UEL : Introduction à la physique quantique du XXI^{e} siècle
La cryptographie quantique

Jean-Baptiste Campesato

8 mai 2010

Résumé

Les premières traces de messages secrets remontent à plus de deux millénaires avant notre ère, elles reposent souvent sur des substitutions de lettres, ce qui était suffisant à l'époque vu le faible taux d'alphabétisation et l'absence d'outils de calcul. Cependant les XIX^{e} et XX^{e} siècles voient apparaître de nouvelles techniques de télécommunication qui se répandent rapidement à travers le monde et que les guerres modernes utilisent de façon abondante. Á partir de ce moment la cryptologie évolue très rapidement : il est en effet aisé d'intercepter des données cruciales, il faut donc les protéger mais aussi décrypter les communications adverses. Cet essor est renforcé au XX^{e} siècle avec l'arrivée de l'informatique et du « tout numérique » : les ordinateurs permettent de tester de très nombreuses combinaisons de substitution ou même de réaliser des attaques plus recherchées comme l'*analyse fréquentielle*. L'idée devient alors de ne plus simplement utiliser des substitutions de lettres mais de faire reposer la sécurité des messages secrets sur des calculs très longs à exécuter, c'est par exemple l'essence même des *algorithmes de cryptographie asymétrique*. Cependant chaque nouvelle génération d'ordinateurs et de techniques repousse les difficultés, il faut donc perpétuellement revoir nos critères de sécurité, ce qui n'est pas très efficace. C'est ici que la physique quantique intervient en nous proposant une solution innovante qui résout tous ces problèmes.

1 La cryptographie classique

La cryptographie (du grec ancien κρυπτός (kruptos) signifiant *caché* et γράφειν (graphein) pour *écrire*) consiste en la conception de mécanismes garantissant :

1. La confidentialité des données : il s'agit de s'assurer que l'information ne s'ébruite pas en dehors des personnes autorisées à l'obtenir, cela revient à garantir l'identité du destinataire. La principale idée présentée ici sera de communiquer une version transformée du message n'ayant aucun sens pour une personne n'étant pas en possession du mécanisme nécessaire pour retrouver le message original.
2. L'authentification : il s'agit de s'assurer que les interlocuteurs sont bien ceux qu'ils prétendent être, cette fois cela revient à garantir l'identité de l'expéditeur. Il y a plusieurs implémentations possibles, certaines étant plus simples à mettre en œuvre, d'autres plus fiables. Cela peut aller de l'utilisation d'un mot de passe, à des méthodes plus travaillées, par exemple on peut se baser sur la cryptographie asymétrique que l'on verra plus loin : l'expéditeur envoie son message crypté avec une méthode dont il est le seul à avoir la clé secrète, si sa clé publique décrypte le message, alors on est sur que c'était bien de lui (principe de *signature numérique*).
3. La non-répudiation : il s'agit de s'assurer qu'un contrat ne peut être remis en cause par l'une des parties. Cela rejoint un peu le point précédent : on doit prouver la participation d'un interlocuteur dans un échange de données.
4. L'intégrité des données : il s'agit de s'assurer que les données ne subissent aucune altération ou destruction volontaire ou accidentelle. D'un point de vu cryptographique on cherche à vérifier que les données n'ont pas été modifiées, on peut par exemple utiliser une fonction de hachage dont le principe est le suivant : on se donne une fonction dite de hachage qui prend en argument des données et dont le résultat est nommé empreinte (ou somme de contrôle), ensuite l'expéditeur envoie des données et l'empreinte qui va avec, et lorsque le destinataire reçoit les données il en calcule à son tour l'empreinte et la compare à celle qu'il a reçu, s'il observe une différence les données ont été modifiées, sinon il y a peu de chance (selon la fonction et le protocole de communication utilisés) qu'il y ait eu une modification. En dehors de la cryptographie, on peut avoir besoin de détecter, et si possible de corriger, les altérations, il s'agit du rôle des *codes correcteurs d'erreurs*.

Les fonctions de hachage peuvent aussi servir à augmenter la vitesse de recherche d'entrées dans une structure contenant des données.

Le présent travail se concentrera sur le premier point : la confidentialité des données.
Définissons d'abord le vocabulaire nécessaire : le processus permettant de transformer le message original est nommé *chiffrement*, le message chiffré est nommé *cryptogramme* et le processus inverse au chiffrement, c'est-à-dire assurant le passage du cryptogramme au message

original, est nommé *déchiffrement* si l'on est en possession du mécanisme nécessaire ou sinon *décryptage* (c'est le cas d'un espion qui obtient le cryptogramme et qui veut retrouver le message original). De même, à l'opposé de la cryptographie, on trouve la *cryptanalyse*, domaine qui s'occupe d'analyser les mécanismes de cryptographie dans le but de décrypter des cryptogrammes. La cryptographie et la cryptanalyse sont les deux branches de la *cryptologie*.

La confidentialité des données a d'abord été primordiale dans le cadre militaire, et ce dès l'antiquité, où il est important de cacher à l'ennemi les différentes stratégies de défense et d'attaque afin que ce dernier ne puisse être en mesure d'y chercher les faiblesses et aussi pour conserver l'effet de surprise. De nos jours, et avec l'avènement de l'informatique, la confidentialité des données est devenue nécessaire dans le cadre commercial (Pour cacher les avancées à la concurrence) et dans le cadre du respect de la vie privée (Les communications s'effectuant de façon numérique, et donc facilement interceptables, on ne souhaite pas qu'un individu quelconque puisse accéder à des informations personnelles, comme des données bancaires par exemple).

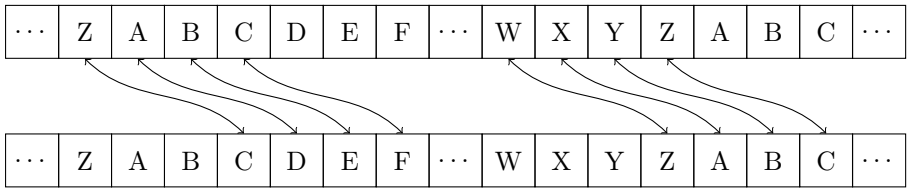
De nos jours on retrouve deux grandes familles d'algorithmes de chiffrement : les algorithmes de cryptographie symétrique et ceux de cryptographie asymétrique.

1.1 Les algorithmes de cryptographie symétrique

Ces algorithmes descendent directement de méthodes de cryptographie connues depuis relativement longtemps, nous présenterons donc deux de ces méthodes avant de vraiment définir ce qu'est un algorithme de cryptographie symétrique.

1.1.1 Le chiffrement par décalage

Le chiffrement par décalage (ou encore *chiffre de César*, car ce dernier l'utilisait avec un paramètre de décalage 3) remonte au premier siècle avant J.-C., la faible alphabétisation de la population le rendant suffisamment fiable pour l'époque.
Les interlocuteurs doivent d'abord se mettre d'accord sur le choix d'un alphabet ordonné (l'ordre des lettres compte, ce que l'on verra dans quelques lignes), c'est-à-dire l'ensemble des lettres qu'ils s'autorisent à utiliser, par exemple l'alphabet latin : $\mathcal{A} = \{\text{A, B, C,}\ldots\text{, Z}\}$ (Pour simplifier nous ne considérerons pas les espaces et les apostrophes comme des lettres et ils seront écrits tels quels, et nous n'utiliserons pas d'accents ou autres caractères spéciaux).
Ils choisissent ensuite un nombre entier positif (0, 1, 2...), il s'agit du *paramètre* de chiffrement (c'est l'ancêtre de la clé secrète des algorithmes de cryptographie symétrique).
Le chiffrement consiste ensuite à décaler chaque lettre du message selon le paramètre choisi, ainsi si le paramètre est 3, alors A devient D, B devient E...
Le déchiffrement consiste à réaliser l'opération inverse : on fait un décalage inverse, D devient A...
Ainsi si le paramètre vaut 3, on a les associations suivantes (Chiffrement : de haut en bas, déchiffrement : de bas en haut) :



Essayez de chiffrer « OUI » avec un paramètre 10, amusant non ?

Ainsi le chiffrement du message « CECI EST UN MESSAGE SECRET » avec un paramètre 3 donne le cryptogramme « FHFL HVW XQ PHVVDJH VHFUHW ».

1.1.2 Le chiffre de Vigenère

On doit le procédé qui suit à Blaise de Vigenère, diplomate français du XVI^{e} siècle. Le principe du chiffre de Vigenère est proche de celui du chiffrement par décalage sauf que cette fois le paramètre dépend de la position de chaque lettre du message d'une façon déterminée selon une clé.

De même que précédemment les interlocuteurs doivent définir un alphabet ordonné commun, sauf que cette fois ce n'est plus un nombre entier positif qu'ils partagent mais un mot formé à partir de lettres de l'alphabet. Ce mot est nommé *clé secrète*.
Le chiffrement d'un message se déroule de la façon suivante : on repète la clé suffisamment de fois de façon à ce qu'elle soit au moins aussi longue que le message et ensuite pour chaque lettre du message on réalise un décalage correspondant à la position dans l'alphabet de la lettre associée dans la clé répétée. Le déchiffrement se déroule en réalisant l'opération inverse dès lors que l'on possède la clé. Pour clarifier, un exemple :
On choisit le mot « BOHR » pour clé, et on veut chiffrer le message « LA PHYSIQUE ATOMIQUE ».
La première ligne du tableau contient la clé répétée, la deuxième ligne contient le déplacement à effectuer pour chaque lettre, la troisième ligne contient le message original et la dernière ligne contient le message chiffré après avoir effectué les déplacements.

L'usage a voulu qu'en pratique la première lettre de l'alphabet (ici A) corresponde au paramètre 0 et non 1.

B	O	H	R	B	O	H	R	B	O	H	R	B	O	H	R	B	O
1	14	7	17	1	14	7	17	1	14	7	17	1	14	7	17	1	14
L	A	P	H	Y	S	I	Q	U	E	A	T	O	M	I	Q	U	E
M	O	W	Y	Z	G	P	H	V	S	H	K	P	A	P	H	V	S

Le cryptogramme est donc : « MO WYZGPHVS HKPAPHVS ».

1.1.3 Les algorithmes de cryptographie symétrique (ou à clé secrète)

Les algorithmes de cryptographie symétrique repose sur le principe de Kerckhoffs (que l'on doit à Auguste Kerckhoffs, 1883). La *maxime de Shannon* résume bien ce principe : « l'adversaire connaît le système ».
L'idée est que la fiabilité doit reposer sur l'existence d'une clé secrète et non sur le mécanisme en lui même. Ainsi les algorithmes de chiffrement et de déchiffrement sont connus de tous, cependant l'utilisation d'une clé commune aux interlocuteurs est nécessaire pour qu'ils puissent appliquer les algorithmes de façon cohérente entre eux. Ainsi un espion peut être en possession du cryptogramme, et bien qu'il connaisse le mécanisme de déchiffrement, il ne peut décrypter le message sans avoir la clé.
La fiabilité d'un tel procédé repose sur la difficulté à obtenir la clé secrète parmi toutes les clés possibles et sur la robustesse de l'algorithme : il doit être extrêmement difficile (et de façon optimale, impossible) de décrypter le cryptogramme sans la clé secrète.
On parle de symétrie parce que les interlocuteurs ont le même niveau d'information : ils possèdent la même clé secrète.

1.1.4 Les limites des algorithmes de cryptographie symétrique

Les algorithmes de cryptographie symétrique ayant un nombre fini de clés ne sont pas fiables : en effet un espion peut appliquer une méthode dite de *brute force* qui consiste à essayer toutes les clés jusqu'à l'obtention d'un message ayant un sens. C'est le cas du chiffrement par décalage où il y a autant de clés que de lettres dans l'alphabet (par exemple 26 dans l'alphabet latin).
Les algorithmes de chiffrement polyalphabétique qui consiste à substituer une lettre par une autre qui n'est pas toujours la même et dont la substitution découle du choix de la clé que l'on répète autant de fois que nécessaire, comme le chiffre de Vigenère, ne sont guère plus fiables : en effet, du fait de la répétition de la clé, ces algorithmes ne cachent pas la structure statistique des messages originaux. L'espion peut repérer les lettres et les groupes de lettres qui reviennent le plus souvent dans les cryptogrammes et les comparer avec les lettres et les groupes de lettres qui reviennent le plus souvent dans la langue des interlocuteurs, il peut ainsi rétablir la clé. Plus la clé est utilisé souvent, plus l'étude de l'espion s'affine et plus il a de chance d'obtenir la bonne clé. On parle d'*analyse fréquentielle*.
Cette dernière attaque se généralise en fait à tous les algorithmes symétriques à partir du moment où la clé est réutilisée plusieurs fois. Deux grandes idées ont été étudiées pour remédier à ce problème, elles sont présentées dans les deux prochains paragraphes.

1.2 Les algorithmes de cryptographie asymétrique

(ou à clé publique)

On parle d'algorithme de cryptographie asymétrique (ou d'algorithme de cryptographie à clé publique) lorsqu'une personne A dispose d'une fonction *à sens unique*, c'est-à-dire injective, très rapide à appliquer tout en étant très difficile à inverser si l'on ne connait pas une brèche que la personne A a en sa possession. Cette fonction est nommée clé publique et la brèche est quant à elle nommée clé privée.
A met à disposition de tout le monde la clé publique mais garde très secrètement la clé privée. Ainsi lorsqu'une autre personne, disons B, veut envoyer un message à A, elle crypte son message en lui appliquant la clé publique et envoie le message chiffré obtenu à A. Comme A est la seule personne connaissant la clé privée, B sait que même si le message est intercepté, seule A pourra le déchiffrer.
La sécurité d'un tel procédé réside dans la difficulté à trouver la clé privée et surtout dans la difficulté à inverser la fonction donnée par la clé publique.
L'asymétrie vient du fait que les interlocuteurs ne sont pas en possession des mêmes informations : le destinataire possède la clé privée, alors que les expéditeurs possèdent la clé publique. C'est en opposition avec l'unique clé secrète que se partagent les interlocuteurs pour les algorithmes de cryptographie symétrique.
L'analyse fréquentielle ne peut rien face aux algorithmes de cryptographie asymétrique, cependant ces derniers sont souvent plus couteux à mettre en œuvre et la difficulté à inverser la fonction à sens unique est sujette à caution : ce qui est considéré comme difficile à un moment donné, peut ne plus l'être plus tard suite aux avancées technologiques. Ainsi, l'algorithme *RSA* repose sur la difficulté que l'on a à factoriser un entier positif en facteurs premiers. Bien que datant de 1977, RSA est toujours considéré comme très sur en prenant garde à prendre des entiers de plus en plus long de façon à compenser la puissance toujours en augmentation des ordinateurs, cependant Peter Williston Shor a exhibé un algorithme qui permettra de venir rapidement à bout de RSA dès qu'un calculateur quantique sera suffisamment développé. D'où la nécessité d'une nouvelle idée.

1.3 Le masque jetable (ou chiffre de Vernam, ou one-time pad)

Ce procédé a été inventé par Gilbert Vernam en 1917 puis perfectionné par Joseph O. Mauborgne (rajout de la clé aléatoire). Claude Shannon a démontré en 1949 que le masque jetable était théoriquement impossible à casser. La fiabilité de ce procédé ne repose pas sur une difficulté de calcul comme pour les algorithmes de cryptographie asymétrique, la sécurité y est donc *inconditionnelle* : elle est indépendante de l'époque. De plus le fait de ne pas reposer sur une difficulté calculatoire fait qu'il s'agit d'un procédé rapide à exécuter et facile à implémenter.
Les interlocuteurs doivent se fixer un alphabet ordonné comme plus haut, c'est-à-dire un ensemble ordonné de lettres qu'ils s'autorisent à utiliser pour communiquer et les clés seront des mots formés par des lettres de l'alphabet.
Étant donné une clé, le procédé de chiffrement et de déchiffrement est exactement celui du chiffre de Vigenère vu plus haut, ce qui change par rapport à ce dernier est que l'on ajoute quelques conditions sur l'utilisation des clés :

1. La clé doit être choisie de façon totalement aléatoire.
2. Une clé est une suite de lettres au moins aussi longue que le message à chiffrer.
3. Chaque clé ne doit être utilisée qu'une seule fois

La sécurité absolue peut s'expliquer de la façon suivante : le premier point permet de s'assurer de la difficulté à obtenir la clé pour un espion, les deux derniers points permettent de n'avoir aucune redondance possible, rendant inutile toute analyse fréquentielle.
L'argument théorique de Shannon est le suivant : d'après le deuxième point tous les textes clairs de même longueur ayant un sens peuvent donner le même cryptogramme en faisant varier la clé, puis d'après le premier point toutes les clés sont équiprobables, donc étant donné un cryptogramme, il peut découler de tous les textes clairs de même longueur que lui avec la même probabilité pour chacun d'entre eux. Le point trois rendant impossible toute analyse fréquentielle pour déterminer la clé.

On a donc obtenu un algorithme de cryptographie théoriquement inviolable, facile à implémenter (il s'agit d'un chiffre de Vigenère), rapide à exécuter et peu couteux. Cependant sa mise en œuvre s'avère assez difficile : comment générer une clé totalement aléatoire ? Comment les interlocuteurs peuvent se partager cette clé en étant sûrs qu'aucun espion ne l'ait intercepté ? C'est ici que la physique quantique rentre en jeu.

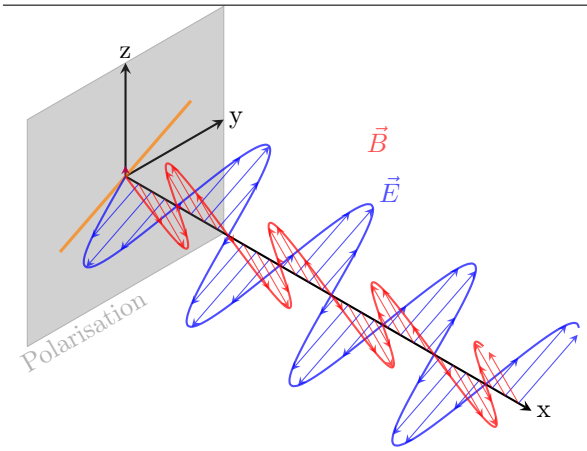
2 La cryptographie quantique

Il s'agit en fait d'implémenter le système du masque jetable grâce à des propriétés de la physique quantique : on va chercher à réaliser un dispositif permettant à l'expéditeur de générer une clé totalement aléatoire et de la partager avec le destinataire en s'assurant qu'elle n'ait pas été interceptée. Il s'agit donc en fait d'implémenter un système de cryptographie classique à l'aide de la physique quantique, c'est pour cela qu'il est préférable de parler de *distribution quantique de clés* plutôt que de *cryptographie quantique*.
Les deux protocoles fondateurs de la cryptographie quantique sont BB84 (Charles H. Bennett et Gilles Brassard, 1984) et E91 (Artur Ekert, 1991).
Nous présenterons le protocole BB84 qui nécessite de rappeller quelques notions sur la polarisation de la lumière.

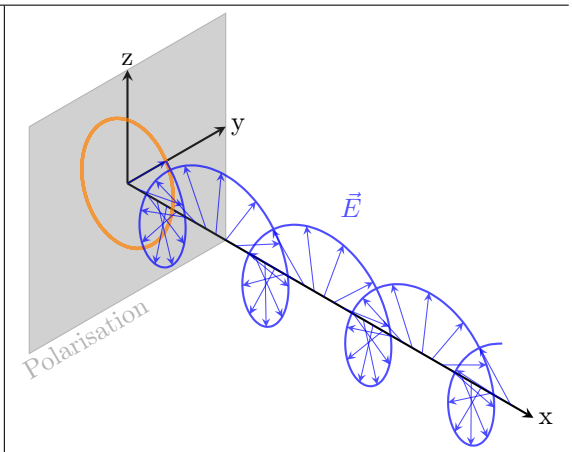
2.1 La polarisation de la lumière

Nous savons que la lumière est de nature électromagnétique, c'est-à-dire qu'elle est constituée d'un champ électrique $\vec{E}$ et d'un champ magnétique $\vec{B}$ orthogonal à $\vec{E}$.

Comme le champ magnétique $\vec{B}$ peut se déduire du champ électrique $\vec{E}$ en utilisant les équations de Maxwell, et que la majorité des instruments sont sensibles au champ $\vec{E}$, nous n'utiliserons plus que ce dernier dans la suite.
La polarisation est le comportement du vecteur champ électrique $\vec{E}$ dans le plan orthogonal à la direction de propagation. On observe trois types de lumière polarisée : elliptique, circulaire et linéaire (en fonction de la figure que l'on obtient dans le plan orthogonal à la direction de propagation). La lumière provenant d'une source incohérente (comme la lumière naturelle) est dite *non-polarisée* : il s'agit d'un mélange statistique d'états de polarisation.

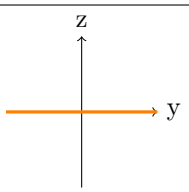
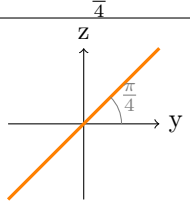
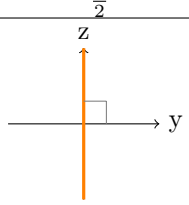
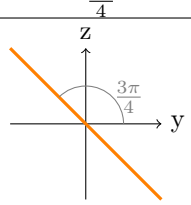


Polarisation linéaire

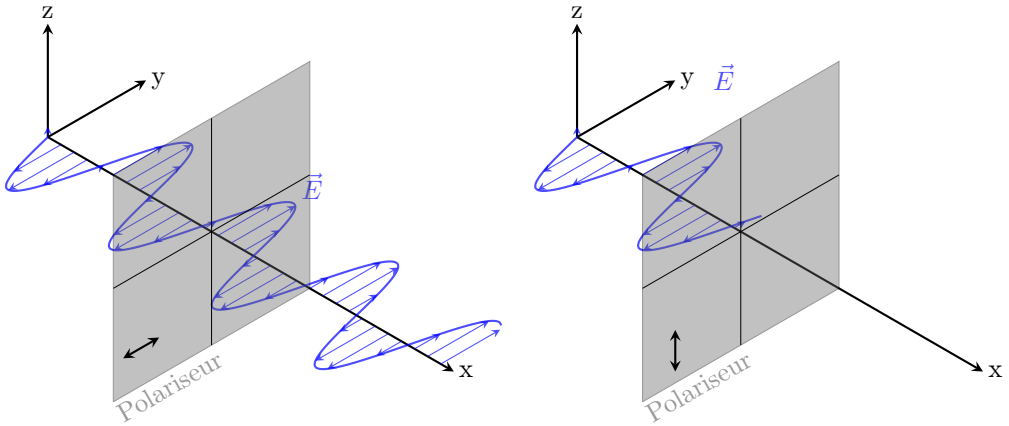


Polarisation elliptique

Dans la suite nous travaillerons avec des photons uniques polarisés de façon linéaire et selon 4 angles différents avec l'axe (Oy) :

Nom	Horizontal	Diagonal	Vertical	Antidiagonal
Angle (rad)	0	$\frac{\pi}{4}$	$\frac{\pi}{2}$	$\frac{3\pi}{4}$
Polarisation				
Vecteur unitaire	$\|\rightarrow\rangle$	$\|\nearrow\rangle$	$\|\uparrow\rangle$	$\|\nwarrow\rangle$

Nous admettons l'existence d'outils permettant de laisser passer la lumière rectilignement polarisée parallèlement à un certain axe : les polariseurs. Nous considérerons des polariseurs horizontaux, verticaux, diagonaux et antidiagonaux (avec les mêmes notations pour les vecteurs correspondants). Ces polariseurs nous permettent d'effectuer des mesures, en effet la probabilité qu'un photon rectilignement polarisée traverse un polariseur est obtenu en élevant au carré le module du produit scalaire (voir le tableau qui suit).
L'ensemble de toutes les polarisations linéaires possibles est un espace de Hilbert de dimension deux dont $\mathcal{B}_{HV} = \{|\rightarrow\rangle, |\uparrow\rangle\}$ et $\mathcal{B}_{DA} = \{|\nearrow\rangle, |\nwarrow\rangle\}$ sont des bases hilbertiennes.



Dans $\mathcal{B}_{HV}$, on a :
$|\rightarrow\rangle = 1\,|\rightarrow\rangle + 0\,|\uparrow\rangle$, $|\uparrow\rangle = 0\,|\rightarrow\rangle + 1\,|\uparrow\rangle$, $|\nearrow\rangle = \frac{1}{\sqrt{2}}\,|\rightarrow\rangle + \frac{1}{\sqrt{2}}\,|\uparrow\rangle$ et $|\nwarrow\rangle = -\frac{1}{\sqrt{2}}\,|\rightarrow\rangle + \frac{1}{\sqrt{2}}\,|\uparrow\rangle$.
Dans $\mathcal{B}_{DA}$, on a :
$|\rightarrow\rangle = \frac{1}{\sqrt{2}}\,|\nearrow\rangle - \frac{1}{\sqrt{2}}\,|\nwarrow\rangle$, $|\uparrow\rangle = \frac{1}{\sqrt{2}}\,|\nearrow\rangle + \frac{1}{\sqrt{2}}\,|\nwarrow\rangle$, $|\nearrow\rangle = 1\,|\nearrow\rangle + 0\,|\nwarrow\rangle$ et $|\nwarrow\rangle = 0\,|\nearrow\rangle + 1\,|\nwarrow\rangle$.

$\langle\Psi_1|\Psi_2\rangle$ est le produit scalaire usuel entre Ψ_1 et Ψ_2.

Ainsi si on choisit le polariseur horizontal $|\rightarrow\rangle$, la probabilité qu'un photon polarisé diagonalement $|\nearrow\rangle$ passe au travers du polariseur est : $|\langle\rightarrow|\nearrow\rangle|^2 = \frac{1}{2}$.
On est donc en mesure de remplir le tableau suivant représentant la probabilité que chaque photon traverse chaque polariseur :

	$\|\rightarrow\rangle$	$\|\uparrow\rangle$	$\|\nearrow\rangle$	$\|\nwarrow\rangle$
$\|\rightarrow\rangle$	1	0	$\frac{1}{2}$	$\frac{1}{2}$
$\|\uparrow\rangle$	0	1	$\frac{1}{2}$	$\frac{1}{2}$
$\|\nearrow\rangle$	$\frac{1}{2}$	$\frac{1}{2}$	1	0
$\|\nwarrow\rangle$	$\frac{1}{2}$	$\frac{1}{2}$	0	1

De façon plus générale on peut vérifier que si un photon est polarisé selon un axe d'angle a alors la probabilité qu'il a de passer au travers un polariseur d'axe d'angle b est de $\cos^2(b-a)$.

Remarquons qu'étant donnée une base ($\mathcal{B}_{HV}$ ou $\mathcal{B}_{DA}$), le choix entre les éléments de la base pour le polariseur importe peu : ils permettent les mêmes conclusions (quitte à intervertir 0 et 1). Á partir de maintenant on associe donc la base $\mathcal{B}_{HV}$ au polariseur $|\rightarrow\rangle$ et la base $\mathcal{B}_{DA}$

au polariseur $|\nearrow\rangle$.

Les propriétés issues du domaine de la physique quantique sont les suivantes :

- Quand la probabilité de passer au travers un polariseur n'est ni 0 ni 1, le passage ou non d'un photon n'est pas déterministe mais imprévisible.
- Le seul moyen de connaître la polarisation d'un photon est d'utiliser un polariseur.
- On ne peut connaître l'axe de polarisation d'un photon que si l'on utilise un polariseur d'axe égal ou perpendiculaire à celui du photon (sinon un photon peut, ou non, passer selon une certaine probabilité).

Ce dernier point va s'avérer crucial dans notre démarche.

2.2 Distribution quantique de clés : le protocole BB84

2.2.1 Les règles de communication

On va utiliser le système du masque jetable avec un alphabet binaire $\mathcal{A} = \{0, 1\}$. Le décalage des lettres se fera donc à l'aide de la porte binaire *ou exclusif*, notée $\oplus$ et définie selon la table de vérité suivante :

$\oplus$	0	1
0	0	1
1	1	0

Voici un exemple de chiffrement et de déchiffrement d'un message pour une clé donnée :

Clé	0	1	1	0
Message clair	1	1	0	1
Cryptogramme	1	0	1	1

Clé	0	1	1	0
Cryptogramme	1	0	1	1
Message clair	1	1	0	1

On fixe les règles suivantes :
Dans la base $\mathcal{B}_{HV}$: $|\rightarrow\rangle$ code pour le bit 0 et $|\uparrow\rangle$ pour le bit 1.
Dans la base $\mathcal{B}_{DA}$: $|\nearrow\rangle$ code pour le bit 0 et $|\nwarrow\rangle$ pour le bit 1.

2.2.2 Le protocole en lui même

Il se déroule en plusieurs étapes que l'on va présenter ci-dessous, puis que nous expliquerons. Pour plus de convivialité, et selon l'usage, nous nommons Alice l'expéditrice, Bob le destinataire et Eve l'éventuelle espionne.

1. Alice génère aléatoirement un bit dans une base ($\mathcal{B}_{HV}$ ou $\mathcal{B}_{DA}$) choisie elle aussi aléatoirement, ce que la physique quantique permet, et transmet le photon obtenu à Bob. Elle repète cette opération autant de fois que nécessaire.
2. Pour chaque photon reçu Bob choisit aléatoirement une base, c'est-à-dire un polariseur, et note si le photon traverse le polariseur.
3. Ensuite s'ensuit une phase de réconciliation : Alice et Bob communiquent entre eux (cela peut se faire publiquement, on verra pourquoi ensuite) et pour chaque photon ils comparent si leurs bases coïncident, si c'est le cas, comme on l'a vu plus haut, ils ont le même bit, qu'ils conservent, si ce n'est pas le cas le photon a pu aléatoirement (selon une probabilité de $\frac{1}{2}$, d'après ce que l'on a vu) traverser la polariseur de Bob et donc ils ne conservent pas le bit en question. Comme tous les bits ne sont pas conservés, une première remarque est qu'Alice doit envoyer un nombre conséquent de photons afin de s'assurer qu'ils aient suffisamment de photons pour obtenir une clé au moins aussi longue que le message. Comme Bob a une chance sur deux de choisir la bonne base, en moyenne on observe N erreurs pour $2N$ photons envoyés.
4. Enfin, Alice et Bob contrôlent la sûreté de la clé : parmi les bits conservés ils en choisissent un certain nombre qu'ils comparent publiquement, s'ils ont été espionnés ils obtiendront en moyenne 25% de bits différents (on explique ce 25% ci-dessous), dans ce cas ils n'utiliseront pas la clé pour se transmettre un message selon le système du masque jetable. S'ils n'ont pas de différences, alors ils peuvent conserver la clé pour l'utiliser ultérieurement. Cependant, attention, les bits choisis pour la comparaison ont été communiqués et donc ont pu être interceptés, Alice et Bob ne doivent donc pas les utiliser dans la clé, ils ont été ainsi sacrifiés.

2.2.3 Explications

Une toute première remarque est que les étapes 3 et 4 font qu'un nombre conséquent de photons envoyés ne sont pas utilisés pour la clé : il faut donc prévoir un excédent suffisant de photons pour obtenir une clé de longueur donnée.
Une propriété découlant de la linéarité de la mécanique quantique est que l'on ne peut pas cloner un photon, ainsi si Eve souhaite intercepter la clé, elle ne peut pas juste cloner les photons et attendre la communication de la phase de réconciliation pour les mesurer. C'est ce qui explique que la phase de reconciliation peut se faire publiquement, et c'est aussi ce qui explique le point 4 :
En effet, comme Eve ne peut pas cloner les photons, elle est dans l'obligation de les intercepter, de les mesurer et de renvoyer à Bob un photon similaire à celui qu'elle a mesuré. Cependant elle a une chance sur deux de choisir la mauvaise base et donc de renvoyer un photon différent de celui qu'Alice avait envoyé à Bob. Puis comme Bob a lui aussi une chance sur deux d'avoir la bonne base, en cas d'espionnage pour chaque photon on a une chance sur 4 (25%) de détecter l'intrusion (Voir l'exemple en fin de section pour plus de détails sur les différentes possibilités). Ainsi, si lors de la quatrième étape Alice et Bob testent n bits, ils ont une probabilité de $1-\left(\frac{3}{4}\right)^n$ de détecter l'intrusion.
Notons que la fiabilité des transmissions peut aussi engendrer un certain pourcentage d'erreurs (du bruit). Il faut donc choisir un seuil d'acceptation au dessus duquel on n'accepte plus les clés (risque d'interception, trop d'erreurs pour les corriger) et en dessous duquel on peut (tenter de) corriger les erreurs (c'est la théorie des *codes correcteurs d'erreurs*).

On peut cependant se demander pourquoi communiquer la clé et non directement le message, il y a deux raisons principales :

- On ne sait générer des photons que de façon aléatoire, ce qui est nécessaire pour la clé dans le système du masque jetable mais qui n'est pas optimal pour envoyer un message donné.
- Le protocole présenté ci-dessus permet juste de détecter les interceptions et non de les empêcher : si une clé est volée, le protocole permet aux interlocuteurs de le savoir, et donc de ne pas l'utiliser pour transmettre un message. Cette mesure de sécurité n'est pas suffisante pour un message : il ne suffit pas de savoir qu'un message a été intercepté, il ne doit pas l'être !

2.2.4 Exemple sans Eve

[*] d'après ce que l'on a vu, si Bob choisit la mauvaise base il a une chance sur deux de mesurer un ou l'autre des éléments de la base qu'il a choisie.

Photon envoyé par Alice	$\|\rightarrow\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$	$\|\uparrow\rangle$	$\|\nwarrow\rangle$	$\|\nearrow\rangle$	$\|\nwarrow\rangle$	$\|\uparrow\rangle$
Base choisie par Bob	$\mathcal{B}_{HV}$	$\mathcal{B}_{DA}$	$\mathcal{B}_{DA}$	$\mathcal{B}_{DA}$	$\mathcal{B}_{HV}$	$\mathcal{B}_{HV}$	$\mathcal{B}_{DA}$	$\mathcal{B}_{HV}$
Résultat de la mesure de Bob[*]	$\|\rightarrow\rangle$	$\|\nearrow\rangle$	$\|\nearrow\rangle$	$\|\nwarrow\rangle$	$\|\uparrow\rangle$	$\|\rightarrow\rangle$	$\|\nwarrow\rangle$	$\|\uparrow\rangle$
Après réconciliation	$\|\rightarrow\rangle$	✗	$\|\nearrow\rangle$	✗	✗	✗	$\|\nwarrow\rangle$	$\|\uparrow\rangle$

On obtient ainsi la clé : 0011.

2.2.5 Exemple avec Eve

Photon envoyé par Alice	$\|\uparrow\rangle$	$\|\nearrow\rangle$	$\|\rightarrow\rangle$	$\|\uparrow\rangle$	$\|\nwarrow\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$	$\|\rightarrow\rangle$
Base choisie par Eve	$\mathcal{B}_{HV}$	$\mathcal{B}_{DA}$	$\mathcal{B}_{DA}$	$\mathcal{B}_{HV}$	$\mathcal{B}_{HV}$	$\mathcal{B}_{DA}$	$\mathcal{B}_{DA}$	$\mathcal{B}_{DA}$
Résultat de la mesure de Eve, qu'elle renvoie à Bob	$\|\uparrow\rangle$	$\|\nearrow\rangle$	$\|\nearrow\rangle$	$\|\uparrow\rangle$	$\|\rightarrow\rangle$	$\|\nwarrow\rangle$	$\|\nearrow\rangle$	$\|\nwarrow\rangle$
Base choisie par Bob	$\mathcal{B}_{HV}$	$\mathcal{B}_{HV}$	$\mathcal{B}_{DA}$	$\mathcal{B}_{DA}$	$\mathcal{B}_{HV}$	$\mathcal{B}_{HV}$	$\mathcal{B}_{DA}$	$\mathcal{B}_{HV}$
Résultat de la mesure de Bob	$\|\uparrow\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$	$\|\nwarrow\rangle$	$\|\rightarrow\rangle$	$\|\uparrow\rangle$	$\|\nearrow\rangle$	$\|\rightarrow\rangle$

Plusieurs cas de figure se présentent à nous :

1. Eve et Bob ont tous les deux la bonne base, alors Eve mesure bien la bonne polarisation qu'elle renvoit à Bob et puis de même pour Bob. Le bit est valable pour la clé et Eve est passée inaperçue. Ex : premier photon envoyé.

2. Eve a la bonne base, mais pas Bob, alors lors de la réconciliation Alice et Bob décident de ne pas utiliser le photon. Eve passe encore inaperçue, mais sa bonne mesure lui est inutile. Ex : le deuxième photon envoyé.
3. Eve a la mauvaise base, mais Bob a la bonne base, alors d'après ce que l'on a vu, Bob a une chance sur deux d'obtenir une mesure compatible avec ce qu'à envoyer Alice. Donc Eve a une chance sur deux d'être detectée, de plus sa mesure est inutile. Ex : sixième photon envoyé (avec détection) et dernier photon envoyé (sans détection).
4. Eve et Bob ont la mauvaise base, alors lors de la réconciliation Alice et Bob décident de ne pas utiliser le photon, Eve passe donc inaperçue. Ex : cinquième photon envoyé.

Une fois la réconciliation terminée il ne reste que les bits des possibilités 1 et 3 qui sont équiprobables. Pour la première possibilité Eve passe inaperçue, et pour la troisième elle a une chance sur deux de se faire détecter. On retrouve bien le 25% ($\frac{1}{2}\frac{1}{2} = \frac{1}{4}$) vu ci-dessus.

2.3 Implémentations et limites de la distribution quantique de clés

2.3.1 Les attaques possibles

Nous avons déjà vu qu'il était impossible de cloner un photon, donc Eve ne peut pas cloner un photon et attendre la réconciliation pour obtenir la clé. Nous avons aussi vu qu'une attaque qui consistait à mesurer selon des bases aléatoires les photons envoyés par Alice et à renvoyer à Bob le résultat de la mesure était vaine : en effet si Alice et Bob testent seulement 32bits ils ont une probabilité de $1 - \left(\frac{3}{4}\right)^{32} = 0.9999$ de détecter l'intrusion.
De même, du fait des propriétés du masque jetable toute analyse fréquentielle ou toute attaque par force brute est inutile.
Ainsi plutôt que d'essayer d'attaquer le protocole en lui même, les cryptanalystes essaient d'attaquer les imperfections de l'implémentation.

Par exemple, il est très difficile d'obtenir une vraie source à photons uniques : ces dernières sont couteuses, très peu performantes en fréquence et les distances de transmission sont très faibles. On utilise donc souvent des lasers que l'on atténue de sorte à obtenir une distribution suivant une loi de poisson. Ainsi la majorité des pulsations envoient soit 0 soit 1 photon, ce qui est le but recherché. Cependant, il arrive un certain nombre de fois que les pulsations envoient au moins deux photons. Ces photons ont les mêmes propriétés et Eve peut cette fois en garder une copie et attendre la réconciliation. La clé ne sera pas complète, mais elle peut être suffisante pour obtenir quelques informations.

Eve peut aussi directement s'attaquer au générateur de photons d'Alice, soit de façon active en le piratant de façon à envoyer des photons prédeterminés, soit de façon passive en obtenant l'état du générateur afin d'essayer de prévoir les photons qu'il va envoyer. Ce dernier point peut se réaliser en envoyant des pulsations de lumière sur les équipements d'Alice entre deux envois de photons afin d'en surveiller les reflets et de tenter d'y déterminer l'état du générateur.

Sinon, Eve peut toujours utiliser certaines attaques classiques de la cryptanalyse. Elle peut ainsi utiliser une attaque par *déni de service* qui consiste à empêcher les photons d'être transmis à Bob, par exemple en coupant la fibre optique, afin de forcer Alice et Bob à utiliser un système moins fiable. Ou encore la célèbre attaque de *l'homme du milieu* (*man in the middle attack*) qui consiste à se faire passer pour un des interlocteurs dans le but de donner une clé corrompue à l'autre interlocuteur (des solutions existent pour se protéger de cela, mais on rentre dans l'étude de l'*authentification*, qui dépasse le cadre du sujet).

2.3.2 Les variantes

Les variantes reposent toutes sur la même idée que celle de BB84 mais utilisent d'autres propriétés quantiques. Ainsi on peut par exemple changer de particule (c'est-à-dire remplacer le photon) et/ou d'observable (c'est-à-dire ne plus mesurer la polarisation, mais une autre grandeur physique).
Ainsi le protocole E91 utilise toujours des photons mais repose sur le paradoxe EPR (Einstein-

Podolsky-Rose). Ce paradoxe stipule que *si deux particules sont émises et qu'une relation de conservation existe entre une de leurs propriétés (par exemple, la somme de leurs spins doit être nulle, c'est-à-dire qu'il y a intrication de l'état du système de ces deux particules), la connaissance de l'état de la première après une mesure effectuée sur celle-ci nous informe de l'état dans lequel se trouve la seconde particule après une mesure effectuée sur celle-là plus tard : si la mesure sur la première particule a donné "+", et que la première particule se trouve donc dorénavant dans l'état "+", la mesure sur la seconde donnera toujours "-".* (Wikipédia)
Ce résultat est assez surprenant (avec cette formulation on peut avoir l'impression qu'une mesure sur une particule modifie immédiatement, donc plus rapidement que la lumière, l'état de l'autre particule) et plusieurs interprétations sont possibles, mais on s'éloigne du sujet.
Le protocole E91 se décrit de la façon suivante : Alice et Bob reçoivent chacun un photon provenant d'une paire de photons intriqués. Alors ils choisissent chacun aléatoirement une base pour mesurer la polarisation du photon qu'ils ont reçu. D'après ce qui précède on sait que s'ils ont choisi la même base alors ils obtiennent deux mesures corrélées (sauf si Eve a effectué une mesure et a donc renvoyé à Alice ou a Bob un photon différent). On peut donc se ramener au processus décrit dans le protocole BB84 : il y a une phase de réconciliation qui consiste à éliminer tous les photons où ils ont choisit une base différente, et ensuite ils sacrifient un certain nombre de bits de la clé pour vérifier qu'ils n'ont pas été espionnés.

2.3.3 Les implémentations

L'université de Cambridge et la société Toshiba ont réussit à implémenter le protocole BB84 à l'aide de fibres optiques avec des débits très corrects pour des distances courtes (1mb/s pour 20km de fibre, et 10kb/s pour 100km de fibre). Le laboratoire national de Los Alamos a réussit à implémenter ce même protocole sur 148.7km de fibre optique.
Ces distances sont courtes du fait des pertes dans la fibre optique. De plus on ne peut pas utiliser d'amplificateurs car ces derniers ne préservent pas la polarisation : du fait de l'impossibilité de cloner des photons, cela reviendrait à effectuer des mesures sur les photons pour les retransmettre à l'identique, mais alors l'amplificateur devrait connaitre la base de polarisation des photons qu'il reçoit, ce qui est en total désaccord avec le but recherché.
Pour augmenter les distances on doit utiliser des canaux de communication ayant le moins de bruit possible, pour cela on peut tenter d'utiliser des fibres optiques de plus en plus pures :

1. On doit éviter la présence d'impuretés pour empêcher tout phénomène d'absorption et de diffusion.
2. On doit éviter au maximum la présence de courbures, en effet, dans ces zones la réflexion n'est plus totale et on observe des pertes par réfraction.
3. On doit éviter au maximum toute épissure, qui consiste à mettre bout à bout deux fibres, en effet les lieux de contacts sont sujets à des pertes par réfraction et réflexion.

Cependant, en pratique, il est impossible d'obtenir une fibre optique sans aucune perte et donc on ne peut augmenter la distance indéfiniment.
Et il en est de même pour tout support de propagation... Peut-on alors s'en passer ?

La mécanique quantique permet de répondre positivement grâce à la *téléportation quantique* qui repose sur le phénomène d'intrication présenté ci-dessus. Il ne s'agit donc pas à proprement parler de transférer de la matière mais un état quantique mesurable entre deux particules éloignées l'une de l'autre. On utilise quand même le terme de téléportation car l'état de la particule initiale ne sera plus comme avant l'expérience une fois une fois le processus arrivé à terme. On dit que le processus est *destructif*. Cette perturbation est un phénomène quantique que l'on a pu observer lorsque l'on mesurait la polarisation d'un photon avec un polariseur.

Bennett et Brassard font partis de l'équipe à avoir initié la téléportation quantique.

Nous présentons le principe sans rentrer dans les détails : on dispose à deux endroits différents deux particules intriquées, alors une mesure sur l'une des particules fixera l'état de la seconde particule. Mais il faut auparavant définir les différents états que l'on accepte d'utiliser et leurs significations, comme ce que l'on a fait dans le cas de la polarisation, on rentre alors dans le domaine de l'*information quantique*. Notons que le protocole de téléportation usuel utilise en fait deux paires de particules intriquées, nécessite une phase proche de celle de réconciliation de BB84 où les interlocuteurs doivent se communiquer leurs mesures et utilise encore le phénomène de polarisation des photons.
La téléportation quantique est toujours au centre des recherches et certaines expériences récentes sont très concluantes.

3 Conclusion

Nous avons présenté différentes méthodes de cryptographie classique : les premières utilisent une clé pour chaque envoi de la part des interlocuteurs, cependant la redondance de lettres et de mots avec la répétition de la clé permettent d'effectuer une analyse fréquentielle dans le but d'obtenir la clé. Pour résoudre cela les cryptographes ont cherché à déplacer la difficulté : plutôt que d'utiliser de simples substitutions et de faire reposer la sécurité sur le nombre de clés possibles, ils ont essayé de faire reposer la sécurité sur des difficultés calculatoires (par exemple, pour RSA, la difficulté que l'on a à factoriser un entier en facteurs premiers). Cela a donné naissance aux algorithmes de cryptographie asymétrique.
Cependant il s'avère que l'augmentation constante de la puissance de calcul de nos machines nécessite de toujours augmenter la difficulté de nos algorithmes, et des fois en vain. Il se peut en effet qu'une nouvelle technologie anéantisse toute la difficulté d'un algorithme (par exemple l'ordinateur quantique avec l'algorithme de Shor pour RSA).
C'est ici que le masque jetable rentre en jeu, on a en effet vu qu'il était inconditionnellement sûr. Du moins en théorie. Car en pratique on doit réussir à générer une clé aléatoire et à la communiquer en vérifiant qu'elle n'a pas été corrompue. C'est ce que permet de faire la mécanique quantique.
On a ainsi présenté un protocole de distribution quantique de clés, BB84, qui est théoriquement incassable. Cependant bien que le procédé soit en lui-même inviolable, l'implémentation rencontre quelques faiblesses. Par exemple, pour des questions de coûts, on ne respecte pas toujours les conditions théoriques (à savoir une source de photons uniques pour BB84) ce qui génère quelques failles. Ainsi les cryptanalystes peuvent reporter leurs recherches, et plutôt que de se concentrer sur les messages, ils peuvent se concentrer sur l'implémentation. De plus, on n'arrive pas encore à implémenter la distribution quantique de clés sur de longues distances.

On a donc un procédé théoriquement inviolable mais il faut bien garder à l'esprit qu'il s'agit de méthodes toujours au cœur des recherches et il ne faut pas non plus sous-estimer la ruse des cryptanalystes.