Cryptographie quantique

Protocole BB84

Philippe Jorrand
CNRS
Laboratoire Leibniz, Grenoble, France
Philippe.Jorrand@imag.fr

Cryptographie

La sécurité d'un canal de communication
n'est jamais garantie à 100%

Cryptographie classique :

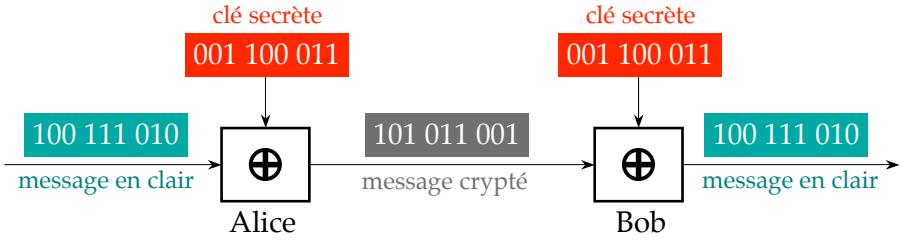
- Cryptographie à clé secrète : Alice crypte avec une clé. Bob décrypte avec la même clé. Cette clé est connue par Alice et Bob, et par personne d'autre.
- Cryptographie à clé publique : Alice crypte avec la clé publique de Bob, connue par tout le monde. Bob décrypte avec sa clé privée, connue de lui seul.

Cryptographie classique : quelques écueils

- Cryptographie à clé secrète
  - Le cryptage peut être absolument sûr, à condition que la clé soit secrète
  - Exige la sécurité absolue du canal par lequel la clé est distribuée
  - L'observation passive d'un canal est toujours possible
  - Recours à une sécurité non prouvée pour distribuer la clé
- Cryptographie à clé publique
  - Sécurité fondée sur des conjectures mathématiques non prouvées (comme la complexité exponentielle de la factorisation des entiers : avec une performance de 100 teraflops, 30 000 ans pour factoriser un nombre de 300 chiffres)
  - Une preuve invalidant une telle conjecture détruirait rétroactivement la sécurité de tout message crypté de cette façon
  - L'algorithme quantique de Peter Shor factorise les entiers en temps polynomial (dès qu'un ordinateur quantique est disponible, moins de 10 secondes pour factoriser un nombre de 300 chiffres)

Le *one-time pad* : sécurité absolue et prouvée

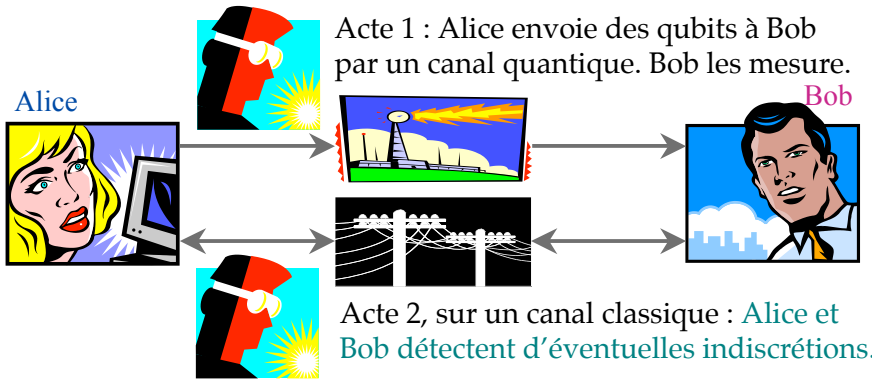
- Gilbert Vernam, AT&T, 1917 : $(m \oplus k) \oplus k = m$



- Joseph Mauborgne, US Army, années 20 : si la clé est une suite aléatoire, le message crypté est une suite aléatoire, sans information si on ignore la clé.
- Deux conditions :
  - La clé doit être secrète
  - La clé ne doit être utilisée qu'une seule fois
- Cryptographie quantique : garantir le secret de la clé sans faire d'hypothèse sur la sécurité offerte par les canaux utilisés pour distribuer la clé.

Cryptographie quantique : acteurs, décor, scénario

Eve intercepte les qubits, les mesure et les fait suivre à Bob.



Acte 1 : Alice envoie des qubits à Bob par un canal quantique. Bob les mesure.

Acte 2, sur un canal classique : Alice et Bob détectent d'éventuelles indiscrétions.

Eve écoute aussi les conversations d'Alice et Bob

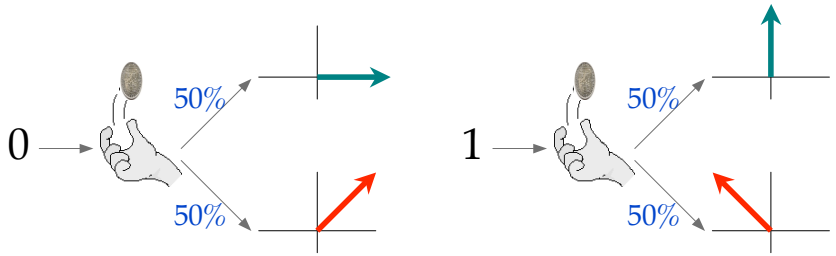
Retour sur la mesure quantique

Etat avant mesure	Dans la base standard: Proba.	Etat après mesure	Valeur obtenue	Dans la base diagonale: Proba.	Etat après mesure	Valeur obtenue
→	1	→	0	0.5	↗	0
				0.5	↘	1
↑	1	↑	1	0.5	↗	0
				0.5	↘	1
↗	0.5	→	0	1	↗	0
	0.5	↑	1			
↘	0.5	→	0	1	↘	1
	0.5	↑	1			

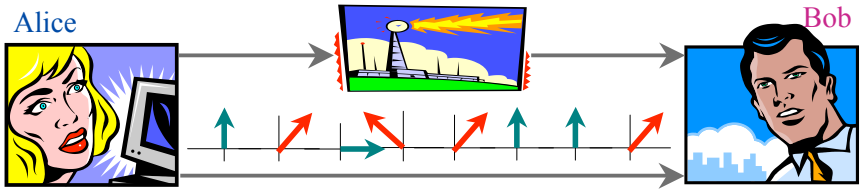
Protocole BB84 (Bennett - Brassard, 1984)

Acte 1, Scène 1 : Alice envoie des qubits à Bob par le canal quantique

- Alice construit d'abord chez elle une suite aléatoire de 0 et de 1, 4 fois plus longue que la clé confidentielle dont Alice et Bob auront besoin plus tard.
- Alice envoie ces 0 et ces 1, un par un, à Bob, codés chaque fois par un qubit. Pour chaque 0 et chaque 1, elle choisit au hasard entre 2 codages possibles :

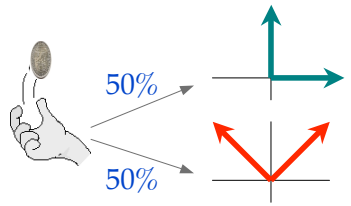


BB84 : Acte 1, Scène 2



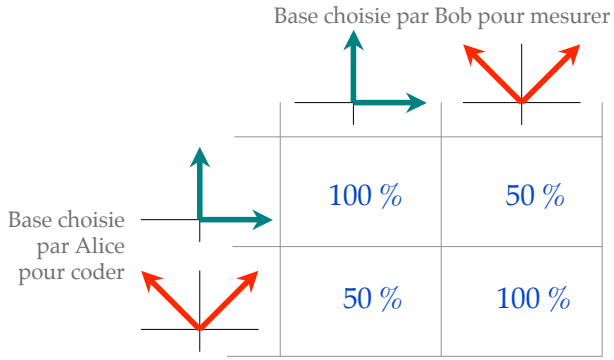
- Pour chaque qubit qu'il reçoit, Bob ne sait :
  - ni si Alice a codé un 0 ou un 1 avec ce qubit
  - ni dans quelle base, standard ou diagonale, Alice a codé ce 0 ou ce 1

- Pour chaque qubit reçu, Bob tire au hasard la base dans laquelle il va le mesurer :

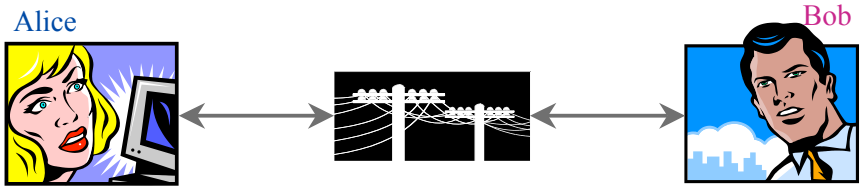


BB84 : situation à la fin de l'Acte 1

- Pour chaque 0 et 1 de la suite aléatoire qu'Alice a chez elle, Bob obtient un 0 ou un 1. Bob construit ainsi chez lui une suite aléatoire de 0 et de 1.
- La probabilité d'avoir la même valeur, 0 ou 1, à la même position dans ces deux suites, dépend des bases choisies par Alice et Bob à cette position :



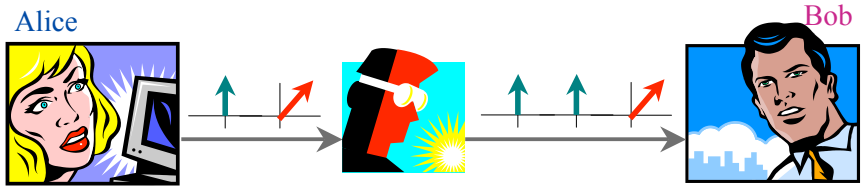
BB84 : Acte 2, Scène 1, sur le canal classique



- Alice dit à Bob la suite des bases qu'elle a utilisées pour coder, sans révéler si c'était un 0 ou un 1 qu'elle avait codé.
- Bob dit à Alice la suite des bases qu'il a utilisées pour mesurer, sans révéler si c'est un 0 ou 1 qu'il a obtenu.
- Ils ne conservent, chacun de leur côté, que les 0 et les 1 des positions pour lesquelles ils ont utilisé les mêmes bases, soit approximativement la moitié des 0 et des 1 de la suite initiale d'Alice.

Ceci pourrait former une clé secrète ... sauf si ...

BB84 : les indiscrétions d'Eve



Pendant l'Acte 1, Eve a pu observer le canal quantique :

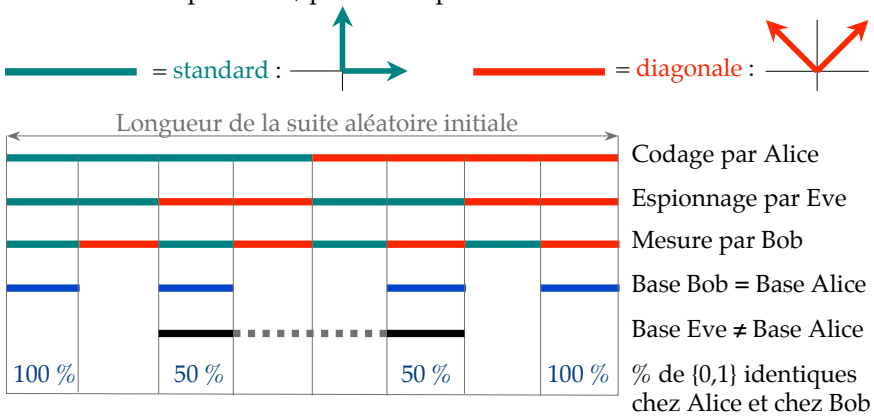
- Intercepter les qubits.
- Les mesurer dans une base qu'elle a dû, comme Bob, choisir au hasard.
- Renvoyer à Bob chaque qubit ainsi intercepté et mesuré, Bob croyant que ce qubit vient d'Alice.

Conséquences :

- Chaque fois qu'Eve choisit la même base qu'Alice, le qubit reçu par Bob est identique à celui envoyé par Alice. Cette indiscrétion est indétectable.
- Mais si Eve ne choisit pas la même base qu'Alice, le qubit reçu par Bob est différent de celui envoyé par Alice. Cette indiscrétion laisse des traces.

BB84 : traces laissées par les indiscrétions d'Eve

- Bases utilisées par Alice, par Eve et par Bob :



- Si Eve a espionné, 25 % des {0,1} conservés par Alice et par Bob sont différents bien qu'ils aient utilisé des bases identiques.

BB84 : Acte 2, Scène 2, encore au téléphone

- Alice et Bob choisissent au hasard 50 % des positions de {0,1} qui avaient été retenues à l'issue de l'Acte 2, Scène 1.
- Ils comparent ces {0,1}, position par position, dans la suite d'Alice et dans la suite de Bob. Ils sacrifient ces positions, car Eve peut écouter.
- La probabilité qu'ils soient tous identiques malgré un espionnage décroit de façon exponentielle avec le nombre n de {0,1} comparés : $(3/4)^n$ (soit 3.10^{-13} pour n=100).
- Si le taux d'erreurs est de l'ordre du taux dû à une ligne normalement bruitée, le 1/4 restant est une clé confidentielle après correction d'erreurs (et amplification de confidentialité si nécessaire). Sinon, ils recommencent.

Cryptographie quantique : état de l'art

- La « cryptographie » quantique n'est pas de la cryptographie, car rien n'est crypté. En anglais : *Quantum Key Distribution* (QKD).
- Plusieurs protocoles :
  BB84 utilise 4 états pour coder les {0,1}
  B92 (Bennet) utilise 2 états non orthogonaux
  EPR (Ekert) utilise des mesures d'états intriqués (paires EPR)
  Et beaucoup de variantes. Ils exploitent tous les perturbations des états quantiques inévitablement provoquées les indiscrétions.
- Ces protocoles doivent être complétés par des procédures classiques de réconciliation (correction d'erreur) et d'amplification de confidentialité.
- Plusieurs formes d'attaques prises en compte, car Eve peut être plus subtile que « *j'intercepte tout, je mesure tout et je renvoie tout à Bob* ».
- Exploitation des propriétés de l'information quantique pour traiter d'autres problèmes : authentification, partage de secrets.

La cryptographie quantique sur le marché

- Expérimentée sur 50 à 100 kilomètres (qubit = photon) sur fibre optique, dans l'air. Performances encore modestes (100 kbps, NEC)
- id Quantique (Genève)
  Premier système commercial de distribution quantique de clés :

- MagiQ Technologies (New York et Boston)
- QIPC « EQUIS » project (Heriot-Watt University et Corning, UK)
  Intégration dans des PC standards
- Thalès, British Telecom, Swiss Telecom, IBM, Lucent, AT&T, NEC, etc.
- Réseaux de distribution envisagés par des institutions financières, échanges de clés terre-satellites en cours de conception (US, Europe)