{dp} = -\log_2 \frac{p}{(1-p)} = 0 \Leftrightarrow \frac{p}{(1-p)} = 1 \Leftrightarrow p = 0.5.$$

Ce qui donne

$$H(0.5) = -[0.5 \log_2 0.5 + (0.5) \log_2 0.5] = 1,$$

d'où H atteint la valeur maximale $H = 1$ pour $p = 0.5$.

Donc pour toute valeur $p \neq 0.5$ nous avons toujours $H < 1$. De plus, comme $x \log x \to 0$ pour $x \to 0$, H est nulle pour $p = 0$ et $p = 1$, puisque l'une et l'autre des deux éventualités est certaine et donc il n'y a pas d'incertitude et l'entropie est nulle.

Dans le cas d'une pièce de monnaie non régulière, où p est la probabilité d'obtenir pile et q d'obtenir face, à chaque jet, un coté est plus susceptible d'apparaître que l'autre. D'où l'entropie est de faible quantité, chaque lancer de la pièce offre moins d'un bit d'information (l'incertitude existe, positive, inférieure à 1).

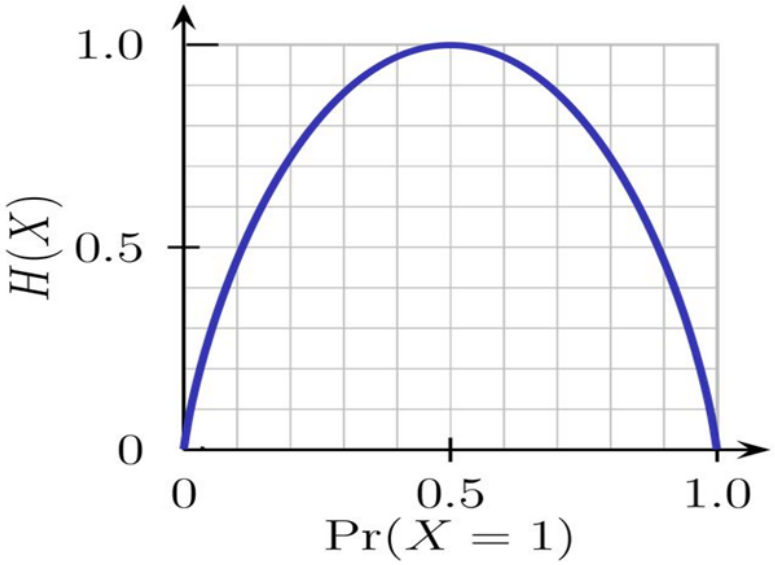
Le cas extrême est celui d'une pièce modifiée de manière à ce qu'une seule face apparaîsse à chaque lancer, l'entropie dans ce cas est nulle (pas d'incertitude, obtenir face est certain) et le jet ne fournit aucune information.

– **Texte et entropie [54]**

Si un mot x apparaît $f(x)$ fois dans un texte de longueur n, la probabilité de tomber sur le mot x par hasard est de $p(x) = \frac{f(x)}{n}$. La quantité d'informations associée au mot x est de $-\log_2 p(x)$. Ainsi, si $p(x)$ est très petit, la quantité est très grande, alors que si $p(x)$ est très grand, elle est presque nulle. En français, cela signifie que le mot "le" apporte très peu d'informations car il est utilisé très fréquemment, alors que le mot "anticonstitutionnellement", qui est assez peu usité, contient beaucoup d'informations. La moyenne de la quantité d'informations dans les mots du texte s'exprime par $-\sum_x p(x) \log_2 p(x)$ et celle dans le texte se mesure par : $-n \sum_x p(x) \log_2 p(x)$. L'un des principaux résultats de la théorie de Shannon est qu'il faut toujours au moins $-n \sum_x p(x) \log^2 p(x)$ bits pour stocker l'ensemble du texte, et ce, malgré l'utilisation de techniques de compression [5] comme zip [6]. Shannon a aussi montré qu'il était possible de s'approcher très près de cette limite théorique de compression.

5. Le terme compression ne renvoie qu'à la " compression sans perte ", où il est toujours possible de reproduire les données d'origine à partir des données compressées. Les méthodes de compression utilisées par les normes MP3, MPEG, JPEG, etc., sont donc exclues.

6. En fait, c'est le minimum de bits nécessaires au stockage d'un texte quand on utilise un code où chaque mot correspond à une séquence de bits unique. Les outils de compression peuvent faire appel à des techniques plus sophistiquées où la séquence de bits utilisée pour représenter un mot dépendra des mots précédemment rencontrés dans le texte. Il faudrait dans ce cas précis utiliser une généralisation du résultat de Shannon.



Exemple 1.2 [54] Prenons un texte de 2 mots, l'un ayant une fréquence de 500 et l'autre, de 250, pour un total de 750 ($n = 750$). Nous avons alors $p(1) = \frac{500}{750}$ et $p(2) = \frac{250}{750}$. La quantité d'informations du premier mot est de $-\log_2(\frac{2}{3}) \approx 0.58$ et la quantité d'informations du second mot est de $-\log_2(\frac{1}{3}) \approx 1.58$. Pour coder le texte, il faut donc au moins $(-\log_2(\frac{2}{3}) - \log_2(\frac{1}{3})) \times 750 \approx 688$ bits, soit environ 86 octets. [7]

L'entropie de Shannon $(-\sum_x p(x) \log p(x))$ est maximale à condition que nous choisissions les mots selon une distribution uniforme. L'entropie est minimale $(= 0)$ quand un seul choix est possible ($p(x) = 1$ pour un certain x, et $p(x\prime) = 0$ autrement). En d'autres termes, un texte généré plus aléatoirement est moins compressible.

– ***n*-grammes et entropie d'une langue [54]**

Un n-gramme est une suite de n caractères (ou n mots selon le cas). Par exemple, "*bi*" ou "*ci*" sont des 2-grammes, appelés aussi des bigrammes. Nous pouvons trouver tous les n-grammes que contient un texte. Par exemple, le mot "Lavie" contient les trigrammes "Lav", "avi" et "vie". De la même façon qu'il est possible de calculer l'entropie des caractères, on peut calculer l'entropie des n-grammes, qui est notée H_n. Shannon a défini l'entropie d'une langue comme étant $H = \lim_{n \longrightarrow \infty} H_n$. Il a estimé que, pour l'Anglais, l'entropie était de $0.6 < H < 1.3$.

Propriétés de l'entropie [19] :

1. Soit X une variable aléatoire à n valeurs.
   – $0 \leq H(X) \leq \log_2 n$.

   Nous avons $\forall i, 0 < p_i < 1, \log p_i < 0$.
   Donc $-p_i \frac{\log p_i}{\log 2} > 0$.
   C'est à dire
   $H(X) = \sum_{i=1}^{n} -p_i \log_2 p_i > 0$.

7. Vous pouvez tester ce résultat en générant un texte de seulement 2 mots qui comporte les fréquences prescrites. Vous constaterez que, quels que soient vos efforts de compression avec zip ou avec un autre outil, vous n'arriverez pas, sans tricher, à un fichier qui fait moins de 688 bits [54].

Soient maintenant deux distributions de probabilité sur le même ensemble fini $(p_1, p_2, \ldots, p_n)$ et $(q_1, q_2, \ldots, q_n)$ avec $\sum_{i=1}^{n} p_i = \sum_{i=1}^{n} q_i = 1$.
On sait que $\ln(x) \leq x - 1$.
Soit $x = \frac{q_i}{p_i}$, on a alors $\ln(\frac{q_i}{p_i}) \leq \frac{q_i}{p_i} - 1$.
Multipliant cette inégalité par p_i

$$p_i \ln(\frac{q_i}{p_i}) \leq p_i(\frac{q_i}{p_i} - 1)$$

Par sommation sur tous les i, on obtient :

$$\sum_{i=1}^{n} p_i \ln(\frac{q_i}{p_i}) \leq \sum_{i=1}^{n} p_i(\frac{q_i}{p_i} - 1) = \sum_{i=1}^{n} q_i - \sum_{i=1}^{n} p_{i=0}$$

Cette inégalité reste vraie si on passe au logarithme base 2.

On a donc : $\sum_{i=1}^{n} p_i \log_2(\frac{q_i}{p_i}) < 0$.
Prenons $q_i = \frac{1}{n}$, on aura :

$$\sum_{i=1}^{n} p_i \log_2(\frac{1}{np_i}) = \sum_{i=1}^{n} p_i \log_2(\frac{1}{p_i}) - \sum_{i=1}^{n} p_i \log_2(n) \leq 0$$

Ce qui donne

$$\sum_{i=1}^{n} p_i \log_2(\frac{1}{p_i}) = H(X) \leq \sum_{i=1}^{n} p_i \log_2(n) = \log_2(n)$$

– $H(X) = 0$ si et seulement si l'un des p_i est un et les autres valent zero.

Il y a un seul événement qui se produit avec une probabilité certaine ce qui ne laisse aucune incertitude sur le résultat.

– $H(X) = \log_2 n$ si et seulement si $p_i = \frac{1}{n}$ pour tout $i, 1 \leq i \leq n$ (c'est-à-dire que tous les résultats sont équiprobables, le cas d'une distribution uniforme).

2. L'entropie conjointe de X et Y est définie comme suit

$$H(X, Y) = -\sum_{x \in X, y \in Y} P(x, y) \log_2(P(x, y)).$$

L'entropie conjointe est une grandeur symétrique $H(X, Y) = H(Y, X)$.
La définition peut être étendue à un nombre quelconque de variables aléatoires.

Si X et Y sont deux variables aléatoires, alors $H(X, Y) \leq H(X) + H(Y)$, avec égalité si et seulement si X et Y sont indépendantes.

– Nous avons

$$H(X, Y) = -\sum_{x \in X, y \in Y} p(x, y) \log_2 p(x, y).$$

Comme $p(x, y) \leq p(x) + p(y)$,

il s'ensuit que

$$H(X, Y) \leq -\sum_{x} \sum_{y} (p(x) + p(y)) \log_2 p(x, y).$$

C'est-à-dire

$$H(X,Y) \leq -\sum_x p(x) \sum_y \log_2 p(x,y) - \sum_y p(y) \sum_x \log_2 p(x,y),$$

il vient

$$H(X,Y) \leq -\sum_x p(x) \log_2 p(x) - \sum_y p(y) \log_2 p(y),$$

d'où

$$H(X,Y) \leq H(X) + H(Y)$$

.

3. Si X et Y sont deux variables aléatoires, l'entropie conditionnelle de X sachant $Y = y$ est :

$$H(X|Y=y) = -\sum_{x \in X} P(X=x, Y=y) \log_2(P(X=x|Y=y)).$$

L'entropie conditionnelle est appelée également l'équivoque de Y sur X

$$H(X|Y) = -\sum_{y \in Y} P(Y=y) H(X|Y=y)$$

Soient X, Y, Z trois variables aléatoires.
- $H(X|Y)$ mesure la quantité d'incertitude demeurant au sujet de X après qu'on ait observé Y.
- $H(X|Y) \geq 0$ *et* $H(X|X) = 0$.

  L'entropie conditionnelle de X sachant Y est la somme de quantités positives ou nulle. Maintenant, si nous avons observé X alors nous n'aurons aucune incertitude sur X.
- $H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$.
  D'abord

$$H(X,Y) = -\sum_{x \in X, y \in Y} p(x,y) \log_2 p(x,y)$$

$$H(X,Y) = -\sum_{x \in X, y \in Y} p(x,y) \log_2 p(x) p(y|x)$$

avec une petite manipulation

$$H(X,Y) = -\sum_{x \in X} \sum_{y \in Y} p(x,y) \log_2 p(x) - \sum_{x \in X} \sum_{y \in Y} p(x,y) \log_2 p(y|x)$$

$$H(X,Y) = -\sum_{x \in X} p(x) \log_2 p(x) - \sum_{x \in X} \sum_{y \in Y} p(x,y) \log_2 p(y|x)$$

d'où

$$H(X,Y) = H(X) + H(Y|X).$$

– $H(X|Y) \leq H(X)$, avec égalité si et seulement si X et Y sont indépendantes.

$H(Y) + H(X|Y) = H(X,Y) \leq H(X) + H(Y)$d'où $H(X|Y) \leq H(X)$.

– $H(X,Y|Z) = H(Y|Z) + H(X|YZ)$ [12]

– $H(X|Y) \leq H(XZ|Y)$ [12]
L'incertitude sur une variable aléatoire X sachant une autre variable aléatoire Y est moins importante que l'incertitude sur deux variables aléatoires X, Z sachant la variable aléatoire Y.

L'entropie quantifie la moyenne de l'information parvenue d'une source d'information, par exemple, quand une variable aléatoire X prend une valeur, l'entropie décrit notre incertitude sur la variable aléatoire avant qu'elle prend sa valeur, ou alternativement, combien d'unités d'information nous avons acquis après avoir lu sa valeur, ces deux vues sont équivalentes.
Pour quantifier la moyenne de l'information combinée parvenue des résultats x et y des deux variables aléatoires X et Y, nous définissons l'entropie conjointe $H(X,Y)$.
L'information mutuelle de deux variables aléatoires X et Y décrit la quantité d'information qu'ils ont en commun $I(X,Y)$ où

$$I(X,Y) = H(X) + H(Y) - H(X,Y).$$

1.3.2 Information réciproque

Définition 1.4 *L'information réciproque ou la transinformation des variables aléatoires X et Y $I(X,Y)$ désigne la quantité d'information gagnée sur X après avoir observé Y, donnée par la relation $I(X;Y) = H(X) - H(X|Y)$ [19]. D'une manière similaire, la tansinformation de X et la paire Y,Z est définie comme étant $I(X;Y,Z) = H(X) - H(X|Y,Z)$.*

Fait (Propriétés de l'information réciproque [19])

1. La quantité $I(X;Y)$ peut être considéré comme étant la quantité d'information que révèle Y sur X. De même, la quantité $I(X;Y,Z)$ peut être considérée comme la quantité d'informations que Y et Z révèlent sur X,
2. $I(X;Y) \geq 0$,
3. $I(X;Y) = 0$ si et seulement si X et Y sont indépendantes (c'est-à-dire, Y ne fournit aucune information sur X),
4. $I(X;Y) = I(Y;X)$.

Définition 1.5 *La transinformation conditionnelle de la paire X,Y sachant Z est [19]*

$$I(X;Y|Z) = H(X|Z) - H(X|Y,Z).$$

Fait (Propriétés de transinformation conditionnelle [19])

1. La quantité $I(X;Y\backslash Z)$ peut être interprétée comme la quantité d'information que fournit Y sur X, étant donné que Z a déjà été observé.
2. $I(X;Y,Z) = I(X;Y) + I(X;Z|Y)$,
3. $I(X;Y|Z) = I(Y;X|Z)$.

1.4 Données aléatoires

Il existe plusieurs définitions de ce qui est vraiment l'aspect aléatoire même, les mathémat-iciens n'arrivent pas à définir ce concept de manière satisfaisante. Mais ici nous adoptons la définition informelle suivante, les données aléatoires sont imprévisibles pour l'attaquant [8], même s'il prend

8. Un tiers qui veut espionner les informations confidentielles échangées par des parties.

des mesures actives pour contrer cet aspect aléatoire [53].

La mesure de l'aspect aléatoire s'appelle l'entropie. L'entropie mesure l'incertitude au sujet de la valeur de l'information cachée.

Les ordinateurs possèdent un certains nombres de sources d'aléatoire : rythme des frappes claviers, mouvements de la souris. Ces sources sont suspectes, car dans certaines situations, l'attaquant peut mesurer cette source ou l'influencer.

Les processus physiques tels que les lois de la physique quantique induisent certains comportements parfaitement aléatoires, ce qui constitue une solution pour assurer l'aléatoire. Cependant, l'attaquant dispose de voies d'attaque sur ce type de solutions. Il peut essayer d'influencer le comportement des particules en question pour le rendre prévisible. Il peut également essayer d'espionner les mesures que les utilisateurs légitimes aient fait, s'il obtient une copie des mesures, les données restent toujours aléatoires, mais elle n'auront pas d'entropie de point de vue de l'attaquant. L'attaquant peut influencer les détecteurs en installant un fort champ magnétique.

L'alternative aux vraies données aléatoires est d'utiliser des données pseudo-aléatoires. Les données pseudo-aléatoires sont produites à partir d'une graine [9] par un algorithme déterministe.

Les ordinateurs modernes possèdent un véritable générateur de nombres aléatoires intégré ce qui rend certaines attaques plus difficiles car le générateur n'est accessible que depuis le système d'exploitation.

Conclusion

Dans ce chapitre, nous avons donné quelques rappels et généralités nécessaires pour comprendre les notions introduites par la suite, et suivre le raisonnement du document.

9. Fichier rassemblant des données aléatoires.

2

A propos de la cryptologie

Contents

Introduction

La cryptologie est un art ancien et une science nouvelle ; un art ancien parce que les anciens tels que Jules César l'utilisaient déjà ; une science nouvelle parce que ce n'est qu'à partir des années soixante dix, a devenu un thème de recherche scientifique. La cryptologie englobe la cryptographie et la cryptanalyse [1].

Le schéma suivant donne une vue sur l'étendu de la cryptologie.

1. Wikipédia

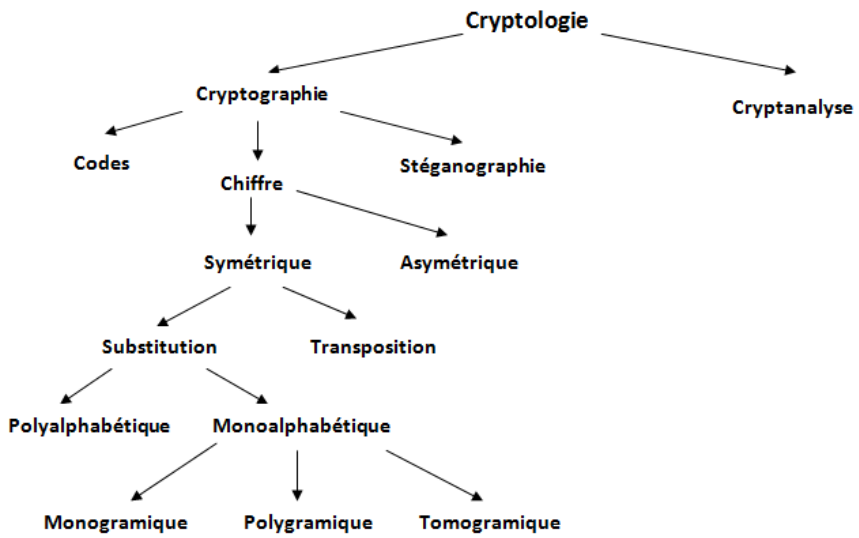


FIGURE 2.1 – Arborescence de la cryptologie

Les acteurs qui rentrent en jeu en cryptologie, sont Alice et Bob ; qui veulent échanger des messages confidentiels d'une manière sécurisée et qui se font confiance mutuelle. Eve, l'espionne, qui essaie d'attraper toute information circulant entre Alice et Bob ou bien de briser leur moyen de communication.

2.1 Mots clés

A ce niveau nous listons quelques mots clés les plus courants en cryptographie et en cryptanalyse [19].

• Confidentialité, secret (confideniality, secrecy) : L'assurance qu'une information donnée ne peut pas être consultée par une partie non autorisée.

• L'intimité (privacy) : L'aptitude d'une personne à contrôler la manière dont laquelle ses informations personnelles sont diffusées dans la société. Ceci peut être vu comme synonyme de secret.

• Code : Un ensemble de symboles représentant une information.

• Théorie du codage (coding theory) : Science de transformation de code, permet de partager l'information à travers des canaux de communication d'une manière fiable. Cette science se concentre sur les canaux bruités et essaie de rendre la récupération d'information réalisable à qui que ce soit (contrairement la cryptographie qui essaie de rendre la récupération d'information réalisable aux parties autorisées seulement).
• Codage, décodage (encode, decode) : Processus fondamental de la théorie du codage : action de transformer l'information en mots codés, ou récupérer l'information des mots codés.

• Chiffre (cipher) : Permet l'expression d'une manière confidentielle en utilisant un processus élémentaire de cryptage.

• Système cryptographique (cryptographic system) : Ensemble d'algorithmes cryptographiques y compris le chiffrement. Cryptosystème est une abréviation de système cryptographique, ce mot

est réservé aux systèmes à clé publique par contre le mot chiffrement indique que le système utilisé est à clé symétrique.

• Texte en clair (cleartext) : information codée via un code connu au public tel que l'alphabet.

• Texte clair (plaintext) : L'input de l'algorithme de cryptage (souvent c'est le texte en clair).

• Texte chiffré, cryptogramme (ciphertext, cryptogram) : L'output d'un cryptosystème.

• Cryptage, chiffrement (encryption, encipherment) : Action de transformer un texte clair en un texte chiffré.

• Décryptage (decryption) : Action de transformer le texte chiffré en texte clair par une partie non autorisée.

•Déchiffrement (decipherment) : Action de transformer le texte chiffré en texte clair par une partie autorisée.

• Briser un cryptosystème (breaking a cryptosystem) : Prouver l'insécurité d'un cryptosystème par exemple en exhibant comment décrypter un message.
Dans la suite du document, nous symbolisons le texte clair par M, le texte chiffré par C et la clé par K.

2.2 Cryptographie

Cryptographie se distingue de la théorie du codage dans le sens que la présence de bruit aléatoire dans cette dernière est remplacée par des adversaires malveillants dans la première. Elle utilise un vocabulaire spécifique et s'appuie sur quelques principes fondamentaux [19].

Après avoir acquis la confidentialité, la cryptographie assure d'autres exigences assez importantes ; à nos jours, comment peut on vérifier que quelqu'un est-il celui qui prétend d'être ? Les opérations commerciales et celles de la banque sont elles valides ? La cryptographie remède à ces interactions sociales quotidiennes par le garanti de [1] :

• L'authentification : Pouvoir vérifier l'origine du message reçu, et un intrus ne doit pas être capable de se faire passer pour quelqu'un d'autre.

• L'intégrité : Pouvoir vérifier que le message reçu n'a pas subi des modifications en cours de transmission, et un intrus est incapables de remplacer le message légitime par un faux message.

• Non-répudiation : L'expéditeur ne doit pas être capable de nier d'avoir envoyer le message.

La cryptographie engendre un certain nombre de manières de faire passé l'information secrète, plus les codes, nous trouvons la stéganographie, la substitution et la transposition qui sont les premières et les plus anciennes, plus les cryptosystème de nos jours. Nous donnons ici, une brève idée sur ces notions.

La stéganographie : Sert à cacher un message secret dans un support (image, vidéo, ondes audio, une peinture...etc). Généralement, l'expéditeur insert son message secret dans un texte en utilisant l'une des astuces historiques comme l'encre invisible et les trous minuscules d'épingle dans des caractères sélectionnés.

La transposition et la substitution : Au passé et avant la sortie de la notion d'ordinateur au monde, les anciens utilisaient la cryptographie en manipulant des lettres et en utilisant des cryptosystèmes où le principe est de remplacer des caractères par d'autres ou transposer les caractères. Pour plus de sécurité, exécuter les deux opérations en même temps plusieurs fois.

Actuellement, le même principe est suivi, sauf qu'au lieu les lettres, les ordinateurs manipulent les bits. Les bons algorithmes cryptographiques combinent toujours des substitutions avec des transpositions.

2.2.1 L'algorithme cryptographique

L'algorithme de cryptographie consiste de deux étapes ; la première étape est achevée par Alice où le message doit être chiffré par une clé. Une fois le message chiffré est transmis via un canal non sécurisé, Bob le reçoit afin de compléter la deuxième phase où il doit utiliser une clé pour récupérer le message clair.

La clé de chiffrement et la clé de déchiffrement appartiennent à l'espace des clés. Le fait que la clé utilisée pour le chiffrement est la même que celle utilisée pour le déchiffrement ou non définit deux catégories de cryptosystèmes :

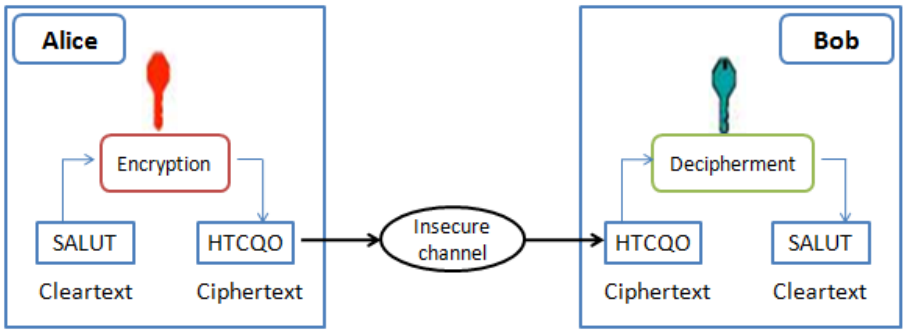


FIGURE 2.2 – L'algorithme de cryptographie

2.2.2 Les algorithmes cryptographiques à clé symétrique

Les algorithmes symétriques, connus aussi sous le nom des algorithmes à clé secrète, sont des algorithmes où la clé de chiffrement et la clé de déchiffrement sont identiques. Pour tels algorithmes, l'émetteur et le récepteur doivent se mettre d'accord sur une clé à utiliser avant d'échanger des messages. La sécurité d'un algorithme à clé secrète repose sur la clé : si celle-ci est dévoilée, alors n'importe qui peut chiffrer et déchiffrer des messages dans ce cryptosystème. Le chiffrement E et le déchiffrement D dans un tel algorithme se font comme suit :

$$\begin{cases} E_k(M) = C, \\ D_k(C) = M. \end{cases}$$

D'après l'arborescence de la figure 2.1, nous distinguons deux grandes familles d'algorithmes :

- **La transposition :** Un chiffre de transposition consiste à changer l'ordre des lettres, donc à construire des anagrammes. Cette méthode est connue depuis l'antiquité, puisque les Spartes utilisaient déjà une scytale.

- **La substitution :** Un chiffre de substitution consiste à remplacer les lettres ou les mots par d'autres symboles. Cela présuppose de choisir un ensemble de symboles qui joueront le rôle de substituts : nous pouvons par exemple utiliser l'alphabet latin classique, l'alphabet grec, cyrillique, des nombres, des traits et des points. . .etc.

  Les chiffres de substitutions peuvent être classés dans deux grands groupes :

  Le premier groupe contient **les chiffres de substitution polyalphabétique** où une même lettre peut être remplacée par plusieurs symboles le long de processus de chiffrement.

  Le deuxième groupe engendre **les chiffres de substitution monoalphabétique**, où une lettre est remplacée par une autre lettre fixe le long de chiffrement, ce qui constitue le premier cas, ou un groupe de lettre qui est le deuxième cas. Si nous sommes dans le premier cas, nous parlons alors de **substitution monogrammique**. Si nous sommes dans le deuxième cas, nous trouvons deux catégories, la catégorie de la **substitution polygrammique**, ce qui signifie qu'une lettre est remplacée par plusieurs lettres, et la catégorie de la **substitution tomogrammique**, dans laquelle chaque lettre est tout d'abord représentée par des groupes de deux ou plusieurs lettres, qui sont ensuite chiffrés séparément par substitution

ou transposition.

Il existe également une famille de substitution qui se situe entre la substitution monoalphabétique et la substitution polyalphabétique, c'est la **substitution homophonique**. Elle consiste à remplacer une lettre non pas par une lettre unique, mais par une lettre choisie au hasard parmi plusieurs. On peut situer l'âge d'or de la substitution homophonique entre 1500 et 1750.

En cryptographie symétrique moderne nous distinguons deux grandes catégories en termes de la manière de traiter l'information lors du chiffrement. Nous trouvons le chiffrement par bloc et le chiffrement par flot.

Le chiffrement par bloc (en Anglais block cipher) possède une structure itérative [2], il consiste de faire des découpages des données en blocs de taille généralement fixe et chiffrer un bloc à la fois avec une même clé. La taille de bloc est comprise entre 32 et 512 bits, dans le milieu des années 1990, le standard était de 64 bits mais depuis 2000, avec l'apparition du l'AES (Advanced Encryption Standard), le standard est devenu de 128 bits. Les blocs sont ensuite chiffrés les uns après les autres. Les algorithmes de chiffrements par bloc, pour la plupart basés sur des le schéma de Feistel, sont actuellement les algorithmes à clef secrète les plus courants. Cependant, depuis l'invention du DES en 1977, la puissance de calcul des ordinateurs a incroyablement progressé, si bien que la longueur des clés est maintenant insuffisante. L'AES a été destiné à prendre la relève du DES, réputé peu sûr depuis quelques années. Après une mise au concours, en 2000, le NIST [3] (censé définir la norme pour le territoire américain, mais dont l'influence dépasse les frontières du pays), a choisi parmi de nombreux candidats pour l'AES un algorithme nommé Rijndael, conçu par des cryptologues belges, Vincent Rijmen et Joan Daemen. Aujourd'hui, le DES et son successeur AES sont tous les deux vulnérables à la cryptanalyse différentielle et linéaire.

Le chiffrement de flux ou chiffrement par flot (en Anglais stream cipher) est la deuxième catégorie de chiffrements modernes en cryptographie symétrique. Un chiffrement par flot arrive à traiter les données de longueur quelconque et n'a pas besoin de les découper.
Il est possible de transformer un chiffrement par bloc en un chiffrement par flot en utilisant un mode d'opération [4] comme ECB [5] (chaque bloc chiffré indépendamment des autres) ou CFB [6] (on chaîne le chiffrement en effectuant un Xor entre les résultats successifs). Une liste non-exhaustive de chiffrements par flot :
· A5/1, algorithme publié en 1994, utilisé dans les téléphones mobiles de type GSM pour chiffrer la communication par radio entre le mobile et l'antenne-relais la plus proche.
· RC4, le plus répandu, conçu en 1987 par Ronald Rivest, utilisé notamment par le protocole WEP du WiFi.
· Py, un algorithme récent de Eli Biham.
· E0 utilisé par le protocole Bluetooth.

Un chiffrement par flot se présente souvent sous la forme d'un générateur de nombres pseudo-aléatoires avec lequel on opère un XOR entre un bit à la sortie du générateur et un bit provenant des données.

2. Concept discuté à la section 5.5.1 au chapitre 5.
3. National Institut of Standards and Technology
4. Un mode d'opération est la manière de traiter les blocs de texte clairs et chiffrés au sein d'un algorithme de chiffrement par bloc.
5. Dictionnaire de codes - Electronic Code Book-.
6. Chiffrement à rétroaction - Cipher Feedback -.

2.2.3 Les algorithmes cryptographiques à clé asymétrique

Les algorithmes à clé asymétrique sont conçus de telle manière que la clé de chiffrement soit différente de la clé de déchiffrement. De plus, la clé de déchiffrement ne peut pas être calculée (du moins en un temps raisonnable) à partir de la clé de chiffrement. Ces algorithmes sont connus aussi sous le nom d'algorithmes à clé publique parce que la clé de chiffrement peut être rendue publique : n'importe qui peut utiliser la clé de chiffrement pour chiffrer un message mais seul celui qui possède la clé de déchiffrement peut déchiffrer le message chiffré résultant. Dans tels algorithmes, la clé de chiffrement est appelée clé publique et la clé de déchiffrement est appelée clé privée. Le chiffrement en utilisant la clé k est donné par :

$$E_k(M) = C.$$

Comme la clé de déchiffrement et de déchiffrement sont différente, alors le déchiffrement est donné par :

$$D_{k'}(C) = M.$$

L'idée de ce système a été proposée en 1976 par Diffie et Hellman, qui ont proposé une méthode totalement nouvelle : une clé pour chiffrer et une autre pour déchiffrer. Bien entendu, il existe un lien mathématique entre ces deux clés, les deux inventeurs l'appellent une "fonction trappe à sens unique". Cette fonction permet de calculer aisément la clé de chiffrement en connaissant la clé de déchiffrement. En revanche, l'opération inverse est pratiquement impossible. Les systèmes à clés publiques les plus connus sont RSA et PGP, mais il en existe d'autres, par exemple le chiffre de Merkle-Hellman et le chiffre de Rabin.

Comme souvent dans l'histoire de la cryptographie, les vrais découvreurs ne sont pas toujours ceux que l'on pense. En effet, l'histoire a retenu les noms de Merkle, Hellman et Diffie car ils ont été les premiers a publié leur invention. En fait, on a appris plus tard que les trois premiers inventeurs de l'idée du système à clef publique était James Ellis, Clifford Cocks et Malcom Williamson, qui travaillaient au Government Communications Headquarters (GCHQ) de Cheltenham, établissement anglais top secret fondé sur les ruines de Bletchley Park après la Seconde Guerre mondiale. Ellis posa les bases dès 1969. Puis, en 1973, Cocks eut une idée de ce qui serait plus tard connu sous le nom de chiffre asymétrique RSA. Il ne put mettre en oeuvre son idée, car les ordinateurs de l'époque n'étaient pas encore assez puissants. En 1974, Cocks expose son idée à Williamson. Ce dernier, qui pense que cela est trop beau pour être vrai, reprend tout à zéro pour trouver une faille. Au lieu de cela, il trouve le système d'échange de clef de Diffie-Hellman-Merkle, à peu près en même temps que Martin Hellman. En 1975, Ellis, Cocks et Williamson avaient donc découvert tous les aspects fondamentaux de la cryptographie à clef publique, mais les trois anglais se turent, secret militaire oblige.

2.2.4 Fonctions de hachage

Il existe également une autre catégorie algorithmes cryptographiques qui est utilisable avec ou sans clé secrète, c'est les fonctions de hachage. Une fonction de hachage sans clé est appelée modification detection code (MDC), nous pouvons nous en servir pour s'assurer de l'intégrité d'un message. Une fonction de hachage avec clé est appelée message authentication code (MAC), où le paramètre additionnel, la clé, permet de vérifier l'intégrité et la provenance du message en même temps [49].

Une fonction de hachage h, tel que :

$$h : \{0,1\}^t \quad \longrightarrow \quad \{0,1\}^n,$$

(parfois appelée fonction de condensation) est une fonction permettant d'obtenir un condensé (typiquement de taille $n = 128$, $n = 160$ ou $n = 256$ bits) appelé aussi condensat ou haché ou en

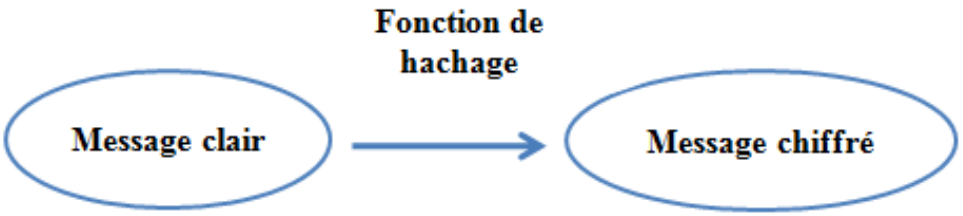


FIGURE 2.3 – Fonction de hachage

Anglais message digest d'un texte de taille t [48], c'est-à-dire une suite de caractères assez courte représentant le texte qu'il condense.
La fonction de hachage doit être telle qu'elle associe un et un seul haché à un texte en clair (cela signifie que la moindre modification du document entraîne la modification de son haché). D'autre part, il doit s'agir d'une fonction à sens unique (one-way function) afin qu'il soit impossible de retrouver le message original x à partir du condensé y tel que $h(x) = y$ cette propriété est appelé résistance à la préimage. S'il existe un moyen de retrouver le message en clair à partir du haché, la fonction de hachage est dite "à brèche secrète". Les fonctions de hachage possèdent d'autres propriétés telles que pour un message x_1, il est impossible de trouver un message $x_2 \neq x_1$ avec $h(x_1) = h(x_2)$, h est dite résistante au second préimage, et qu'il est difficile de trouver un couple de message (x_1, x_2) avec $h(x_1) = h(x_2)$. Cette propriété est appelé résistance au collision [49].
Ainsi, le haché représente en quelque sorte l'empreinte digitale (en Anglais finger print) du document. Les algorithmes de hachage les plus utilisés actuellement sont :
MD5 (MD signifiant Message Digest) développé par Rivest en 1991, MD5 crée une empreinte digitale de 128 bits à partir d'un texte de taille arbitraire en le traitant par blocs de 512 bits. Il est courant de voir des documents en téléchargement sur Internet accompagnés d'un fichier MD5, il s'agit du condensé du document permettant de vérifier l'intégrité de ce dernier.
SHA (pour Secure Hash Algorithm, pouvant être traduit par Algorithme de hachage sécurisé) crée des empreintes d'une longueur de 160 bits. SHA-1 est une version améliorée de SHA datant de 1994 et produisant une empreinte de 160 bits à partir d'un message en le traitant par blocs de 512 bits.

Nous introduisant ici le principe de fonctionnement de la fonction de hachage SHA afin d'illustrer l'application de hachage à un message donné M.
SHA a été conçu par le NIST (Institut National des Standards et de la Technologie Américain) en collaboration avec l'Agence Nationale de Sécurité Américaine (NSA) pour être utilisée dans le DSA [7].
D'abord, le message à haché ou compressé M est complété de manière à ce que sa longueur soit un multiple de 512 (ajouter un 1 suivi d'autant de 0 que nécessaire pour remplir les 64 bits manquants par rapports à un multiple de 512).
Ensuite, cinq variables de 32 bits (pour produire une empreinte à 160 bits) sont initialisées comme suit :

$A = 0x67452301$
$B = 0xefcdab89$
$C = 0x98badcfe$
$D = 0x10325476$
$E = 0xc3d2e1f0$

La boucle principale de l'algorithme commence. Elle traite les 512 bits du message à la foi et

7. Algorithme de Signature Numérique, proposé par NIST (développé par NSA) en 1991 pour les applications de signature numériques fédérales. À une certaine étape, l'algorithme fait appel à la fonction de hachage SHA.

continue tant qu'il y a des blocs de 512 bits.
Les cinq variables sont copiées dans différentes variables : a reçoit A, b reçoit B, c reçoit C, d reçoit D et e reçoit E.
La boucle principale a 4 rondes de 20 opérations chacune. Chaque opération applique une fonction non linéaire sur trois des variables A, B, C, D et E puis effectue des décalages et des additions.
L'ensemble des fonctions non linéaires de SHA est donné par :

$f_t(X,Y,Z) = (X \wedge Y) \vee ((\neg X) \wedge Z),\ pour\ t = 0, \ldots, 19,$
$f_t(X,Y,Z) = X \oplus Y \oplus Z,\ pour\ t = 20, \ldots, 39,$
$f_t(X,Y,Z) = (X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z),\ pour\ t = 40, \ldots, 59,$
$f_t(X,Y,Z) = X \oplus Y \oplus Z,\ pour\ t = 60, \ldots, 79.$

L'algorithme utilise 4 constantes :

$k_t = 0x5a827999,\ pour\ t = 0, \ldots, 19,\ (0x5a827999 = \sqrt{2}/4.2^{32})$
$k_t = 0x6ed9eba1,\ pour\ t = 20, \ldots, 39,\ (0x6ed9eba1 = \sqrt{3}/4.2^{32})$
$k_t = 0x8f1bbcdc,\ pour\ t = 40, \ldots, 59,\ (0x8f1bbcdc = \sqrt{5}/4.2^{32})$
$k_t = 0xca62c1d6,\ pour\ t = 60, \ldots, 79.\ (0xca62c1d6 = \sqrt{10}/4.2^{32})$

À ce niveau le message est transformé d'un ensemble de 16 mots de 32 bits $(M_0, \ldots, M_{15})$ en un message étendu découpé en 80 mots de 32 bits $(W_0, \ldots, W_{79})$ suivant l'algorithme :
$\mathrm{W}_t = M_t,\ pour\ t = 0, \ldots, 15,$

$\mathrm{W}_t = (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}) <<< 1,\ pour\ t = 16, \ldots, 79.$

Avec t le numéro de l'opération (de 0 à 79) et W_t le $t^{ème}$ sous-bloc du message étendu et $<<<\ s$ représente un décalage circulaire à gauche de s bits. Alors la boucle principale est sous la forme :
Pour t variant de 0 à 79
$\mathrm{TEMP} = (\mathrm{a} <<< 5) + \mathrm{f}_t(b,c,d) + e + W_t + K_t$
e = d
d = c
c = b <<< 30
b = a
a = TEMP
La figure 2.4 illustre une opération. Après tout cela, a, b, c, d, e sont ajoutés à A, B, C, D, E respectivement et l'algorithme passe au bloc de données suivant. l'output final est la concaténation de A, B, C, D et E.
Pour une table de Hachage [8] de taille m, la collection finie H de fonctions de hachage est dite universelle si pour tout couple de textes (x, y), le nombre de fonctions telles que $H(x) = H(y)$ vaut $\frac{1}{m}$. Les fonction de hachage sont vulnérables à l'attaque des anniversaires qui vise la résistance forte aux collisions.
Les cryptosystèmes doivent être partagés entre les utilisateurs à travers le monde, de là, nous déduisons la nécessité que toute tentative de cryptage doit dépendre d'un paramètre appelé la clé. Pour assurer la sécurité des opérations cryptographiques, des principes et des lois sont posés dans ce sens [19].

2.2.5 Principe de Kerckhoffs 1883

les cryptosystèmes sont conçu pour résister face au pire des scénarios : un adversaire qui possède de grandes ressources de calcul, et qui peut accéder aux paires texte claire/texte chiffré et donc capable d'étudier la relation entre chaque paire, et qui connaît les algorithmes de chiffrement et

8. Structure informatique.

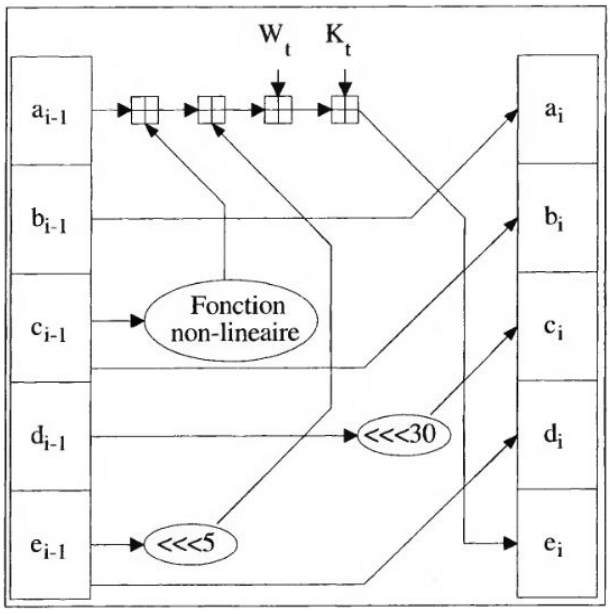


FIGURE 2.4 – Une opération de SHA [1].

de déchiffrement utilisés, il ne peut pas accéder et dévoiler un seul élément, la clé secrète et donc la sécurité d'un cryptosystème dépend uniquement de la clé. Ceci est la philosophie de conception depuis longtemps, formulé par Auguste Kerckhoffs en 1883 dont l'énoncé du principe [46],[47] :

> "La sécurité d'un cryptosystème ne doit pas dépendre sur le fait de garder secret l'algorithme cryptographique. La sécurité dépend uniquement de garder secrète la clé."

Il s'ensuit que, garder la sécurité et la confidentialité de la clé est une exigence fondamentale de chiffrement, que ce soit pour un cryptosystème classique ou quantique.
• **Loi de Moore :** Moore a formulé une loi empirique dont l'énoncé dit que la vitesse des processeurs doubles tous les 18mois. Si un cryptosystème est conçu pour préserver le secret à long terme, la clé secrète doit être suffisamment longue pour résister à la recherche exhaustive en utilisant les futures technologies [53].
• **Loi de Murphy :** S'il y a un unique trou de sécurité, l'exposition du cryptosystème assure que quelqu'un finira par le trouver. Même si cette personne est honnête, des malveillants pourraient la connaître. Nous devons garder en tête que la sécurité ne tient pas debout : les systèmes sont aussi sûrs que leur maillon le plus faible [53].

2.3 Cryptanalyse

La cryptanalyse est un ensemble de méthodes et techniques qui servent à reconstituer le texte en clair sans connaître la clé utilisée. Une cryptanalyse peut fournir soit le texte en clair, soit la clé, soit des informations supplémentaire sur le cryptosystème. Ce concept est traité en détail dans le chapitre 5.

2.4 Chiffre de Vernam

C'est un cryptosystème, malgré sa simplicité, il offre une sécurité parfaite qui a été reconnue par les spécialistes ainsi que les militants, connu sous le nom du masque jetable. Dans sa forme

classique, le masque jetable n'est rien d'autre qu'une très longue suite aléatoire de lettres, écrite sur des pages reliées ensemble pour former un bloc.
Le chiffre de Vernam a été inventé en 1917 par un ingénieur d'AT&T, Gilbert S. Vernam [55], qui pensait qu'il deviendrait largement utilisé pour le chiffrement automatique et le déchiffrement des messages télégraphiques.
Le chiffre de Vernam est un chiffre de substitution polyalphabétique appartient aux cryptosystèmes à clé secrète. Le principe de l'algorithme de chiffrement est que si une clé aléatoire est additionnée à un message, les bits de la chaîne qui en résulte sont aussi aléatoires et ne portent aucune information au sujet du message. Si nous utilisons la logique binaire, contrairement Vernam qui a travaillé avec un alphabet de 26 lettres, l'algorithme de chiffrement E peut être écrit comme

$$E_k(M) = (M_1 + k_1, M_2 + k_2, ..., M_n + k_n)\ mod\ 2,$$

où $M = (M_1, M_2, ..., M_n)$ est le message à chiffrer, et $k = (k_1, k_2, ..., k_n)$ est la clé composée de bits aléatoires. Le message et la clé sont additionnés bit à bit modulo 2, c'est à dire le ou exclusif. Le déchiffrement D de texte chiffré C est identique au chiffrement, donné par

$$M = D_k(C) = (C_1 + k_1, C_2 + k_2, ..., C_n + k_n)\ mod\ 2.$$

Pour que ce système soit inconditionnellement sûr, trois exigences sont imposées sur la clé : (1) La clé doit être aussi longue que le message, (2) elle doit être purement aléatoire, (3) elle peut être utilisé qu'une seule fois. Ceci a été démontré par Claude E. Shannon [2], qui a établi les fondements de la théorie de la communication du point de vue cryptographique. Jusqu'en 1949, lorsque son article a été publié, le chiffre de Vernam est considéré comme incassable, mais ça n'a pas été prouvé mathématiquement. Si aucune de ces conditions n'est pas respectée, la sécurité du système est compromise.
Tous cela parait idéal, et bien qu'il soit le plus robuste, il possède des inconvénients, nous citons ici quelques uns :

- Le cryptosystème devient vulnérable si la même clé est utilisée plus d'une fois, une expérience concrète est donnée par les soviétiques pendant la deuxième guerre mondiale, où le KGB (Komitet Gossoudarstvennoi Bezopasnosti, c'est le Comité pour la Sécurité de l'Etat, le service de renseignement de l'Union Soviétique) utilisaient le chiffre mais avec une réutilisation de quelques fragments de clés plusieurs fois ce qui a conduit au décryptage des messages par la NSA [24](National Security Agency, c'est le Service Central de Sécurité, un organisme gouvernemental d'Etats-Unies) ;
- La robustesse du cryptosystème n'est atteinte que si la clé est vraiment aléatoire, et les clés qui sont pseudo aléatoires mènent à une implémentation peu sûre ;
- N'est pas évident ou facile d'obtenir des séquences purement aléatoires ;
- La manière la plus sûre pour transporter la clé est la valise diplomatique, c'est ce qui n'est pas donné à des utilisateurs hors le secteur diplomatique ;
- L'émetteur et le récepteur doivent être synchronisés, si un seul bit est décalé, le massage déchiffré n'aura aucun sens. Si quelques bits sont modifiés durant la transmission, seuls ces bits seront mal déchiffrés ;
- Le masque jetable ne permet aucune authentification.

Une question qui peut traverser notre esprit est pourquoi ne pas essayer toutes les clés possibles pour décrypter un message chiffré par Vernam ? [15]
La réponse est : ce serait trop long de tester ça sur ordinateur. Par exemple, un PC de 1Ghz effectue 10^9 opérations/seconde, pour une clé à 128 bits nous avons $2^{128} \approx 3.4 * 10^{38}$ clés possibles donc il nous faut $3.4 * 10^{38}/10^{19} = 3.4 * 10^{29}$ secondes. Or l'âge de l'univers est 15 milliard$*365 * 24 * 60 * 60 = 4.7 * 10^{17}$ secondes !!

2.5 Théorie de Shannon

2.5.1 Le secret de la communication

Le but du cryptage est d'assurer le secret de la communication. Nous supposons que nous voulions communiquer ce qui signifie transmettre l'information à travers un canal. Le canal n'set pas supposé être sécurisé.

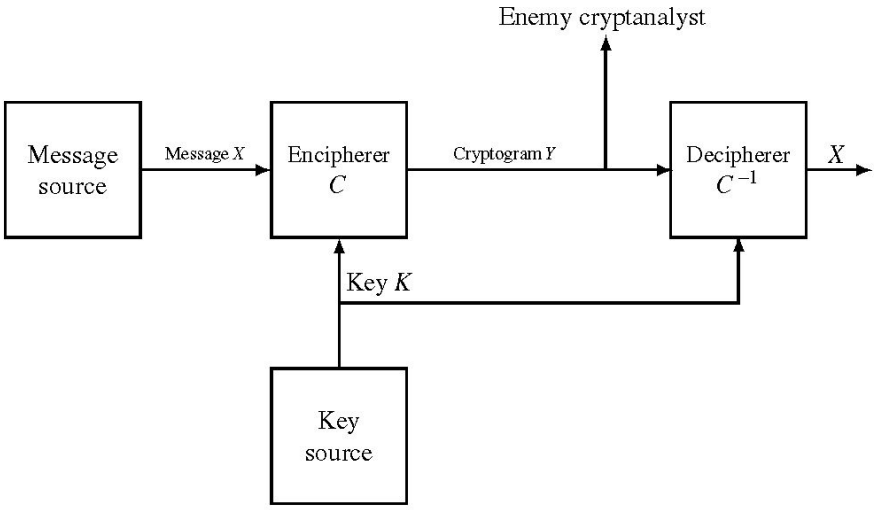


FIGURE 2.5 – Le modèle de cryptage de Shannon [2]

Suivant la théorie de Shannon, nous ne cryptons pas de messages fixes, mais des messages parvenant d'une source de texte clair (vocabulaire, l'ensemble des langues vivantes, le dictionnaire). La source de texte clair génère des textes aléatoires selon une distribution de probabilité donnée. Par exemple, avec la distribution de textes clairs en Anglais, la probabilité que le texte clair soit HELLO WORD est beaucoup plus grande qu'il soit GBWIUBOAFP [19]. Afin de transmettre un message en toute sécurité, nous devons d'abord mettre en place une clé et de la transmettre en toute sécurité. Mais, nous devons faire attention à deux points, d'abord la clé peut être un morceau très court d'information facile à protéger que le message lui-même. Alors nous pouvons l'envoyer à travers un canal diplomatique en toute sécurité. Deuxièmement la clé peut être longue (le cas de chiffre de Vernam) et le canal sécurisé (la valise diplomatique) peut ne pas être disponible tout le temps ou les délais de transmission sont plus longs (le voyage par avion), même si ce n'est pas le cas le canal est prestigieux non accessible par tout le monde. Pour résumer, la clé secrète K doit être transmise de manière sécurisée, alors nous avons besoin d'un canal sécurisé. Pour remédier à ces soucis, nous pouvons transformer tout autre canal en un canal confidentiel en faisant appel à une notion mathématique de probabilités dite l'entropie due à Claude Shannon. Dans cette optique, si un cryptosystème répond aux mesures d'entropie, alors nous considérons que nous avons un cryptosystème parfaitement sécurisé.

2.5.2 Le secret parfait

Le secret parfait signifie que la distribution à posteriori du texte clair après avoir observé le texte chiffré est égale à la distribution à priori du texte clair : la distribution conditionnelle de M sachant C est égale à la distribution originale. Formellement, pour tout m et c tels que $P(C = c) \neq 0$, nous avons $P(M = m|C = c) = P(M = m)$ [2].
Autrement dit, la connaissance de C ne donne aucune information sur M.
Ceci signifie aussi que la distribution à posteriori du texte chiffré après avoir observé le texte clair est égale à la distribution à priori du texte chiffré. Pour tout m et c tels que

$P(M = m) \neq 0$, nous avons $P(C = c|M = m) = P(C = c)$(théorème dans[19]).

Théorème 2.1 *[2] Le secret parfait est équivalent à* $H(M|C) = H(M)$.

Preuve *Sous l'hypothèse d'indépendance de* M *et* C *nous avons*

$$H(M|C) = H(M)$$
$$\Updownarrow$$
$$H(M|C) + H(C) = H(M) + H(C)$$
$$\Updownarrow$$
$$H(M, C) = H(M) + H(C)$$

à partir de l'hypothèse initaile, on obtient

$$P(M|C) = P(M).$$

Théorème 2.2 *[2] Un secret parfait implique* $H(K) \geq H(M)$.

Preuve $H(M) = H(M|C) \leq H((M, K)|C) = H(K|C) + H(M|K, C) = H(K|C) \leq H(K)$ *(La preuve se trouve dans [13]).*

Supposons que nous avons une clé de longueur infinie où nous avons besoin qu'à une longueur L_k pour chiffrer un message de longueur L_M. Un système parfait requiert

$$\log L_M \leq \log L_k,$$

par conséquent $L_M \leq L_k$ [2].

Théorème 2.3 *[19] Le chiffre de Vernam est inconditionnellement sûr.*

Preuve *Soient* M *un texte clair de longueur* n *écrit en binaire,* K *la clé de chiffrement de longueur* n $\forall i$, $1 \leq n$, k_i *est uniformément aléatoire choisi dans* $\{0, 1\}$ *avec*
$P(k_i = 0) = P(k_i = 1) = \frac{1}{2}$.
Pour tout m *et* c *nous avons*

$$P(M = m, C = c) = P(M = m, K = m \oplus c) = P(M = m) * P(K = m \oplus c) = P(M = m) * 2^{-n}$$

Par sommation sur touts les m *nous obtenons* $P(C = c) = 2^{-n}$.
Nous avons $P(M|C) = \frac{P(C,M)}{P(C)} = \frac{P(M)*2^{-n}}{2^{-n}} = P(M)$.
D'où, on déduit que $P(M = m|C = c) = P(M = m)$ *pout tout* m *et* c. *Par conséquent Vernam fournie une sécurité parfaite [13].*

Conclusion

Garder la confidentialité des communications était toujours un besoin et un objectif. Depuis des milliers d'années la cryptographie à tenter de protéger ces deux piliers qui ont mené à sa transformation d'un art en une science face aux attaques successives de la cryptanalyse, jusqu'a l'arrivée du chiffre de Vernam rapportant avec lui la sécurité parfaitement sûre avec un inconvénient majeur la nécessité de distribuer une clé secrète aussi longue que le message à chiffrer. Ce chiffre a trouvé jusqu'à présent des applications principalement dans les services militaires et diplomatiques.
La difficulté de la distribution de clés secrètes peut être retirée en vertu de la distribution quantique de clés comme nous le verrons dans le chapitre suivant. D'où le chiffre de Vernam fournie une valeur inestimable en raison de sa capacité à assurer la sécurité inconditionnelle et la facilité d'utilisation.

3

Cryptographie Quantique

"I think I can safely say that no one understands quantum mechanics"
Richard Feynman

Contents

Introduction

L'information et les communications sont les piliers de nos sociétés modernes. L'information possède une valeur intrinsèque qui suscite bien des convoitises à tel point qu'il est souvent nécessaire de la protéger.
Les systèmes informatiques fonctionnent dans un environnement distribué où l'échange de données joue un rôle essentiel, de sorte que l'écoute des lignes de communications constitue une menace potentielle extrêmement sérieuse pour la confidentialité des données échangées. Il est par exemple facile d'écouter les lignes de communications qui passent par des câbles en cuivre et même par fibres optiques. Donc les utilisateurs des lignes de communications ne peuvent pas se protéger contre ce type d'attaques simplement en renforçant leurs lignes de défense locales ; ils doivent aussi protéger l'information envoyée.
Le problème de la confidentialité de l'information a été résolu par la cryptographie. Le certificat du fait que le chiffre de Vernam est inconditionnellement sûr, a transformé le problème de garantir le secret de l'information en un problème de distribution de la clé secrète utilisée dans le processus de chiffrement entre deux parties.
Jusqu'aux années 80, un seul moyen de distribuer la clé secrète à part la main à la main, été d'utiliser des algorithmes dont la sécurité est basée sur la complexité computationnelle. Les clés générées par tels algorithmes sont raisonnablement secrètes mais pas inconditionnellement secrètes. La cryptographie quantique est née au début des années soixante-dix quand Stephen Wiesner a écrit "Conjugate Coding" [4] en décrivant le fondement de ce domaine. Cependant, Charles H. Bennett (qui connaissait l'idée de Wiesner) et Gilles Brassard ont pris le sujet en

1984 [5] où ils présentent au monde le premier protocole quantique de distribution de clé publique dont la sécurité est inconditionnelle car la confidentialité se base sur des impossibilités imposées par les lois de la physique [6]. Ce protocole a été mis en œuvre en 1989 en faisant appel aux efforts de F. Bessette, L. Salvail et J. Smolin, une description complète du prototype a été publiée en 1991 [7].
Une explication visuelle du concept quantique appliqué à la cryptographie peut être illustrée par l'exemple suivant, si la clé est inscrite sur une balle de tennis, il est possible de la rattraper, lire la clé et de la renvoyer, ni vu ni connu. Dans ce cas l'émetteur et le récepteur ignorent s'il y a eu lieu un espionnage ou non. Mais si la clé est inscrite sur une bulle de savon, la rattraper signifie la détruire. La fragilité d'états quantiques, dans ce cas les bulles de savon, et l'impossibilité de les copier garantissent la sécurité inconditionnelle des protocoles de distribution de clé quantiques. Pour désigner la distribution quantique de clé, nous utilisons l'abréviation Anglaise QKD Quantum Key Distribution qui est devenu un terme universel.

Remarque 3.1 Les figures qui ne possèdent pas de référence sont prises de Wikipédia.

3.1 Aperçu sur la mécanique quantique

La physique quantique signifie littéralement physique des quanta (pluriel latin de quantum qui signifie quantité) ce mot apparaît dans le registre de la physique en 1900 grâce à l'Allemand Max Planck qui a postulé l'idée originale selon laquelle les échanges d'énergie entre la lumière et la matière ne peuvent se faire que par paquets discontinus que l'on appelle les quanta.
A la fin du $19^{ème}$, siècle James Maxwell définit la lumière comme étant un faisceau d'ondes électromagnétiques se déplaçant à vitesse constante dans le vide $C = 3.10^8\ m/s$.

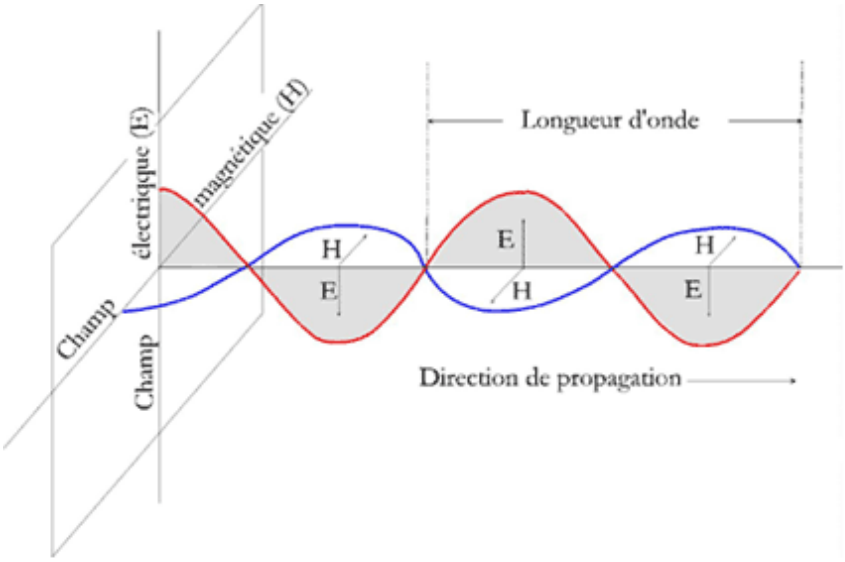


FIGURE 3.1 – L'onde lumineuse

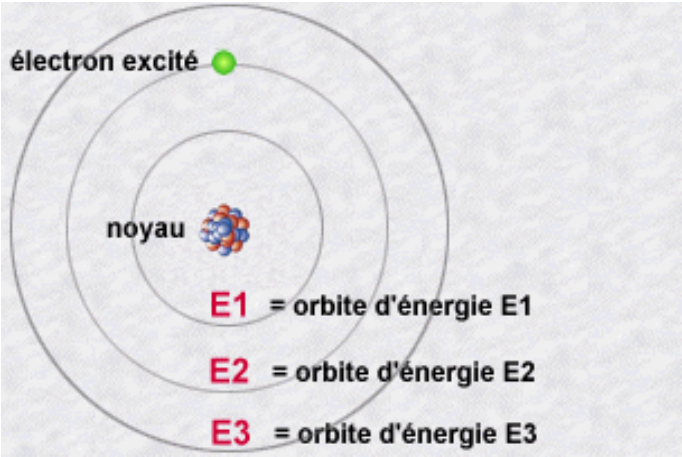


FIGURE 3.2 – Electron excité [21].

En 1905, Albert Einstein soutient que l'énergie de la lumière est en quelque sorte granuleuse, ces grains d'énergie seront appelés Photon en 1926, cette nouvelle particule immatérielle et sans masse firent l'objet d'énormes recherches dans les quelques années suivantes.
Chaque photon d'un rayonnement (lumière, ondes radios, rayons X...) est porteur d'un quantum d'énergie caractéristique de sa fréquence (fréquence de la lumière = couleur).
La physique classique distingue deux sortes d'entités fondamentales :
– Les corpuscules, qui sont des sortes de billes microscopiques.
– Les ondes, qui se propagent dans l'espace un peu comme le mouvement d'une vague sur la mer.
La physique quantique ne retient pas cette classification, les objets qu'elle considère ne sont ni des corpuscules ni des ondes, mais autre chose. Considérons l'analogie suivante : regarder sous deux angles différents, un cylindre nous apparait tantôt comme un cercle, tantôt comme un rectangle. Pourtant il est ni l'un ni l'autre. Ainsi il en est du photon, d'électron ou de toute particule élémentaire dont l'image corpusculaire ne serait qu'une facette d'une entité plus complexe.
La physique quantique permet de mieux comprendre comment la lumière est émise par la matière. Le modèle de l'atome de Niels Bohr explique le mécanisme de l'émission de la lumière par un atome.
Cette émission s'explique par le saut qu'effectue un électron d'une orbite $E2$ à une orbite $E1$. Pendant ce saut vers l'orbite moins énergétique (une orbite plus intérieure), l'électron va céder une partie de son énergie sous forme d'un photon émis vers l'extérieur. D'où l'énergie de photon sera $E2 - E1 = h.\nu$
Où h est la constante de Planck, $h = 6.6210^{-34}$ $joule.seconde$, et ν est la fréquence de la lumière (ou photon). Cette fréquence est le nombre d'oscillations de l'onde lumineuse par seconde, elle se mesure en Hertz. Plus la fréquence de la lumière est élevée, plus son énergie est importante et plus la couleur tend vers le bleu (voir Fig.3.4). Un électron faisant un grand saut d'une orbite atomique à une autre, émettra un photon d'autant plus énergétique et donc de fréquence d'autant plus élevée.
Inversement, l'électron d'un atome pourra absorber un photon d'énergie donnée ainsi sauter d'une orbite peu énergétique à une orbite plus énergétique : il sera ainsi excité. C'est en désexcitant qu'il pourra réémettre un photon.
Chaque couleur de la lumière (voir Fig.3.5) est en fait une fréquence particulière (et donc un niveau d'énergie) de photon.
Comme toute particule quantique élémentaire, le photon possède un spin qui est un entier égale à 1. Le spin est une propriété quantique intrinsèque associé à chaque particule, caractéristique de la nature de la particule [8]. Le spin est la rotation d'une particule élémentaire autour

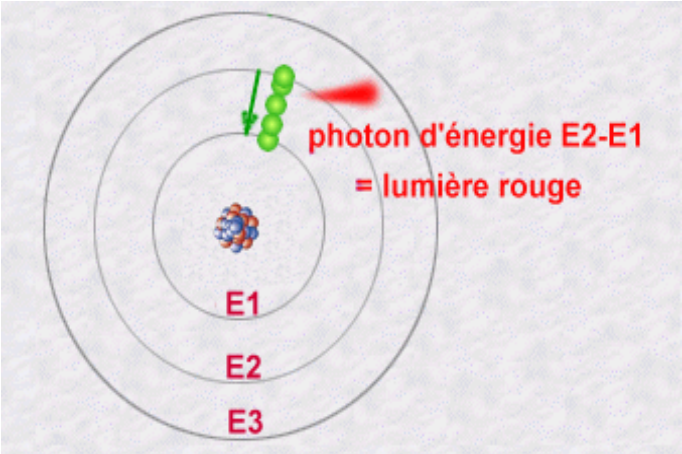


FIGURE 3.3 – Saut de l'électron [21].

d'elle-même, c'est un phénomène qui n'a pas d'analogue en mécanique classique, nous pouvons imaginer une simulation de ce phénomène par la rotation de la terre autour d'elle-même et autour du soleil, l'électron aussi fait une rotation autour lui-même et autour du noyau. Le spin génère un champ magnétique ce qui rend l'électron par exemple un aimant, il fait tourner l'électron uniquement dans deux directions, soit dans le sens des aiguilles d'une montre soit dans le sens inverse c'est pour cela qu'il ne prend que deux valeurs $+\frac{1}{2}$ et $-\frac{1}{2}$.
Les ondes électromagnétiques sont des ondes transverses c'est-à-dire que les vecteurs champ électrique et champ magnétique sont partout perpendiculaires à la direction de propagation de l'onde [40].
Les spécialistes ont choisi de repérer la direction du champ électrique qu'ils considèrent par convention, direction de polarisation de l'onde. D'où l'axe de polarisation de l'onde est perpendiculaire à son axe de propagation (Fig.3.1).

Définition 3.1 *[40] Si la direction de propagation $\overrightarrow{u}$ est unique dans tout l'espace et à tout instant, alors la valeur de la grandeur qui se propage dépend du temps mais ne dépend pas du point considéré dans un plan (P) quelconque orthogonal à la direction de propagation.*
Un tel plan (P) est appelé plan d'onde, et une telle onde est appelée onde plane. $\overrightarrow{u}$ unitaire dans le sens de la propagation de l'onde.
Le trièdre $(\overrightarrow{E}, \overrightarrow{H}, \overrightarrow{u})$ est direct[1] *:*

$$\begin{array}{ccc} \overrightarrow{E} & \perp & \overrightarrow{u} \\ \overrightarrow{H} & \perp & \overrightarrow{u} \\ \overrightarrow{E} & \perp & \overrightarrow{H} \end{array}$$

Dans ce cas, il y a, à tout instant, une direction de vibration de $\overrightarrow{E}$ et $\overrightarrow{H}$. Nous distinguons plusieurs possibilités [40] :
– Soit cette direction de vibration évolue au cours du temps, où la direction de la vibration tourne au cours du temps ; on parle de polarisation rotatoire, qui peut elle-même être circulaire (si le vecteur champ reste constant en norme)

1. On appelle trièdre direct un triplet $(v1, v2, v3)$ de vecteurs de l'espace linéairement indépendants dont l'orientation est donné par la règle du tire-bouchon.

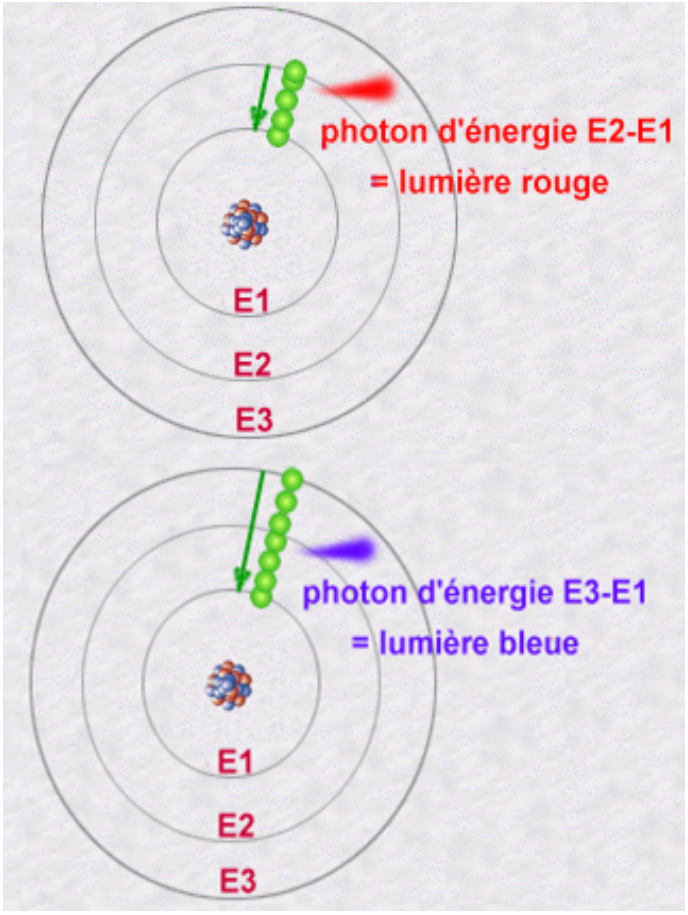


FIGURE 3.4 – Saut plus énergétique de l'électron [21]

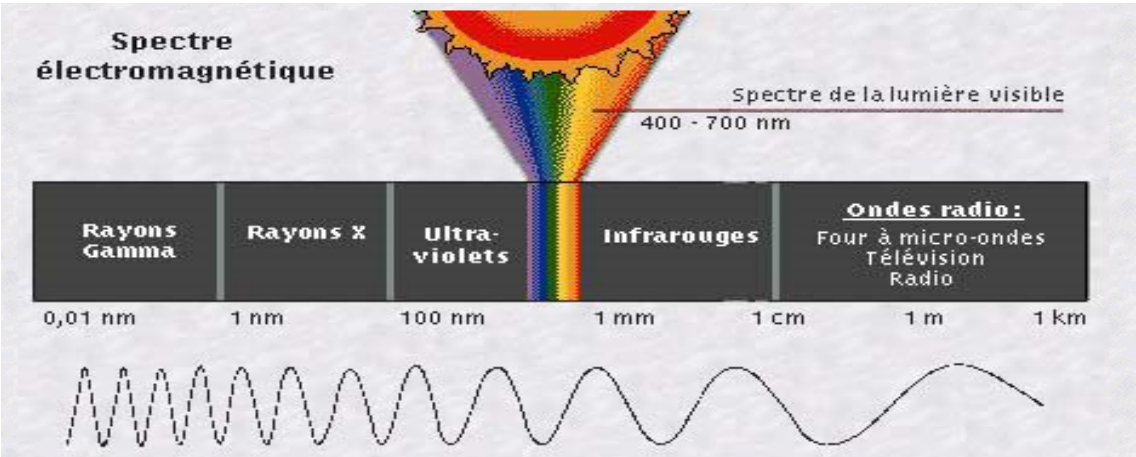
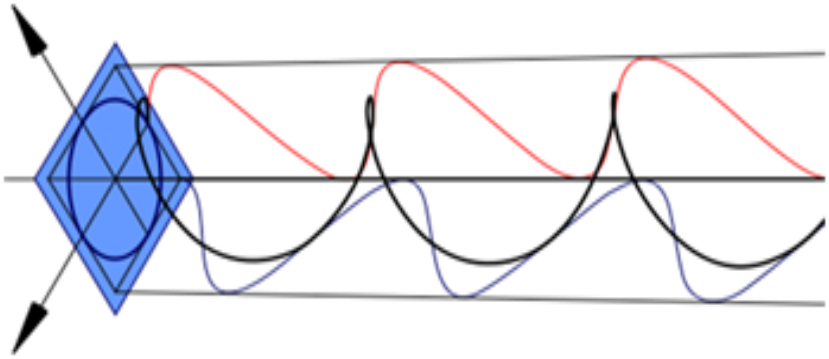
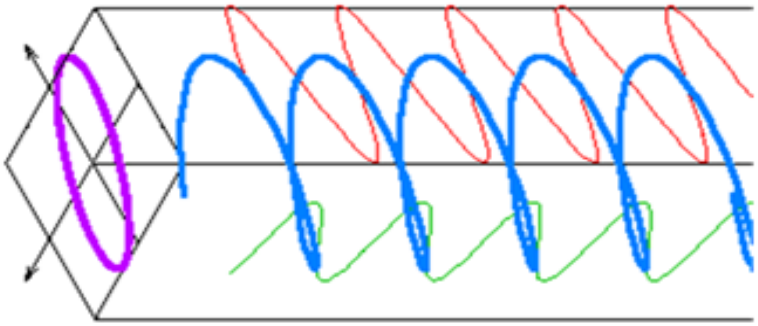


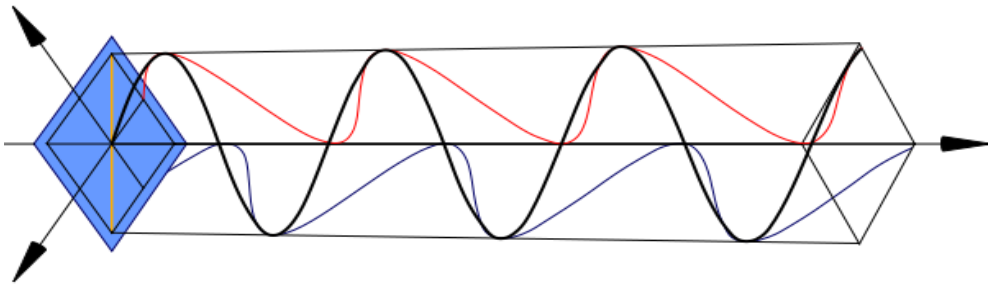
FIGURE 3.5 – Le spectre [21].



ou elliptique (si le vecteur champ tourne en décrivant une ellipse).



– Soit cette direction de vibration est unique et reste fixée ; les champs $\overrightarrow{E}$ et $\overrightarrow{H}$ gardent une direction déterminée au cours de la propagation. L'onde est dite alors polarisée rectilignement. Cette situation est celle d'une onde fabriquée par un dispositif polariseur.



Polariser un photon c'est fixer l'orientation de son champ électromagnétique. Pour ce faire, il suffit de faire passer des faisceaux de lumière à travers un appareil polarisant dans la direction visée [20]. Par exemple nous pouvons utiliser un filtre polarisant ou un cristal de calcite [29].

> **Note :** La polarisation de la lumière peut se faire par : réflexion, double réfraction ou dispersion. Dans la suite du document, nous considérons que la polarisation obtenue par double réfraction.

Soit un faisceau lumineux sous forme d'une onde plane polarisée rectilignement, qui passe par un polariseur (un cristal de calcite par exemple) parallèle à l'axe Oy (voir Fig.3.7). θ l'angle que fait la polarisation avec l'axe polariseur c'est-à-dire que si le photon est polarisé selon un angle γ et que le filtre est orienté selon un angle β, alors $\theta = \gamma - \beta$. L'onde sortante est alors polarisée selon l'axe du polariseur Oy. Le faisceau lumineux est ainsi séparé en un faisceau polarisé suivant Ox

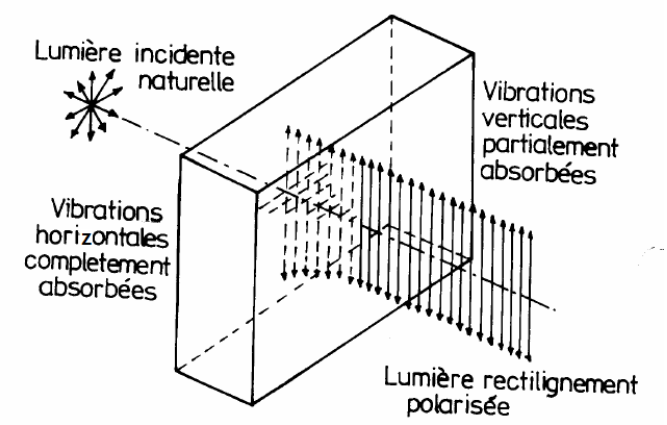


FIGURE 3.6 – Polariser un photon rectilignement

et un faisceau polarisé selon Oy, et où le vecteur intensité champ électrique $\overrightarrow{E}$ peut être remplacé par ses deux composantes $E_x = \overrightarrow{i}\, E \sin\theta$ perpendiculaire sur la direction de polarisation et $E_y = \overrightarrow{j}\, E \cos\theta$ parallèle avec elle. En outre, l'intensité régis par la loi de Malus, $I = I_0 \cos^2\theta$ où I et I_0 désignent respectivement l'intensité incidente et sortante, et est séparée selon les deux axes. D'où les intensités étant respectivement $I \sin^2\theta$ et $I \cos^2\theta$ [41].
D'où, il s'ensuit que :

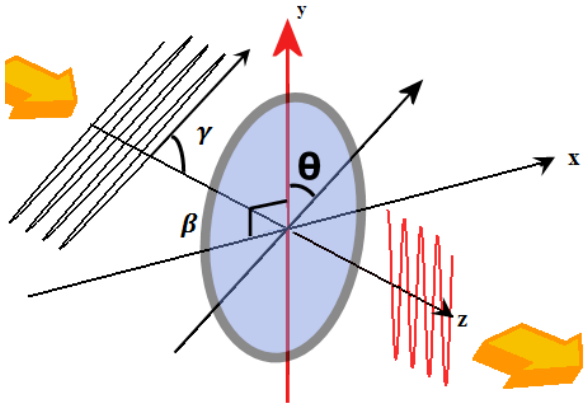


FIGURE 3.7 – L'angle de polarisation du photon fait un angle θ avec l'angle d'orientation du filtre.

- Si les photons du faisceau sont polarisés parallèlement à l'angle d'orientation du filtre, alors ces photons seront transmis sans changement de polarisation.
- Si les photons sont polarisés perpendiculairement à l'angle d'orientation du filtre, alors ces photons seront absorbés.
- Si les photons sont polarisés selon une direction intermédiaire, alors ces photons seront transmis avec probabilité $\cos^2(\theta)$. Si les photons sont transmis, alors leur nouvelle polarisation correspond à l'angle d'orientation du filtre ce qui signifie que la polarisation initiale des photons est complètement perdue même si les photons rencontrent un autre filtre polariseur orienté selon un autre angle ; pour la raison que les photons transmis, passant déjà à travers un filtre polariseur d'angle β, émergent exactement avec une polarisation d'angle β tout en perdant la mémoire à propos de leur polarisation initiale α.

À partir de ce dernier point, nous constatons que :

1. Plus la polarisation du photon incident au filtre est près de l'angle d'orientation du filtre plus la probabilité que le photon soit transmis est grande.
2. Si $\theta = 0^{\circ}$, alors le photon est transmis avec certitude : $\cos^2(0) = 1$.
3. Si $\theta = 90^{\circ}$, alors le photon est certainement absorbé : $\cos^2(90) = 0$ ou de façon complémentaire $1 - \cos^2(\theta) = \sin^2(\theta) = \sin^2(90) = 1$.
4. Le comportement est complètement aléatoire, c'est-à-dire le photon est transmis ou absorbé avec probabilité $\frac{1}{2}$, soit lorsque $\theta = 45^{\circ}$ ou $\theta = 135^{\circ}$.

3.2 L'approche quantique

En théorie de l'information et en cryptographie, il est connu et il est garanti que les communications numériques peuvent toujours être passivement surveillées ou copiées. En revanche, quand l'information est encodée en états quantiques non-orthogonaux, tels que les photons avec les directions de polarisation $0, 45, 90$ et 135 degrés, fournit un canal de communication dont les transmissions, en principe, ne peuvent pas être lues ou copiées de manière fiable par un espion ignorant de certaines informations clés utilisées dans le design de la transmission. L'espion ne peut même pas obtenir des informations partielles sur une telle transmission sans provoquer des perturbations détectables par les utilisateurs légitimes du canal. L'intervention de la mécanique quantique en mathématique et en informatique a connu une réussite incroyable, ceci remonte au début du $20^{ème}$ siècle ce qui a permis l'élaboration de la théorie de l'information quantique basée sur la superposition linéaire et l'intrication quantique. Dans les communications classiques, il est toujours possible d'opérer des attaques passives sur le flux d'informations échangées en effectuant une déviation du flux et réaliser des mesures dessus. Les cryptosystèmes quantiques éliminent cet effet en codant chaque bit d'information en un objet quantique individuel, tel qu'un photon simple. Un photon simple ne peut pas être dupliqué, copié ou amplifié sans présenter des perturbations discernables [15].

3.2.1 Etat quantique

Un état est une description complète d'un système physique. En mécanique quantique, un état est un vecteur dans l'espace de Hilbert (sur C)[8].
Les vecteurs seront notés $|\psi\rangle$ appelés *ket* et ils sont de norme 1 : $\langle\psi|\psi\rangle = 1$ [11].

3.2.2 L'unité de l'information quantique

Nous pouvons stocker l'information dans des photons en considérant que la polarisation horizontale (polarisation linéaire suivant Ox) est représentée par $|0\rangle$ et la polarisation verticale (polarisation linéaire suivant Oy) est représentée par $|1\rangle$. La notation $|.\rangle$, appelée notation de Dirac, est la convention utilisée pour décrire des états quantiques. Une information stockée de cette manière prend le nom de bits quantiques ou qubits.
Nous considérons $|0\rangle$ et $|1\rangle$ comme deux vecteurs orthonormaux dans l'espace de Hilbert à 2 dimensions (vecteurs de base de l'espace de Hilbert) [10] ; tel que

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{3.1}$$

$|0\rangle$ et $|1\rangle$ sont dits *états propres* du système.
Le produit scalaire de deux vecteurs $|\psi\rangle$ et $|\phi\rangle$ est noté par $\langle\psi||\phi\rangle$; couramment écrit sous la forme $\langle\psi|\phi\rangle$.
Un bit classique est toujours 0 ou 1. La différence essentielle dans les qubits est la capacité d'être les deux $|0\rangle$ et $|1\rangle$, ce phénomène est connu comme la superposition des deux états. Par exemple, en additionnant l'état horizontal et l'état vertical, le photon peut être polarisé dans la direction

diagonale. Géométriquement, nous pouvons décrire cette direction comme étant la combinaison de ces deux états de la base. Tout état de polarisation pourra se décomposer suivant cette base, d'où quand une polarisation diagonale de photon est mesurée dans la direction linéaire, le résultat est horizontal ou vertical, mais choisi d'une manière aléatoire. L'état $|\psi\rangle$ d'un *qubit simple* en superposition est

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{3.2}$$

où $|\alpha|^2$ et $|\beta|^2$ sont les probabilités de mesurer $|0\rangle$ et $|1\rangle$ respectivement. Selon la mécanique quantique, α et β, se réfèrent aux amplitudes et peuvent être des complexes. Par la loi de la probabilité, ils doivent satisfaire $|\alpha|^2 + |\beta|^2 = 1$.
Soit un photon polarisé avec un angle γ, le qubit associé à ce photon est donné par $q = \cos(\gamma)|0\rangle + \sin(\gamma)|1\rangle$ qui peut être représenté sous forme vectorielle comme suit $q = (\cos(\gamma), \sin(\gamma))$. L'ensemble de tous ces vecteurs de norme 1 forme un espace de Hilbert de dimension 2.
Nous pouvons préparer des états quantiques aléatoires à partir de plusieurs états purs [2], nous parlons alors d'état *quantique mixte*. Une représentation d'un état quantique qui peut tenir compte des états mixtes est la matrice de densité. La matrice de densité d'un état pur $|\psi\rangle$ est donnée par :

$$\rho = |\psi\rangle\langle\psi|,$$

où $\langle\psi|$ est le transposé conjugué de $|\psi\rangle$ (voir page 5).
Supposons qu'un état est préparé à partir des n états purs suivants $\{|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_n\rangle\}$ avec les probabilités respectives $\{p_1, p_2, ..., p_n\}$, alors la matrice de densité de l'état mixte est donné par

$$\rho = \sum_{i=1}^{n} |\psi_i\rangle\langle\psi_i|. \tag{3.3}$$

3.2.3 Principe d'incertitude d'Heisenberg

Une autre caractéristique des objets quantiques est la suivante : en mesurant la position d'un quanta, soit un photon ou un électron ou autre chose, nous ne pouvons pas connaître sa vitesse d'une manière exacte et vice versa, mesurer la vitesse et la position en même temps n'est pas évident. À un instant donné, l'interaction du quanta avec l'appareil de mesure d'une grandeur physique, perturbe immédiatement les informations portées sur les autres grandeurs. C'est ça le principe d'incertitude d'Heisenberg.
Les mesures exactes exercées sur les quanta détruisent leurs propriétés ondulatoires et font disparaître l'interférence et la superposition quantique [45]. Le principe ne se limite pas à la position et la vitesse, il affecte toute paire conjuguée d'états : ce sont les états où les mesures ne sont pas commutatifs ; mesurer A puis B ne donne pas le même résultat que mesurer B puis A. Polkinghorne [44] déclare que "les observables viennent en paires qui épistémologiquement les uns détruisent les autres" et que "cette demi-connaissance est une caractéristique quantique". Par conséquent, le principe d'incertitude est à la base de plusieurs effets du monde quantique.

3.2.4 Intrication quantique

Nous avons vu que les qubits simples peuvent être en état de superposition, n'importe quel nombre de qubits peuvent être en état de superposition formant un system quantique. Un système quantique à n-qubits peut être exprimé comme étant un vecteur d'état dans l'espace de Hilbert de dimension 2^n. Si le vecteur d'état de ce système est inexprimable comme étant le produit tensoriel des vecteurs d'états de chaque qubit, les qubits sont dit de former un état intriqué.

Remarque 3.2 Dans ce mémoire, le mot "système quantique" réfère à un système **d'état de photon polarisé**.

2. Par la suite, nous revenons à cette notion.

L'intrication ne possède pas d'analogue classique, puisque les collections de bits classiques dans n'importe quel état sont toujours exprimables en spécifiant l'état de chaque bit individuellement, alors que ceci n'est pas vrai pour les collections de bits quantiques.
Supposons que nous avons deux qubits aux états purs suivants : $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ et $|\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$ respectivement. Le vecteur représentant le système total, ou l'état conjoint est donné par $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$. Ceci montre que nous ne sommes pas devant un état d'intrication car le vecteur $|\psi\rangle$ peut être décomposé en produit tensoriel des vecteurs d'état des deux qubits [10] :

$$\begin{aligned}
|\psi\rangle &= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle \\
|\psi\rangle &= \alpha_1\alpha_2|0\rangle \otimes |0\rangle + \alpha_1\beta_2|0\rangle \otimes |1\rangle + \beta_1\alpha_2|1\rangle \otimes |0\rangle + \beta_1\beta_2|1\rangle \otimes |1\rangle \\
|\psi\rangle &= (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) \\
|\psi\rangle &= |\psi_1\rangle \otimes |\psi_2\rangle
\end{aligned}$$

Par contre, l'état $|\psi\rangle = \frac{1}{2}(|00\rangle + |11\rangle)$ est un état intriqué [28].
L'intrication est une ressource principale dans le traitement de l'information quantique. Ce phénomène possède d'énormes applications en cryptographie quantique et dans le domaine de la téléportation quantique, où les spécialistes devraient être en mesure d'exprimer la quantité d'intrication dans un état quantique d'un système donné. Cependant, la physique quantique prédit les corrélations entre les objets quantiques constituant le système, et de plus il n'existe aucun accord général sur la façon de quantifier l'intrication.

3.2.5 Opérations unitaires

Dans cette section, nous allons discuter les manipulations des qubits, commençant d'abord par les qubits simples puis les qubits mixtes. Pour le calcul classique, le sujet des opérations appliquées sur un bit est très limité. Un bit simple doit être 0 ou 1. Peu importe que le bit soit 0 ou 1, la seule opération que peut subir ce bit est la conversion de 0 en 1 et 1 en 0, c'est le retournement du bit (bit-flip operation).
Les états à qubit simple peut subir une gamme plus large de transformations mais sous une seule restriction que toute opération valide sur un système fermé doit être linéaire (en réalité représentée par un opérateur unitaire), donnée par le postulat fondamental de la mécanique quantique [10](Nous avons vu dans §1.1 que l'opérateur $\widetilde{A}$ est unitaire si $\widetilde{A}\widetilde{A}^\dagger = \widetilde{A}^\dagger\widetilde{A} = \mathbb{1}$ où $\mathbb{1}$ est la matrice identité donnée par $\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$).
Un opérateur $\widetilde{A}$ convertit un état $|\psi\rangle$ à $\widetilde{A}|\psi\rangle$. L'opération sur un état générique est donnée par :

$$\widetilde{A}(\alpha|0\rangle + \beta|1\rangle \quad = \quad \alpha\widetilde{A}|0\rangle + \beta\widetilde{A}|1\rangle. \tag{3.4}$$

Quatre opérateurs importants sont les matrices de Pauli. Une matrice est la matrice d'identité, les trois autres sont :

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{3.5}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{3.6}$$

$$Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}. \tag{3.7}$$

Pour observer le comportement de ces quatre matrices, nous regardons leur action sur les états de base $|0\rangle$ et $|1\rangle$ définis en Eq.3.1. La matrice identité $\mathbb{1}$ laisse ces états inchangés.
L'opérateur X convertit $|0\rangle$ en $|1\rangle$ et $|1\rangle$ en $|0\rangle$, cet analogue au retournement de bit classique. Ainsi, X est appelé l'opérateur de retournement de bit pour les états quantiques [34].

L'opérateur Z laisse $|0\rangle$ intact mais convertit $|1\rangle$ en $-|1\rangle$. Le signe est une fonction inconnue pour le bit classique, elle est appelée une phase. Z est appelé l'opérateur de retournement de phase (phase flip operator) pour les états quantiques [34].
L'opérateur $Y = iXZ$ est une combinaison de retournement de bit et de phase.
Une autre opération est très importante aussi dans le domaine de l'information quantique est l'opérateur de Hadamard [34]

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{3.8}$$

Il prend à la fois $|0\rangle$ et $|1\rangle$ à des superpositions

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{3.9}$$

$$H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle. \tag{3.10}$$

Très souvent ces états sont notés

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{3.11}$$

$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle. \tag{3.12}$$

En ce qui concerne les qubits mixtes, la description générale pour leur évolution est donnée par un superopérateur. Un superopérateur O transforme la matrice de densité ρ (voir Eq.3.3) en $O(\rho)$ [33] comme suit :

$$O(\rho) = \sum_{k=1}^{K} E_k \rho E_k^{\dagger}.w \tag{3.13}$$

E_K est appelé opérateur de Kraus vérifiant

$$\sum_{K} E_K E_K^{\dagger} = \mathbb{1}. \tag{3.14}$$

3.2.6 Observable et Mesure quantique

Afin d'effectuer des opérations de mesure en mécanique quantique pour des valeurs d'un paramètre physique (position, vitesse, ...), nous introduisons la notion d'observable. À chaque grandeur physique A, il est toujours possible d'associer une observable $\widetilde{A}$ qui est un opérateur linéaire hermitien agissant sur les vecteurs d'états d'un espace de Hilbert [11].
Nous considérons un opérateur auto-adjoint $\widetilde{A}$ de dimension finie n ($n \leq dimH$), l'ensemble des valeurs propres [3] $\{\lambda_i,\ i = 1, 2, \ldots, n\}$, les vecteurs propres normalisés $|v_{\lambda_i}\rangle$ correspondants

$$\widetilde{A}|v_{\lambda_i}\rangle = \lambda_i |v_{\lambda_i}\rangle, \tag{3.15}$$

et rappelons que $\lambda_i \in \mathbb{R},\ \forall i,\ i = 1, 2, \ldots n$ et que $|v_{\lambda_i}\rangle$ et $|v_{\lambda_j}\rangle$ sont orthogonaux pour $i \neq j$.
D'après le théorème spectral dû à Frédéric Brezis [35], l'ensemble $|v_{\lambda_i}\rangle$ des vecteurs propres orthonormés de l'opérateur auto-adjoint $\widetilde{A}$, forme une base hilbertienne de H. Par conséquent, tout vecteur $|\psi\rangle$ peut être décomposé sur cette base comme suit

$$|\psi\rangle = \sum_{i=1}^{n} \alpha_i |v_{\lambda_i}\rangle, \tag{3.16}$$

3. Pour simplicité, nous nous restreignions au cas où les valeurs propres ne sont pas dégénérées.

avec $\alpha_i = \langle v_{\lambda_i}|\psi\rangle$. Les états s'exprimant avant la mesure sous cette forme sont dits *états propre ou pur* . En outre $\widetilde{A}$ possède une décomposition spectral et il peut être écrit comme suit

$$\widetilde{A} = \sum_{i=1}^{n} \lambda_i |v_{\lambda_i}\rangle\langle v_{\lambda_i}|, \tag{3.17}$$

d'où

$$\widetilde{A} = \sum_{i=1}^{n} \lambda_i P_{\lambda_i}. \tag{3.18}$$

Pour spécifier complètement l'état arbitraire d'un qubit, une infinité d'informations, en général, est nécessaire ; il faut préciser les valeurs exactes des nombres complexes α et β de l'Eq. 3.2. Néanmoins, en raison de la nature des mesures quantiques, uniquement peu d'informations peuvent être extraites d'un qubit. Donc, les valeurs exactes de α et β d'un état inconnu d'un qubit ne peuvent pas être jamais lues avec certitude.
Le formalisme des mesures quantiques définit la quantité d'informations qui peuvent être obtenues sur un ensemble de qubits, avec un système de mesure spécifique. Il est à noter qu'en mécanique quantique, les mesures sont la seule façon permettant d'acquérir une connaissance sur un système physique auparavant inconnu.
Notons que la valeur moyenne λ d'un opérateur $\widetilde{A}$ dans l'état $|\psi\rangle$ est définie par [11] :

$$\langle\lambda\rangle = \langle\psi|\widetilde{A}|\psi\rangle. \tag{3.19}$$

Si $\widetilde{A}$ est auto-adjoint, la valeur moyenne de $\widetilde{A}$ est réelle : $\langle\lambda\rangle = \overline{\langle\lambda\rangle}$.

Soit maintenant $|\psi\rangle$, l'état dans lequel se trouve le système au moment où l'on effectue la mesure de l'observable $\widetilde{A}$. Les seules résultats possibles de la mesure de $|\psi\rangle$ par $\widetilde{A}$ sont les valeurs propres λ_i de $\widetilde{A}$ [8]. Notons $\widehat{P}_{\lambda_i}$ l'opérateur de projection sur le sous-espace associé à la valeur propre λ_i. La probabilité de trouver la valeur λ_i lors d'une mesure de $\widetilde{A}$ est :

$$P(\lambda_i) = \|\widehat{P}_{\lambda_i}|\psi\rangle\|^2 = \langle\psi|\widehat{P}_{\lambda_i}|\psi\rangle. \tag{3.20}$$

Immédiatement après la mesure ayant donné λ_i, l'état du système $|\grave{\psi}\rangle$ est

$$|\grave{\psi}\rangle = \frac{\widehat{P}_{\lambda_i}|\psi\rangle}{\|\widehat{P}_{\lambda_i}|\psi\rangle\|}. \tag{3.21}$$

Pour effectuer des mesures d'une observable, il faut choisir une base de vecteurs, d'où toute paire de vecteurs orthogonaux dans l'espace de Hilbert est candidate pour constituer cette base. Les choix communs sont les vecteurs propres des opérateurs de Pauli (section précédente), par exemple, les vecteurs propres associé à l'opérateur Z : $\{|0\rangle, |1\rangle\}$, les vecteurs propres associés à l'opérateur X : $\{|+\rangle, |-\rangle\}$, qui sont le résultat de l'application de l'opérateur de Hadamard au vecteurs de la base Z et les vecteurs propres associés à l'opérateur Y :
$\{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$.

3.2.7 Sphère de Bloch

Nous avons vu qu'un état quantique d'un système à deux niveaux [4] peut être représenté comme une superposition des deux états propres du système (Eq3.2). Alternativement, nous pouvons le représenter géométriquement à travers les coordonnées sphériques comme suit [38] :

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \exp i\varphi \sin\frac{\theta}{2}|1\rangle \tag{3.22}$$

4. Système quantique décrit par un espace vectoriel complexe de dimension deux.

Où $0 \leq \theta \leq \pi$, $0 \leq \varphi \leq 2\pi$. Les paramètres θ et φ spécifient de manière unique un point sur la sphère unité de $\mathbb{R}^3$ ayant pour coordonnées sphériques

$$\begin{aligned} x &= \sin 2\theta \times \cos\varphi, \\ y &= \sin 2\theta \times \sin\varphi, \\ z &= \cos 2\theta. \end{aligned}$$

Nous parlons alors de représentation géométrique des états quantiques, ce qui permet de visualiser le système et son évolution.
Le long des axes X,Y et Z se trouve les vecteurs propres associés aux opérateurs X,Y et Z. Tout vecteur normalisé dans l'espace de Hilbert à deux dimension se situe dans cette sphère ; en fait tous les états purs peuvent être représentés par des vecteurs atteignant la surface de la sphère. En revanche tous les états mixtes peuvent être représentés par des vecteurs de longueurs moins de l'unité.

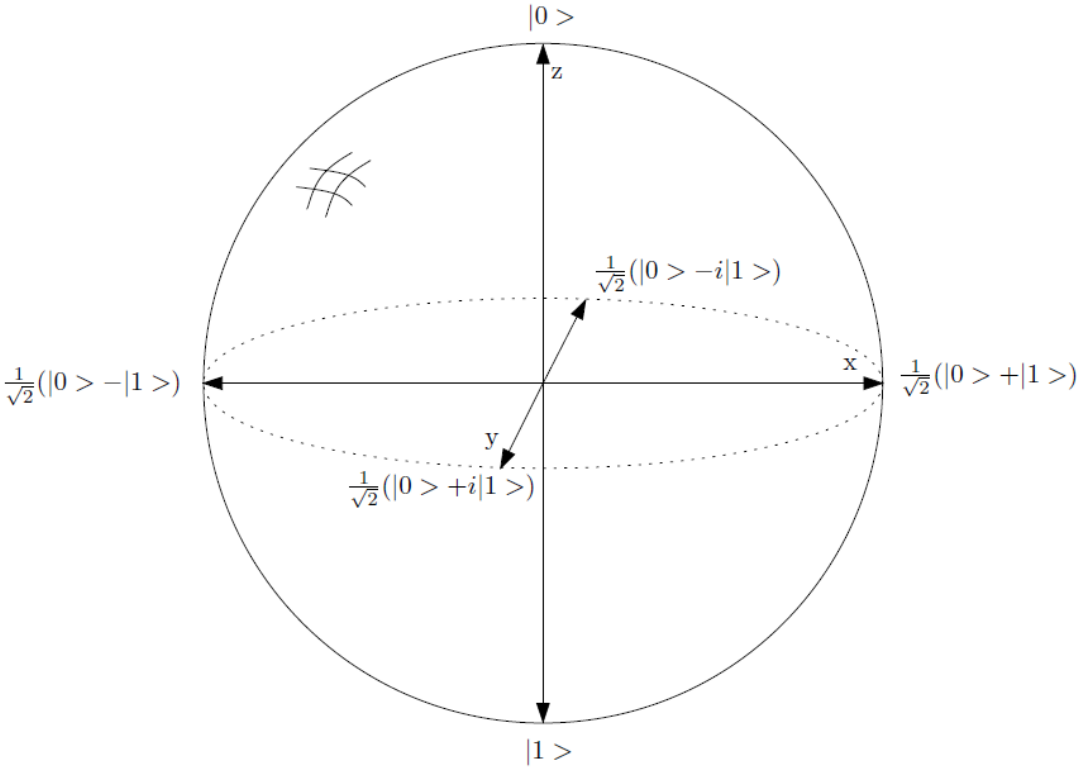


FIGURE 3.8 – La sphère de Bloch

3.2.8 Clonage quantique

En 1982, Wooters et Zurek ont répondu (dans [31])à la question suivante : *Est-t-il possible d'amplifier un état quantique, c'est-à-dire produire plusieurs copies d'un système quantique (photon polarisé dans le cas présent) chaque copie possède la même polarisation que le photon original ?* par NON.
Pour illustrer le phénomène, imaginant un dispositif qui copie l'état d'un photon (copieur linéaire qui est une transformation quantique correspondante à un opérateur linéaire). Quand le photon original est en entrée du dispositif, il en résulte deux copies en sortie, chacune possède la même polarisation que le photon original. Si le dispositif réussit à effectuer cette tâche, il convertissait l'état $|\clubsuit\rangle$ en $|\clubsuit\clubsuit\rangle$ et $|\spadesuit\rangle$ en $|\spadesuit\spadesuit\rangle$, où $|\clubsuit\rangle$ et $|\spadesuit\rangle$ représentent des états arbitraires. Le problème se pose quand il s'agit d'une combinaison linéaire, $|s\rangle = \alpha|\clubsuit\rangle + \beta|\spadesuit\rangle$. Si $|\clubsuit\rangle$ et $|\spadesuit\rangle$ sont clonés correctement, alors à cause de la linéarité de la mécanique quantique le résultat de leur superposition doit être la superposition des résultats,

$$|e\rangle \quad = \quad \alpha|\clubsuit\clubsuit\rangle + \beta|\spadesuit\spadesuit\rangle. \tag{3.23}$$

Mais nous voulons la copie $|ss\rangle$ de l'état original $|s\rangle$:

$$|s\rangle|s\rangle \quad = \quad (\alpha|\clubsuit\rangle + \beta|\spadesuit\rangle)(\alpha|\clubsuit\rangle + \beta|\spadesuit\rangle) \tag{3.24}$$

$$|s\rangle|s\rangle \quad = \quad \alpha\alpha|\clubsuit\rangle|\clubsuit\rangle + \beta\beta|\spadesuit\rangle|\spadesuit\rangle + \alpha\beta|\clubsuit\rangle|\spadesuit\rangle + \beta\alpha|\spadesuit\rangle|\clubsuit\rangle \tag{3.25}$$

ce qui ne ressemble pas à l'état $|e\rangle$. Il y a donc incompatibilité entre le clonage et la linéarité. D'après Wooters et Zurek, la linéarité de la mécanique quantique n'interdit pas l'amplification d'un état donné par un dispositif conçu spécialement pour cet état (un dispositif qui peut amplifier deux polarisations spéciales orthogonales, telles que la polarisation verticale et la polarisation horizontale à cause de la relation d'unitarité (conservation de la probabilité), mais elle exclut l'existence d'un dispositif capable d'amplifier un état arbitraire (polarisation quelconque non connue au préalable) [31]. Par conséquent, un amplifiant quantique peut être opérationnel uniquement quand les états en question sont orthogonaux ($|\clubsuit\rangle$ orthogonal à $|\spadesuit\rangle$, il s'ensuit que $\langle\clubsuit|\spadesuit\rangle = 0$) [42].
En résumé, nous ne pouvons pas faire des copies parfaites d'un état quantique inconnu (de polarisation inconnue), car sans connaissance préalable de la polarisation, il est impossible de choisir l'amplifiant adéquat pour accomplir la copie. Cette formulation est une manière commune pour énoncer le théorème de non-clonage (résumé de Wooters et Zurek [42]).

3.3 Distribution quantique de clé

> *Le principe de base de fonctionnement d'un processus d'échange quantique d'information est l'utilisation des états quantiques non-orthogonaux correspondants aux vecteurs des deux bases conjuguées rectilinière et diagonale. Une fois le photon est transmis, en effectuant des mesures dessus, l'émetteur et le récepteur seront en mesure de savoir s'il y a eu espionnage grâce aux lois de la physique quantique par le biais du principe d'incertitude d'Heisenberg, le principe de superposition et le théorème de non-clonage qui permettent d'interdire toute tentative d'espionnage ou dans le pire des cas la révéler de manière certaine.*

Distribution quantique de clé ou Quantum Key Distribution (QKD : convention internationale) réfère à tout système permettant à deux parties éloignées d'établir un échange d'une suite secrète de bits en toute sécurité, dans laquelle la sécurité est basée sur les lois de la physique quantique. C.H.Bennett et G.Brassard étaient les premiers qui ont proposé un protocole pratique pour QKD [6], connu sous le nom " Le Protocole BB84 ", où la première réalisation expérimentale a eu lieu

en 1989 sur une distance de 32 *cm* (publié en 1991 [7]). Depuis, la communauté scientifique a fait rentrer plusieurs modifications sur le $BB84$, en décrivant de nouveaux protocoles.
Tous les protocoles quantiques consistent en deux phases [9] :
– Dans un premier temps une des parties envoie à l'autre partie des signaux quantiques que celle-ci mesure.
– Dans un second temps les deux parties se livrent à un traitement de résultats de mesure via un canal classique.

La cryptographie quantique est une invention récente fondée sur l'incompatibilité de deux bases conjuguées d'états de polarisation linéaire [6]. Dire cryptographie quantique ne signifie pas chiffrer des messages à l'aide de la physique quantique, mais d'utiliser celle-ci pour s'assurer que la transmission de la clé n'a pas été espionnée.
Un photon polarisé d'un angle α par rapport à l'horizontale, il est décrit par le vecteur d'état $(\cos\alpha, \sin\alpha)$ par conséquent, il sera polarisé verticalement avec la probabilité $\sin^2\alpha$ et polarisé horizontalement avec probabilité $\cos^2\alpha$ [43]. La transmission d'une information peut se faire en utilisant ces deux états orthogonaux représentés par $r_1 = (1, 0)$ pour la polarisation horizontale et $r_2 = (0, 1)$ pour la polarisation verticale. Les deux vecteurs orthogonaux r_1 et r_2 illustrent la résolution d'un espace de Hilbert de dimension 2 en deux sous-espaces orthogonaux de dimension 1 [6]. Nous disons que r_1 et r_2 forment la base rectilinière pour l'espace de Hilbert. Une base alternative pour le même espace de Hilbert est fournie par les deux directions de polarisation à 45° et à 135°. Les vecteurs de cette base sont $d_1 = (\gamma, \gamma)$ et $d_2 = (\gamma, -\gamma)$ où $\gamma = \frac{\sqrt{2}}{2}$.

`Notion de bases conjuguées selon Stephen Wiesner :`

Soient $\{a_i\};\ i = 1, 2, \ldots, N$ et $\{b_i\};\ i = 1, 2, \ldots, N$, deux bases orthonormales pour un espace de Hilbert de dimension N. Nous appelons une telle paire, paire conjuguée si et seulement si : $|(a_i, b_j)|^2 = \frac{1}{N}\ \forall i, j$.
Physiquement, si un système est dans un état décrit par $a_i,\ i = 1, 2, \ldots, N$, alors il doit avoir une probabilité égale d'être trouvé dans n'importe quel état $b_i,\ i = 1, 2, \ldots, N$ et vice versa, s'il est dans un état b_i il doit avoir une probabilité égale d'être trouvé dans n'importe quel état a_i. D'autre terme, deux bases (rectilinière et diagonale par exemple) sont conjuguées si un système préparé dans un état spécifique d'une des deux bases, il se comportera entièrement aléatoirement et il perd toutes ses informations stockées, quand il est soumis à une mesure correspondante à l'autre base. L'espace de Hilbert à deux dimensions admet une troisième base conjuguée aux deux bases rectilinière et diagonale, constituée des deux polarisations circulaires $c_1 = (\gamma, \gamma i)$ et $c_1 = (\gamma i, \gamma)$ [4].

Nous pouvons attribuer par convention 0 à la polarisation r_1 et 1 à la polarisation r_2 : chaque photon transporte un bit d'information. Par exemple, soit le message 1001110 sera codé par Alice grâce à la séquence de photons $yxxyyyx$, qu'elle expédiera à Bob par exemple par fibre optique. À l'aide d'une lame biréfringente, Bob sépare les photons de polarisation verticale et horizontale (voir Fig.3.10), et deux détecteurs placés derrière la lame lui permettent de décider si le photon était polarisé horizontalement donc détecté par le détecteur D_x ou verticalement s'il a été détecté par le détecteur D_y, il peut donc reconstruire l'information.
Remarquons que si Eve s'installe sur la fibre, détecte les photons et envoie à Bob des photons de polarisations identiques à ceux expédiés par Alice, Bob ne peut pas savoir que la ligne a été espionnée. Il serait de même pour tout dispositif fonctionnant de façon classique (c'est-à-dire sans utiliser le principe de superposition : prend en charge que les deux polarisations horizontale et verticale) : si l'espion prend suffisamment de précautions, il est indétectable.
C'est ici que la mécanique quantique et le principe de superposition viennent au secours d'Alice et Bob, en leur permettant de s'assurer que le message n'a pas été intercepté : le message n'a pas besoin d'être long, il s'agira en général de transmettre une clé permettant de chiffrer un message ultérieur. Alice envoie à Bob quatre type de photons : polarisés suivant r_1, r_2, d_1 et d_2, correspondant respectivement aux bits 0 et 1. De même, Bob analyse les photons envoyés par Alice à l'aide d'un polariseur dit analyseur qui peut être une lame biréfringente ou un cristal

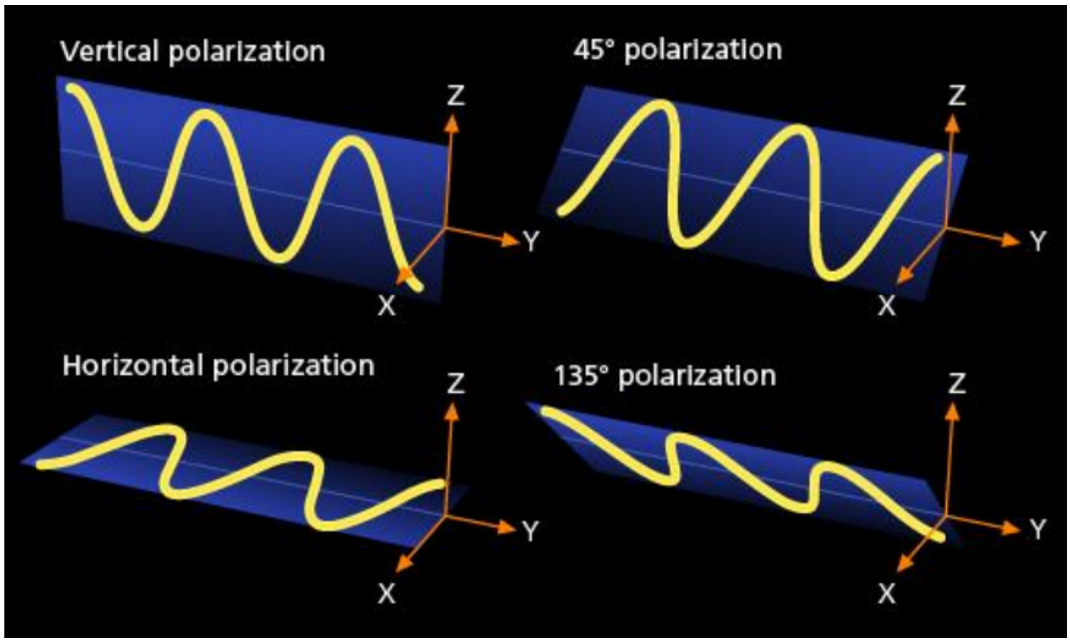


FIGURE 3.9 – Polarisation d'un photon dans des directions conjuguées [57].

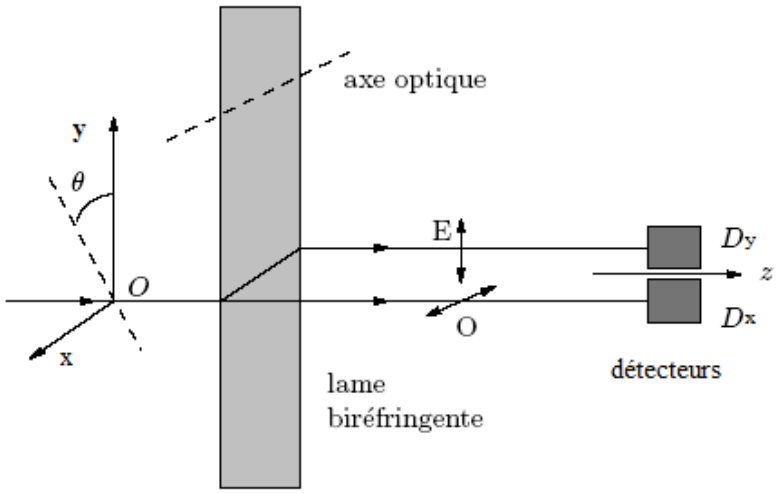


FIGURE 3.10 – Polarisation par une lame biréfringente [43].

biréfringent par exemple, pouvant prendre quatre directions : verticale/horizontale et $\pm 45^{\circ}$, puis détecte les photons sortant de ce cristal comme dans la figure 3.11. Dans la figure 3.12 par exemple, Bob enregistre 1 si le photon est polarisé verticalement ou à 135°, 0 s'il est polarisé horizontalement ou à 45°. Après enregistrement d'un nombre suffisamment grand de photons, Bob annonce publiquement la suite des analyseurs qu'il a utilisé, mais non ses résultats. Alice compare sa séquence de polariseurs à celle de Bob et lui donne toujours publiquement la liste de polariseurs compatibles avec ses détecteurs. Les bits qui correspondent à des détecteurs et de polarisations incompatibles sont rejetés (−), et, pour les bits restants, Alice et Bob sont certains que leurs valeurs sont les mêmes : ce sont les bits qui serviront à composer la clé, et ils sont

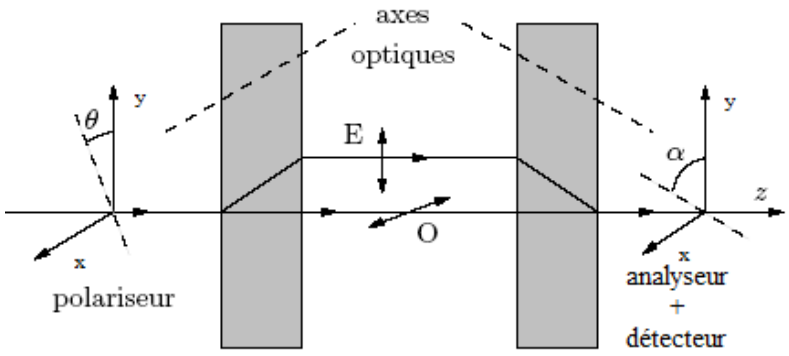


FIGURE 3.11 – Détection de photon polarisé à l'aide biréfringente [43].

connus seulement de Bob et Alice, car l'extérieur ne connaît que la liste des orientations pas les résultats.

polariseurs d'Alice	↕	↔	↗	↕	↗	↗	↘	↕	↘
séquences de bits	1	0	0	1	0	0	1	1	1
analyseurs de Bob	+	×	+	+	×	×	+	+	×
mesures de Bob	1	1	0	1	0	0	1	1	1
bits retenus	1	–	–	1	0	0	–	1	1

FIGURE 3.12 – Transmission de photons polarisés entre Alice et Bob.

Commentaire : Pour une base donnée et une direction bien précise pour cette base, le photon polarisé envoyé doit être détecté avec la même polarisation (direction-base) car : Si Alice envoie un photon polarisé verticalement, par exemple (base rectilinière), et si Bob positionne son polariseur selon une des directions de la base diagonale, alors quand le photon traverse le polariseur, il se comportera de manière aléatoire : il sera détecté selon D_x ou selon D_y ou il sera complètement perdu parce que les deux bases sont conjuguées. Maintenant, si Bob oriente sans polariseur selon une des deux directions de la base rectilinière (base choisie par Alice) ; si le photon est détecté par D_x, alors le photon était polarisé horizontalement et si le photon était détecté par D_y alors il était polarisé verticalement. Si le photon a été détecté dans la bonne base mais dans la mauvaise direction, Alice et Bob constatent qu'ils étaient espionnés.

Maintenant, il faut s'assurer que la clé partagée est inconditionnellement secrète. Comme Alice et Bob partagent un canal quantique non sécurisé probablement bruyant et canal classique authentifié alors l'intervention d'Eve se reflète dans la perturbation du canal quantique en interceptant les photons pour les empêcher d'atteindre leur destination ou en les alternant. Mais ça diffère dans le canal classique, Eve a accès à l'information, le fait qu'Alice et Bob échangent les informations en utilisant un processus d'authentification, ceci empêche à changer les messages ou prendre le rôle d'Alice ou de Bob dans la communication. Il est important à mentionner que l'authentification constitue une partie indispensable dans la cryptographie quantique. Sans une

bonne authentification, la cryptographie quantique devient vulnérable à l'attaque Man-in-the-midlle. Par conséquent, pour assurer une sécurité inconditionnelle, l'authentification doit être inconditionnellement sûre. Il est à noter que la norme en cryptographie quantique est l'utilisation du procédure d'authentification de Wegman-Carter, qui est inconditionnellement sûre et est basée sur l'idée d'hachage universel.

3.3.1 Le protocole $BB84$

En se basant sur l'idée de Wiener, Charles Bennett et Gilles Brassard proposèrent en 1984 un protocole QKD en utilisant quatre états quantiques $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Les paires $\{|0\rangle, |1\rangle\}$ et $\{|+\rangle, |-\rangle\}$ sont en fait les vecteurs propres associés aux opérateurs Z et X respectivement et ils forment deux bases orthonormales, la base rectilinière et la base diagonale.
Nous définissons ces deux bases conjuguées par la notation suivante :

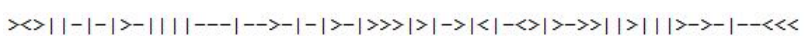
$$B_0 = \{|B_{0,0}\rangle = |0\rangle,\ |B_{0,1}\rangle = |1\rangle\}, \tag{3.26}$$
$$B_1 = \{|B_{1,0}\rangle = |+\rangle,\ |B_{1,1}\rangle = |-\rangle\}. \tag{3.27}$$

Le protocole de Bennett et Brassard 1984 ($BB84$) :

1. Alice choisit aléatoirement deux chaînes binaires, h^A et k^A de longueur au minimum $4n$. La première conserve la polarisation et la seconde indique le choix de la base fait par Alice pour chaque photon.
2. Soient h_i^A et k_i^A, qui dénotent le i^{eme} bit dans les deux chaînes h^A et k^A respectivement. Pour chaque i, Alice prépare l'état quantique associé $|b_{k_i^A, h_i^A}\rangle$. Alice envoie tous les états préparés à Bob via un canal quantique non sécurisé.
3. Bob choisit aléatoirement une chaîne binaire k^B de longueur au minimum $4n$ (la même longueur est fixée par Alice et Bob).
   Bob mesure le $i^{ème}$ qubit dans la base $B_{k_i^B}$. Si la mesure rapporte $|b_{k_i^B,0}\rangle$ alors Bob fixe $h_i^B = 0$. Contrairement, si la mesure donne $|b_{k_i^B,1}\rangle$, alors Bob fixe $h_i^B = 1$.
4. Alice annonce publiquement la chaîne k^A, en indiquant la basse utilisée pour chaque bit.
5. Alice et Bob via une discussion publique, se mettent d'accord pour rejeter le i^{eme} bit si $k_i^A \neq k_i^B$ ils n'ont pas utilisé la même base.
   La moitié des bits sont susceptible d'être retenus.
6. Alice doit choisir aléatoirement un sous ensemble des bits retenus de l'étape précédente pour effectuer un teste pour détecter les perturbations et indique à Bob les positions de ces bits.
7. Via une discussion publique, Alice et Bob comparent les bits de ce sous-ensemble. S'ils trouvent un grand nombre de désaccords, ils abandonnent le protocole.
8. Dans le cas contraire, ils poursuivent les étapes. Alice et Bob effectuent une correction des erreurs et une amplification de confidentialité sur les bits restants pour créer la clé secrète.

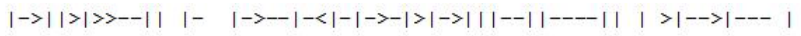
Alice et Bob effectuent le test des bits pour détecter les perturbations dans le canal. Quand il y a un taux élevé de perturbations, Alice et bob laissent tomber le protocole, en assurant la présence d'Eve. Par contre, s'il y a peu de perturbations, la correction des erreurs et l'amplification de confidentialité peuvent assurer qu'Eve possède une insignifiante quantité d'informations concernant la clé résultante.

Exemple 3.1 [30] Déroulement du $BB84$ afin d'obtenir une clé secrète aléatoire à partir de 64 photons transmis d'Alice à Bob en utilisant deux bases conjuguées (rectilinière et circulaire).
Alice envoie les 64 photons suivants dont la polarisation est choisie selon les bases rectilinéaire et circulaire :



Eve intercepte les photons et pour chacun mesure sa polarisation selon l'une des deux bases rectilinéaire ou circulaire, elle obtient :

Pour chaque mesure, il y a une probabilité de 0.2 que le photo-détecteur ne détecte pas le photon envoyé, alors les mesures d'Eve deviennent :



Bob mesure au hasard la polarisation de chaque photon selon l'une des deux bases :

Et aussi, il y a une probabilité de 0.2 que le photo-détecteur ne détecte pas le photon envoyé, alors les mesures de Bob deviennent :

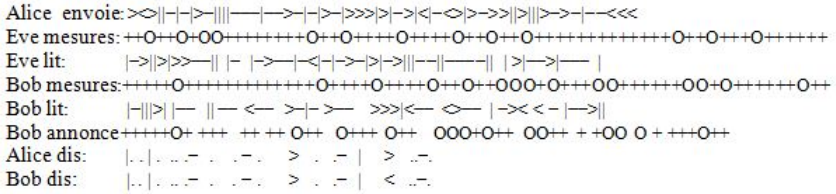
Bob annonce à travers le canal classique la base choisie pour chaque mesure :

Alice indique le choix adéquat en utilisant des points, elle annonce :

Comme les photo-détecteurs ne détectent pas 20% des photons envoyés et de plus Bob fera le bon choix de mesure la moitié du temps, alors il reste 25.6 photons utiles. Pour cet exemple il reste 23 photons utiles.
Alice et Bob vont déterminer s'ils ont été espionnés. Ils comparent un sous ensemble de données (la moitié) prises aléatoirement parmi les données restantes, même un espion ne peut pas détecter quelles sont les données comparées :

Bob annonce les données vérifiées :

Comme il y a une erreur dans les données vérifiées, Alice et Bob constatent qu'ils ont été espionnés.



Commentaire : Les remarques introduites ainsi sont des remarques personnelles sur le déroulement du $BB84$.

Remarques 3.1 – A l'étape 5 du protocole, il y a une perte de données lors de la comparaison des résultats entre Alice et Bob via le canal classique.
– A l'étape 7 de protocole, dans le cas où il y a eu espionnage, Alice et Bob doivent rejeter leurs données et recommencer de nouveau ce qui constitue une perte de données et un gaspillage des ressources.
– Il est impossible de déterminer si les erreurs corrigées étaient dues aux photo-détecteurs ou à l'espionnage.
– Les propriétés des fibres optiques limitent l'utilisation du protocole car le signal de faible intensité s'atténue en parcourant la fibre, il sera donc indétectable à la sortie du canal. Ainsi pour mieux réussir, il faudrait réaliser des progrès dans la qualité des fibres optiques ou encore utiliser les canaux de transmission sous-vide.

Pour pouvoir réaliser un prototype d'un protocole QKD ($BB84$), nous avons besoin des dispositifs suivants :
– Une source de photons, une lampe diode verte ou un laser (par exemple).
– Un polariseur, une lame biréfringente ou un Crystal de calcite, pour avoir des photons polarisé selon une base donnée.
– Un canal quantique composé de fibre optique ou un canal de transmission rectiligne sous vide, pour la transmission de photons d'Alice à Bob.
– Un analyseur pour séparer les photons selon leur polarisation.
– Deux photo-détecteurs pour détecter les photons.

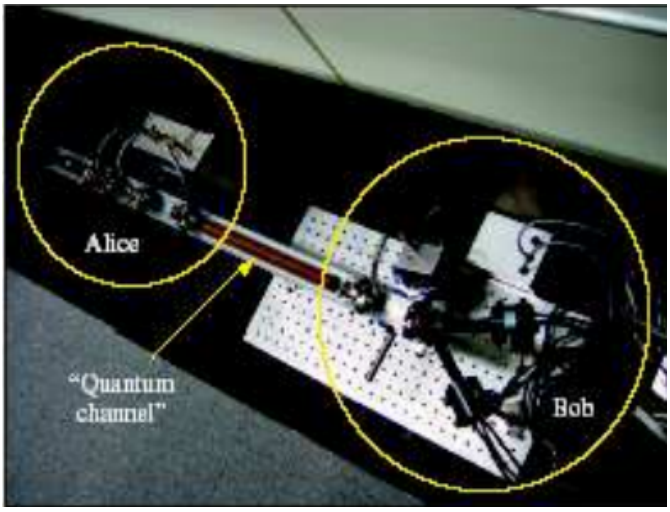


FIGURE 3.13 – Les vrais dispositifs utilisés pour réaliser le prototype $BB84$.[60]

Espionnage

Il reste à s'assurer que le message n'a pas été intercepté et que la clé peut être utilisée sans risque. Grâce au théorème de non-clonage, Alice et Bob sont certains qu'Eve ne possède pas une copie des photons transmis, tout ce qu'elle peut faire est d'intercepter les photons, effectuer des mesures dessus et les renvoyer. Ceci est connu par "intercept/resend attack".
Comme Alice alterne ses bases aléatoirement, Eve ne connaît pas la base adéquate pour chaque photon afin d'effectuer des mesures dessus, et elle va choisir les bases aléatoirement. En fait, en interceptant et mesurant la polarisation des photons envoyé par Alice, Eve fera en moyenne 1 fois sur 2 le mauvais choix pour la base. Même si Eve envoie à Bob un photon de polarisation en accord avec son choix de base (choix de base de Bob), elle enverra 1 fois sur 2 un mauvais photon. Par conséquent, Eve introduit une incohérence dans 25% des données échangée entre Alice et Bob. En comparant un sous-ensemble de leurs bits, Alice et Bob sont en mesure de déterminer avec quasi-certitude s'il y a eu espionnage sur le canal quantique.
Eve peut intervenir d'une autre manière comme un obstacle entre Alice et Bob en effectuant un autre type d'attaque. Cette fois ci, Eve se concentre sur l'intensité des impulsions lumineuses transmises d'Alice à Bob. Il est connu que les impulsions lumineuses contenant exactement un photon sont techniquement quasiment impossibles à produire. D'où, Eve aura la chance chaque fois qu'une impulsion est transmise de dévier vers sont appareil un des photons de l'impulsion et de mesurer la polarisation selon l'une des deux bases. Ce type d'attaque est connu sous le nom 'beam splitting attack', il est tout à fait indétectable tant et aussi longtemps qu'Eve prend soin de toujours laisser les photons non-déviés de l'impulsion atteindre l'appareil de Bob sans être perturbés, et que l'intensité d'une impulsion lumineuse soit grande. Par conséquent, la clé partagée entre Alice et Bob n'est pas purement secrète car Eve possède une connaissance à propos de l'échange effectué. Pour remédier à ce problème, ils doivent ajouter une étape de purification au protocole [30], nous pouvons exprimer cette étape comme suit : Alice et Bob réconcilient leurs suites de bits retenus en utilisant quelques techniques de correction d'erreurs pour arriver en fin à une séquence de bits identique. Cette séquence n'est pas complètement secrète, Eve peut avoir une connaissance partielle à propos. Pour éliminer cette connaissance, ils font appel à une procédure d'amplification de confidentialité dite "Privacy amplification". L'amplification de confidentialité est une méthode qui leur permette d'extraire une suite de bits secrète à partir de leurs données de telle sorte qu'Eve ait connaissance d'au maximum 1 bit de cette suite extraite avec une très faible probabilité.
Il convient de mentionner que les appareils physiques ne sont pas efficace à 100% (photo-détecteur ne sont pas efficace à 100%) et sans bruit. Même à l'absence d'Eve, Alice et Bob trouvent toujours des désaccords dans leurs résultats. Ainsi, ils ne peuvent pas différencier entre les incohérences dues au bruit, les erreurs du canal et l'espionnage. Il s'agit donc d'une fausse détection, c'est-à-dire : Il est probable qu'ils ne détectent pas un photon, donc certains photons envoyés par Alice seront perdus. Ou bien, ils détectent un photon non envoyé par Alice et ceci est dû au bruit à l'intérieur des photo-détecteurs, il s'agit alors d'un 'dark count'. Pour remédier à ce problème, il faut ajouter une étape supplémentaire au protocole, soit une étape afin de permettre à Alice et Bob de corriger les erreurs dans leurs données. Pour ce faire Alice et Bob doivent exécuter via le canal classique un protocole de correction des erreurs [30].

Conclusion

Dans ce chapitre, nous avons donné un aperçu sur la mécanique quantique en se basant sur les concepts qui font l'objet de l'échange quantique de l'information. En second lieu, nous avons expliqué l'approche quantique en cryptographie, en indiquant comment exploiter les lois et les notions de la physique quantique pour servir la confidentialité en cryptographie. Puis, une explication du processus d'échange quantique de clé est fournie suivie du protocole $BB84$. Nous avons vu que la distribution quantique de clé peut fournir une sécurité inconditionnelle, mais ça n'empêche pas de dire que l'utilisation d'un canal classique authentifié constitue une critique

pour les protocoles QKD, de plus, sans l'authentification, ces protocoles deviennent vulnérables. Cependant, l'authentification peut constituer une faille dans le processus QKD en augmentant les espérances de la cryptanalyse pour attaquer la cryptographie quantique comme l'avait mentionné Jan-*A*ke Larsson (énoncé traité par son étudiant dans [71]). Un autre facteur peut contribuer aux tentatives d'attaque des QKDs, il s'agit d'un élément indispensable dans la transmission et la réception des photons, c'est les photo-détecteurs. Un résultat à propos a été publié le dans [59], c'est le succès d'une collaboration internationale permettant de déjouer une vulnérabilité dans les systèmes de cryptographie quantique commerciaux, en indiquant qu'il est possible de gagner de l'information lors du déroulement d'un protocole quantique en appliquant une technique récemment découverte permettant la manipulation des photo-détecteurs et exactement le control du composant compteur de photons [58].

4
Protocole BC10

Contents

Introduction

Les protocoles cryptographiques est un domaine très large de recherches, il existe d'énormes productions (livres, thèses de doctorats,...) dans la littérature sur leur conception, niveau de sécurité et l'étude critique de leur mise en oeuvre. Dans le premier paragraphe de ce chapitre, nous donnons un aperçu général sur la notion de protocole puis par la suite nous présentons les étapes du $BC10$, le protocole que nous avons conçu afin de générer et partager des clés secrètes au profit de l'utilisation du chiffre de Vernam.

4.1 Le protocole

Un protocole est une série d'étapes qui a un début et une fin, impliquant deux ou plusieurs participants, conçu pour accomplir une tache. Chaque étape doit être exécutée à son tour et aucune autre étape ne peut être exécutée avant que la précédente ne soit finie. Une personne isolée ne peut pas accomplir un protocole, il est vrai qu'une personne seule peut réaliser une série d'étapes pour accomplir une tache, par exemple cuir un gâteau, mais ce n'est pas un protocole [1].
Les protocoles possèdent d'autres caractéristiques :
- Chaque participant d'un protocole doit connaître le protocole et toutes les étapes à suivre d'avance.
- Chaque participant impliqué dans un protocole doit être d'accord pour adhérer au protocole.
- Le protocole doit être non ambigu : chaque étape doit être bien définie et il ne doit pas y avoir de possibilité de mésentente.

– Un protocole doit être complet : il doit y avoir une action spécifique à chaque situation possible.

Les protocoles cryptographiques concernent un échange de messages entre participants qui peuvent être des amis qui ont confiance les uns en les autres ou ils peuvent être des ennemis (l'un des participants viole les règles afin d'essayer d'obtenir un avantage). Le protocole cryptographique utilise certains algorithmes cryptographiques, bien que le but d'un protocole ne se limite pas à la simple confidentialité mais il permet d'engendrer une suite aléatoire, assurer l'authentification entre les participants et garantir la signature simultanée des contrats [53].
En résumé, en cas d'interactions engendrant aussi l'échange d'informations secrètes, il doit être impossible de faire ou d'apprendre plus que ce qui est prévu dans le protocole.

Acteurs et types de protocoles

Afin d'illustrer les protocoles, Bruce Schneier a engagé des personnages [1] qui sont devenu les acteurs dans les protocoles où chaque personnage réfère à un rôle précis. Par la suite, ceci est devenu une convention entre les gens du domaine.

TABLE 4.1 – Les acteurs et leur rôle

Alice	*participante de tous les protocoles*
Bob (*Bernard*)	*participant de tous les protocoles*
Carol (*Christine*)	*participante des protocoles à trois ou à quatre participants*
Dave (*David*)	*participant des protocoles à quatre participants*
Eve (*Estelle*)	*espionne*
Mallory (*Martin*)	*attaquant malveillant actif*
Trent (*Ivan*)	*arbitre intègre*
Walter (*Gatien*)	*gardien : il surveille Alice et Bob dans certains protocoles*
Peggy (*Patricia*)	*plaideuse*
Victor	*vérificateur* (*contrôleur*)

Alice et Bob sont les acteurs principaux. Dans tous les protocoles, Alice initiera le déroulement du protocole et Bob répondra. Les autres acteurs joueront des rôles spécifiques dont leur intervention détermine le type de protocole.
Les protocoles où nous marquerons la présence de Trent sont dits protocoles arbitrés. L'arbitre est un tiers, personne de confiance et désintéressé qui veille au bon déroulement du protocole. Il est impliqué dans le protocole et tous les participants considèrent ce qu'il dit et ce qu'il fait comme vrai et correct. Ces protocoles aident au bon accomplissement de protocoles entre des participants méfiants.
Dans le monde réel, les hommes de loi jouent souvent le rôle d'arbitre, les bourses et les banques aussi agissent comme arbitre entre les acheteurs et les vendeurs.
Les protocoles arbitrés peuvent être divisés en deux sous-protocoles [1] : le premier non-arbitré exécuté chaque fois que le protocole est utilisé, le second est arbitré auquel nous ne faisons appel que s'il y a un litige entre les participants, ici, nous ne parlerons pas d'arbitre mais de juge-arbitre. Le juge-arbitre possède les mêmes caractéristiques qu'un arbitre sauf qu'il n'est pas impliqué dans le protocole. Le juge-arbitre n'est appelé que pour déterminer si une transaction a été effectuée honnêtement. La différence entre l'arbitre et le juge-arbitre est que ce dernier n'est pas toujours nécessaire, son intervention est liée à l'existence d'une contestation. Les protocoles informatiques avec juge-arbitre reposent sur l'hypothèse que les participants sont honnêtes mais si quelqu'un triche le juge-arbitre détermine s'il y a eu tricherie, ces protocoles détectent la tricherie et la partie responsable.
Il existe une autre catégorie de protocoles, c'est le cas où le protocole lui-même garantit l'intégrité des transactions et le règlement de conflits. Nous parlons alors de protocoles à discipline intrinsèque [1]. Si l'un des participants essaie de tricher, l'autre participant le détecte immédiatement et le protocole sera interrompu. Pour des raisons de sécurité, tout protocole devrait être à discipline intrinsèque ce qui n'est pas possible pour tout type de transactions.

Attaques des protocoles

Il y a plusieurs façons d'attaquer un protocole. Quelqu'un qui n'est pas impliqué dans le protocole peut espionner tout ou partie de celui-ci. C'est ce que l'on appelle une attaque passive parce que l'attaquant ne modifie pas le protocole, tout ce qu'il peut faire c'est observé le protocole et ainsi essayer de collecter de l'information. Les attaques passives sont difficiles à détecter, les protocoles essayent de s'en prémunir plutôt que de les détecter. Un tel attaquant est appelé Eve, selon la classification de Bruce Schneier.
Un attaquant peut aussi essayer d'altérer le protocole pour le tourner à son avantage. Il peut prétendre être quelqu'un d'autre, introduire ou supprimer des messages, substituer un message par un autre, détruire le canal de communication ou encore modifier l'information enregistrée par un ordinateur. Nous parlerons alors d'attaques actives car elles requièrent une attitude active de la part de l'attaquant. L'attaquant dans ce genre d'attaque est appelé Mallory selon la même classification.
Avant de passer à la description du protocole $BC10$, nous donnons ici un aperçu sur le problème de partitionnement d'un ensemble.

4.2 Problème de partitionnement d'un ensemble

Le problème de partition est un problème NP-complet. Le problème est de partitionner un ensemble E en une famille de sous-ensembles tels qu'ils sont disjoints deux à deux et la réunion dont est l'ensemble E.

Partitions

Une famille de sous-ensembles S_i d'un ensemble S est une partition de S si [22] :

• Chaque S_i est non vide.

• Les sous-ensembles sont deux à deux disjoints ; $S_i \cap S_j = \emptyset$ *si* $i \neq j$.

• La réunion des S_i donne S ; $\bigcup_{i \in I} S_i = S$ où I désigne l'ensemble des indices.

Chaque S_i est un bloc de la partition.

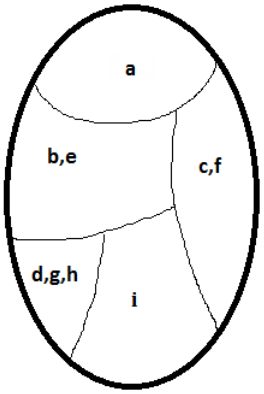


FIGURE 4.1 – Une partition de S

Par exemple, considérons l'ensemble $S = \{a, b, c, d, e, f, g\}$. Alors $\pi = \{\{a\}, \{b, e\}, \{c, f\}, \{d, g, h\}, \{i\}\}$ est une partition de S. Les sous-ensemble $k_1 = \{a\}$, $k_2 = \{b, e\}$, $k_3 = \{c, f\}$, $k_4 = \{d, g, h\}$ et $k_5 = \{i\}$ sont les blocs de la partition.
• Le nombre de façons de partitionner un ensemble à n éléments en k sous-ensembles non vides ($k \leq n$) est donnée par les nombres de Stirling de deuxième espèce $S(n, k)$ noté $\left\{ \begin{array}{c} n \\ k \end{array} \right\}$.
Pour $n > 0$ entier, nous avons

$$\left\{ \begin{array}{c} n \\ k \end{array} \right\} = k * \left\{ \begin{array}{c} n-1 \\ k \end{array} \right\} + \left\{ \begin{array}{c} n-1 \\ k-1 \end{array} \right\},$$

avec :

$$\left\{ \begin{array}{c} 0 \\ 0 \end{array} \right\} = 1; \left\{ \begin{array}{c} 0 \\ 1 \end{array} \right\} = 0; \left\{ \begin{array}{c} n \\ 1 \end{array} \right\} = 1 \; et \; \left\{ \begin{array}{c} n \\ n \end{array} \right\} = 1.$$

Pour $n, k \in \mathbb{N}$; nous avons la formule explicite suivante :

$$\left\{ \begin{array}{c} n \\ k \end{array} \right\} = \frac{1}{k!} \sum_{i=0}^{k} (-1)^i \left(\begin{array}{c} k \\ i \end{array} \right) (k-i)^n.$$

• Le nombre de toutes les partitions que peut admettre un ensemble à n éléments est donné par le $n^{ième}$ nombre de $Bell(n) = \sum_{k=0}^{n} \left\{ \begin{array}{c} n \\ k \end{array} \right\}$ qui possède un comportement asymptotique exponentiel.
Ce concept constituera l'objet du prochain paragraphe où nous allons décrire un protocole basé sur la k-partition de l'ensemble $[n] = \{1, 2, \ldots, n\}$.

4.3 Description du protocole $BC10$

Le protocole appelé $BC10$ "*Bouroubi Charchali* 2010", inspiré du protocole quantique $BB84$ "Bennett Brassard 1984", basé sur le problème de partitionnement d'un ensemble de n éléments en k classes discernables et nécessite deux participants qui se font confiance mutuellement.
L'objectif attendu du protocole est la production et la distribution de clés secrètes qui seront utilisées pour assurer des communications confidentielles entre les participants en interchangeant des messages cryptés par le chiffre de Vernam.
Tout d'abord, les deux parties impliquées dans le protocole doivent partager **une partition** π de l'ensemble $[n]$ en k blocs deux à deux disjoints (n est supposé assez grand).
Les acteurs traditionnels qui doivent animer un échange d'informations en cryptographie sont Alice et Bob, les deux concernés par l'émessions et la réception des messages secrets et bien sûre Eve l'intruse qui veut espionner Alice et Bob.
Supposons qu'Alice souhaite transmettre un message M à Bob; alors les étapes à suivre sont :

1. Alice calcule le nombre de caractères L_M du message à chiffrer.
2. Alice fixe le paramètre m tel que $m = L_M * S$ (S un entier positif permettant d'obtenir une longueur considérablement longue assurant l'obtention de la clé dés le premier déroulement du protocole afin de minimiser l'échange d'informations entre Alice et Bob (voir Etape 9)).
3. Alice génère de manière aléatoire une séquence de nombres entiers compris entre 1 et n de taille m et pour chaque entier de la séquence, elle met dans une liste T_A l'indice de la classe à laquelle cet élément appartient dans la partition π.
4. Alice envoie **le paramètre** m à Bob.

5. Bob génère à son tour de manière aléatoire une séquence de nombres entiers compris entre 1 et n de taille m et pour chaque entier de la séquence, il met dans une liste T_B l'indice de la classe à laquelle cet élément appartient dans la partition π.
6. Bob envoie **la liste** T_B à Alice.
7. Alice reçoit la liste de Bob, et la compare avec la sienne. S'il y a correspondance, c'est à dire pour le même indice, elle trouve la même classe dans les deux listes, elle met un " + ", si ce n'est pas le cas elle met un " − ". Procédant ainsi elle crée une nouvelle liste dite T dont les éléments sont " + " et " − ".

$$T[i] = \begin{cases} + \ si\ T_A[i] = T_B[i] \\ \\ - \ si\ T_A[i] \neq T_B[i] \end{cases}, \forall i = 1, ..., m.$$

8. Alice interprète chaque " + " comme étant le résultat d'une fonction f (sera définie ci-dessous) choisie parmi trois fonctions (par exemple), agissant sur les éléments de la classe correspondante. La concaténation de ces résultats constitue la clé secrète de longueur L_C. Pour trouver f, Alice considère le premièr " + " rencontré dans la liste T, Alice écrit le numéro de classe correspondant à ce " + ", soit j, en binaire, puis elle considère que les deux premiers bits vers la droite. Si les bits sont :
   • identiques ("00" ou "11") alors la fonction f est interprétée comme la somme des éléments de cette classe.
   • "10" alors la fonction f est interprétée comme étant le produit des éléments de cette classe.
   • "01" dans ce cas, la fonction f est interprétée comme l'élément maximum de la classe j élevé à la puissance j.
9. Alice compare L_M à L_C. Si $L_M \leq L_C$, elle envoie à Bob **la séquence** T et le message chiffré, puis Bob effectue l'étape 8 pour obtenir la clé. Sinon, Alice doit retourner à l'étape 2 et, à ce niveau, elle peut garder la taille m ou la modifier.

   Le protocole permet de mettre entre les mains d'Alice et Bob une clé secrète aléatoire tout en partageant le minimum d'informations ce qui mène à maximiser l'incertitude concernant π pour Eve.
   Les données échangées lors du déroulement du protocole, et qui sont attrapées par Eve, sont T et T_B. L'élément maximum de T_B peut être le nombre de classe de la partition π (ou bien non, dans le cas où aucun élément de la $k^{ème}$ classe a été généré dans la liste d'Alice et la liste de Bob). Partant de cet effet, nous voyons que si Alice et Bob laissent tomber le protocole en se limitant à l'échange de T_A et T_B entre eux, Eve pourrait dévoiler k.

La confidentialité absolue exige le partage du paramètre clé π, la partition secrète, qui garantit que la clé obtenue est confidentielle et n'est pas connue, que par les utilisateurs légitimes du protocole. Par conséquent, la clé générée par $BC10$ offre la confidentialité à l'information transmise cryptée suivant le cryptosystème Vernam, en assurant l'impossibilité de décryptage de ce qui a été chiffré par un espion.

4.4 Implémentation du protocole $BC10$

Dans ce paragraphe, nous passons à l'implémentation du $BC10$ afin d'obtenir des clés secrètes aléatoires qui seront utilisées pour le chiffrement des textes clairs.
L'application *CryptoStrumento version 1.0* effectue essentiellement deux tâches, la première étant la génération d'une partition aléatoire d'un ensemble $[n]$ en k classes (n et k quelconque, à choisir). Tandis que la seconde consiste à dérouler le protocole $BC10$ puis injecter la clé fournie dans Vernam, le cryptosystème adopté, pour sortir en fin avec le texte chiffré.

L'environnement de programmation choisi est Delphi 7. Les avantages de ce langage sont évidentes en ce qui concerne les tâches à effectuer, notamment en raison de l'aspect de l'orienté objet qu'il possède.

4.4.1 Génération de la partition

L'algorithme mentionné ci-dessous, est un algorithme polynômial, il donne une partition aléatoire d'un ensemble.
Algorithme ;
Entrées $\rightarrow n, k$,
Sortie $\rightarrow$ *la partition* π.
Début
Si $k > n$ **alors** *"Le partitionnement est impossible*
Sinon Si $k = 1$ **alors** $\pi := \{1, 2, \ldots, n\}$
Sinon
$\pi := \emptyset$;
$T := \{1, 2, \ldots, k\}$;
$liste := \{1, 2, \ldots, n\}$;
Générer aléatoirement un nombre x *tel que* $x \in liste$;
Tant que $T \neq \emptyset$ **Faire**
Choisir i, $i \in T$;
$C_i := C_i \cup \{x\}$;
$\pi := \pi \cup C_i$;
$T := T \setminus \{i\}$;
$liste := liste \setminus \{x\}$;
Fait ;
Tant que $liste \neq \emptyset$ **Faire**
Générer un nombre aléatoire x *tel que* $x \in liste$;
Choisir un indice i, $C_i := C_i \cup \{x\}$;
$liste := liste \setminus \{x\}$;
Fait ;
$\pi := \{C_1, C_2, \ldots, C_k\}$;

Fin Sinon ;

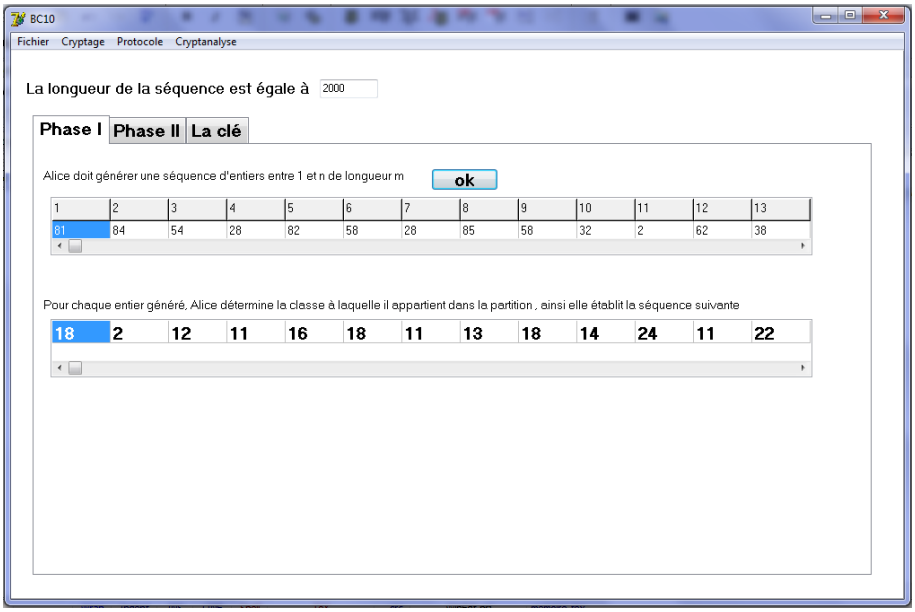
Fin Algorithme.

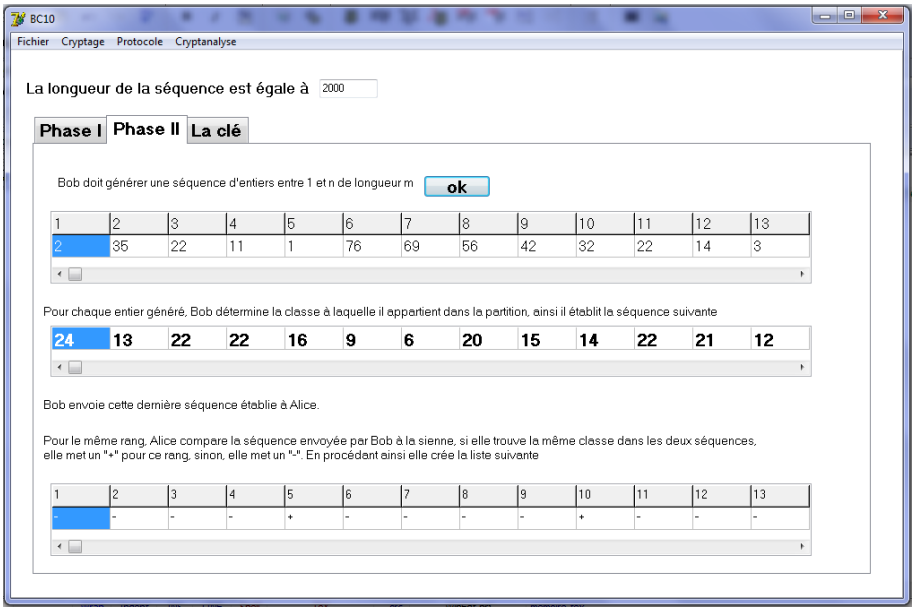
Exemple 4.1 Soit $n = 86$, nous voulons avoir une partition π de l'ensemble [86] en 25-classes disjointes, non vides. La partition fournie par CryptoStrumento est donnée dans la figure suivante :
$\pi := \{\{16, 39, 29\}, \{84, 10, 80\}, \{21, 17\}, \{60\}, \{74, 5, 43, 40\}, \{9, 57, 69\}, \{37, 86, 15, 52\}, \{19,$
12,49,27},{76,24,8},{47,78,45,4},{28,62},{70,3,54,65,51},{18,35,85,63},{23,32,73},
{53,44,42,30,13},{87,1,82},{55,31,33},{36,64,58,81},{6,25,48,61},{56,59,7,83},{72,
14,77,66},{22,38,11,71},{68,50,75},{34,26,79,20,2},{41,46}}

4.4.2 Génération de clé

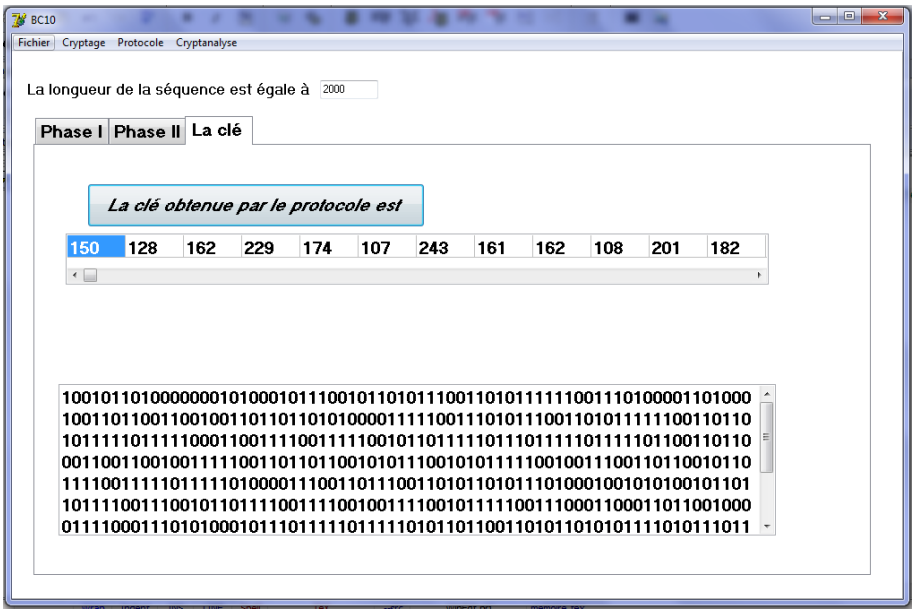
Une fois la partition clé π est partagée, les utilisateurs du CryptoStrumento passent à la deuxième phase (obtention de la clé de chiffrement), en faisant appel au protocol $BC10$. Le programme exécutant cette tâche est le suivant :
Algorithme ;
Entrées→m, la partition clé π
Sortie→ *la clé secrète de chiffrement.*
Début
$premierplus := 0$;
$clé := \emptyset$;
Pour i← 1 à m **Faire**
$l_A[i] := x$, x généré aléatoirement et $1 \leq x \leq n$;
$l_B[i] := y$, y généré aléatoirement et $1 \leq y \leq n$;
Fin Pour ;
$indice := 1$;
Tant que $indice \leq m$ **Faire**
Pour i← 1 à m **Faire**
Trouver $j, j^{'}$ tel que $l_A[i] \in C_j$ et $l_B[i] \in C_{j'}$, $j \in \{1, 2, \ldots, k\}$ et $j^{'} \in \{1, 2, \ldots, k\}$;
$T_A[i] := j$;
$T_B[i] := j^{'}$;
Fin Pour
Si $T_A[indice] = T_B[indice]$ **alors**
Début Si ;
$T[indice] := +$;
premierplus :=premierplus+1 ;
Si $premierplus = 1$ **alors** ;
Début Si
chaine :=Binaire($T_A[indice]$) ; //Binaire($T_A[indice]$) : fonction de conversion de caractère en binaire
Si BitDroit(chaine)=11 **ou** BitDroit(chaine)=00 **alors** Appliquer : f : la Somme
//BitDroit(chaine) : fonction qui donne la valeur des deux bits de droite dans un octet
Sinon Si BitDroit(chaine)=10 **alors** Appliquer f : le Produit
Sinon Appliquer f : $(\max(C_{T_A[indice]}))^{T_A[indice]}$;
Fin Si ;
$clé := clé \cup f(C_{T_A[indice]})$;
Fin Si
Sinon $T[indice] := -$;
incrémenter(indice) ;
Fin Tant que
Concaténer(clé) ;
$clé$:=Binaire($clé$);
Fin Algorithme.

Exemple 4.2 Nous voulons maintenant, générer une clé secrète aléatoire pour chiffrer le message suivant *"Il est plus facile de faire la guerre que la paix."* en utilisant Vernam.



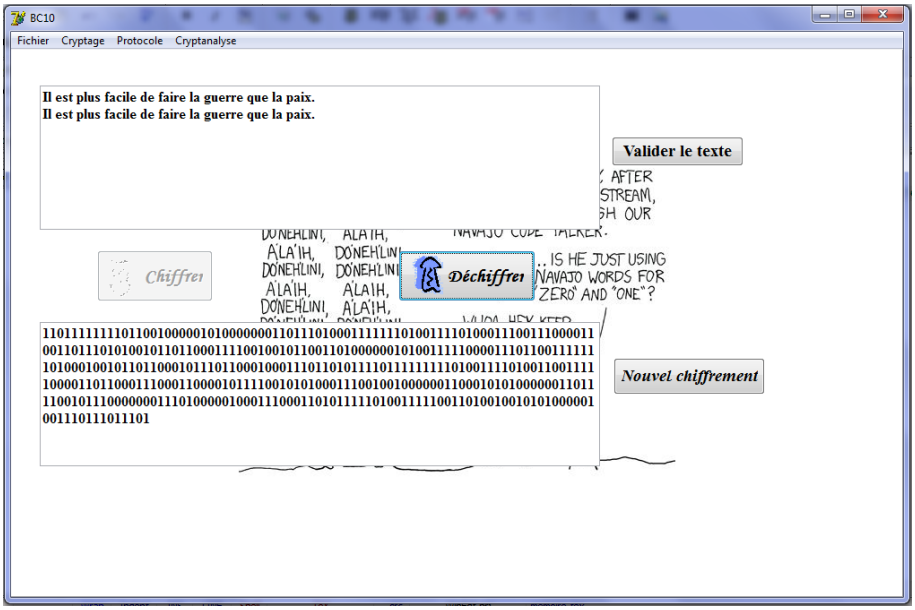


La clé fournie par *BC*10 :



4.4.3 Chiffrement par le chiffre de Vernam

Exemple 4.3 Finalement, le message chiffré en utilisant la clé secrète obtenue antérieurement est donné par :



Conclusion

Dans ce chapitre, nous avons exposé la conception et le déroulement du *CryptoStrumento version 1.0*. L'application effectue deux tâches en réalisant les objectifs attendus. Le premier objectif visé étant la production d'une clé aléatoire au moins aussi longue que le message à chiffrer en assurant la synchronisation entre l'émetteur et le récepteur en mettant en ouvre le protocole $BC10$. Le second est l'incapacité d'une tierce personne, soit Eve, de déterminer la clé générée dans un temps raisonnable. C'est parce que si Eve intercepte toutes les données échangées entre Alice et Bob, elle n'a aucune information sur la partition π et la clé secrète. Pour pouvoir déterminer π afin de trouver la clé, Eve est face au problème suivant : Chercher les k classes d'un ensemble de la forme $[k+i] = \{1, 2, ..., k+i\}$ $i = 1, 2, ...$, pour chaque partition obtenue, dérouler le protocole afin de générer toutes les clés aléatoires possibles puis mener une attaque exhaustive pour trouver la bonne clé, ce qui n'est pas faisable dans un temps raisonnable, au moins pendant la durée de vie du secret partagé entre Alice et Bob. Finalement, l'implémentation du cryptosystème Vernam.

5
Cryptanalyse

Contents

Introduction

Etudier la cryptanalyse est difficile parce que nous ne trouvons pas un manuel standard, et nous ne savons pas quels sont les problèmes cryptanalytiques convenables pour les différents niveaux d'études annonça Bruce Schneier [14]. Ce document tente à rassembler et organiser la littérature existante de la cryptanalyse afin d'une bonne compréhension des techniques cryptanalytiques et les manières de casser de nouveaux algorithmes.
La cryptanalyse (du grec, "caché", et l'analýein, " pour se desserrer " ou " pour délier ") est l'étude des méthodes pour obtenir la signification d'une information chiffrée, sans accès à l'information secrète qui est sensée de l'être. Typiquement, ceci implique de savoir comment le système fonctionne et trouver la clé secrète. Dans le langage non technique, nous parlons de bris de code ou cracking de code, bien que ces expressions aient également une signification technique spécialisée. Elle est également employé pour se rapporter à n'importe quelle tentative de circonvenir la sécurité d'autres types d'algorithmes et protocoles cryptographiques en général et pas seulement le cryptage.
Les méthodes et les techniques de la cryptanalyse ont changé rigoureusement à travers l'histoire de la cryptographie, s'adaptant à la croissance de la complexité cryptographique, s'étendant des méthodes de papier et stylo de passé, par les ordinateurs colossaux pendants la deuxième guerre mondiale, aux arrangements sur ordinateur du présent. Les résultats de la cryptanalyse ont également changés, il n'est plus possible d'avoir le succès illimité dans le déchiffrement, et il y a une classification hiérarchique de ce qui constitue une attaque. Au milieu des années 70, une nouvelle classe de cryptographie a été présentée : cryptographie asymétrique. Les méthodes pour

casser ces systèmes cryptographiques sont en général radicalement différentes d'avant, et impliquent habituellement de résoudre des problèmes complexes des mathématiques pures, le plus connu, le problème de factorisation d'un nombre entier.

5.1 Que signifie briser un chiffrement ?

Le contenue de la section 5.1 vient de [14].
Briser un chiffrement ne signifie pas nécessairement trouver un moyen pratique pour une personne à l'écoute de récupérer le texte en clair en utilisant seulement le texte chiffré. Dans la cryptographie académique, les règles sont beaucoup plus souples. Briser un chiffrement revient à trouver une faiblesse dans le chiffrement qui peut être exploitée avec une complexité inférieure à une attaque de force brute. Peu importe que l'attaque par force brute requiert 2^{128} chiffrements ; une attaque demandant 2110 chiffrements sera considérée comme un succès. Briser un chiffrement pourrait aussi demander un nombre non-réaliste de textes en clair choisis, 2^{56} blocs, ou bien des quantités irréalistes de stockage : 2^{80}. Simplement dit, briser un algorithme peut être une "faiblesse certifiée" : une preuve que le chiffrement ne fonctionne pas comme prévu.
Une cryptanalyse réussie peut signifier la révélation d'un brisement d'une forme réduite du chiffrement, un DES de 8 rondes contre les 16 rondes formant un DES complet, par exemple ou une variante simplifiée du chiffrement. La plupart des cryptanalyses commencent par une cryptanalyse d'une variante aux nombres de rondes réduites, et sont éventuellement (parfois des années plus tard) étendues au chiffrement complet.

5.2 Classification des attaques

Le modèle d'attaque spécifie l'information dont l'adversaire dispose lorsqu'il tente d'attaquer un système cryptographique.
Il y a 4 types génériques d'attaques [18] :

1. Attaque à texte chiffré seulement : le cryptanalyste dispose du texte chiffré de plusieurs messages, tous ayant été chiffré par le même algorithme. La tâche est de retrouver le texte clair du plus grand nombre de messages possibles ou mieux encore de retrouver la ou les clés utilisées ce qui permettrait de déchiffrer d'autres messages chiffrés avec ces mêmes clés.
   Données : $C_1 = E_{k_1}(M_1); C_2 = E_{k_2}(M_2); \ldots; C_i = E_{k_i}(M_i)$ les k_i peuvent être distincts ou les mêmes.
   Requis : obtenir soit $M_1, M_2, \ldots, M_i$ soit k ou les k_i, soit un algorithme permettant de déduire M_{i+1} à partir de $C_{i+1} = E_{k_{i+1}}(M_{i+1})$.
2. Attaque à texte clair connu : le cryptanalyste a non seulement accès aux textes chiffrés mais aussi à leur texte en clair correspondants. La tache est de retrouver la ou les clés utilisées pour le chiffrement ou un algorithme qui permet de déchiffrer n'importe quel nouveau message chiffré avec la même clé.
   Donnée : $M_1, C_1 = E_k(M_1); C_2 = E_k(M_2); \ldots; C_i = E_k(M_i)$.
   Requis : soit K soit un algorithme permettant de déduire M_{i+1} à partir de $C_{i+1} = E_k(M_{i+1})$.
3. Attaque à texte en clair choisi : le tiers a accès aux textes chiffrés et les textes clairs correspondants et même il peut choisir les textes en clair à chiffrer. Cette attaque est plus efficace que l'attaque à texte en clair connu car le cryptanalyste peut choisir des textes clairs spécifiques qui donnent plus d'informations sur la clé, la tache consiste à retrouver la ou les clés utilisées ou un algorithme qui permette de déchiffrer n'importe quel nouveau message chiffré avec la même clé.
   Données : $M_1, C_1 = E_k(M_1); M_2, C_2 = E_k(M_2); ..; M_i, C_i = E_k(M_i)$ où le cryptanalyste choisit $M_1, M_2, \ldots, M_i$.
   Requis : soit k, soit un algorithme permettant de déduire M_{i+1} à partir de $C_{i+1} = E_k(M_{i+1})$.

4. Attaque à texte clair choisi adaptative : c'est un cas particulier d'une attaque à texte en clair choisi. Non seulement le cryptanalyste peut choisir les textes en clair mais il peut adapter ses choix en fonction des textes chiffrés précédents. Dans une attaque à texte en clair choisi, il est juste autorisé à choisir un grand bloc de texte en clair au départ tandis que dans cette attaque, il choisit un bloc initial plus petit et ensuite il peut choisir un autre bloc en fonction du résultat du premier et ainsi de suite.

Il y a au moins trois autres types d'attaques cryptanalytiques :

1. Attaque à texte chiffré choisi : le cryptanalyste peut choisir différents textes chiffrés à déchiffrer. Il obtient donc les textes en clair associés. Par exemple il a un dispositif qui fait le déchiffrement automatiquement, la tache est de trouver la clé.
   Données : $C_1, M_1 = D_k(C_1); \ldots; C_i, M_i = D_k(C_i)$.
   Requis : k.
   Cette attaque est principalement applicable aux cryptosystèmes à clé publique et même parfois applicable aux cryptosystèmes symétriques. Cette attaque et l'attaque à texte clair choisi est parfois appelé attaque à texte choisi.
2. Attaque à clé choisi : cela ne signifie pas qu'il peut choisir la clé mais il a quelques informations entre différentes clés. C'est étrange et obscur. Ce n'est pas très pratique.
3. Cryptanalyse de caoutchouc-tuyau : le cryptanalyste menace, fait des chantages, ou torture quelqu'un jusqu'à ce qu'ils lui donnent la clé. La corruption est parfois mentionnées comme une attaque très puissante et souvent la meilleure manière de casser un algorithme.

L'importance pratique d'une attaque dépend des réponses aux questions suivantes :

1. L'attaquant à quelle connaissance et capacité a-t-il besoin ?
2. Combien d'information additionnelle est déduite ?
3. Quelle est la complexité du calcul requis ?
4. Est-ce que l'attaque casse le cryptosystème tout entier, ou juste une version affaiblie ?

Les résultats d'une attaque varient en utilités. En 1998 Lars Knudsen a classé les différents types d'attaque selon la qualité et la quantité d'information découverte. Les critères pris en considération sont :
– Casse totale : l'attaquant déduit la clé secrète.
– Déduction globale : l'attaquant découvre un algorithme équivalent fonctionnel pour le cryptage et le décryptage mais sans avoir la clé.
– Déduction occasionnelle (locale) : l'attaquant découvre d'autres textes clairs (ou chiffrés) non connu au préalable.
– Déduction d'information : l'attaquant gagne quelques informations de Shannon sur le texte clair (ou chiffré) non connues au préalables.
– Algorithme distingué : l'attaquant peut distinguer le texte chiffré à partir d'une permutation aléatoire.

Les attaques peuvent être caractérisées par les ressources qu'elles exigent. Ces ressources inclurent [18] :
• Temps : le nombre d'étapes de calcul (comme le cryptage) qui doivent être exécutées.
• Mémoires : la quantité de stockage requise pour exécuter l'attaque.
• Données : la quantité de textes clairs et textes chiffrés requise.
Parfois c'est difficile de prévoir ces quantités avec précision, spécialement pour une attaque non pratique pour la mise en application pour le test.

5.3 L'analyse fréquentielle

Le contenu de cette section vient de [27].
L'analyse fréquentielle, ou analyse de fréquences, est une méthode de cryptanalyse découverte par Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah Oòmran ibn Ismaïl al-Kindi au $IX^{ème}$ siècle, il

expose les fondements de cette méthode de cryptanalyse dans son traité intitulé *Manuscrit sur le déchiffrement des messages cryptographiques*. Il découvre qu'un message chiffré conserve la trace du message clair original en gardant les fréquences d'apparitions de certaines lettres. Elle sera réinventée par Charles Babbage au $XIX^{ème}$ siècle pour permettre le déchiffrement du Chiffre de Vigenère réputé à cette époque incassable. Sa découverte restera inusitée pendant près d'un siècle. Elle consiste à examiner la fréquence des lettres employées dans un message chiffré. Cette méthode est fréquemment utilisée pour décoder des messages chiffrés par substitution (comme par exemple le Chiffre de Vigenère ou le Chiffre de César).
L'analyse fréquentielle est basée sur le fait que, dans chaque langue, certaines lettres ou combinaisons de lettres apparaissent avec une certaine fréquence. Par exemple, en français, le e est la lettre la plus utilisée, suivie du s et du a. Inversement, le w est peu usité.
Ces informations permettent aux cryptanalystes de faire des hypothèses sur le texte clair, à condition que l'algorithme de chiffrement conserve la répartition des fréquences, ce qui est le cas pour des substitutions mono-alphabétiques et poly-alphabétiques. Une deuxième condition est nécessaire pour appliquer cette technique : c'est la longueur du message à décrypter. En effet, un texte trop court ne reflète pas obligatoirement la répartition générale des fréquences des lettres. De plus, si la clé est de la même longueur que le message, il ne pourra y avoir des répétitions de lettres et l'analyse fréquentielle sera impossible.

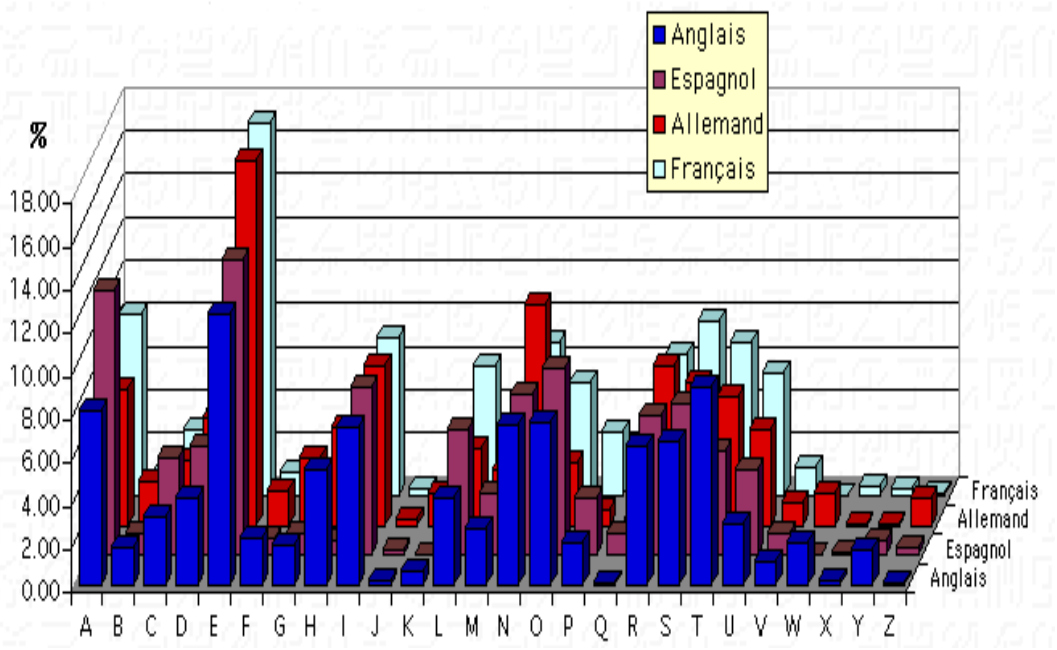


FIGURE 5.1 – Fréquences des lettres dans différentes langues [68].

5.3.1 Applications

L'analyse fréquentielle est à la base de la cryptanalyse. Elle a notamment permis le déchiffrement du chiffre de Vigenère et de bien d'autres codes fondés sur un principe similaire. Mais l'analyse fréquentielle a également permis le déchiffrement et la compréhension du linéaire B [1], qui est une langue ancienne inusitée de nos jours.

5.3.2 Limites

L'analyse fréquentielle ne peut être utilisée que pour des codes de substitutions simples (elle est par exemple inefficace contre RSA et DES). Elle ne fonctionne pas pour les chiffres de transposition.
L'analyse de fréquences ne peut pas non plus être usitée si la longueur du message est très faible, car la clé se répétera très peu et nous ne pourrons observer de particularités dans la fréquence des lettres. C'est aussi pour cette raison que l'on ne peut pas décrypter un message chiffré avec une longueur de clé égale à celle du message, car on pourrait aboutir à plusieurs textes possibles pour le même message chiffré. Nous ne pouvons donc pas dans ce cas précis déterminer le sens général du message, c'est le principe du masque jetable qui garantit un chiffrement parfaitement sûre du message.
Pour se prémunir d'une cryptanalyse par analyse fréquentielle, il existe plusieurs parades utilisées dans les algorithmes de chiffrements. Nous pouvons utiliser un chiffre homophonique. Nous pouvons également utiliser le surchiffrement, qui consiste à rechiffrer le texte chiffré pour ne pas permettre de faire des hypothèses sur les lettres les plus fréquentes. Un texte surchiffré sera donc plus difficile à déchiffrer.

1. Le linéaire B était un syllabaire utilisé pour l'écriture du mycénien, une forme archaïque du grec ancien.

5.4 Comment reconnaître un chiffre ?

En cryptanalyse nous considérons que l'attaquant connaît le cryptosystème utilisé, mais dans la réalité généralement ce n'est pas le cas. Voici quelques pistes pour reconnaître quelques chiffres [68].

Utilisation des histogrammes

En observant un message chiffré nous pouvons faire des statistiques concernant le nombre de lettres, la fréquence d'apparition de chaque lettre nous établissons ainsi un histogramme.

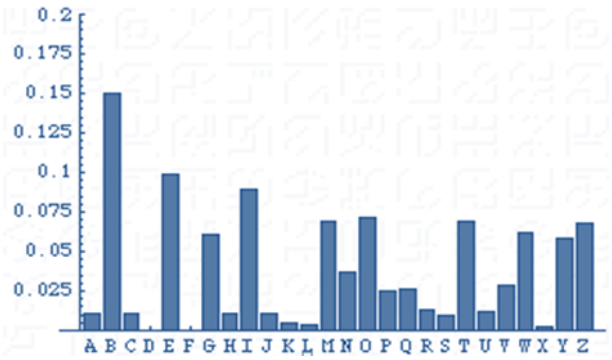


FIGURE 5.2 – Exemple d'histogramme d'une substitution simple (en français) [68].

Dans le cas d'une substitution simple, nous devons retrouver des pics correspondants aux lettres les plus fréquentes de la langue (par exemple, dans l'histogramme ci-dessus le E est très probablement remplacé par le B).

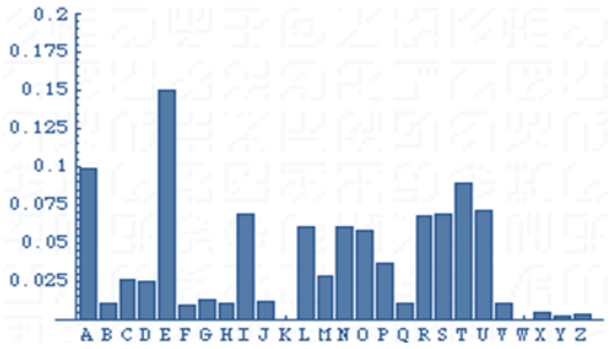


FIGURE 5.3 – Exemple d'histogramme d'une transposition (en français) [68].

Si nous ne retrouvons pas de pics, c'est que l'on a affaire à un autre type de chiffrement.

FIGURE 5.4 – Exemple d'histogramme caractéristique d'un chiffre de Vigenère (en français) [68].

Les symboles utilisés dans le cryptogramme sont des lettres
Soit n le nombre de lettres du cryptogramme.
- Si on a un nombre pair de lettres et qu'il n'y a que peu de lettres différentes, on peut les regrouper par deux et les interpréter comme des coordonnées dans une grille (voir le chiffre ADFGVX).
- S'il n'y a que 9 lettres différentes, c'est peut-être un chiffre de Collon.
- Si on a supposé qu'il s'agit d'une transposition, disposer les lettres en a lignes et b colonnes, avec $a \times b = n$. Essayer ensuite de retrouver la règle de transposition.
- Si n est un carré (p. ex 64, 81, 100, etc), il faut penser à l'utilisation d'une grille carrée, et peut-être d'une grille tournante.
- Il peut aussi s'agir d'une substitution homophonique.
- Le cryptogramme peut aussi avoir été construit à partir d'un système à répertoire.

Les symboles utilisés dans le cryptogramme sont des chiffres
Il y a plusieurs façons d'interpréter ces chiffres. En voici quelques-unes :
- Si les nombres sont compris entre 1 et 26, il s'agit peut-être d'une substitution simple, où un nombre remplace une lettre (par exemple $A = 1$, $B = 2$, etc.). Pour en être sûr, faire un histogramme.
- Si les nombres données sont compris entre -25 et 25, il s'agit peut-être de décalages par rapport à l'alphabet usuel ou à un texte qui sert de clef.
- Si on a un nombre pair de chiffres, on peut les regrouper par deux et les interpréter comme des coordonnées dans une grille (voir le chiffre de Polybe).
- Il s'agit aussi peut-être de la position d'une lettre dans un texte qui sert de clef (voir le chiffre du livre).
- Il peut aussi s'agir d'une substitution homophonique.
- Le cryptogramme peut aussi avoir été construit à partir d'un système à répertoire.

5.5 Les techniques de cryptanalyse

Comme les algorithmes cryptographiques se divisent en deux familles, la famille des algorithmes symétrique et celle des algorithmes asymétriques, alors chaque familles il lui est associé des attaques cryptanalytiques spécifiques. En outre, la cryptanalyse s'étend en deux périodes, la cryptanalyse classique et la cryptanalyse moderne. Dans la suite, nous allons exposer l'essentiel des catégories d'attaques ainsi que les techniques qui dérivent de chaque catégorie.

5.5.1 Attaques sur les algorithmes symétriques

Pour cette catégorie d'algorithmes, nous distinguons deux classes de techniques, la première concerne les cryptosystèmes classiques, quand à la deuxième s'occupe des cryptosystèmes modernes.
Techniques classiques
Attaque au niveau des clés : une solution très évidente pour trouver la clé de chiffrement qui peut traverser l'esprit est d'essayer toute les clés possibles cette solution est connu sous le non de l'attaque exhaustive ou attaque par force brute, alors si par exemple, la clé est de 56 bits, cela nécessite 2^{56} clés à tester. En raison de 100 milliards de tentative par seconde, il faudrait 10^{58} secondes pour tester toutes les clés sachant que l'âge de l'univers en seconde est 432043200000000000 secondes (10^{17} *qui donne* $137.10^{6} si\grave{e}cles$). Tous les chiffrements basés sur la substitution ou le décalage peuvent être décrypté par cette technique.
Si la clé cherchée est sous forme d'un mot de passe, le cryptanalyste a des chances à trouver la clé en testant des mots appartenant à un ensemble de mots qui sont susceptibles d'avoir constitué le mot de passe. L'ensemble engendrant touts les mots à tester est appelé dictionnaire et cette attaque est dite attaque par dictionnaire. Elle est souvent couplée à l'attaque par force brute. Une autre technique est de supposer l'existence d'un mot susceptible d'être présent dans le texte claire, comme dans le cas de substitution monoalphabétique, un mot chiffré a le même aspect que le mot clair, il suffit alors de faire des correspondances entre les caractères pour déterminer le mot en question, nous parlons alors d'attaque par mot probable.
Test de Kasiski
Teste de Kasiski dû à au Major Polonais Friedrich Kasiski 1863, est une méthode d'attaque des chiffrements de substitution polyalphabétique. Il est aussi connu que le mathématicien Britanique Charles Babbage a découvert ce teste de manière indépendante en 1846.
Le teste sert à déduire la clé utilisée dans le chiffrement. Il est basé sur l'observation de deux segments du texte clair identiques de longueur au moins trois qui sont chiffré à un même texte chiffré, pour chaque position x nous avons $x \equiv 0 \ mod \ m$ avec m la longueur de la clé.

> Congruence :
> Deux entiers relatifs sont congrus modulo p s'ils ont le même reste dans la division euclidienne par p. Ou de manière équivalente on dit qu'ils sont congrus modulo p si leur différence est un multiple de p.

En revanche, si nous observons deux segments dans le texte chiffré chacun de longueur au moins trois, alors fort possible qu'ils correspondent au même segment dans le texte clair.
Le principe de fonctionnement du teste est comme suit : nous cherchons, dans le texte chiffré, les segments identiques de longueur au moins trois. Puis, nous enregistrons les distances entre le débit de chaque segment, soient $d_1, d_2, \ldots$, après nous conjecturons que m divise le plus grand diviseur commun des d_i. Nous pouvons retenir ou rejeter la valeur conjecturée de m en appliquant un autre test dit L'indice de coïncidence. Un exemple de cryptanalyse du chiffre de Vigenère est donné dans [18].

Indice de coïncidence

L'indice de coïncidence est une technique inventé par le cryptologue militaire William Frederick Friedman en 1920 pour attaquer les chiffres de substitution polyalphabétique tel que le chiffre de Vigenère.
On appelle indice de coïncidence d'un texte la probabilité pour que, si on prenne deux lettres au hasard dans ce texte, ce soient les mêmes. Le Test de Kasiski part de l'idée que si des séquences de lettres apparaissent plusieurs fois dans un texte chiffré, c'est qu'elles proviennent d'une même séquence du texte en clair et qu'elles ont été cryptées avec la même partie de la clé, elles doivent donc être décalées d'une distance correspondant à un multiple de la longueur du mot clé (postulat [70]).
L'indice de coïncidence va permettre de préciser l'ordre de grandeur de ce mot clé.

Définition 5.1 *Supposons que $x = x_1 x_2 \ldots x_n$ soit une chaîne alphabétique à n caractères. L'indice de coïncidence de x noté $I_c(x)$ est défini comme étant la probabilité que deux éléments aléatoires de x d'indices distincts soient identiques.*
Notons les fréquences de d'apparition de A, $B, \ldots, Z$ dans x par f_0, f_1, $\ldots$, f_{25} respectivement. Nous pouvons choisir deux éléments de x de $\binom{n}{2}$ manières différentes. Pour chaque i, $0 \leq i \leq 25$, il y a $\binom{f_i}{2}$ façons de choisir les deux éléments à être la lettre correspondante à l'indice i. D'où, nous avons la formule [18] :

$$I_c(x) \quad = \quad \frac{\sum_{i=0}^{25} f_i(f_i - 1)}{n(n-1)}.$$

– Chaque langue possède un I_c qui lui est propre, voici la table établie par Friedman :
Nous pouvons trouver des I_c différents selon les sources, tout dépend bien entendu du texte d'origine sur le quel il a été calculé.

Supposons que x est une suite obtenue d'un texte en français. Notons les probabilités prévues de l'occurrence des lettres A, $B, \ldots,$ Z par p_0, $p_1, \ldots, p_{25}$ respectivement. Alors nous attendrions à ce que :

$$I_c \quad \simeq \quad \sum_{i=0}^{25} p_i^2 = 0.074, \tag{5.1}$$

puisque la probabilité que deux éléments aléatoires soient identiques est p_i^2 [18].
Supposons maintenant que nous avons un texte chiffré $y = y_1 y_2 \ldots y_m$ obtenu par le chiffre de Vigenère. Soient les m sous chaînes suivantes y_1, $y_2, \ldots,$ y_m obtenues en écrivant y en colonne dans une matrice $m \times (n/m)$. Les lignes de cette matrice sont les sous chaînes y_i, $1 \leq i \leq m$.
Sous l'hypothèse que m soit la longueur de la clé, alors chaque $I_c(y_i)$ doit être approximativement égale à 0.074. Par contre, si m n'est pas la longueur de la clé alors les sous chaînes y_i seront beaucoup plus aléatoires, puisqu'ils auront été obtenus par chiffrement en

Langue	Indice
Russe	0,0529
Serbe	0,0643
Suédois	0,0644
Anglais	0,0667
Esperanto	0,0690
Grec	0,0691
Norvégien	0,0694
Danois	0,0707
Finnois	0,0737
Italien	0,0738
Portugais	0,0745
Arabe	0,0758
Allemand	0,0762
Hébreu	0,0768
Espagnol	0,0770
Japonais	0,0772
Français	0,0778
Néerlandais	0,0798
Malaysien	0,0852

FIGURE 5.5 – Table d'indice de coïncidence pour quelques langues

utilisant des clés différentes. Sachant qu'une suite complètement aléatoire aurait :

$$I_c \approx \sum_{i=1}^{26}(\frac{1}{26})^2 = 26(\frac{1}{26})^2 = 0.038 \tag{5.2}$$

Les deux valeurs 0.074 et 0.038 sont suffisamment éloignées pour que nous puissions déterminer correctement la longueur de la clé ou bien confirmer la valeur conjecturée obtenue par application du teste de Kasiski.
Un exemple illustratif a été traité par Douglas Stinson dans [18] (section "cryptage du chiffre de Vigenère") mettant en oeuvre le teste de Kasiski et l'indice de concîdence afin de déterminer la clé de chiffrement et par conséquent le texte clair associé.

Techniques modernes

Afin de discuter ces techniques, nous allons élargir notre vision sur les algorithmes de chiffrement par bloc. Comme nous l'avons précisé déjà, le chiffrement par bloc a une structure itérative. La plus part des techniques de cryptanalyse sur les chiffrements par blocs reposent sur le fait qu'il s'agit de chiffrements itératifs. En effet, une manière pour construire un algorithme de chiffrement qui soit à la fois rapide et solide est de répéter un certain nombre de fois une transformation relativement simple. Sous l'espoir que plusieurs itérations de cette fonction, l'algorithme de chiffrement assure la sécurité du système. De façon plus formelle, pour chiffrer un bloc de message, on lui applique une fonction F paramétrée par k_1, la sous clé du premier tour, puis on applique au résultat la même fonction F paramétrée par k_2, la sous clé du deuxième tour. Après r itérations, on obtient alors le texte chiffré. Les r sous-clés $k_1, \ldots, k_r$ sont généralement obtenues à partir de la clé secrète du système K au moyen d'un algorithme de cadencement de clé.

> L'algorithme de cadencement de clé permet de calculer la clé K du $i^{éme}$ tour en fonction de la sous-clé K_{i-1} du $(i-1)^{ème}$ tour, K_0 étant la clé secrète (voir figure

5.6). Les 16 octets de la clé K_{i-1} sont pris 4 à 4. Aux 4 derniers octets, on commence par faire subir une permutation, puis on réutilise la même permutation que celle de la fonction F afin de permuter les bits de chaque octet. Ensuite, on additionne au premier octet du nouvel ensemble l'élément a_i. Cet élément est un octet qui dépend du numéro i du tour considéré. Enfin pour obtenir K_i, on ajoute bit à bit les 4 octets obtenus aux 4 premiers octets de K_{i-1}, puis le résultat obtenu est additionné aux 4 octets suivants et ainsi de suite.

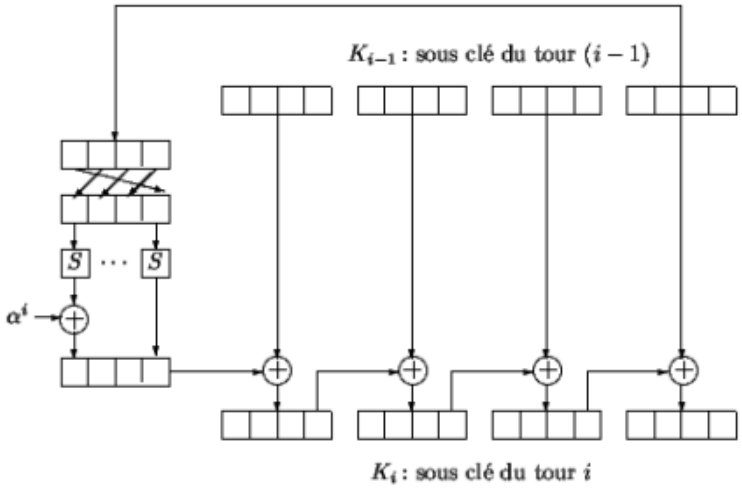


FIGURE 5.6 – Algorithme de cadencement de clés [61]

Le *DES* comporte 16 itérations d'une même fonction ; les 16 sous-clés comportent chacune 48 bits et sont dérivées d'une même clé secrète de 56 bits. De même, l'*AES* utilisant une clé de 128 bits est constitué de 10 tours, chaque tour étant paramétré par une sous-clé de 128 bits.

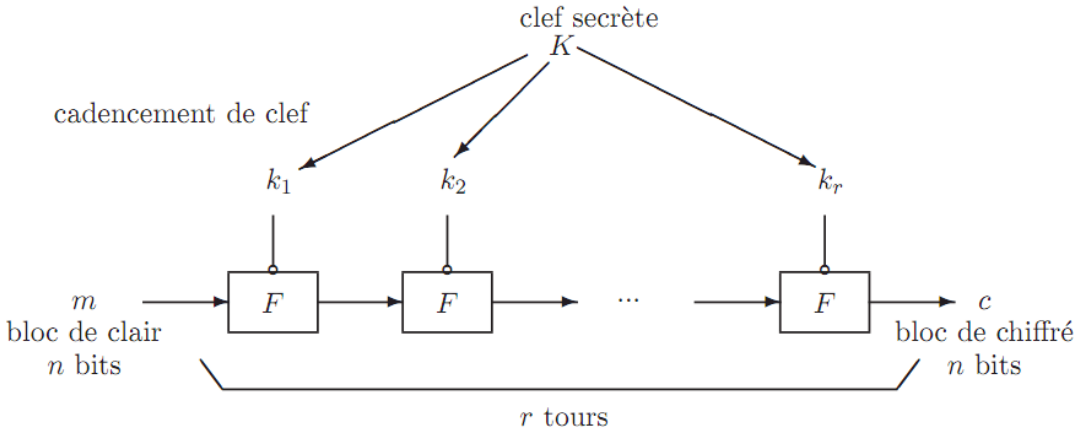


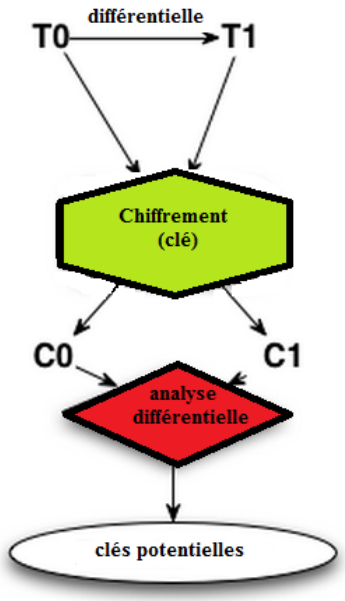
FIGURE 5.7 – Principe d'un chiffrement itératif [56].

Les attaques cryptanalytiques s'exercent sur le dernier tour car elles ont pour but de retrouver la sous-clé utilisée à la dernière itération. Après avoir mené une attaque sur le dernier tour en obtenant la clé k_r, l'attaquant peut retrouver successivement les autres sous-clés $k_{r-1}, \ldots, k_1$. En effet la découverte de k_r lui permet de supprimer la dernière itération et de se ramener à

l'attaque d'un chiffrement à $r-1$ rondes. D'où, il est possible de retrouver k_{r-1} en appliquant une attaque sur le dernier tour à ce chiffrement réduis, puis les autres sous-clés en répétant ce procédé.
Les attaques sur le dernier tour sont des attaques à clair connu ou à clair choisi. Cela signifie la connaissance d'un certain nombre de couples texte chiffré. Pour mesurer la complexité d'une attaque de ce type, on prend donc en compte son temps d'exécution de calcul mais aussi le nombre de couples clairs-chiffrés nécessaires.

Cryptanalyse différentielle

La cryptanalyse différentielle publié en 1990 par Eli Biham et Adi Shamir [51][52], était la première technique cryptographique à être découverte en dehors du monde des agences d'intelligence. Elle était la première technique permettant l'attaque des chiffrements par bloc, en premier lieu le "DES" ; de manière plus rapide que la recherche exhaustive [69].
C'est une technique qui étudie comment faire des changements spécifiques dans un texte clair, l'input de l'algorithme de chiffrement, afin d'observer des changements produits dans l'output, le texte chiffré. L'idée de base, dans sa forme la plus simple, c'est que nous sommes en mesure de sélectionner un ensemble de textes clairs, et de les crypter. Puis, sur la base des textes chiffrés obtenus nous essayons de calculé la clé.
La cryptanalyse différentielle est une forme des attaques à texte clair choisi contre les chiffrements par bloc, elle a eu cette caractéristique (différentielle) du fait qu'elle utilise des familles liées de textes en clair. Par exemple, soit la famille de textes clairs $T_0, T_1, \ldots$, où chaque T_i n'est rien d'autre que T_0 avec quelques petites différences (une petite différence signifie une différence au niveau d'un bit).
Maintenant, pour craquer un chiffrement, d'abord, ce dernier est supposé connu par le cryptanalyste. Par exemple, un DES à une clé de 56 bits, a été utilisé. Le cryptanalyste prend le premier texte clair T_0, il crypte T_0 ce qui donne C_0 en sortie. Puis, en changeant un bit dans T_0, il obtient T_1 qui donnera C_1 après le cryptage. C_1 diffère de C_0 en quelques bits. en observant l'évolution des différences entre les paires $texte\ clair/texte\ chiffré$, il est possible d'attribuer des probabilités à chaque clé possible. À force d'analyse des paires de textes, il finit soit par trouver la clé, soit par réduire suffisamment le nombre de clés possibles pour pouvoir mener une attaque exhaustive rapide.



Toute la subtilité de cette technique se situe dans le choix des textes en clair à utiliser. Cette technique était la première qui a pu casser le DES après quinze ans de sa création ce qui a

nécessité 2^{47} paires *texte clair/texte chiffré*. Un exemple de cryptanalyse d'un DES à 4−rounds est traité par Anne Canteaut dans [56].

Cryptanalyse linéaire

La cryptanalyse linéaire a été proposée par Mitsuru Matsui en 1993 [65]. Elle était conçue pour attaquer les cryptosystèmes à chiffrement par bloc, c'est une attaque à texte clair connu dans laquelle l'attaquant exploite des approximations linéaires de quelques bits des textes clairs, textes chiffrés et la clé pour les $(r-1)$ ou $(r-2)$ rounds du cryptosystème.
L'idée de base [64] est de rapprocher le fonctionnement d'une partie de l'algorithme de chiffrement par une expression linéaire où la linéarité se réfère à l'opération Xor bit à bits des inputs et outputs de l'algorithme de chiffrement. Une telle expression est de la forme

$$x_{i_1} \oplus x_{i_2} \oplus \ldots \oplus x_{i_u} \oplus y_{j_1} \oplus y_{j_2} \oplus \ldots \oplus y_{j_v} = 0. \tag{5.3}$$

Autrement dit, le cryptanalyste tente de trouver une équation linéaire
$x_1 \oplus x_2 \oplus \ldots \oplus x_i = y_1 \oplus y_2 \oplus \ldots \oplus y_j$ des bits des textes clairs et textes chiffrés en question dans une partie du cryptosystème (les parties dans les algorithmes du type DES signifient les rounds) qui maintiennent cette équation vérifiée avec une probabilité suffisamment différente de 0.5. Cela signifie que pour une attaque à texte clair connu mettant en œuvre un nombre faisable de textes clairs connus, le nombre de textes clairs pour les quels l'équation se vérifie est significativement supérieur à la moitié de la totalité.

Définition 5.2 [66] Pour une approximation linéaire donnée pour une partie du chiffrement, soit p la probabilité que l'approximation soit vraie. On réfère à $|p - 05|$ comme étant le biais de l'approximation.

Dans l'attaque d'un DES (ou ses variantes) à r rounds, nécessitant 2^{43} textes clairs connus [66], les approximations linéaires sont obtenues par la combinaison des approximations de chaque round des $(r-1)$ ou $(r-2)$ rounds sous l'hypothèse d'indépendance des clés des r rounds. Une explication bien détaillée suivie d'un exemple illustrant cette attaque sur un cryptosystème du type fiestel se trouve dans [65].
Meet-in-the-middle ou rencontre au milieu est une attaque cryptographique qui a été développée la première fois comme une attaque sur une expansion essayée du chiffrement par bloc par Diffie et Hellman en 1977. Quand nous essayons d'améliorer la sécurité d'un chiffrement par bloc, nous pourrions avoir l'idée d'employer simplement deux clefs indépendantes pour chiffrer les données deux fois. Simplement, nous pourrions penser que ceci double la sécurité de système en double-chiffrage. Certainement, une recherche exhaustive de toutes les combinaisons possibles de clés nécessite 2^{2n} tentatives si chaque clé est de longueur de n bits, par contre 2^n tentatives sont requises si une seule clé a été utilisée.

5.5.2 Attaques sur les algorithmes asymétriques

Le contenu de cette section apparait dans le document d'introduction à la cryptographie de Ghislaine Labouret [63].
Avec les algorithme asymétriques, le problème n'est pas de trouver la bonne clé par attaque exhaustive, mais de dériver la clé secrète à partir de la clé public. La plus part des algorithmes asymétriques reposant sur des problèmes mathématiques difficiles à résoudre, cela revient généralement à résoudre ce problème. C'est pour quoi les paramètres qui influencent la difficulté de résolution du problème sont les éléments déterminant la sécurité. Généralement, cela se traduit par la nécessitées d'utiliser de grands nombres, la taille de ces nombres ayant une répercussion sur la longueur des clés. Cela explique que les clés utilisées par la cryptographie à clé public soient généralement plus longues que celles utilisées par la cryptographie à clé secrète. Par exemple, dans le cas de RSA, l'élément déterminant est la taille du module. La factorisation d'un module de 512 bits est à la portée d'une agence gouvernementale, 1024 bits est considéré comme sûr actuellement, et 2048 bits garantit une sécurité à long terme (données fournies en 2005). Une étude détaillée sur l'attaque de RSA et ses variantes est donné par Jason Hinek (référence [62]).

Un point faible des algorithmes à clé public est le caractère public de la clé de chiffrement : le cryptanalyste ayant connaissance de cette clé, il peut mener une attaque à texte en clair deviné, qui consiste à tenter de deviner le texte en clair et à le chiffrer pour vérifier son exactitude. Cette particularité implique donc une restriction sur l'utilisation des algorithmes asymétriques : il faut absolument éviter de les utiliser avec un ensemble de textes en clair possibles restreint (c'est-à-dire de faible entropie). En effet, si tel était le cas, un attaquant pourrait aisément se constituer une liste exhaustive des textes en clair possibles et des textes chiffrés correspondants. Il n'aurait alors aucun mal à retrouver le texte en clair correspondant à un cryptogramme donné. D'autre part, la plupart des algorithmes asymétriques sont vulnérables aux attaques à texte chiffré choisi. Il convient donc, si l'on utilise le même algorithme pour le chiffrement et pour la signature, de s'assurer que les protocoles employés ne permettent pas à un adversaire de faire signer n'importe quel texte. Mieux, on peut avoir recours à des couples (clé public, clé privée) distincts pour ces deux opérations.

5.5.3 Attaque des fonctions de hachage

Dans cette section, nous exposons une attaque simple à la résistance forte aux collisions d'une fonction de hachage, appelée l'attaque des anniversaires. L'attaque d'anniversaire est un type d'attaque cryptographique qui exploite les techniques mathématiques qui se trouvent derrière le problème d'anniversaire (introduit ci-dessous) dans la théorie de probabilité. Cette attaque peut être utilisée pour abuser des communications entre deux ou plusieurs parties. Concernent les fonctions de hachage, l'attaque consiste à calculer autant de valeurs hachées que le temps et l'espace le permettent, et à les ranger (dans un ordre donné) avec leur images inverses, afin de chercher une collision.
Les signatures numériques peuvent être vulnérables à une attaque d'anniversaire. Un message m est généralement signé en calculant d'abord $f(m)$, où f est une fonction de hachage cryptographique, puis utiliser une clé secrète pour signer $f(m)$. Supposons qu'Alice souhaite tromper Bob à signer un contrat frauduleux. Alice prépare un contrat juste $m$et un frauduleux m'. Elle trouve alors un certain nombre de positions où m peut être modifié sans changer le sens, tels que les virgules insertion, les lignes vides, en remplacement de synonymes, etc. En combinant ces changements, elle peut créer un grand nombre de variations sur m qui sont tous des contrats équitables. De la même façon, Alice crée également un grand nombre de variations sur le contrat frauduleux m'. Elle applique ensuite la fonction de hachage pour toutes ces variations, jusqu'à ce qu'elle trouve une version du contrat équitable et une version du contrat frauduleux qui ont la même valeur de hachage, $f(m) = f(m')$. Elle présente la version juste à Bob pour la signature. Une fois Bob a signé, Alice prend la signature et elle l'attache au contrat frauduleux. Cette signature "prouve" que Bob a signé le contrat frauduleux. La stratégie d'Alice est de générer des paires d'un juste contrat et d'un contrat frauduleux en utilisant le problème d'anniversaire, Alice sait calculer la probabilité de tomber sur les couples (m, m') nécessaires pour effectuer l'attaque à partir de ses version générées précédemment. Pour cet exemple, l'équation de problème d'anniversaire exige n nombre d'hachés, tandis qu'Alice avait généré $2n$ hachés.
En probabilité, le problème d'anniversaire dérive ou bien il est un cas particulier du problème d'occupation classique.
Problème d'occupation[16] : Soit une urne contenant m boules numérotées de 1 à m. Supposons que n boules ont été tirées de l'urne au même temps, avec remise, et où leur numéros sont listés. La probabilité que t boules différentes ont été tirées est :

$$P(m,n,t) = \left\{ \begin{matrix} n \\ t \end{matrix} \right\} \frac{m^{\underline{t}}}{m^n},\ 1 \leq t \leq n. \tag{5.4}$$

Où $\left\{ \begin{matrix} n \\ t \end{matrix} \right\}$ désigne le nombre de Stirling de second espèce, et $m^{\underline{t}}$ la $t^{ième}$ puissance factorielle descendante de m, $m^{\underline{t}} = m(m-1)\dots(m-t+1)$.
Il s'ensuit que le problème d'anniversaire soit défini comme suit [16] : Une urne contenant m boules numérotées de 1 à m. Supposons que n boules ont été tirées de l'urne au même temps,

avec remise, et où leur numéros sont listés. La probabilité d'au moins une coincidence c'est-à-dire qu'une boule soit tirée au moins deux fois est :

$$P(m,n) = 1 - P(m,n,n) = 1 - \frac{m^{\underline{n}}}{m^n},\ 1 \leq n \leq m. \tag{5.5}$$

Supposons que dans une salle, il y ait 23 personnes. La probabilité que 2 personnes aient le même jour d'anniversaire est $P(365, 23) \approx 0.507$, qui est une grande probabilité ($P(365, n)$ est directement proportionnelle avec l'accroissement de n) ce qui explique pourquoi la distribution de probabilité 5.5 est appelée le paradoxe d'anniversaire.

5.5.4 Attaque des protocoles cryptographiques

Les protocoles cryptographiques ainsi que les algorithmes d'échange de clé de type Diffie-hellman sont vulnérable au man in the middle attack.
Le principe de l'attaque est que, pendant que deux parties procèdent à un échange de clé, un adversaire se positionne entre les deux parties et intercepte les échanges. De cette façon, il procède à un échange de clé avec chaque partie. À la fin du protocole, chaque partie utilisera donc une clé différente, chacune de ces clés étant connue de l'intercepteur. Pour chaque message transmis par la suite, l'intercepteur procédera à son déchiffrement avec la clé correspondante puis le rechiffrera avec l'autre clé avant de l'envoyer à son destinataire : les deux parties croiront communiquer de façon sûre alors que l'intercepteur pourra en fait lire tous les messages, voire même introduire de faux messages.
Par exemple considérons l'algorithme de Diffi-Hellman avec (G, g, A, n) et a désignent respectivement la clé publique et la clé privée d'Alice et (G, g, B, n) et b désignent respectivement la clé publique et la clé privée de Bob (G groupe d'ordre n). L'attaque se déroule comme suit :
- Alice envoie clé public $A = g^a mod\ n$ à Bob ; Eve remplace cette clé public par la sienne. Bob reçoit donc $I = g^i mod\ n$.
- Bob envoie sa clé public $B = g^b mod\ n$à Alice ; Eve remplace là aussi cette clé par la sienne.
- Alice génère le secret $K_{AI} = I^a mod\ n$. Eve génère le même secret en calculant $A^i mod\ n$.
- Bob génère le secret $K_{AI} = I^b mod\ n$. Eve génère le même secret en calculant $B^i mod\ n$.

Alice et Bob croient tous les deux être en possession d'un secret partagé, mais en fait chacun d'eux partage un secret différent avec Eve.
- Les attaques par canaux auxiliaires ou Side channel attack font partie d'une vaste famille de techniques cryptanalytiques qui exploitent des propriétés inattendues d'un algorithme de cryptographie lors de son implémentation logicielle ou matérielle. En effet, une sécurité « mathématique » ne garantit pas forcément une sécurité lors de l'utilisation en « pratique ». Les attaques portent sur différents paramètres : le temps, le bruit, la consommation électrique, etc. On en distingue deux grandes catégories :
  Les attaques invasives qui endommagent le matériel (voire le détruisent totalement).
  Attaque par sondage : elle consiste à placer une sonde directement dans le circuit à étudier, afin d'observer son comportement (généralement utilisée dans le cas des bus chiffrés).
  Les attaques non-invasives qui se contentent de procéder à une observation extérieure du système :
  Attaque temporelle : étude du temps mis pour effectuer certaines opérations.
- Cryptanalyse acoustique : étude du bruit généré par un ordinateur ou une machine qui chiffre. En effet, le processeur émet du bruit qui varie en intensité et en nature selon sa consommation et les opérations effectuées (typiquement des condensateurs qui se chargent ou se déchargent émettent un claquement facilement mesurable).
- Analyse d'émanations électromagnétiques : similaire à la cryptanalyse acoustique mais en utilisant le rayonnement électromagnétique (émission d'ondes, analyse d'une image thermique, lumière émise par un écran, etc.).
- Analyse de consommation : une consommation accrue indique un calcul important et peut donner des renseignements sur la clé.

– Attaque par faute : introduction volontaire d'erreurs dans le système pour provoquer certains comportements révélateurs. Ce type d'attaque peut être considérée comme invasive dans certains cas (un laser par exemple peut abîmer le matériel).

Ces attaques peuvent être combinées pour obtenir des informations secrètes comme la clé de chiffrement. Leur mise en œuvre est étroitement lié au matériel ou au logiciel attaqué.

Conclusion

La cryptanalyse est un ensemble de techniques et d'astuces dont l'objectif est de dévoiler l'information secrète et de fleurer toute tentative d'échange confidentiel. Elle bat l'intimité et elle sollicite le partage du secret. Comme il y a des gens qui sanctifie la confidentialité ; il y avait le besoin de créer la cryptographie et faire l'impossible pour protéger ses algorithmes et les garder solides et performants. D'autre part, il y avait aussi des gens obsédés par la divulgation de tout ce qui est secret ; ce qui a mener à fonder la cryptanalyse. La cryptanalyse, telle que la décrit Bruce Schneier, est un domaine rapidement mobile de telle sorte que tout livre de techniques serait obsolète avant qu'il soit imprimé. Il indique aussi que la seule façon pour apprendre la cryptanalyse est à travers la pratique (selon Bruce Schneier, il faut casser au moins un cryptosystème chaque semaine). Dans ce chapitre, nous avons mis un pieds dans ce champ. Nous avons expliqué que signifie l'attaque d'un chiffrement et que peuvent être les résultats obtenus. Puis nous avons classé les attaques cryptanalytiques en citant quelques grandes familles de techniques couramment utilisées par les cryptanalystes.

Conclusion générale

La cryptographie a été utilisée tout au long de l'histoire et a atteint de nos jours un niveau de sécurité jusqu'ici inégalé, et qui grâce aux avancées scientifiques et technologiques ne demande qu'à s'amplifier. De très nombreux chiffrements et autres moyens pour sécuriser une information ont été utilisés et seulement une très légère part de ces moyens de chiffrement reste considérée comme "sûre" de nos jours. Parmi les victoires de la cryptographie, nous pouvons retenir le Chiffre de Vernam, le géant Enigma qui protégea longtemps les transmissions nazies, ou encore tout récemment le robuste code AES qui chiffre les transmissions commerciales.
D'un autre côté, la cryptanalyse est parvenue de nombreuses fois à déjouer ces ruses. Par exemple, le savant Al-Kindi, qui cassa les codes de substitution mono-alphabétiques grâce à des tables de fréquence ; ou, il y a peu, le cassage du chiffrement DES, ou encore la découverte de collisions dans l'algorithme du hachage.
Malgré ces avancées technologiques faramineuses, les méthodes de chiffrement suivent les progrès technologiques et la cryptanalyse. En effet, la puissance des ordinateurs et la recherche d'algorithmes encore plus complexes a permis de dévoiler des facettes du chiffrement jusque-là jamais atteintes. Des clés de plus en plus complexes sont utilisées et des moyens très modernes sont mis en place dans le but de sécuriser au maximum les diverses informations qui peuvent circuler, par exemple sur Internet.
L'information a toujours joué le rôle d l'arme élégant, le besoin d'intimité et le désir de contrôle en poussé la cryptographie de passer du style classique au quantique en se basant sur des phénomènes naturelles en donnant naissance au concept de cryptographie quantique.
La cryptographie quantique promet de révolutionner la communication sécurisée en assurant la sécurité basée sur les lois fondamentales de la physique quantique, au lieu de l'état actuel des algorithmes mathématiques ou de technologie informatique. Les dispositifs de mise en œuvre de telles méthodes existent et la performance des systèmes de démonstration est constamment améliorée. Actuellement, des échanges d'informations se font à base de cryptographie quantique. les leadeurs de ces expériences sont la Belgique qui a marqué un record de distance dans le laboratoire de 250 km en dépassant le record pratique américain qui était de 184.6 km. Dans les prochaines années, sinon des mois, ces systèmes pourraient commencer à chiffrer certains secrets gouvernementaux et industriels classés top secret.
Dans ce manuscrit, un balayage de cryptographie constitue l'ouverture du document. Le document s'étale sur deux espaces. Le premier espace étant la cryptographie quantique, où nous avons donné un éclaircissement du concept en explorant le fond mathématique qui s'y trouve derrière. Des explications de certaines notions telles que l'état quantique, polarisation de photons, mesure quantique, distribution quantique de clés et autres ont été introduites. L'étude du premier protocole quantique nous a inspiré à créer le protocole BC10, protocole permettant la distribution de clés aléatoires secrètes qui peuvent être utiliser pour crypter des messages par le Chiffre de vernam. Ce qui a mené par la suite, au développement de l'application *CryptoStrumento version* 1.0. Tandis que le second espace est présenté sous forme d'un aperçu de cryptanalyse, accompagné d'une présentation des techniques cryptanalytiques les plus connues et les plus efficaces pour briser un cryptosystème.
Ce que nous pouvons dire, est que le présent mémoire dans une partie est sous forme d'une initiation à la cryptographie quantique, en ouvrant l'intervalle au futures recherches pour faire face aux expériences scientifiques dans les pays leadeurs avec la connaissance que cela est possible, en particulier, parce que ce domaine forme un champ jeune et fertile, où les portes de recherches et concurrence sont ouvertes dans la disponibilité du climat approprié. La création du

$BC10$ constitue une provocation pour une réalisation concrète du prototype et par conséquent réaliser des expérimentations de cryptage et de décryptage des messages chiffrés moyennant les clés fournies par ce dernier. Dans une autre partie, le mémoire est sous forme d'une enquête sur la cryptanalyse, ce qui sollicite à fournir plus d'efforts pour faire partie de cet entourage.

Bibliographie

[1] B. Schneier. *Applied Cryptography, Protocols, Algorithems, ans Source Code in C.* second edition,John Wiley and sons, Inc, 1996.

[2] C.E. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, Volume : 28 , Page : 657-715, 1949.

[3] D. Stebila. Classical Authenticated Key Exchange and Quantum Cryptography. *Thesis for degree of doctor of philosophy in Combinatorics and Optimisation, University of Waterloo, Ontario, Canada*, 2009.

[4] S. Wiesner. Conjugate coding. *unpublished manuscript circa 1970 ; subsequently made available in SIGACTNews*, Volume : 15 , Number : 1, Pages : 78-88, 1983.

[5] G. Brassard. A Bibliography of Quantum Cryptography. *Département IRO, Université de Montréal, Canada*, 3 December 1993.

[6] C.H. Bennett, G. Brassard. Quantum Cryptography : Public Key Distribution And Coin Tossing. *Proccedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Pages : 175-179, Bangalore, India, 1984.

[7] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, J.A. Smolin. Experimental Quantum Cryptography. *Journal of Cryptology*, Volume :5, Numéro : 1 Pages : 3-28, 1992.

[8] J. Preskill. *Lecture Notes for Physics 229 : Quantum Information and Computation.* California Institute of Technology, September 1998.

[9] E. Karpov, T. Durt, F.V. Berge, N.J. Cerf, T. D'Hondt. Cryptographie Quantique. *Publication de Cryptax, Phase 1, cryptax.vub.ac.be*, 2007-2010.

[10] A. Messiah. *Quantum Mechanics.* Dover, New York, 1996.

[11] J.L. Basdevant, J. Dalibart. *Mécanique Quantique.* Edition de L'école Polythechnique, 91128 Palaiseau Cedex, Mars 2008.

[12] http ://www.engineering.usu.edu/ Binary Entropy Function, ECE7690, Lecture 2 : Definitions and Basic Facts. *Publication de Cryptax, Phase 1, cryptax.vub.ac.be*, February 02, 2000.

[13] J.L. Roch. Security Models : Proofs, Protocols and Certification, Master2- Security. *Cryptography and Coding of Information Systems ENSIMAG-INP-UJF, Grenoble university, France*, 27 Octobre 2007.

[14] B. Schneier. Cours Individuels de Cryptanalyse. *http ://www.apprendre-en-ligne.net/crypto/bibliotheque/PDF/cours-cryptanalyse.pdf*, 16 Janvier 2001.

[15] S. Varrette. Introduction à la cryptographie. *Laboratoire LACS, Université du Luxemburg*, 11 Novembre 2008.

[16] A.J. Menezes, P.C. Van Oorschot, S.A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, Edition1, Canada, December 16^{th},1996.

[17] Y. Mori. *Electronique pour le traitement du signal : Théorie de l'information et du codage.* Lavoisier, Volume : 5, 2006.

[18] D. Stinson. *Cryptography : Theory and Practice.* CRC Press, March 17^{th}, 1995.

[19] S. Vaudenay. *A Classical Introduction to Cryptography : Applications for Communications Security.* Swiss Federal Institute of Technologies, Springer Science+Bussiness Media, 2006.

[20] B. Gagnon. Recherche sur la physique moderne : La cryptographie quantique. *Dans le cadre du cours d'Ondes et Physique Moderne, Collège Gérald Godin, Sainte-Geneviève, Québec, Canada*, 1 Juin 2005.

[21] La physique quantique. molaire1.perso.sfr.fr/quantic.html.

[22] T. Koshy. *Catalan Numbers with Applications.* Framingham State College, Oxford University Press, 2009.

[23] C. Berger. Topologie pour la licence : Cours et exercices. *Université de Nice-Sophia*, 24 Janvier 2004.

[24] Venona Documents. *http ://www.nsa.gov*, June 1942.

[25] M. Hendrych. Experimental Quantum Cryptography. *Doctoral Thesis, Department of Optics, Faculty of Natural Sciences, Palacky University, Olomuc, Czech Republic*, September 2002.

[26] H. F. Gaines. *A Cryptanalysis : A study of ciphers and their solution.* Dover Publications INC., 1956.

[27] S. Simon. *The Code Book.* First Anchor Books Edition, September 2000.

[28] O. Ahonen. Quantum Cryptography Protocol Based on Sending Entangled Qubit Pairs. *Master's Thesis, Department of Ingineering Physics and Mathematics, Helsinky University of Technology*, March 1^{st} 2007.

[29] G. Brassard. *Lecture Notes in Computer Science.* Edited by G. Goos and H. Hartmanis, Springer-Verlag Berlin Heidelberg, 1988.

[30] M. Langlois. Cryptographie Quantique - Solution au problème de distribution de clefs secrètes. *Université d'Ottawa*, Décembre 1999.

[31] W.K. Wooters, W.H. Zurek. A Single Quantum Cannot Be Cloned. *Nature 299*, Pages : 802-803, 1982.

[32] R.G. Newton. *Quantum Physics : A Text for Graduate Students.* Springer-Verlag New York, Inc., 2002.

[33] Chaire de Physique Atomique et Moléculaire. $3^{ème}$ cours : Les photons, une source de perturbation pour les atomes, Chapitre 05 : Les super-opérateurs quantiques, Décomposition de Kraus. *Collège de France*, 12 Mai 2004.

[34] J. Batuwantudawe. New Techniques for Security Proofs of Quantum Cryptography. *Master's Thesis of Mathematics in Computer Science, University of Waterloo, Ontario, Canada*, 2005.

[35] H. Brezis. *Analyse Fonctionnelle : Théorie et Applications.* Masson, 1987.

[36] L. Gallardo. Espace de Hilbert, Chapitre 05 : Opérateurs dans Les Espaces de Hilbert. Notions d'opérateur adjoint. *Laboratoire de Mathématique et Physique Théorique, Université François Rabelais, France*, 18 Mars 2008.

[37] L. Gallardo. Espace de Hilbert, Chapitre 02 : Le théorème de projection et ses applications. *Laboratoire de Mathématique et Physique Théorique, Université François Rabelais, France*, 21 Décembre 2007.

[38] R. Folman. Course : Atomes and Molecules. Lecture 10 : Walks on the Bloch sphere : Coherent manipulations of an atomic two-state system. *Ben Gurion University, Negev*, November 28^{th}, 2006.

[39] Optique Ondulatoire. Chapitre 08 : Polarisation, introduction aux milieux biréfringents, éléments d'optique non-linéaire. *UFR de Physique, Université Denis Diderot Paris 7*, 01 Juillet 2008.

[40] Université en Ligne. Ondes éléctromagnétiques. *uel.unisciel.fr*, 26 Avril 2010.

[41] J. M. Courty. Notes de cours : Ondes éléctromagnétiques et rayons lumineux. *Université Pierre et Marie Curie, France*, Mai 2006.

[42] W.K. Wooters, W.H. Zurek. The no-cloningtheorem. *Quick study of Physics, Today Journal, American Institute of Physics*, Pages : 76-77, February 2009.

[43] M. Le Bellac. *Physique Quantique.* EDP Sciences/CNRS éditions, 2003.

[44] J. Polkinghorne. *Quantum Theory : A Very Short Introduction.* Oxford University Press, 2002.

[45] S. Cobourne. Quantum Key Distribution Protcols and Applications. *Technical Report, Department of Mathematics, University of London*, March 8^{th}, 2011.

[46] A. Kerckhoff. La cryptographie militaire. *Journal des sciences militaires*, Volume : 09, Pages : 05-83, Janvier 1883.

[47] A. Kerckhoff. La cryptographie militaire. *Journal des sciences militaires*, Volume : 09, Pages : 161-191, Février 1883.

[48] T. Peyrin. Les fonctions de hachage, un domaine à la mode. *Paris*, 17 Mars 2009.

[49] L. Fousse. Cours crypto : Fonctions de hachage. 10 Novembre 2008.

[50] J. McLaughlin. Differential cryptanalysis. *Technical Report, Department of Computer Science, University of York*, May 2011.

[51] E. Biham, A. Shamir. Differential cryptanalysis of DES-like cryptosystem. *Technical report CS90-16, Weizmann Institute of Science*, July 1990.
http ://www.cs.technion.ac.il/ biham/Report/Weizmann/cs90-16.ps.gz.

[52] E. Biham, A. Shamir. Differential cryptanalysis of DES-like cryptosystem (extended abstract). *In A.J. Menezes and S.A. Vanstone, editors, Advances in cryptology - crypt'90, volume 537 of Lecture Notes in Computer Science*, Pages : 2-21, IACR, Springer, 1990.

[53] N. Ferguson, B. Schneier. *Cryptographie en pratique : Primitives, Algorithmes, Protocoles, Standards, Gestion de clé.* Wiley Sons 2003, Vuibert Paris 2004.

[54] D. Lemire. Théorie de l'information. *Cours en ligne, Semaine 02 : Théorie de l'information, Université à distance de L'Uqam, Canada*, 12 - 19 Juin 2011.

[55] G. S. Vernam. Cipher Printing Systems for Secret Wire and Radio Telegraphic Communications. *J. AIEE 45*, Pages : 109-115, 1926.

[56] A. Canteaut. Cryptanalyse de chiffrement à clef secrète par blocs. *Article paru dans MISC - Le magazine de la sécurité informatique*, Mars 2002.

[57] http ://www.nikon.com/about/feelnikon/light/chap04/sec01.htm, March 2010.

[58] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics 4, 686–689 (2010) doi :10.1038/nphoton.2010.214 Received 02 April 2010 Accepted 11 July 2010* Published online 29 August 2010.

[59] Vulnerability in commercial quantum cryptography tackled by international collaboratio. *Press release.*August 29^{th}, 2010.

[60] H. M. Phuong. Descritption du protocole BB84 en trois dimensions. *Mémoire de fin d'études, Institut de la Francophonie pour l'Informatique, Ecole National Supérieure de Télécommunication*, 1 Avril 2005.

[61] P. Loidreau. Introduction à la cryptographie. *LinuxFocus article http ://linuxfocus.org*, Number 243, 14 Janvier 2005.

[62] M. J. Hinek. *Cryptanalysis of RSA and its Variants.* CRC Press, Taylor Francis Group, USA 2009.

[63] G. Labouret. Introduction à la cryptographie. *http ://www.labourte.net/crypto/*, 4 Avril 2005.

[64] H. M. Heys. A tutorial on linear and differential cryptanalysis. *Cryptologia*, XXVI(3) :189–221, 2002.

[65] M. Matsui. Linear cryptanalysis method for *DES* cipher. *In EUROCRYPT '93 : Workshop on the theory and application of cryptographic techniques on Advances in cryptology, Springer-Verlag New York, Inc*, Pages 386–397, Secaucus, NJ, USA, 1994.

[66] J. McLaughlin. Linear cryptanalysis. *Technical Report, Department of Computer Science, University of York*, May 2011.

[67] L. R. Knudsen. *Block Ciphers- A Survey.* Lecture Notes In Computer Science 1528, Springer-Verlag, 1997.

[68] http ://www.apprendre-en-ligne.net/crypto/decrypt/reconnaitre.html.

[69] E. Biham, A. Shamir. Differential cryptanalysis of the full 16-round DES. *In E.F. Brickell, Editor, Advances in Cryptology - Crypto'92, Lecture Notes in Computer Science, IACR Springer*, Volume : 740, Pages : 486-496, 1992.

[70] http ://www.gymnase-yverdon.vd.ch/branches/mathematique/cryptographie/textes /indiceexpl.htmhaut, November 2011.

[71] A. Abidin. Weaknesses of Authentication in Quantum Cryptography and Strongly Universal Hash Functions. *PHD Thesis, Division of Applied Mathematics, Department of Mathematics, Linköping University, Sweden*, June 3^{rd}, 2010.

Résumé

Résumé *: Introduction à la cryptographie quantique et aux techniques de cryptanalyse.*

La cryptographie a longtemps été réservée aux milieux diplomatique et militaire. Le développement de la société de l'information et l'évolution des réseaux de communications ont conduit à sa démocratisation, en même temps qu'ils ont fait apparaître de nouvelles exigences : assurer la confidentialité des messages ne suffit plus, il faut également assurer leur intégrité et leur authenticité. Dans cette science, on distingue la cryptographie et la cryptanalyse. La première définit et étudie les systèmes utilisés, alors que la seconde, qui fait l'objet d'une partie de notre travail, cherche à casser ces systèmes. Le chiffre de Vernam, également appelé le masque jetable, est un système qui offre une sécurité théorique absolue comme l'a prouvé Claude Shannon en 1949*, et il est considéré comme le meilleur et le plus robuste cryptosystème. Mais comme tout autre algorithme de chiffrement, il possède des difficultés de mise en œuvre, nous citons ici ; le problème de la transmission des clés. Une solution très prometteuse à ce problème a été apportée par la cryptographie quantique, qui constitue l'autre partie de notre travail. Celle-ci, quoique théoriquement parfaitement sûre, comporte encore des limites pratiques contraignantes, concernant la distance maximale et le débit plus le coût élevé de réalisation des protocoles. Pour ces raisons, nous avons développé un protocole classique inspiré du protocole quantique* $BB84$ *appelé* $BC10$ *qui sera utilisé pour fournir des clés aléatoires pour le chiffre de Vernam partagées via un canal classique.*

Mots clés : *Cryptographie, Chiffre de Vernam, Clé, Cryptographie Quantique, Protocole* $BC10$*.*

Abstract *: Introduction to quantum cryptography and to cryptanalysis techniques.*

Cryptography has long been reserved for military and diplomatic circles. The development of information society and the evolution of communications networks have led to its democratization, at the same time they did show up new requirements : to ensure the confidentiality of messages is not enough anymore, we must also ensure their integrity and authenticity. In this science, we distinguish cryptography and cryptanalysis. The first defines and explores the systems used, while the second, which is the subject of part of our work, seeks to break these systems. The Vernam cipher, also known as the one-time pad is an encryption system that provides a theoretical absolute security as demonstrated Claude Shannon in 1949 and is considered as the best and most robust cryptosystem. But like any other encryption algorithm, it has difficulties in implementation ; we quote here the problem of key transmission. A very promising solution to this problem has been provided by quantum cryptography, which constitutes the other part of our work. The latter, through theoretically perfectly secure, there are still practical limits binding on the maximum range, the throughput and the high cost of implementation of the protocols. For these reasons, we had the idea to develop a classical protocol, inspired from the $BB84$ *quantum protocol, will be used to provide keys for one-time pad cipher shared via a classical channel.*

Keywords : *Cryptography, Vernam Cipher, Key, Quantum Cryptography,* $BC10$ *protocol.*