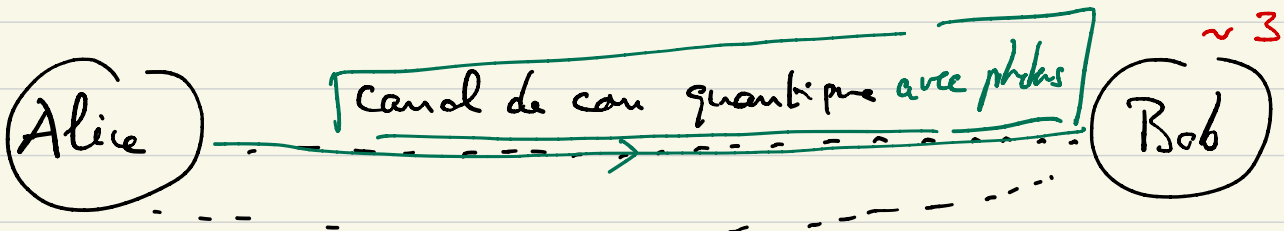
Cryptographie Quantique.

- Etude protocole de génération de clé secrète "one-time pad" de Bennett et Brassard (1984)



en théorie ce protocole est inviolable : car nous verrons que si Eve intercepte un bit quantique elle va modifier l'état (via projection) et A & B vont être capable de détecter la présence d'Eve.

Alice et Bob génère un secret commun sous forme commune entre eux de bits aléatoire ... 1 0 0 1 1 0 1 0 1 0 1 ....

Sert de clé secrète : "one time pad"

One time pad : $z_1\ z_2 \cdots z_N$; $z_i \in \{0,1\}$. → partagée par A et B.

Message de A : $m_1\ m_2 \cdots m_N$; $m_i \in \{0,1\}$.

A l'envoie à Bob : $z_1 \oplus m_1\ \ z_2 \oplus m_2 \cdots z_N \oplus m_N \mod 2$.

Eve intercepte le message → elle ne peut décoder.

Bob décode : $z_1 \oplus m_1 \oplus z_1 = m_1$ $\quad z_2 \oplus m_2 \oplus z_2 = m_2$ $\quad \cdots \quad z_N \oplus m_N \oplus z_N = m_N$

1) Etapes du Protocole : génération du one-time-pad.

2) Test de sécurité que font A & B avant d'utiliser le one-time-pad.

3) Attaques de la part d'Eve.

(1) Etapes du Protocole : → 4 étapes.

✓ (a) Encodage chez Alice. (secrète)

✓ (b) Décodage chez Bob (secrète)

✓ (c) Phase de communication publique via un canal classique.

✓ (d) A & B génèrent des bits secrets communs. (one-time-pad.).

ⓐ Procédé d'encodage d'Alice.

A génère une suite binaire $x_1 \dots x_N$ $\quad x_i \in \{0,1\}$

aléatoire et secrète.

génère également $e_1 \dots e_N$ $\quad e_i \in \{0,1\}$

aléatoire et secrète.

- **Pour $e_i = 0$** on fabrique un qubit dans l'état

$|x_i\rangle \in \{|0\rangle, |1\rangle\}$ (photon de l'état $|x\rangle$ ou $|y\rangle$).

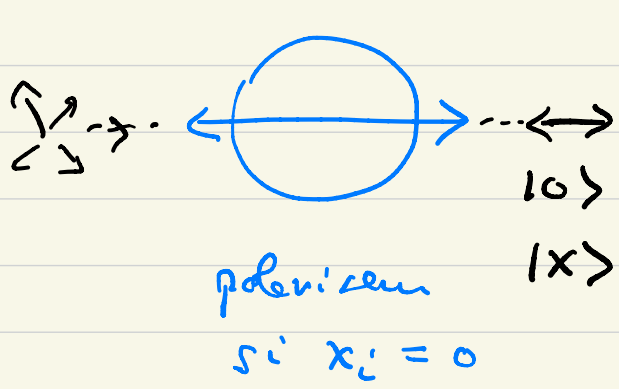
base orthonormée de $\mathbb{C}^2$

↑

esp d'Hilbert du 1 qubit

Terminologie base $\mathbb{Z}$ ou base computationnelle

Physiquement on peut faire cela avec des photons et le degré de polarisation des photons



Pour $c_i = 1$: Alice prépare un qubit (photon) dans l'état $\left\{ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{et} \quad \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right\}$

si $x_i = 0$ si $x_i = 1$.

Ces deux états constituent une base de $\mathbb{C}^2$

On appelle cette base la base de Hadamard ou bien la base X.

↗ terminologie.

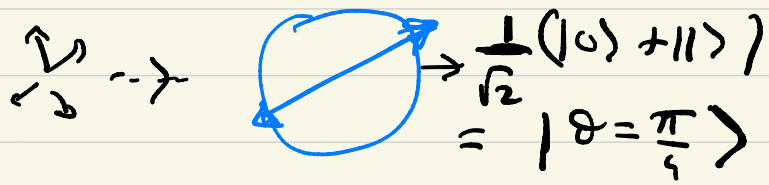
En fait si $H \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ est la matrice de Hadamard

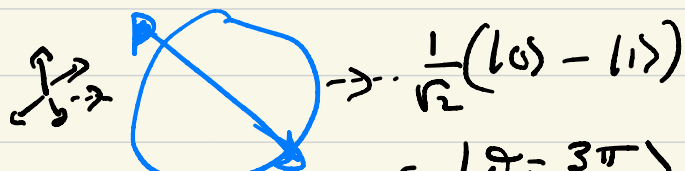
on voit que :

$$\underbrace{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)}_{\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}} = H|0\rangle \quad \underbrace{\begin{pmatrix}1\\0\end{pmatrix}}_{} \quad \text{et} \quad \underbrace{\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)}_{\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}} = H|1\rangle \quad \underbrace{\begin{pmatrix}0\\1\end{pmatrix}}_{}$$

En Résumé Alice prépare qubit de l'état $H|x_i\rangle$.
si $c_i = 1$.

Physiquement on peut utiliser le Pol du photon :





Récapitulation de procédure d'encodage d'Alice :

$x_1 \cdots x_N \in \{0,1\}^N$ secrète et aléatoire

$e_1 \cdots e_N \in \{0,1\}^N$

instant i : préparer un qubit dans l'état : $H^{e_i} |x_i\rangle$.

si $e_i = 0$ $\quad H^{e_i} |x_i\rangle = |x_i\rangle \in \{|0\rangle, |1\rangle\}$ base $\mathcal{Z}$.

photon polarisem horizontal et vertical
$x_i = 0$ $\quad$ $x_i = 1$.

si $e_i = 1$ $\quad H^{e_i} |x_i\rangle = H |x_i\rangle \in \left\{ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \text{ et } \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right\}$

base X.

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

$$|x_i\rangle \in \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ ou } \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

photon préparer avec polarisem tourné $\theta = \frac{\pi}{4}$ et $\theta = \frac{3\pi}{4}$.
$x_i = 0$ $\quad$ $x_i = 1$.

- Alice envoie le photon polarisé dans un des états :

$$|0\rangle \quad , \quad |1\rangle \quad , \quad \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad , \quad \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\left(|x\rangle \quad , \quad |y\rangle \quad , \quad |\vartheta = \frac{\pi}{4}\rangle \quad , \quad |\vartheta = \frac{3\pi}{4}\rangle \; . \right)$$

- Bob reçoit à chaque instant un photon dans un de ces états ci-dessus.

Procédure de décodage de Bob.

Bob génère aussi suite aléatoire (de bits classique) $d_1 \dots d_N$ séries

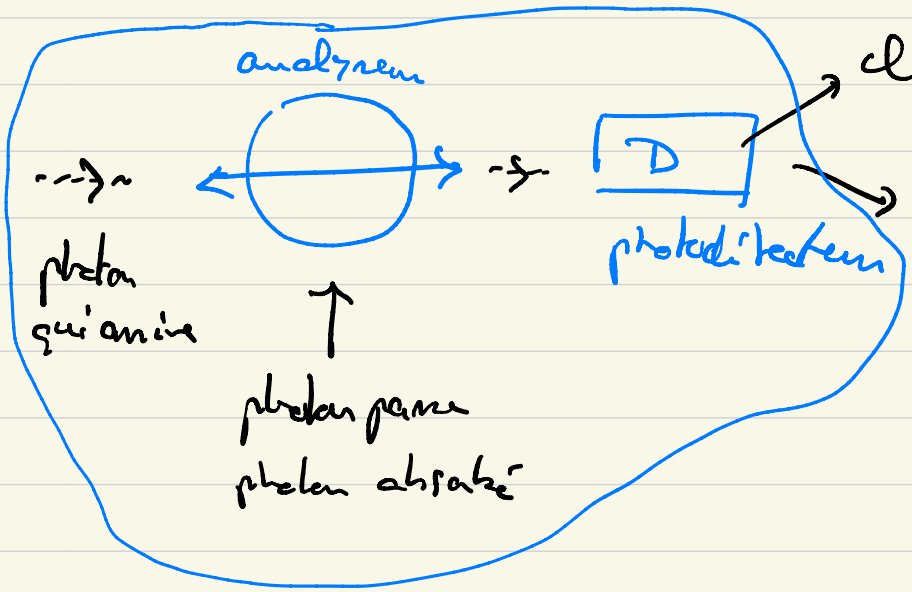
$$d_i \in \{0, 1\}.$$

- Si $d_i = 0$: Bob effectue une mesure de l'état de pol du photon dans la base $\mathcal{Z}$: $\{|0\rangle, |1\rangle\}$.

- Si $d_i = 1$: Bob effectue dans la base X : $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ et $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Physiquement :

si $d_i = 0$.



clic $|x\rangle$ ou $|0\rangle$ $\rightsquigarrow$ $y_i = 0$

pas de clic. $|y\rangle$ ou $|1\rangle \rightsquigarrow y_i = 1$

L'état du photon après la mesure est ici

$|y_i\rangle \in \{|0\rangle, |1\rangle\}$.

une des états de base.

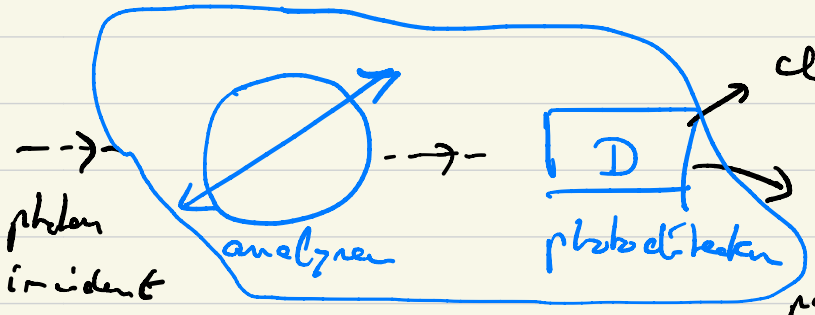
et Bob enregistre cet état.

et le bit classique :

$y_i \in \{0, 1\}$.

clic ↙ ↘ pas de clic.

si $d_i = 1$.



clic $|\frac{\pi}{4}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \rightsquigarrow y_i = 0$.

$|\frac{3\pi}{4}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightsquigarrow y_i = 1$.

pas de clic

L'état du photon après la mesure $\in \{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$

et Bob observe cet état (clics) et enregistre $y_i = 0$ ou 1.

Récapitulation du décodage de Bob :

- génère $d_1\ d_2 \cdots d_N \in \{0,1\}^N$ aléatoirement.
- puis il utilise appareil de mesure selon sa base
  $d_i = 0 \rightarrow$ analyseur horizontal + photodétecteur $|\gamma_i\rangle \in \{|0\rangle, |1\rangle\}$.

  $d_i = 1 \rightarrow$ analyseur à 45° + photodétecteur. $|\gamma_i\rangle \in \left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}; \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$.
- Obtient les résultats de mesure : l'état du photon après la mesure $|\gamma_i\rangle^{d_i}$.

il possède la suite binaire $\gamma_1 \cdots \gamma_N \in \{0,1\}^N$.

↓

aléatoire car les résultats des mesures quantique (clic / pas de clic) sont aléatoire.

+1.

(c) Phase de Communication Publique entre A & B.

Jusqu'ici les suites $e_1 \cdots e_N$ et $d_1 \cdots d_N$ étaient gardées secrètes. Maintenant A & B révèlent les deux suites $e_1 \cdots e_N$ et $d_1 \cdots d_N$.

Tant en gardant les autre suites $x_1 \cdots x_N$ et $y_1 \cdots y_N$ secrètes.

(d) Générant la clé secrète.

- Si $e_i = d_i$ on prouvera que $x_i = y_i$ avec probabilité 1.
  et les bits x_i et y_i sont conservés pour constituer ce one time pad.

- Si $e_i \neq d_i$ on prouvera que $x_i = y_i$ avec prob $1/2$ et $x_i \neq y_i$ avec prob $1/2$ et ces bits sont rejetés.

En fin de compte le one-time-pad sera constitué de la sous-suite de $x_1 \dots x_{2N}$ ou $y_1 \dots y_{2N}$ telle que $e_i' = d_i$ (et donc $x_i' = y_i$).

Comme $\text{Prob}(e_i' = d_i') = 1/2$ en gros la longueur du one-time-pad est $\frac{N}{2}$.

✸

Lemme (base du protocole de BB84).

$$\left.\begin{array}{l} \text{Prob}(x_i = y_i \mid e_i = d_i) = 1. \\ \text{Prob}(x_i \neq y_i \mid e_i = d_i) = 0 \end{array}\right\}.$$

$$\left.\begin{array}{l} \text{Prob}(x_i = y_i \mid e_i \neq d_i) = 1/2 \\ \text{Prob}(x_i \neq y_i \mid e_i \neq d_i) = 1/2 \end{array}\right\}.$$

→ prochain vidéo.

Lemme suivant.

- suite d'A : $x_1 \dots x_N$ et $c_1 \dots c_N$ $\mathrm{Ber}(1/2)$
- suite de B : $\underbrace{d_1 \dots d_N}_{\mathrm{Ber}(1/2)}$ et $\underbrace{y_1 \dots y_N}_{\text{résultat des mesures}}$.

✓. $\mathrm{Prob}(x_i = y_i \mid c_i = d_i) = 1$ et $\mathrm{Prob}(x_i \neq y_i \mid c_i = d_i) = 0$

✓. $\mathrm{Prob}(x_i = y_i \mid c_i \neq d_i) = 1/2$ et $\mathrm{Prob}(x_i \neq y_i \mid c_i \neq d_i) = 1/2$.

Preuve : utilise la règle de Born du principe de la mesure en physique quantique.

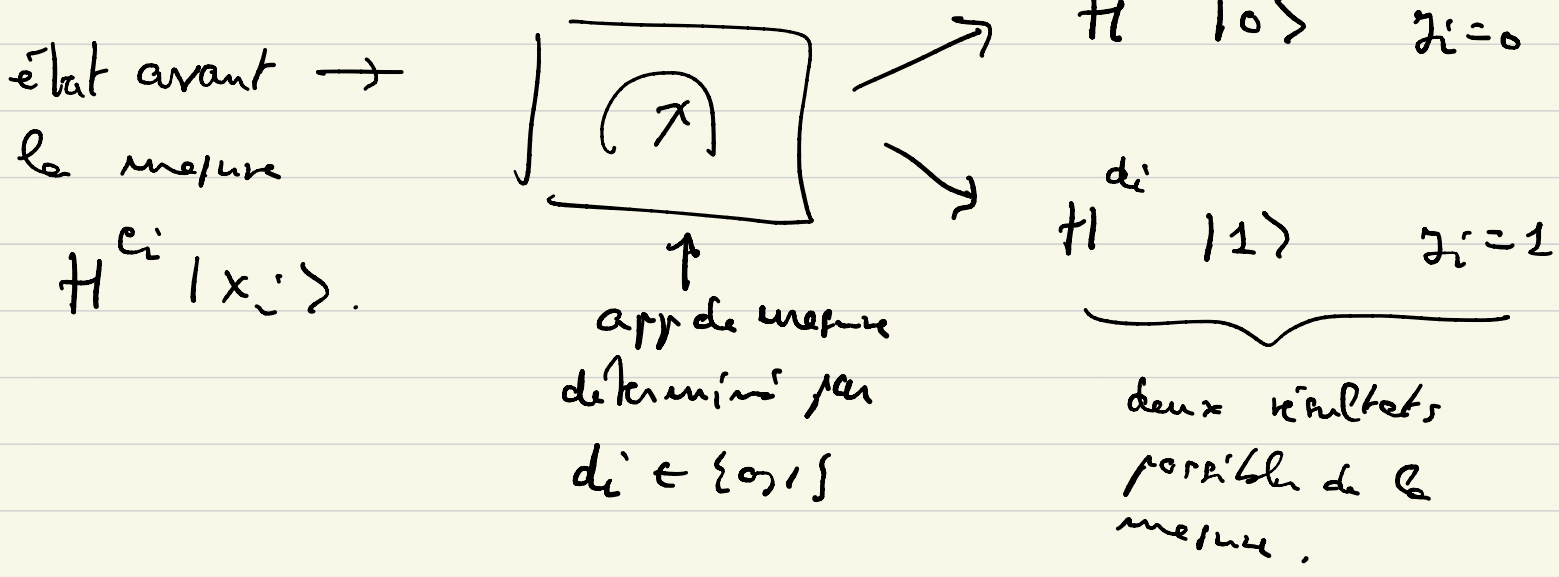
Alice envoie des bit quant à Bob dans un des 4 états :

$$H^{c_i} |x_i\rangle \qquad c_i = 0,1 \quad x_i = 0,1$$

$|0\rangle$; $|1\rangle$; $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$; $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Bob effectue la mesure à chaque instant i et l'état juste après la mesure est projeté aléatoirement et vaut

$H^{d_i} |y_i\rangle$ ..... $\underline{d_i = 0,1}$ → choix de l'appareil de mesure et $\underline{y_i = 0,1}$



* $\text{Prob}\left(H^{c_i}|x_i\rangle \to \underbrace{H^{d_i}|0\rangle}_{\equiv y_i}\right) = \left|\underbrace{\langle 0|H^{d_i}}_{\text{conjugué de Dirac de l'état après mesure}} \underbrace{H^{c_i}|x_i\rangle}_{\text{l'état avant la mesure.}}\right|^2$

si $c_i = d_i$

$H^{d_i} H^{c_i} = H^{d_i + c_i} = \begin{cases} H^0 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ H^2 = I \end{cases}$

$\text{Prob} = |\underbrace{\langle 0|x_i\rangle}_{\equiv y_i}|^2 = \begin{cases} 1 \text{ si } x_i = 0 \\ 0 \text{ si } x_i = 1. \end{cases}$

* $\text{Prob}(H^{c_i}|x_i\rangle \to \underbrace{H^{d_i}|1\rangle}_{\equiv y_i}) = |\langle 1|H^{d_i} H^{c_i}|x_i\rangle|^2.$

$= |\langle 1|x_i\rangle|^2 = \begin{cases} 0 \text{ si } x_i = 0 \\ 1 \text{ si } x_i = 1. \end{cases}$

$x_i = y_i$

Résumé : quand $c_i = d_i$ avec certitude on a

$\text{Prob}(x_i = y_i \mid c_i = d_i) = 1.$

$$\text{Prob}\left(H^{e_i}|x_i\rangle \to H^{d_i}|y_i\rangle\right) = \left|\langle y_i|H^{d_i} H^{e_i}|x_i\rangle\right|^2$$

état avant la mesure — état après la mesure

si $e_i \neq d_i$ $\quad (e_i, d_i) = (0,1)$ ou bien $(e_i, d_i) = (1,0)$

$e_i + d_i = 1$. et $H^{d_i} H^{e_i} = H$

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

à vérifier.

$$H|x_i\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_i}|1\rangle\right)$$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad (-1)^0 = 1$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad (-1)^1 = -1$$

$$\text{Prob} = |\langle y_i|H|x_i\rangle|^2 = \left|\langle y_i|\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}(-1)^{x_i}|1\rangle\right)\right|^2$$

$$= \frac{1}{2}\left|\langle y_i|0\rangle + (-1)^{x_i}\langle y_i|1\rangle\right|^2 \quad (y_i = 0,1)$$

$$= \frac{1}{2} \quad \checkmark$$

En résumé $\quad \text{Prob}(x_i = y_i \,/\, e_i \neq d_i) = \text{Prob}(x_i \neq y_i \,/\, e_i \neq d_i) = 1/2.$

2) A & B font sécurité pour s'assurer que personne n'observe ou n'intercepte les bits quantiques.

Puisque quand $e_i = d_i$ il faut nécessairement que $x_i = y_i$ l'idée est de sacrifier une petite partie $\in \frac{N}{2}$ du one time pad et tester empiriquement que $x_i = y_i$ pour cette partie $\in \frac{N}{2}$.

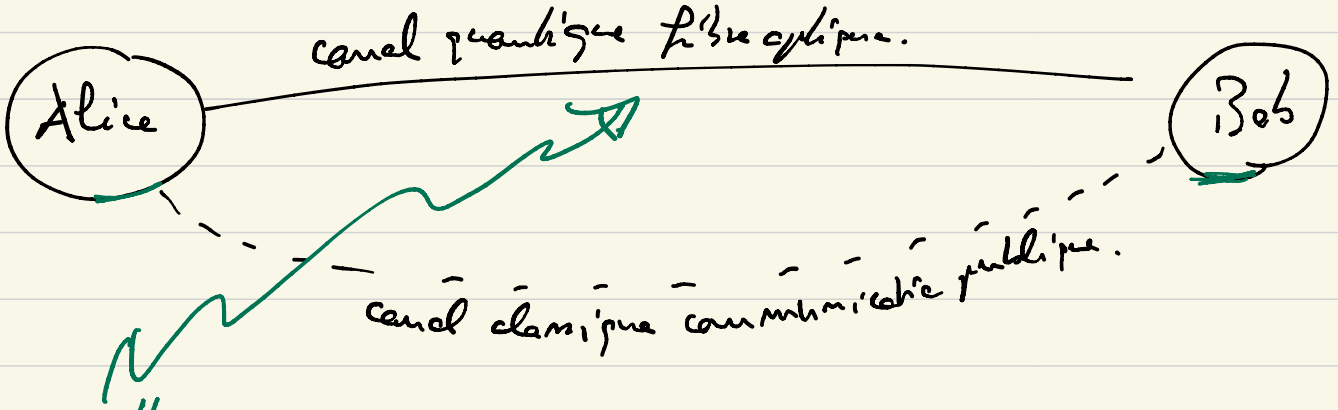
(ici $0 < \epsilon \ll 1$. p.ex $\epsilon = \frac{1}{100}$.).

Longueur finale du one time pad :

$$\frac{N}{2} - \epsilon \frac{N}{2} = (1-\epsilon)\frac{N}{2}.$$

on les échange publiquement et on efface du one time pad.

3) Attaques de la part de Eve.



attaque Eve sur la fibre optique.

interception des photons ou les bits quantiques

↙ ↘

Eve fait une mesure.

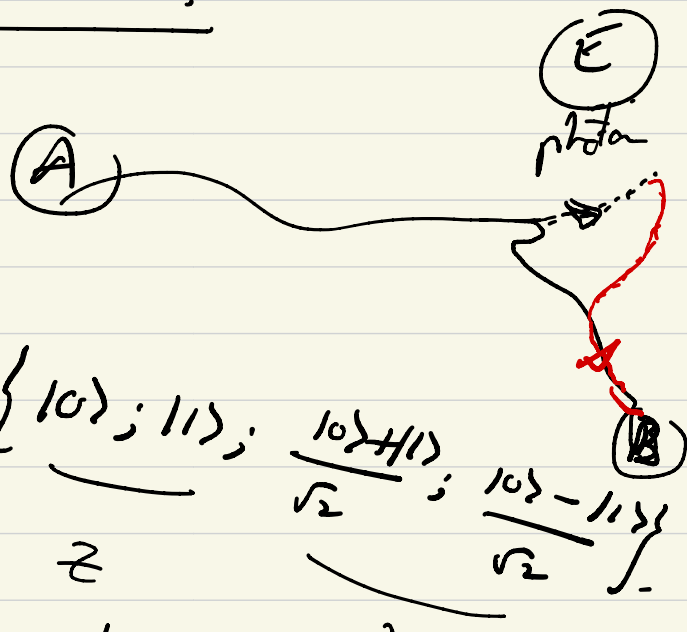
ⓐ possible mais A & B peuvent détecter cette mesure grâce au test de sécurité. ✓

Eve essaye de copier l'état du photon. → impossible quantiquement.

ⓑ Thm de non clonage ✓

Cas particuliers et une preuve générale tient compte de toutes les possibilités.

(a) Attaque lorsque Eve fait une mesure.



- intercepte un photon que Alice à envoyer

de l'état $H^{e_i}|x_i\rangle \in \left\{ |0\rangle ; |1\rangle ; \frac{|0\rangle + |1\rangle}{\sqrt{2}} ; \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\}$

$|0\rangle, |1\rangle$: Z ; $\frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$: X.

- Eve fait une mesure avec une base déterminée par $d_i^E = \begin{cases} 0 & \text{base } Z \\ 1 & \text{base } X \end{cases}$

> l'état de pol après la mesure d'Eve est
> $$H^{d_i^E} |y_i^E\rangle \quad \text{avec } y_i^E \in \{0, 1\}$$

- Si base E = base A c.a.d $d_i^E = e_i$ alors
$y_i^E = x_i$

- Si base $E \neq$ base A c.a.d $d_i^E \neq e_i$ alors
$y_i^E = x_i$ avec proba $1/2$ et $y_i^E \neq x_i$ avec proba $1/2$.

- Eve envoie le photon à Bob et Bob le réceptionne dans l'état $H^{d_i^E}|y_i^E\rangle$ au lieu de $H^{e_i}|x_i\rangle$.

- Bob va faire la mesure sur l'état $H^{d_i^E} | y_i^E \rangle$.

Il obtient sa suite y_i' et $H^{d_i} | y_i' \rangle$. car ce qu'il obtient (comme proj aléatoire) et d'écrire par sa base la mesure.

- Dans le plan de Canal Public A & B lient par une fraction de bits si $\text{Prob}(x_i = y_i / c_i = d_i) = \frac{1}{2}$

$$\epsilon \frac{N}{2}.$$

Théorie en présence de Eve

$d_i^E = d_i$ Eve + Bob choisissent la même base

$$\text{Prob}(x_i' = y_i' | c_i' = d_i') = \underbrace{\text{Prob}(x_i' = y_i' | c_i' = d_i' ; c_i = d_i^E)}_{\text{vrai}} \cdot \underbrace{\text{Prob}(c_i' = d_i^E)}_{1} \cdot \underbrace{\text{Prob}(c_i = d_i^E)}_{1/2}$$

$$+ \underbrace{\text{Prob}(x_i' = y_i' | c_i' = d_i' ; c_i \neq d_i^E)}_{1/2} \cdot \underbrace{\text{Prob}(c_i \neq d_i^E)}_{d_i \neq d_i^E} \cdot \underbrace{\text{Prob}(c_i' \neq d_i^E)}_{1/2}$$

$$= \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \left(\frac{3}{4}\right)$$

→ le test de sécurité ne passe pas car une fraction 25% de $\epsilon \frac{N}{2}$

→ Bob et Alice détectent la présence de Eve : bits vont être différents.

(6) Attaque du type copie du photon ?

Idée : Eve reçoit $H^{e_i}|\lambda_i\rangle$; elle ferait une soi-disant copie ;

elle envoie l'original et garde la copie ;

ferait des mesures après la phase de communication connaissant les bonnes bases e_i et d_i

elle obtiendrait alors les $\hat{n}$ résultats que Bob. au mieux quand $e_i = d_i$.

Impossible : car la copie des quatre états

$|0\rangle$; $|1\rangle$; $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ et $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

est impossible. ← Thm de Non clonage

Sécurité du protocole tient au fait que ces quatre états envoyés par Alice ne sont pas tous orthogonaux entre eux.

(B92 qui utilise deux états $|0\rangle$; $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, voir exercice. non orthogonaux.

Théorème de Non clonage :

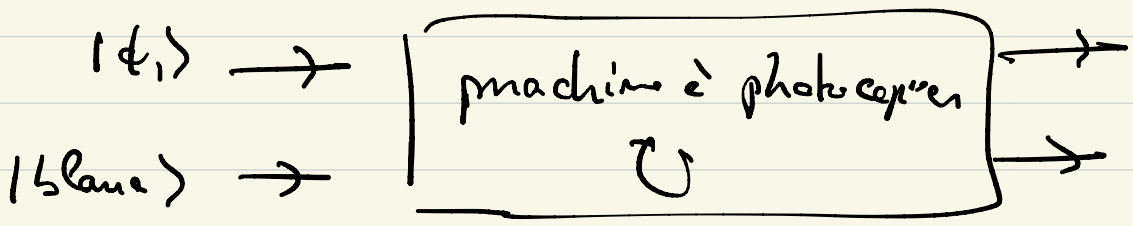
(chap 2 des notes).

Soit $|\phi_1\rangle$ et $|\phi_2\rangle$ t.q $\langle\phi_1|\phi_2\rangle \neq 0$. → pas identique et aussi $\langle\phi_1|\phi_2\rangle \neq 1$.

(Non orthogonaux). Alors ~~∃~~ n'existe pas matrice unitaire U qui effectue l'opération de copie suivante :

$$\begin{cases} U\ |\phi_1\rangle \otimes |\text{Blanc}\rangle = |\phi_1\rangle \otimes |\phi_1\rangle . \\ U\ |\phi_2\rangle \otimes |\text{Blanc}\rangle = |\phi_2\rangle \otimes |\phi_2\rangle . \end{cases}$$

{ espace d'Hilbert $\mathcal{H}_{\text{original}} \otimes \mathcal{H}_{\text{copie}}$.
photon et sa pol $\mathbb{C}^2 \otimes \mathbb{C}^2$.



Remarque : Si $\langle\phi_1|\phi_2\rangle = 0$ c.a.d $|\phi_1\rangle \perp |\phi_2\rangle$ alors il existe U. En particulier une base orthonormale d'états peut être copiée. Mais pour chaque base il faut une autre U base.

Preuve : par l'absurde : $\exists U$? t.q

$$U\ |\phi_1\rangle \otimes |\text{blanc}\rangle = |\phi_1\rangle \otimes |\phi_1\rangle . \quad \checkmark$$

$$U\ |\phi_2\rangle \otimes |\text{blanc}\rangle = |\phi_2\rangle \otimes |\phi_2\rangle .$$

conjugué de Dirac :

$$\langle\phi_2| \otimes \langle\text{blanc}|\ U^{T,*} = \langle\phi_2| \otimes \langle\phi_2| . \quad \checkmark$$

Pr scalaire entre $\checkmark$ et $\checkmark$

$$\langle\phi_2| \otimes \langle\text{blanc}|\ \underbrace{U^{T,*} U}_{\text{I unitarité}}\ |\phi_1\rangle \otimes |\text{blanc}\rangle = \langle\phi_2| \otimes \langle\phi_2|\phi_1\rangle \otimes |\phi_1\rangle$$

$$\big(\langle\phi_2| \otimes \langle\text{blanc}|\big)\big(|\phi_1\rangle \otimes |\text{blanc}\rangle\big) = \big(\langle\phi_2| \otimes \langle\phi_2|\big)\big(|\phi_1\rangle \otimes |\phi_1\rangle\big)$$

$$\langle\phi_2|\phi_1\rangle \underbrace{\langle\text{blanc}|\text{blanc}\rangle}_{1} = \langle\phi_2|\phi_1\rangle\langle\phi_2|\phi_1\rangle .$$

$$\underbrace{\langle\phi_2|\phi_1\rangle}_{\neq 0}\Big(\underbrace{1 - \langle\phi_2|\phi_1\rangle}_{\neq 0}\Big) = 0 .$$

contradiction

■