DÉPARTEMENT DE PHYSIQUE
FACULTÉ DES SCIENCES
PRINTEMPS DES SCIENCES 2003

Cryptographie quantique

ou distribution de clefs secrètes

Printemps des Sciences 2003 : La communication de l'électron au papillon

Présentation : Dramaix Florence, van den Broek Didier, Wens Vincent

Comment Alice et Bob peuvent-ils secrètement se transmettre un message ?

Alice et Bob devront d'abord s'envoyer une clef (c'est-à-dire une suite de bits) connue d'eux seuls, qui leur permettra de coder et de déchiffrer un message. Ils utilisent cette clef et le code de Vernam pour le crypter.

Code de Vernam

XOR :

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

message à crypter		10100	message reçu(crypté)		11001
clef	$\oplus$	01101	clef	$\oplus$	01101
message crypté		11001	message initial		10100

Pour mettre tout ceci en œuvre, Alice et Bob vont faire appel à la *cryptographie quantique* qui se base sur la *mécanique quantique*. Les trois propriétés principales utilisées sont :

–Les résultats d'une mesure quantique sont distribués de manière probabiliste.
–Le principe de superposition empêche la *duplication parfaite*.
–Toute mesure perturbe le système.

Ceci est dédié à Coralie, Bénédicte, Chouchou et à nos mamans.

Remerciements à : Nicolas Cerf, Sofyan Iblisdir, Stefano Pironio.

Principe de la cryptographie quantique

Toute écoute d'un canal quantique provoque des perturbations. (erreurs chez Bob)

Le protocole utilisé : Bennett et Brassard 1984 (BB84)

Alice utilise des photons polarisés soit horizontalement, soit verticalement (base H/V), soit diagonalement ou anti-diagonalement (base D/A), pour envoyer des bits à Bob.
Plusieurs cas se présentent :

- Bob a choisi la même orientation du polariseur (même base), alors il est sûr de trouver l'état de polarisation envoyé par Alice ;
- Bob a choisi l'autre orientation, il a alors une chance sur deux de trouver l'état de polarisation envoyé par Alice.

Les attaques

Ève veut espionner Alice et Bob et découvrir leur clef.

Alice et Bob envoient leurs photons via un canal quantique. Alice choisit aléatoirement ses bases et l'état de polarisation des photons ; Bob fait de même pour ses bases et mesure les photons. Via un canal classique authentifié, ils s'échangent le choix des bases et gardent les bases communes.

Théorème 1 *Alice et Bob abandonnent leur clef dès que Ève possède autant d'information que Bob sur celle-ci.*

Étudions deux types d'attaque :

Interception et réémission : "Intercept and resend"

Avec une probabilité ω, Ève choisit une base, mesure et envoie l'état de polarisation trouvé à Bob. Comme elle *mesure*, elle perturbe la polarisation du photon et Bob aura des erreurs dans sa chaîne de bits.

Les informations de Bob $\mathbf{I_{AB}}$ et d'Ève $\mathbf{I_{AE}}$ sont $I_{AB} = \log_2\left(2 - \frac{\omega}{2}\right) + \frac{\omega}{4}\log_2\left(\frac{4}{\omega} - 1\right)$ $I_{AE} = \frac{1}{2}\log_2\left(1 - \frac{\omega^2}{4}\right) + \frac{\omega}{4}\log_2\left(\frac{1+\frac{\omega}{2}}{1-\frac{\omega}{2}}\right)$	Si $\omega < 1 \Rightarrow$ clef pas connue d'Eve Si $\omega = 1 \Rightarrow$ clef abandonnée $P_{\text{erreur}} = 0.25$ pour $\omega = 1$

Duplication : "L'attaque des clones"

Ève possède une machine qui *clone* les photons. Après avoir éliminé les mauvaises bases, elle a en principe autant d'information que Bob. Cependant...

Théorème 2 *On ne peut cloner un ensemble d'états non orthogonaux ; la duplication parfaite d'un photon est* impossible.
Ève utilise comme transformation "cloneuse" :

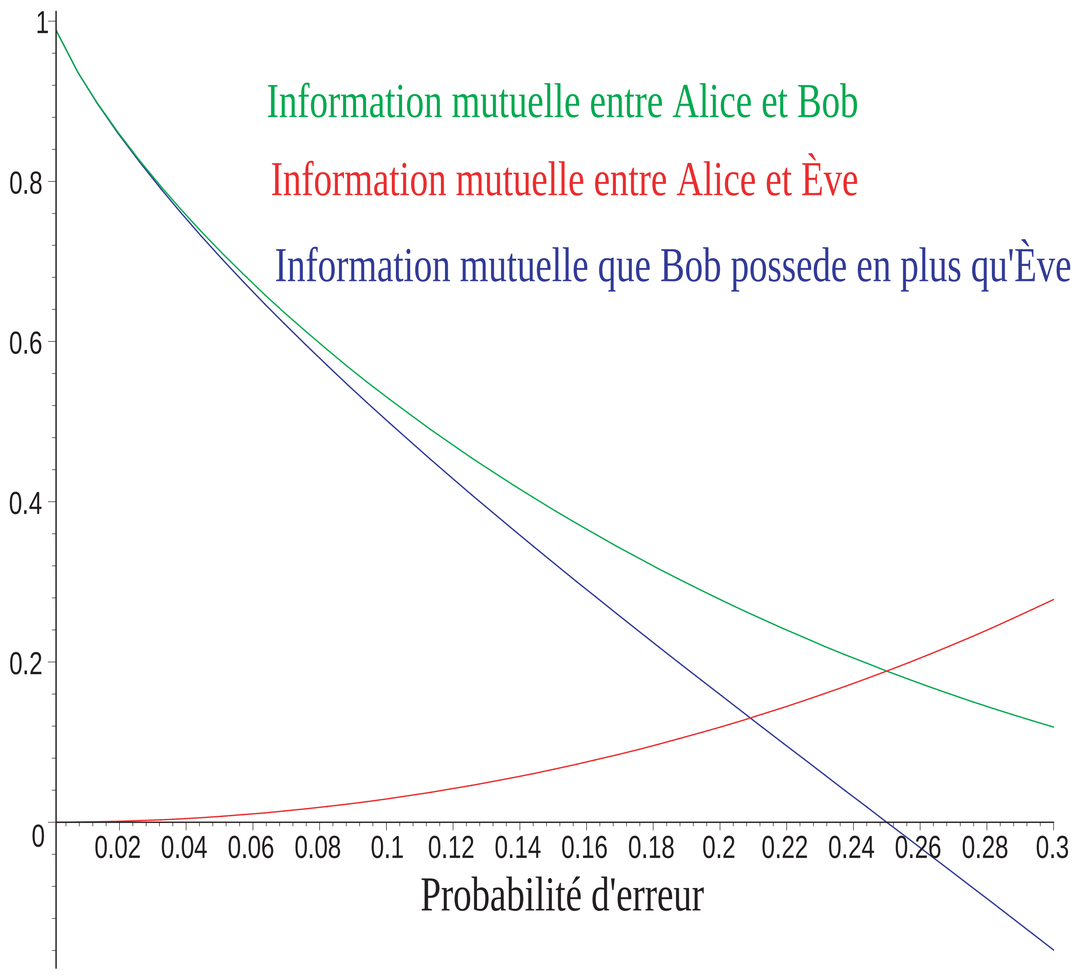
$$U\left(|0\rangle_{yA}|0\rangle_{yE}\right) = |0\rangle_{yA}|0\rangle_{yE}$$
$$U\left(|1\rangle_{yA}|0\rangle_{yE}\right) = \cos(\theta)|1\rangle_{yA}|0\rangle_{yE} + \sin(\theta)|0\rangle_{yA}|1\rangle_{yE}$$

Par ce théorème, Ève perturbe encore le photon d'Alice, et pourra alors être détectée.

Les informations de Bob $\mathbf{I_{AB}}$ et d'Ève $\mathbf{I_{AE}}$ sont
$I_{AB} = \frac{1}{2}\left[(1+\cos\theta)\log_2(1+\cos\theta) + (1-\cos\theta)\log_2(1-\cos\theta)\right]$
$I_{AE} = \frac{1}{2}\left[(1+\sin\theta)\log_2(1+\sin\theta) + (1-\sin\theta)\log_2(1-\sin\theta)\right]$
Si $\theta < \frac{\pi}{4} \Rightarrow$ clef pas connue d'Eve
Si $\theta \geq \frac{\pi}{4} \Rightarrow$ clef abandonnée
$P_{\text{erreur}} = 0.1464 \quad \text{pour} \quad \theta = \frac{\pi}{4}$

où θ est un paramètre contrôlé par Ève représentant la force de l'attaque.
Pour une quantité d'information donnée, Ève introduit plus d'erreur chez Bob avec "intercept and resend" qu'avec la duplication.

Informations mutuelles ("Intercept and resend")



Informations mutuelles (Duplication)