# La cryptographie dans un monde quantique

Sébastien Gambs

Chercheur post-doctorant CNRS

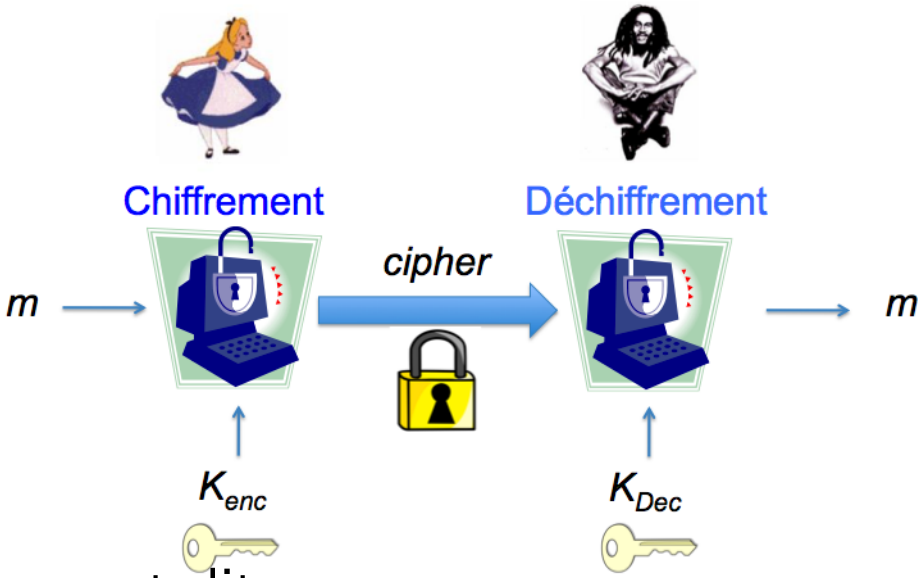
Laboratoire d'Analyse et d'Architecture des Systèmes (LAAS)
Groupe : Tolérance aux fautes et Sûreté de
Fonctionnement informatique (TSF)

28 avril 2009

# Introduction

# Cryptographie

La cryptographie est la "*science du secret*".
Exemple de tâche cryptographique : permettre à deux personnes de communiquer de manière confidentielle.




Un cryptosystème est dit :

- symétrique si $K_{Enc} = K_{Dec}$.
- asymétrique (ou *à clé publique*) si $K_{Enc} \neq K_{Dec}$.

# Cryptographie à clé publique

- Concept inventé dans les années 1970 [1].
- Fonctionnement : la clé de chiffrement est diffusée librement alors que la clé de déchiffrement est gardée secrète.
- Avantage principal : communication confidentielle possible sans échange de clés préalable entre Alice et Bob.
- Sécurité : basé sur l'existence de *fonctions à sens unique* $f$.
  - Facile : calculer $f(x)$ étant donné $x$ (utilisé pour le chiffrement).
  - Difficile : retrouver $x$ étant donné $f(x)$ (utilisé pour le déchiffrement).
- Exemple de fonction à sens unique : factorisation.

1. Plusieurs parents : Diffie et Hellman ; Rivest, Shamir et Adelman (RSA) ; service des renseignements britannique.

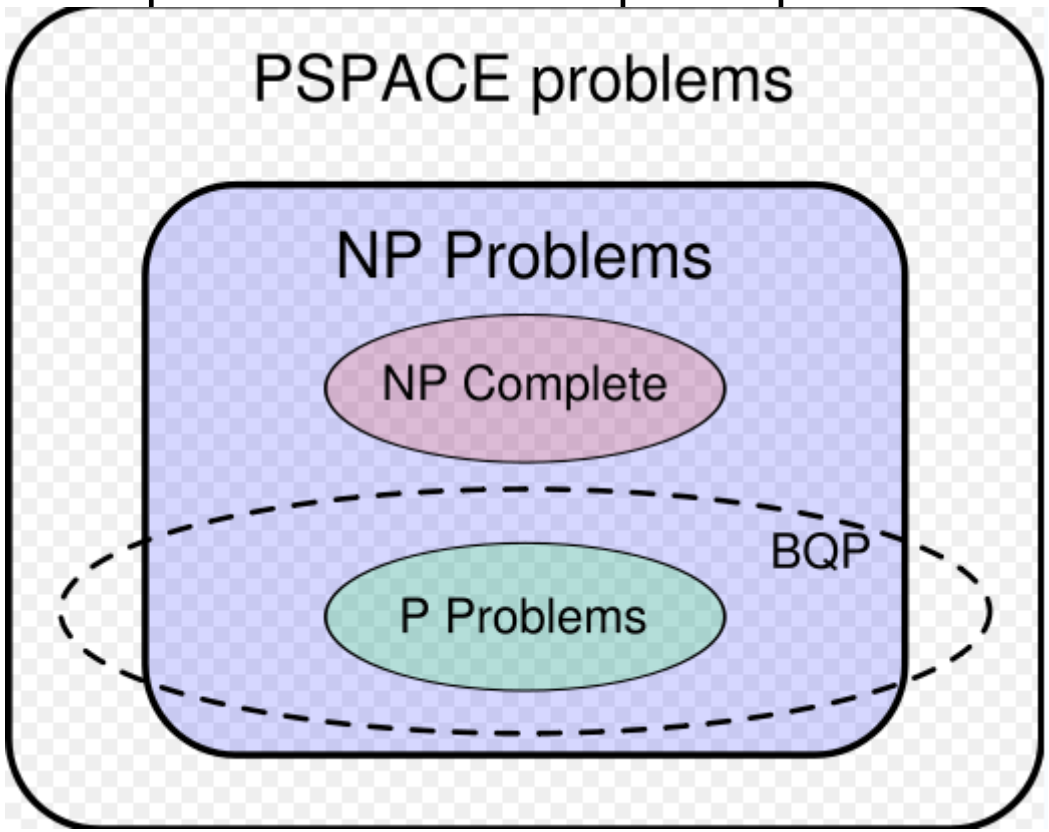
# Un petit détour par la complexité

- Classe de complexité P : problèmes pouvant être résolus en temps polynomial par un ordinateur classique.
  Exemples : plus court chemin dans un graphe, programmation linéaire, plus grand commun diviseur, ...
- Classe de complexité NP : problèmes dont la solution peut être vérifiée en temps polynomial mais où la trouver semble demander un temps exponentiel (non-prouvé).
  Exemples : problème du voyageur de commerce, coloration de graphe, SAT, ...
- Question fondamentale en informatique[2] : $P \neq NP$ ?
- Question fondamentale en cryptographie : où se situe la factorisation et le logarithme discret ?

2. Prix de 1 million de dollars offert par le Clay Mathematics Institute.

# Relation suspecté de BQP avec les autres classes

Classe de complexité BQP : problèmes pouvant être résolus en temps polynomial par un ordinateur quantique.



# Difficulté de la factorisation

- Facile : multiplier deux grand nombres premiers $x$ et $y$ ($x \times y = z$).
- Difficile : retrouver $x$ et $y$ (les facteurs) à partir de $z$.
- Meilleur algorithme classique : *cribe général de corps de nombres* (temps sous-exponentiel).
- L'algorithme de Shor (1994) résout ce problème en temps polynomial avec un ordinateur quantique (BQP).
- Conséquences : le jour où un ordinateur quantique de taille raisonnable existera en pratique, la plupart des cryptosystèmes à clé publique utilisés actuellement ne seront plus sécuritaires.
- Solution possible : cryptographie quantique.

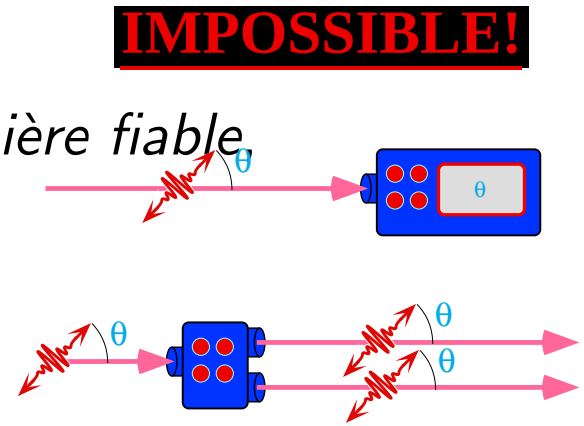
# Informatique quantique

# Information quantique

L'informatique quantique s'intéresse aux *implications de la mécanique quantique aux fins de traitement de l'information*.

L'information quantique est très différente de sa contrepartie classique, ainsi les états quantiques :

- peuvent exister dans une *superposition* d'états classiques,
- peuvent être *intriqués*,
- peuvent être *téléportés*,
- ne peuvent pas être *mesurés de manière fiable*,
- sont *perturbés par l'observation*,
- ne peuvent pas être *clonés*,
- ...



# Bit quantique

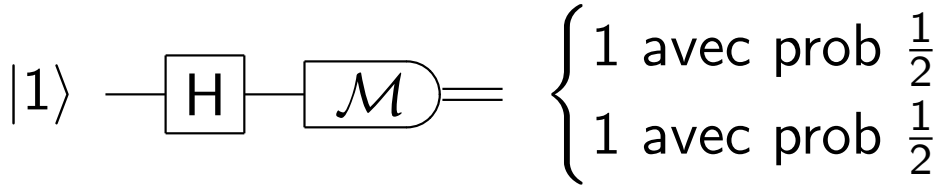
- Le qubit (ou *bit quantique*) est l'analogue quantique du bit classique.
- Il peut exister dans une *superposition* d'états.
  Exemple : un qubit est décrit comme $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ où $\alpha$ et $\beta$ sont des nombres complexes qui correspondent aux *amplitudes* des états $|0\rangle$ et $|1\rangle$ respectivement.
- Exemple d'implémentation physique d'un qubit : la polarisation d'un photon :
  $|0\rangle = |\leftrightarrow\rangle$ (polarisation horizontale)
  $|1\rangle = |\updownarrow\rangle$ (polarisation verticale)
- Effet de la mesure : quand $|\psi\rangle$ est mesuré, $|0\rangle$ est observé avec probabilité $|\alpha|^2$ ou $|1\rangle$ avec probabilité $|\beta|^2$ (et $|\alpha|^2 + |\beta|^2 = 1$).

# Porte quantique

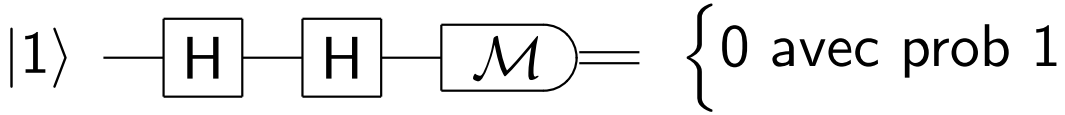
- La mesure est le seul acte *irréversible*.
- Toutes les autres opérations quantique sont *réversibles*.
- Exemple de porte quantique unaire : Walsh-Hadamard (H).

$$|0\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$
$$|1\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

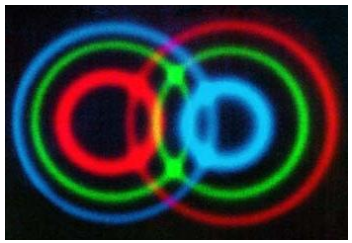
- Exemple d'un générateur aléatoire :




- Walsh-Hadamard est auto-inverse :



# Intrication

- Existence d'états quantiques qui ne peuvent par être décrits séparément dit intriqués
  Exemple : deux photons 
- Appelé par Einstein "*spooky action at a distance*" (1935).
- Mesuré expérimentalement par Alain Aspect (1982).
- Exemple d'état : $|\phi^+\rangle = \frac{1}{\sqrt{2}}|0_A 0_B\rangle + \frac{1}{\sqrt{2}}|1_A 1_B\rangle$.
  Effet de la mesure : si Alice mesure 0 sur le premier photon, Bob va mesurer 0 aussi, et inversement.
- Important : les corrélations offertes par l'intrication sont une *ressource* pour des tâches distribuées.

# Algorithmes quantiques et cryptographie

Algorithme de Shor (1994) :

- Résout efficacement le problème de factorisation et du logarithme discret.
- Implication : permet de briser des cryptosystèmes à clé publique tel que RSA et Diffie-Hellman.

Algorithme de Grover (1996) :

- Chercher dans un espace de recherche non-structuré de taille $n$ en temps $\Theta(\sqrt{n})$.
- Implication : permet d'accélérer la recherche de clés dans les cryptosystèmes symmétriques (tel que triple DES ou AES) par un facteur quadratique.

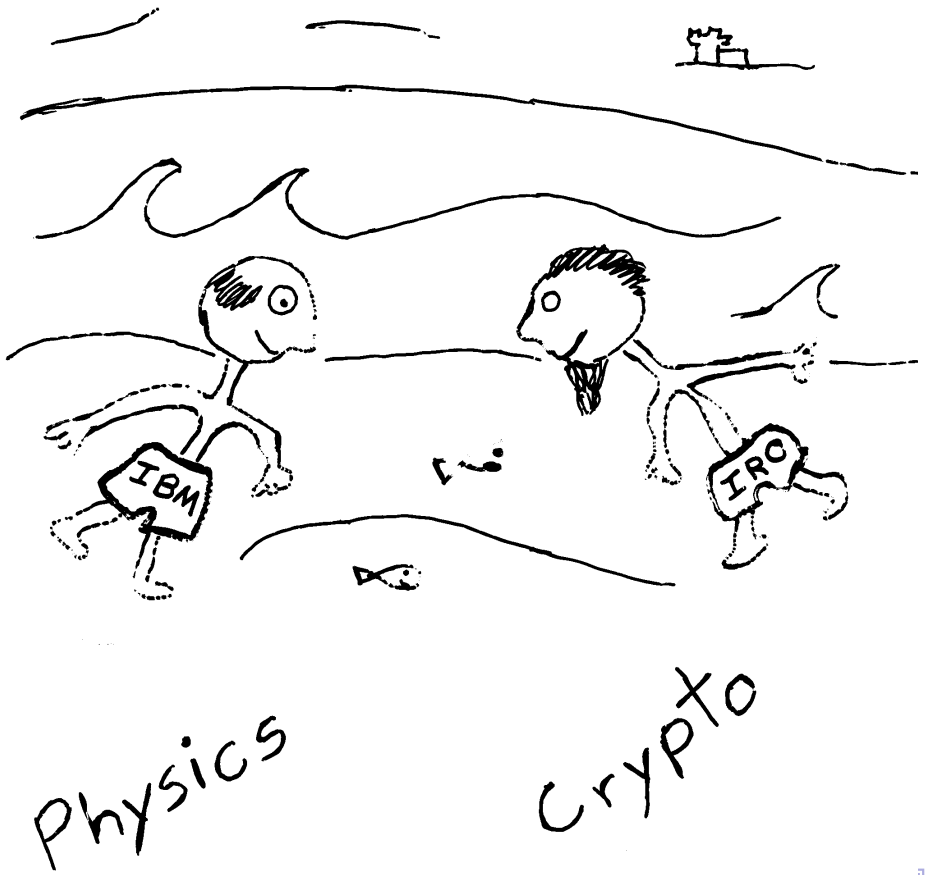
# Distribution quantique de clés

# Masque jetable

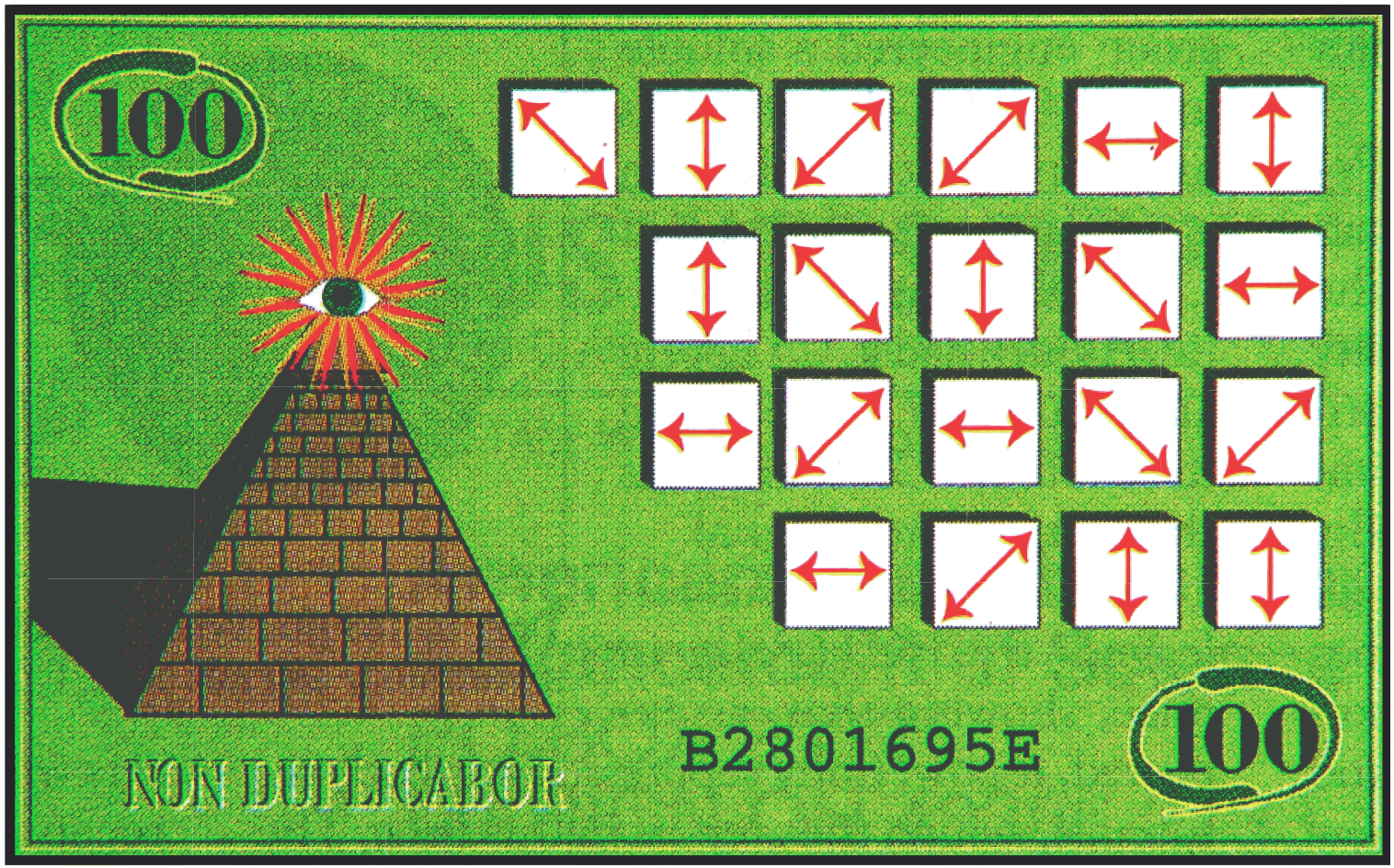
- Masque jetable (*one-time pad* en anglais) :
  - chiffrement symétrique inventé par Vernam (1917),
  - amélioré par Mauborgne et
  - prouvé inconditionnellement sécuritaire par Shannon (1949).
- Exemple de fonctionnement ($m, k \in \{0,1\}^n$) :
  - Chiffrement : $m \oplus k = c$.
  - Déchiffrement : $c \oplus k = m$.
- La clé doit être au moins aussi longue que le message et ne peut-être utilisée qu'une seule fois.
- Problème : distribution de clés.

# Version russe du masque jetable

# Rencontre Charles Bennett et Gilles Brassard (par Chris Fuchs)



# Billets de banque quantiques (Wiesner)



# Cryptographie quantique

- Protocole de distribution quantique de clés inventé par Charles Bennett et Gilles Brassard (1984).


- S'inspire d'idées antérieures de Wiesner [3].
- S'utilise en conjonction avec le masque jetable.
- Sécurité inconditionnelle : basée sur les principes de la mécanique quantique (comme théorème de non-clonage).
- Espionnage de la ligne de communication $\Rightarrow$ perturbation de l'état quantique $\Rightarrow$ détection par Alice et Bob

3. 1970 mais non-publié avant 1984

# Préparation et transmission des états

## Préparation des états :

1. Alice prépare deux chaînes aléatoires de $n$ bits aléatoires $a$ et $b$ ($a, b \in_R \{0,1\}^n$).
2. Pour $i = 1$ à $n$
   - Chaque bit $a_i$ est encodé dans le qubit correspondant : $|\psi_i\rangle = |0\rangle$ si $a_i = 0$ ou $|\psi_i\rangle = |1\rangle$ si $a_i = 1$.
   - Pour chaque état quantique $|\psi_i\rangle$, Alice applique H si $b_i = 1$ et ne fait rien sinon.

## Transmission sur le canal quantique :

3. Alice envoie les états $|\psi_1\rangle, \ldots, |\psi_n\rangle$ à Bob.
   $\Rightarrow$ Eve peut essayer de mesurer certains qubits $|\psi_i\rangle$ pour apprendre de l'information.

# Étape de mesure

Étape de mesure :

4. Bob génère une chaîne de bits aléatoire $b \in_R \{0,1\}^n$.
5. Pour chaque état quantique $|\psi_i\rangle$, Bob mesure dans la base de Hadamard H si $b'_i = 1$ et dans la base standard sinon.
   Soit $a'_i$ le bit mesuré par Bob.
6. En utilisant un canal classique public, Bob communique à Alice son choix de base $b'$ et Alice fait de même en communiquant $b$.
7. Alice et Bob "jettent" les bits de $a$ et $a'$ où $b \neq b'$.
8. Alice et Bob révèlent publiquement une partie de leurs bits restants dans $a$ et $a'$ choisis aléatoirement pour estimer le bruit présent.
   trop de bruit $\Rightarrow$ abandon du protocole

# Illustration de BB84 (tiré de wikipedia)

| Basis | 0 | 1 |
|---|---|---|
| + | ↑ | → |
| × | ↗ | ↘ |

| Alice's random bit | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
|---|---|---|---|---|---|---|---|---|
| Alice's random sending basis | + | + | × | + | × | × | × | + |
| Photon polarization Alice sends | ↑ | → | ↘ | ↑ | ↘ | ↗ | ↗ | → |
| Eve's random measuring basis | + | × | + | + | × | + | × | + |
| Polarization Eve measures and sends | ↑ | ↗ | → | ↑ | ↘ | → | ↗ | → |
| Bob's random measuring basis | + | × | × | × | + | × | + | + |
| Photon polarization Bob measures | ↑ | ↗ | ↗ | ↘ | → | ↗ | ↑ | → |
| PUBLIC DISCUSSION OF BASIS | | | | | | | | |
| Shared secret key | 0 | | 0 | | | 0 | | 1 |
| Errors in key | ✓ | | ✘ | | | ✓ | | ✓ |

# Réconciliation d'information et amplification de secret

Réconciliation d'information :

- Forme de *correction d'erreurs* entre Alice et Bob pour arriver à la même clé.
- Décomposition en blocs de la chaîne $a$ et $a'$ et échange de parité pour déterminer les endroits où il y a des différences.
- Problème : permet à Eve d'apprendre de l'information sur la clé.

Amplification de secret :

- Méthode pour réduire l'information qu'Eve a sur la clé commune de Alice et Bob.
- Utilise une *fonction de hachage universelle*.
- Génère une clé beaucoup plus courte mais sur laquelle Ève a très peu d'information.

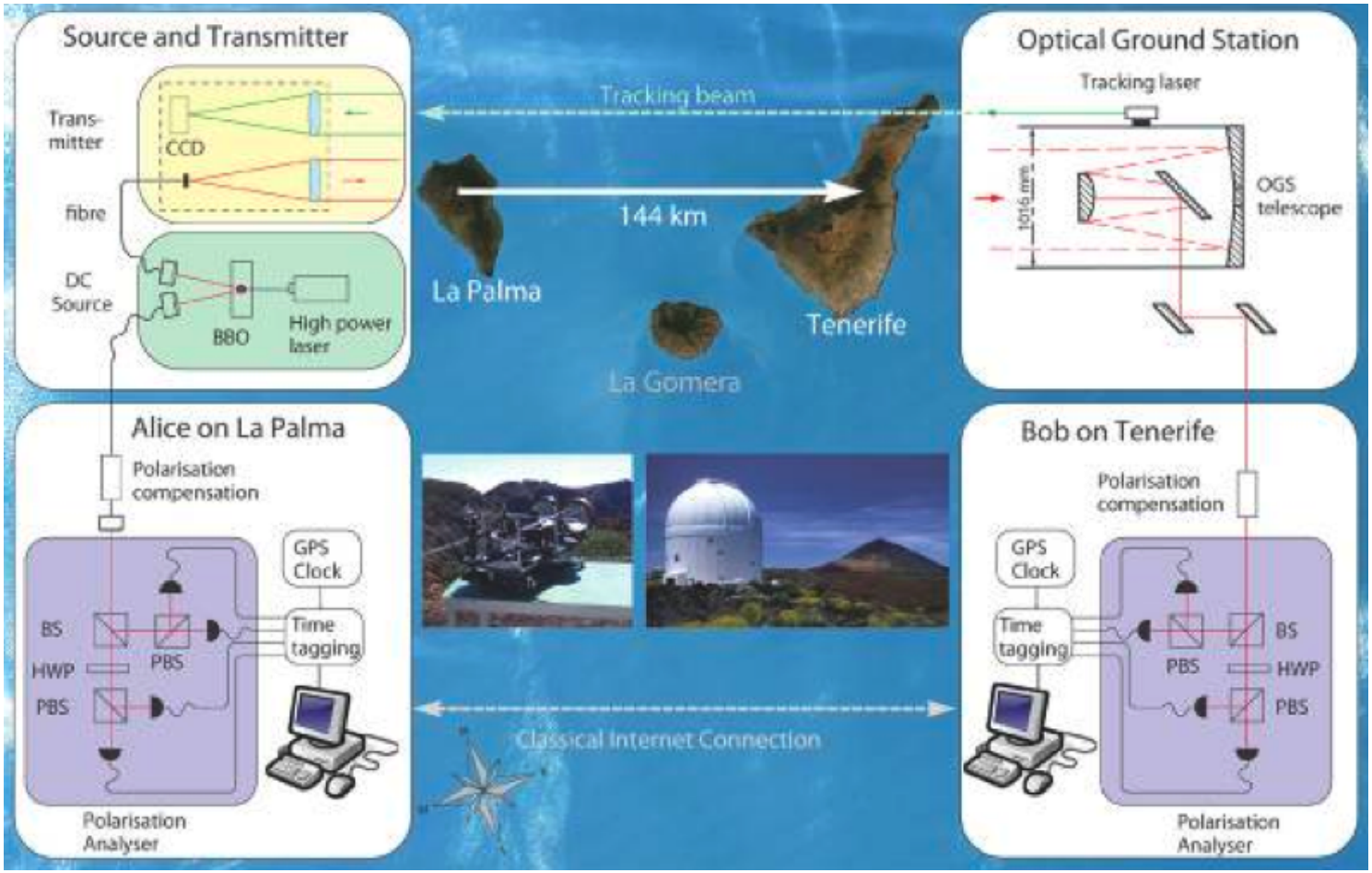
# Implémentations pratiques

Première technologique quantique suffisament mature pour qu'on puisse acheter Alice et Bob en ligne.

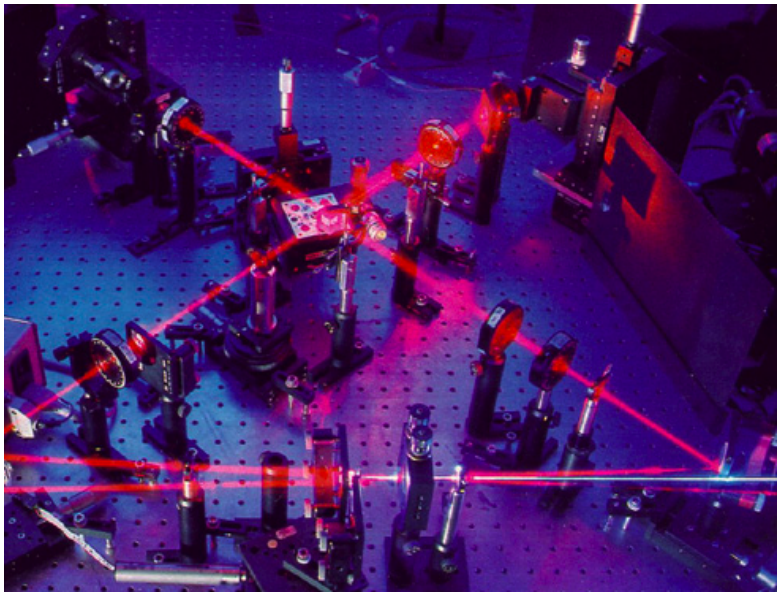

Implémentations pratiques :

- 1989 : premier prototype sur 32.5 cm.
- 2006 : implémentation à ciel ouvert entre deux îles aux Canaries (144 km).
- 2007 : utilisé pour transmettre le résultat de votes lors d'élections cantonales en Suisse.
- 2008 : réseau entre 6 villes en Autriche pour une distance totale de 200 km.
- Prochaine étape : liaison terre-satellite ?

# Implémentation à ciel ouvert entre deux îles aux Canaries



# Attention aux canaux cachés



*"... power supplies make noise, and not the same noise for the different voltages needed for different polarizations. ... Thus, our prototype was unconditionally secure against any eavesdropper who happened to be deaf ! :-)"*, *Gilles Brassard*

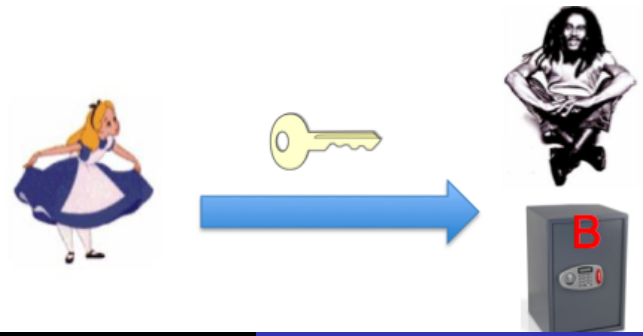
# Mise en gage de bit et pile-ou-face quantiques

# Mise en gage de bit

Primitive cryptographique composé de deux phases :

1. Phase de mise en gage : Alice met en gage un bit $b$ et l'envoie à Bob.


2. Phase de révélation : Alice donne l'information à Bob pour ouvrir $b$.



# Espoir d'une version quantique inconditionnellement sécuritaire

Applications : preuves à divulgation nulle (*zero-knowledge proofs* en anglais), partage de secrets, calcul multiparti sécuritaire.

Propriétés :

- Camouflage : Bob ne pas ouvrir $b$ sans l'aide d'Alice.
- Engagement : Alice ne peut pas ouvrir $b$ à une autre valeur que la valeur initiale.

Impossibilité classique : aucun protocole classique de mise en gage de bit ne peut être à la fois parfaitement camouflant (*concealing* en anglais) et parfaitement liant (*binding* en anglais).

Espoir quantique : protocole de mise en gage de bit parfaitement camouflant et parfaitement liant basé sur la mécanique quantique.

# Preuve d'impossibilité quantique

- De 1993 à 1997 plusieurs procotoles ont été proposés par Brassard, Crépeau et co-auteurs. . .
- et plusieurs fois brisés par Dominic Mayers (étudiant de Brassard) jusqu'à . . .
- la preuve d'impossibilité totale en 1997.
- Problème : ne provient pas des preuves de sécurité mais d'une attaque subtile basé sur l'intrication
  $\Rightarrow$ possibilité pour une Alice malhonnête de choisir la valeur du bit qu'elle souhaite révelée *a posteriori*
- Solution : protocole inconditionnellement sécuritaire basé sur la relativité (Kent 1999).

# Pile-ou-face (Blum 81)

Primitive cryptographique où deux participants veulent se mettre d'accord sur la valeur d'un bit aléatoire.

Scénario :

- Alice et Bob ont récemment divorcés et habitent maintenant dans des villes différentes.
- Ils veulent jouer à pile-ou-face qui va garder la voiture.
- Comment se mettre d'accord par téléphone ?

# Impossibilité classique

Mise en gage de bit $\Rightarrow$ pile-ou-face

Biais $\delta$ : probabilité avec laquelle un participant malhonnête peut biaiser le résultat du pile-ou-face.
Exemple : $\frac{1}{2} + \delta$

- Si $\delta = 0 \Rightarrow$ protocole équitable.
- Si $\delta = \frac{1}{2} \Rightarrow$ un participant malhonnête peut toujours choisir la sortie désirée.

Impossibilité (Cleve 86) : il n'existe aucun protocole classique de pile-ou-face sécuritaire dans le sens de la théorie de l'information pour lequel $\delta < \frac{1}{2}$.

# Pile-ou-face quantique

- Premier protocole décrit et brisé dans l'article de BB84.
- L'attaque utilisée de l'envoi de la moitié d'une paire intriquée.
- Borne inférieure sur le biais : $\frac{1}{\sqrt{2}}$ (Kitaev).
- Borne supérieure sur le biais : $\frac{1}{4}$ (Ambainis 2002).
- Protocole d'Ambainis :
  1. Alice choisit aléatoirement $a \in_R \{0,1\}$ et prépare $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|2\rangle$ si $a = 0$ et $|\psi\rangle = \frac{1}{\sqrt{2}}|1\rangle + \frac{1}{\sqrt{2}}|2\rangle$ si $a = 1$.
  2. Alice envoie $|\psi\rangle$ à Bob.
  3. Bob envoie un bit aléatoire $b \in_R \{0,1\}$ à Alice.
  4. Alice envoie $a$ à Bob.

# Communication anonyme quantique

# Communication anonyme quantique

Communication anonyme quantique (BBFGT [4] 07) : envoi d'un message quantique tel que l'identité du receveur et de l'envoyeur du message sont protégés (ainsi que le contenu du message).

Modèle de communication :

- canal quantique sécuritaire entre chaque paire de participants,
- canal de diffusion classique,
- canal anonyme classique.

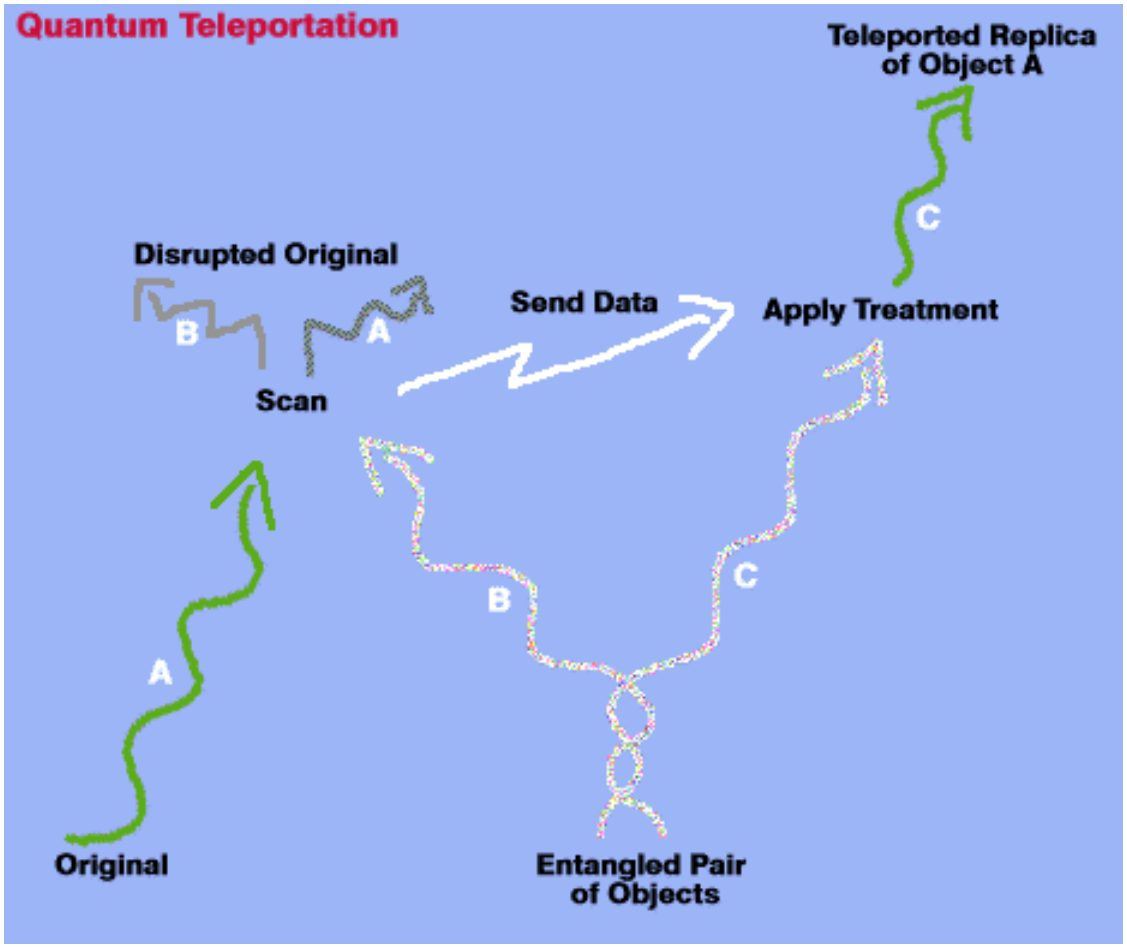
4. Brassard, Broadbent, Fitzsimons, Gambs et Tapp.

# Téléportation quantique (BBCJPW[5] 1993)

- Primitive de la théorie de l'information quantique.
- Alice d'envoyer un qubit inconnu $|\psi\rangle$ à Bob en "consommant" la moitié d'une paire intriquée $|\phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ et en envoyant deux bits classiques.
- À la fin de la téléportation, l'état quantique est dans les mains de Bob et plus d'Alice, d'où le terme.
- Ne permet pas de communiquer plus vite que la lumière car il faut temps pour que les deux bits classiques arrivent chez Bob.

5. Bennett, Brassard, Crépeau, Jozsa, Peres et Wootters

# Illustration de la téléportation quantique



# Principe de base de la communication anonyme quantique

- Intrication anonyme : le receveur est intriqué avec l'envoyeur mais sans connaître son identité.
- L'envoyeur téléporte l'état quantique en envoyant les deux bits de la téléportation par un canal anonyme classique.
- Difficulté : générer l'intrication anonyme.
- Solution : partir d'un état intriqué multiparti (appelé "état chat") $|\psi\rangle = \frac{1}{\sqrt{2}}|0^n\rangle + \frac{1}{\sqrt{2}}|1^n\rangle$ pour générer $|\psi^+\rangle$.
- Fail-safe teleportation : protège l'intégrité du message quantique en cas de problème (important à cause du non-clonage).
- Travaux en cours : pouvoir tolérer une minorité de participants malveillants.

# Conclusion et perspectives futures

# Conclusion

L'informatique quantique :

- brise la plupart des cryptosystèmes à clé publique utilisés actuellement grâce à l'algorithme de Shor mais ...
- permet aussi de communiquer de manière inconditionellement sécuritaire grâce à la cryptographie quantique (protocole BB84)
- ne résout pas magiquement tout (impossibilité de mise en gage de bit quantique),
- mais permet de réaliser certaines fonctionnalités avec un avantage comparé au classique (pile-ou-face).

# Perspectives futures

- Étude de cryptosystèmes classiques pouvant résister à la vague quantique.
  Exemples : cryptosystème de McEliece basé sur les codes correcteurs (1976), chiffrement sur les *lattices*, ...
- Développement de nouvelles variantes quantiques de primitives cryptographiques.
- Passage de l'utilisation à grande échelle et intégration progressive dans les technologies courantes.

# C'est la fin !

Merci pour votre attention.
Questions ?

# Registre quantique et circuit quantique

- Un registre quantique $|\phi\rangle$ de $n$ qubits est décrit par $2^n$ nombres complexes $\alpha_0$, $\alpha_1$,..., $\alpha_{2^n-1}$ tel que $|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$, avec la condition de normalisation $\sum |\alpha_i|^2 = 1$.
- Modèle de calcul : circuit quantique (Deutsch 89).
- Les opérations physiques réalisées sur les états quantiques correspondent à des transformations unitaires.
- Toutes les opérations sauf la mesure sont *réversibles*.