

Cryptographie dans un monde quantique

AMUSEC 2026

Forum d'Aix-Marseille Université de la Cybersécurité

Léo COLISSON PALAIS

leo.colisson-palais@univ-grenoble-alpes.fr



Plan

- ① Les étranges **lois** de la physique quantique
- ② **L'informatique** quantique
- ③ **Ordinateur** quantique : la quête du Graal
- ④ Cryptographie **post-quantique**
- ⑤ Échange quantique de **clés et téléportation** quantique
- ⑥ **Calcul délégué** quantique à l'aveugle

Plusieurs niveaux de lecture, et parties globalement **indépendantes**

Sortez de quoi écrire ! (exercices)



<https://pixnio.com/fr/objets/papier-crayon-minimalisme-objet>

Sortez de quoi écrire ! (exercices)



<https://pixnio.com/fr/objets/papier-crayon-minimalisme-objet>

🎲 Questions que vous pouvez préparer en avance, ou pour aller plus loin.

Sortez de quoi écrire ! (exercices)



<https://pixnio.com/fr/objets/papier-crayon-minimalisme-objet>

🎲 Questions que vous pouvez préparer en avance, ou pour aller plus loin.

+ posez des **questions** !

Les étranges lois de la physique quantique

Cosmic Eye

a state-of-the-art view of the universe

version 2.0

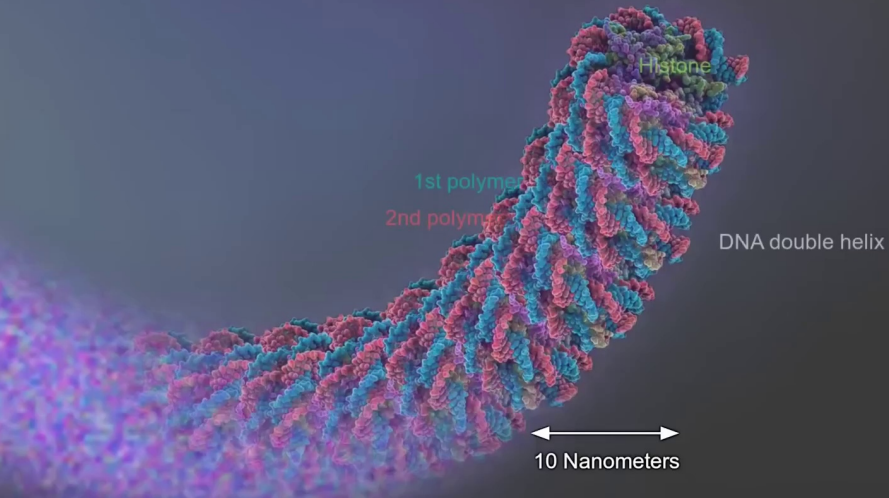
Danail Obreschkow

Smiling Face



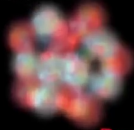
10 Centimeters

10-nm Fiber



Protons and Neutrons

Neutron



Proton



10 Femtometers

Les étranges lois du monde quantique



Les étranges lois du monde quantique



Les étranges lois du monde quantique



Les étranges lois du monde quantique

Observer un objet
le modifie/détruit!



Les étranges lois du monde quantique

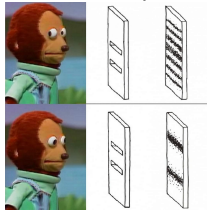
Observer un objet
le modifie/détruit!



Les étranges lois du monde quantique

Observer un objet
le modifie/détruit!

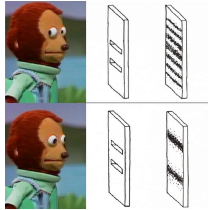
Aie!



cf fentes de
young

Les étranges lois du monde quantique

Observer un objet
le modifie/détruit!

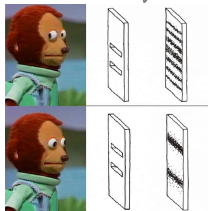


Copier/coller... Impossible!

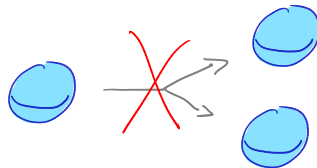


Les étranges lois du monde quantique

Observer un objet
le modifie/détruit!

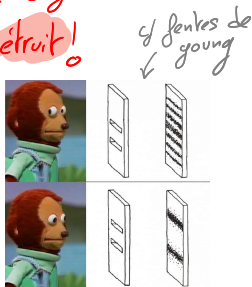


Copier/coller... Impossible!

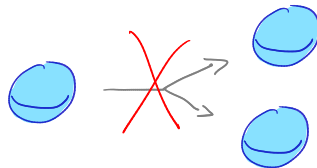


Les étranges lois du monde quantique

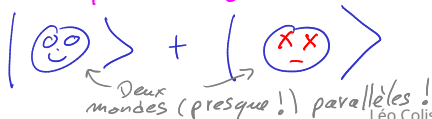
Observer un objet
le modifie/détruit!



Copier/coller... Impossible!



Être en superposition
possible !

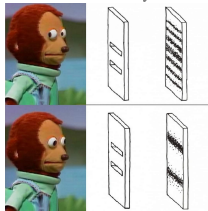


Les étranges lois du monde quantique

Observer un objet
le modifie/détruit!



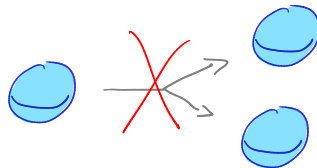
cf portes de
young



Être en superposition
possible ?

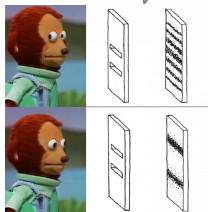


Copier/coller... Impossible!



Les étranges lois du monde quantique

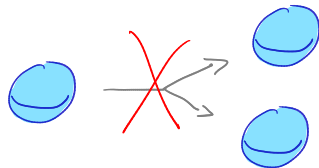
Observer un objet
le modifie/détruit!



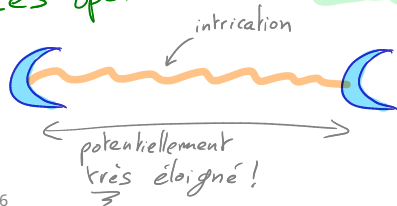
Être en superposition
possible!



Copier/coller... Impossible!



Les opérations sont non-locales!

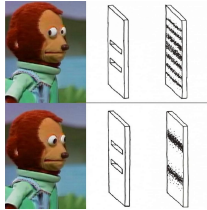


Les étranges lois du monde quantique

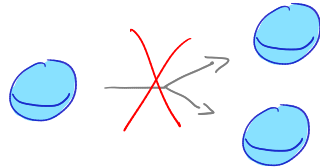
Observer un objet
le modifie/détruit!



Être en superposition
possible ?

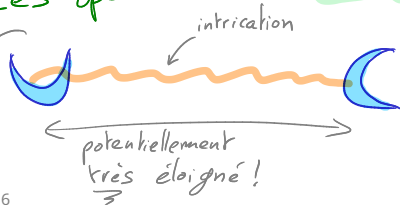


Copier/coller... Impossible!



Les opérations sont non-locales!

On applique
une opération
ici...

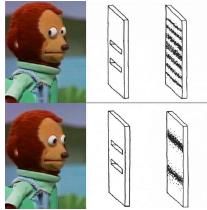


Les étranges lois du monde quantique

Observer un objet
le modifie/détruit!



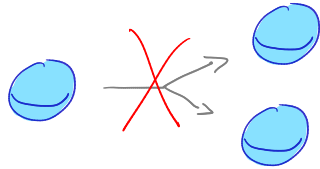
Aïe!



Être en superposition
possible ?



Copier/coller... Impossible!



Les opérations sont non-locales!

On applique
une opération
ici...



intrication



... une
opération est
instantanément

appliquée
de l'autre
côté!

potentiellement
très éloigné!

Quantique : les modifications sont non-locales

Attention !!!

Même si l'état est modifié instantanément, il est toujours
**impossible de communiquer plus vite que la
vitesse de la lumière !**



<https://drgoulu.com>

L'informatique quantique

Qubits

Qubits

Made from infinitesimally small particles:



Qubits

Made from infinitesimally small particles:

E.g.:

- photons

Qubits

Made from infinitesimally small particles:



E.g.:

- photons
- cold atoms
- ...

Qubits



Qubits



Qubits

0



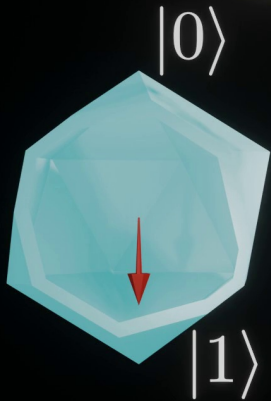
Qubits

0



1

Qubits



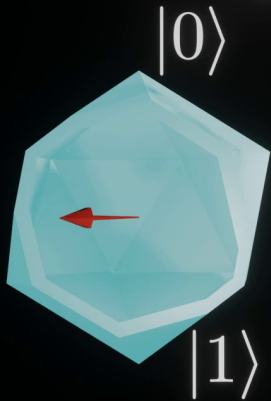
Qubits



Superposition

$$a_0 |0\rangle + a_1 |1\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

Qubits



Superposition

$$a_0 |0\rangle + a_1 |1\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

$$|+\theta\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta} |1\rangle)$$

Qubit

Un qubit est un vecteur $|\psi\rangle := \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{C}^2$ ^{$\rightarrow$ Espace de Hilbert} de norme 1, i.e. $|a|^2 + |b|^2 = 1$.

On note $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Qubit

Un qubit est un vecteur $|\psi\rangle := \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{C}^2$ de norme 1, i.e. $|a|^2 + |b|^2 = 1$.

On note $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Lequel de ces vecteurs est un qubit?



$$A := \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$$

$$B := \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$$

C: Autre (aucun/les deux)

Qubit

Un qubit est un vecteur $|\psi\rangle := \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{C}^2$ de norme 1, i.e. $|a|^2 + |b|^2 = 1$.

On note $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Lequel de ces vecteurs est un qubit?



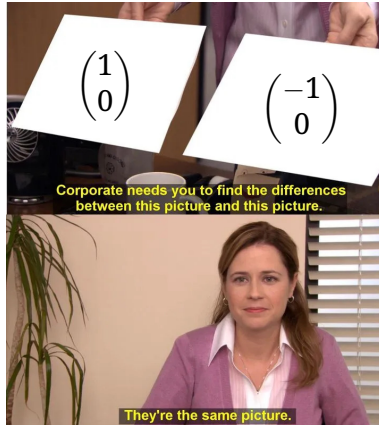
$$A := \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$$

$$B := \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} \checkmark$$

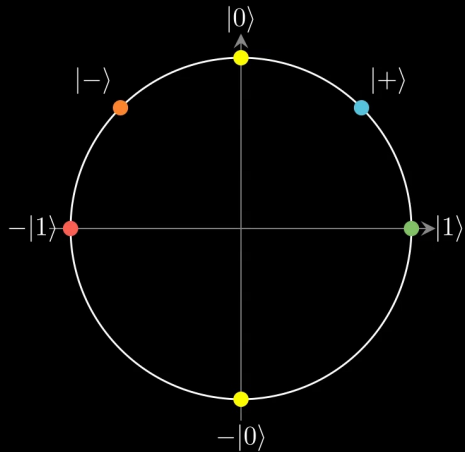
C: Autre (aucun/les deux)

Qubits

La **phase globale** d'un état n'est PAS physiquement observable !

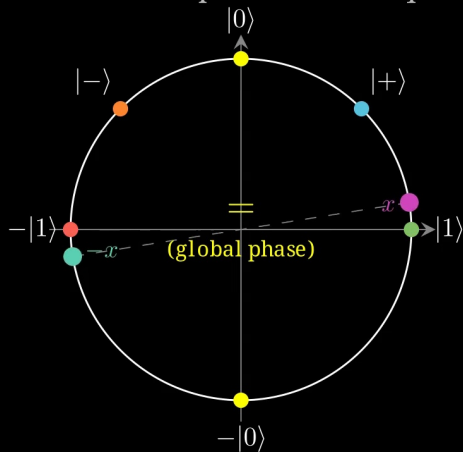


Explanation of the bloch sphere

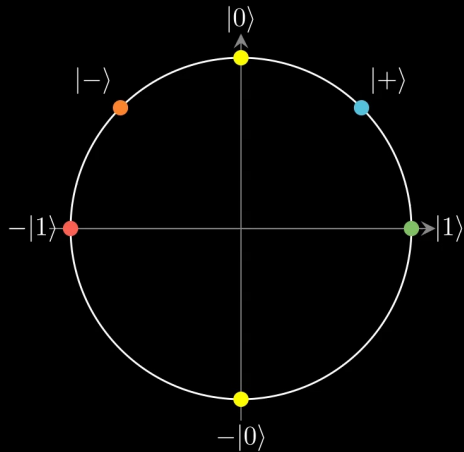


Explanation of the bloch sphere

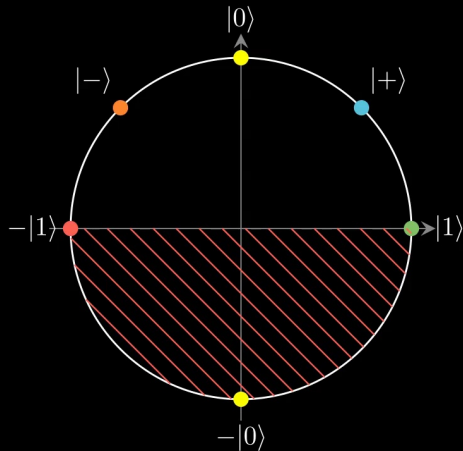
x and its antipodal $-x$ are equal



Explanation of the bloch sphere

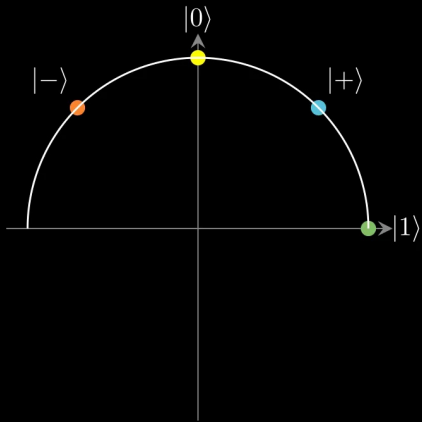


Explanation of the bloch sphere

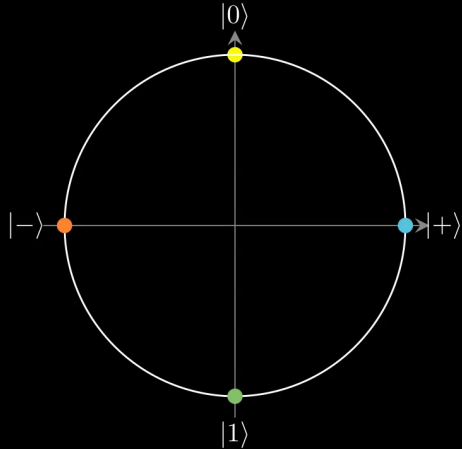


Bottom half is redundant ($e^{i\varphi}|\psi\rangle \sim |\psi\rangle$)

Explanation of the bloch sphere

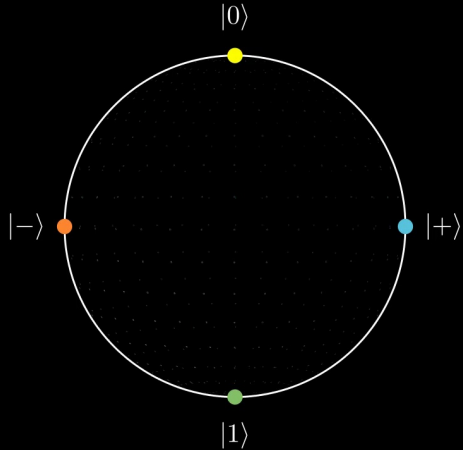


Explanation of the bloch sphere

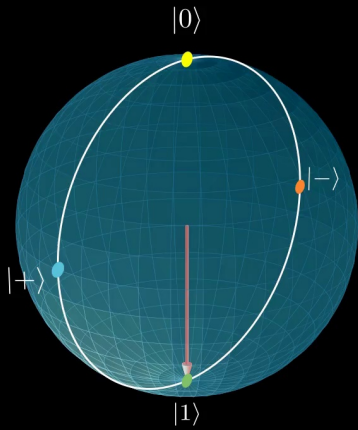


Folding the half-circle onto a full circle: $\theta_{\text{new}} = 2\theta_{\text{old}}$

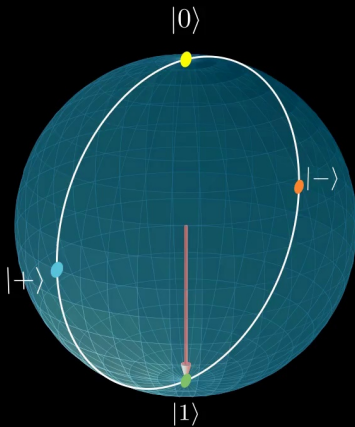
Explanation of the bloch sphere



We can similarly do this with the other dimension



Orthogonal states = antipodal points on the Bloch sphere



Qubits

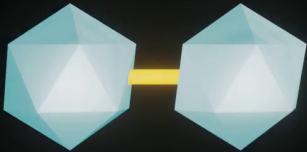
Entanglement

$$a_0 |0\rangle + a_1 |1\rangle$$



Qubits

Entanglement



$$\begin{aligned} &a_0 |0\rangle \\ &+a_1 |1\rangle \\ &+a_2 |2\rangle \\ &+a_3 |3\rangle \end{aligned}$$

Qubits

Entanglement



$$\begin{aligned} &a_0 |0\rangle \\ &+a_1 |1\rangle \\ &+a_2 |2\rangle \\ &+a_3 |3\rangle \\ &+a_4 |4\rangle \\ &+a_5 |5\rangle \\ &+a_6 |6\rangle \\ &+a_7 |7\rangle \end{aligned}$$

Qubits

Entanglement



Parallelize an operation on exponentially many inputs: speedup (sometimes...)

$$\begin{aligned} & a_0 |0\rangle |f(0)\rangle \\ & + a_1 |1\rangle |f(1)\rangle \\ & + a_2 |2\rangle |f(2)\rangle \\ & + a_3 |3\rangle |f(3)\rangle \\ & + a_4 |4\rangle |f(4)\rangle \\ & + a_5 |5\rangle |f(5)\rangle \\ & + a_6 |6\rangle |f(6)\rangle \\ & + a_7 |7\rangle |f(7)\rangle \end{aligned}$$

Produit tensoriel = composer plusieurs systèmes

Definition produit tensoriel (Kronecker product)

Le produit tensoriel $\otimes$ est défini comme:

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,m} \\ a_{2,1} & a_{2,2} & \dots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,m} \end{pmatrix}, B = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,m} \\ a_{2,1} & a_{2,2} & \dots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,m} \end{pmatrix}$$

$$A \otimes B = \begin{pmatrix} a_{1,1}B & a_{1,2}B & \dots & a_{1,m}B \\ a_{2,1}B & a_{2,2}B & \dots & a_{2,m}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1}B & a_{n,2}B & \dots & a_{n,m}B \end{pmatrix}$$

Produit tensoriel = composer plusieurs systèmes

Propriétés produit tensoriel

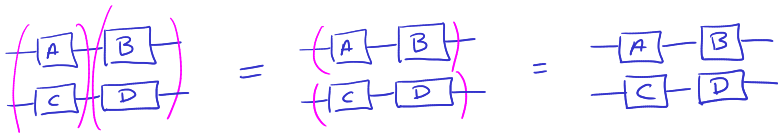
- **Associativité:** $(A \otimes B) \otimes C = A \otimes (B \otimes C)$: omit brackets

- $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$

Très utile: $(X |\phi\rangle) \otimes (H |\psi\rangle) = (X \otimes H)(|\phi\rangle \otimes |\psi\rangle)$.

$$\rightarrow ((|0\rangle \otimes |1\rangle) \otimes |1\rangle) \\ = |011\rangle$$

- **Distributivité:** $A \otimes (B + C) = A \otimes B + A \otimes C$,
 $(A + B) \otimes C = A \otimes C + B \otimes C$.
- $(\alpha A) \otimes B = A \otimes (\alpha B) = \alpha(A \otimes B)$



On peut
dessiner des
circuits!

Combien vaut $|10\rangle$?

Et de manière plus générale, $|x\rangle$ pour $x \in \{0, 1\}^n$?

?

A $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$

B $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

C $\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

Combien vaut $|10\rangle$?

Et de manière plus générale, $|x\rangle$ pour $x \in \{0, 1\}^n$?

A $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$

B $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

C $\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

?

✓ $|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

Produit tensoriel

Combien vaut $|10\rangle$?

Et de manière plus générale, $|x\rangle$ pour $x \in \{0, 1\}^n$?

A $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$

B $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

C $\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

?

$\checkmark |10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

= 2 en binaire

"1" à la 2^e position en indexant à 0.

Produit tensoriel

Combien vaut $|10\rangle$?

Et de manière plus générale, $|x\rangle$ pour $x \in \{0, 1\}^n$?

A $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ $|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ $|01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ $|10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ $|11\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$

B $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

C $\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

$= 2$ en binaire

"1" à la 2^e position en indexant à 0.

Produit tensoriel

Combien vaut $|10\rangle$?

Et de manière plus générale, $|x\rangle$ pour $x \in \{0, 1\}^n$?

A $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ $|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ $|01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ $|10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ $|11\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$

= Computational basis

B $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

C $\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

"1" à la 2^e position en indexant à 0.

Holevo



Holevo



NON!! (Théorème d'Holevo simplifié)

Étant donné n qubits (i.e. un état quantique de dimension 2^n), il est impossible d'extraire plus que n bits d'information.

Holevo



Mais pratique en
cryptographie!

NON!! (Théorème d'Holevo simplifié)

Étant donné n qubits (i.e. un état quantique de dimension 2^n), il est impossible d'extraire plus que n bits d'information.

Holevo



Mais pratique en
cryptographie!
+ il faut être malin
en algorithmique!

NON!! (Théorème d'Holevo simplifié)

Étant donné n qubits (i.e. un état quantique de dimension 2^n), il est impossible d'extraire plus que n bits d'information.

Unitaires

On peut appliquer sur n'importe quel état quantique $|\psi\rangle$ n'importe quelle matrice U dite **unitaire**, i.e. telle que $U^\dagger U = I$ avec $U^\dagger$ (prononcer "dag-ger" la transposée conjuguée). On obtient alors $U|\psi\rangle$.

Unitaires

→ Préserve la norme + inversible

Unitaires

On peut appliquer sur n'importe quel état quantique $|\psi\rangle$ n'importe quelle matrice U dite **unitaire**, i.e. telle que $U^\dagger U = I$ avec $U^\dagger$ (prononcer "dag-ger" la transposée conjuguée). On obtient alors $U|\psi\rangle$.

Unitaires

On peut appliquer sur n'importe quel état quantique $|\psi\rangle$ n'importe quelle matrice U dite **unitaire**, i.e. telle que $U^\dagger U = I$ avec $U^\dagger$ (prononcer "dagger" la transposée conjuguée). On obtient alors $U|\psi\rangle$.

Quelles matrices sont unitaires ?



$$A := \begin{pmatrix} 1 & i \\ i & 0 \end{pmatrix}$$

$$B := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$C := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

D : Autre (aucune/plusieurs)

🧐 Calculez $C|0\rangle$ puis $C|0\dots 0\rangle$ puis $C|x\rangle$.

Unitaires

On peut appliquer sur n'importe quel état quantique $|\psi\rangle$ n'importe quelle matrice U dite **unitaire**, i.e. telle que $U^\dagger U = I$ avec $U^\dagger$ (prononcer "dagger" la transposée conjuguée). On obtient alors $U|\psi\rangle$.

Quelles matrices sont unitaires ?



$$A := \begin{pmatrix} 1 & i \\ i & 0 \end{pmatrix}$$

$$B := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \checkmark$$

$$C := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \checkmark$$

D : Autre (aucune/plusieurs) $\checkmark$

 Calculez $C|0\rangle$ puis $C|0\dots 0\rangle$ puis $C|x\rangle$.

Unitaires

Unitaires

On peut appliquer sur n'importe quel état quantique $|\psi\rangle$ n'importe quelle matrice U dite **unitaire**, i.e. telle que $U^\dagger U = I$ avec $U^\dagger$ (prononcer "dag-ger" la transposée conjuguée). On obtient alors $U|\psi\rangle$.

Quelles matrices sont unitaires ?



$$A := \begin{pmatrix} 1 & i \\ i & 0 \end{pmatrix}$$

$$B := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \checkmark$$

Porte X

$$C := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \checkmark$$

D: Autre (aucune/plusieurs) $\checkmark$

Porte H

🔗 Calculez $C|0\rangle$ puis $C|0 \dots 0\rangle$ puis $C|x\rangle$.

Soit $H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Que vaut $H |0\rangle$?



- A $|1\rangle$
- B $\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$
- C $\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle$
- D Autre

🧐 Calculez $H |0 \dots 0\rangle$

puis $H |x\rangle$

Soit $H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Que vaut $H|0\rangle$?



- A $|1\rangle$
- B $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ ✓
- C $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$
- D Autre

🧐 Calculez $H|0\dots 0\rangle$ puis $H|x\rangle$

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Soit $H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Que vaut $H |0\rangle$?

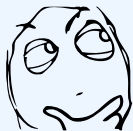


- A $|1\rangle$
- B $\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$
- C $\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle$
- D Autre

🧐 Calculez $H |0 \dots 0\rangle = \sum_x |x\rangle$ puis $H |x\rangle = \sum_b (-1)^{b \cdot x} |b\rangle$

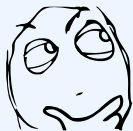
$$H |0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$$

Comment extraire de l'information ?



Mais alors, comment **extraire** de l'information quantique pour la ramener dans le **monde classique** ?

Comment extraire de l'information ?



Mais alors, comment **extraire** de l'information quantique pour la ramener dans le **monde classique** ?



Faire des **mesures** !

Qubits

Measurement: extract information



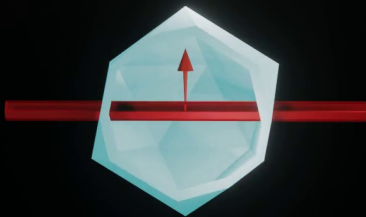
Qubits

Measurement: extract information



Qubits

Measurement: extract information



Qubits

Measurement: extract information

1

Qubits

Measurement: extract information

1

⇒ not easy to exploit benefits of superposition

Qubits

Measurement: extract information

1



⇒ not easy to exploit benefits of superposition

Qubits

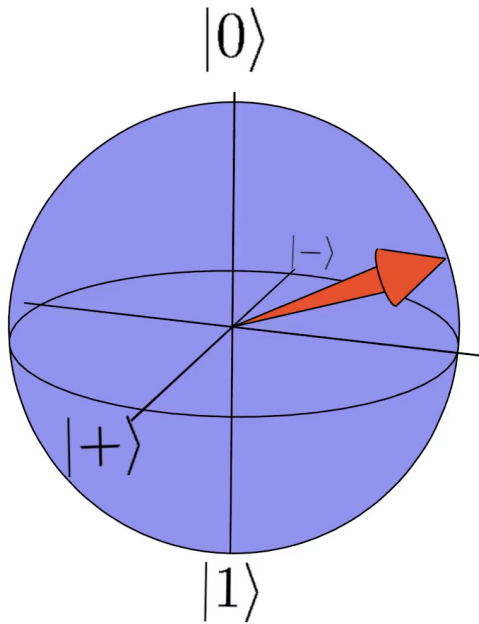
Measurement: extract information

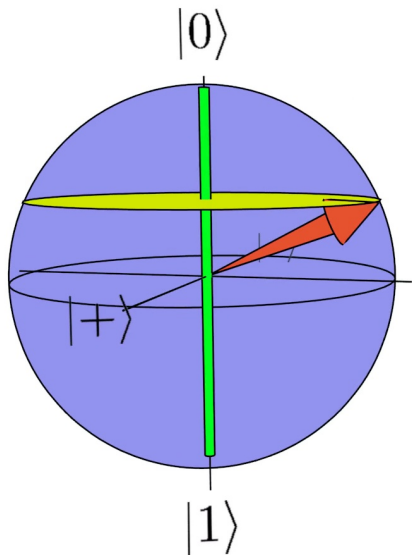
No cloning principle

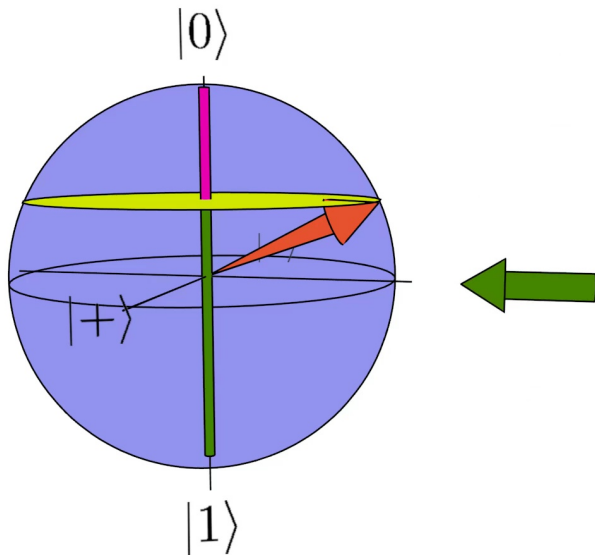
1

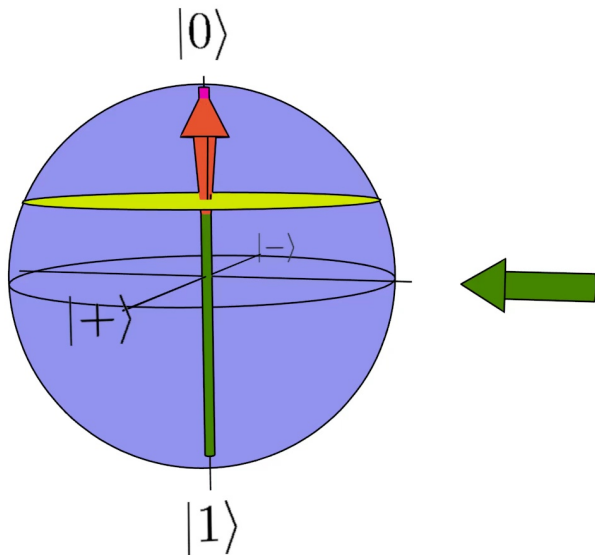


⇒ not easy to exploit benefits of superposition









Bra ket

Étant donné un état $|\psi\rangle$ (appelé “ket”) on définit le “bra” $\langle\psi| := |\psi\rangle^\dagger$ (transposée conjuguée, notation bracket), ainsi $\langle\psi|\psi\rangle = \langle\psi|\psi\rangle = \|\psi\|^2$.



Combien vaut $\langle 01|01\rangle$?

$$A : 0 \quad B : 1 \quad C : \frac{1}{\sqrt{2}} \quad D : \textit{autre} \quad (1)$$

Bra ket

Étant donné un état $|\psi\rangle$ (appelé “ket”) on définit le “bra” $\langle\psi| := |\psi\rangle^\dagger$ (transposée conjuguée, notation bracket), ainsi $\langle\psi|\psi\rangle = \langle\psi|\psi\rangle = \|\psi\|^2$.



Combien vaut $\langle 01|01\rangle$?

A : 0 B : 1 ✓ C : $\frac{1}{\sqrt{2}}$ D : autre (1)

Bra ket

Étant donné un état $|\psi\rangle$ (appelé “ket”) on définit le “bra” $\langle\psi| := |\psi\rangle^\dagger$ (transposée conjuguée, notation bracket), ainsi $\langle\psi|\psi\rangle = \langle\psi|\psi\rangle = \|\psi\|^2$.



Combien vaut $\langle 01|01\rangle$?

A : 0 B : 1 ✓ C : $\frac{1}{\sqrt{2}}$ D : autre (1)

$$\langle 01|01\rangle = \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

Bra ket

Étant donné un état $|\psi\rangle$ (appelé “ket”) on définit le “bra” $\langle\psi| := |\psi\rangle^\dagger$ (transposée conjuguée, notation bracket), ainsi $\langle\psi|\psi\rangle = \langle\psi|\psi\rangle = \|\psi\|^2$.



Combien vaut $\langle 01|01\rangle$?

$A : 0$ $B : 1$ ✓ $C : \frac{1}{\sqrt{2}}$ $D : autre$ (1)

$$\langle 01|01\rangle = \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \text{ Plus généralement, } \langle x|x'\rangle = 1 \text{ ssi } x = x', 0 \text{ sinon.}$$

Mesure

Étant donné des matrices $\{A_i\}_i$ telles que $\sum_i A_i^\dagger A_i = I$. On peut alors **mesurer** $|\psi\rangle$ et obtenir de manière **non-déterministe** pour sortie classique i avec probabilité $p_i := \|A_i |\psi\rangle\|^2$, et l'état post-mesure sera $\frac{A_i |\psi\rangle}{p_i}$.



On considère $A_0 = |0\rangle\langle 0|$ et $A_1 = |1\rangle\langle 1|$. Quelle est la probabilité d'obtenir le résultat 0 en mesurant $|\psi\rangle := a|0\rangle + b|1\rangle$?

$A : a$ $B : b$ $C : |a|^2$ $D : |b|^2$ $E : \text{autre}$

Mesure

Étant donné des matrices $\{A_i\}_i$ telles que $\sum_i A_i^\dagger A_i = I$. On peut alors **mesurer** $|\psi\rangle$ et obtenir de manière **non-déterministe** pour sortie classique i avec probabilité $p_i := \|A_i |\psi\rangle\|^2$, et l'état post-mesure sera $\frac{A_i |\psi\rangle}{p_i}$.



On considère $A_0 = \langle 0|$ et $A_1 = \langle 1|$. Quelle est la probabilité d'obtenir le résultat 0 en mesurant $|\psi\rangle := a|0\rangle + b|1\rangle$?

$A : a$ $B : b$ $C : |a|^2$ ✓ $D : |b|^2$ $E : \text{autre}$

$$p_0 = \|\langle 0| (a|0\rangle + b|1\rangle)\|^2 = \|a\langle 0|0\rangle + b\langle 0|1\rangle\|^2 = |a|^2$$

Motivation produit tensoriel

+ précisément $\sqrt{\text{proba}}$

$$\text{Qubit}_1 = \begin{pmatrix} \sqrt{0.3} \\ \sqrt{0.7} \end{pmatrix} \begin{matrix} \leftarrow \text{Proba } (0) \\ \leftarrow \text{Proba } (1) \end{matrix}, \quad \text{Qubit}_2 = \begin{pmatrix} \sqrt{0.6} \\ \sqrt{0.4} \end{pmatrix} \begin{matrix} \leftarrow \text{Proba } (0) \\ \leftarrow \text{Proba } (1) \end{matrix}$$

Motivation produit tensoriel

$$\text{Qubit}_1 = \begin{pmatrix} \sqrt{0.3} \\ \sqrt{0.7} \end{pmatrix} \begin{matrix} \leftarrow \text{Proba } (0) \\ \leftarrow \text{Proba } (1) \end{matrix}, \quad \text{Qubit}_2 = \begin{pmatrix} \sqrt{0.6} \\ \sqrt{0.4} \end{pmatrix} \begin{matrix} \leftarrow \text{Proba } (0) \\ \leftarrow \text{Proba } (1) \end{matrix}$$

$$\text{Qubits}_{1,2} = \begin{pmatrix} \sqrt{0.3} \times \sqrt{0.6} \\ \sqrt{0.3} \times \sqrt{0.4} \\ \sqrt{0.7} \times \sqrt{0.6} \\ \sqrt{0.7} \times \sqrt{0.4} \end{pmatrix}$$

Motivation produit tensoriel

$$\text{Qubit}_1 = \begin{pmatrix} \sqrt{0.3} \\ \sqrt{0.7} \end{pmatrix} \begin{matrix} \leftarrow \text{Proba } (0) \\ \leftarrow \text{Proba } (1) \end{matrix}, \quad \text{Qubit}_2 = \begin{pmatrix} \sqrt{0.6} \\ \sqrt{0.4} \end{pmatrix} \begin{matrix} \leftarrow \text{Proba } (0) \\ \leftarrow \text{Proba } (1) \end{matrix}$$

$$\text{Qubits}_{1,2} = \begin{pmatrix} \sqrt{0.3} \times \sqrt{0.6} \\ \sqrt{0.3} \times \sqrt{0.4} \\ \sqrt{0.7} \times \sqrt{0.6} \\ \sqrt{0.7} \times \sqrt{0.4} \end{pmatrix} \begin{matrix} \leftarrow \text{Proba } (0, 0) \\ \leftarrow \text{Proba } (0, 1) \\ \leftarrow \text{Proba } (1, 0) \\ \leftarrow \text{Proba } (1, 1) \end{matrix}$$

Motivation produit tensoriel

$$\text{Qubit}_1 = \begin{pmatrix} \sqrt{0.3} \\ \sqrt{0.7} \end{pmatrix} \begin{matrix} \leftarrow \text{Proba } (0) \\ \leftarrow \text{Proba } (1) \end{matrix}, \quad \text{Qubit}_2 = \begin{pmatrix} \sqrt{0.6} \\ \sqrt{0.4} \end{pmatrix} \begin{matrix} \leftarrow \text{Proba } (0) \\ \leftarrow \text{Proba } (1) \end{matrix}$$

$$\text{Qubits}_{1,2} = \begin{pmatrix} \sqrt{0.3} \times \sqrt{0.6} \\ \sqrt{0.3} \times \sqrt{0.4} \\ \sqrt{0.7} \times \sqrt{0.6} \\ \sqrt{0.7} \times \sqrt{0.4} \end{pmatrix} \begin{matrix} \leftarrow \text{Proba } (0, 0) \\ \leftarrow \text{Proba } (0, 1) \\ \leftarrow \text{Proba } (1, 0) \\ \leftarrow \text{Proba } (1, 1) \end{matrix} = \begin{pmatrix} \sqrt{0.3} \\ \sqrt{0.7} \end{pmatrix} \otimes \begin{pmatrix} \sqrt{0.6} \\ \sqrt{0.4} \end{pmatrix} = \begin{pmatrix} \sqrt{0.3} \times \begin{pmatrix} \sqrt{0.6} \\ \sqrt{0.4} \end{pmatrix} \\ \sqrt{0.7} \times \begin{pmatrix} \sqrt{0.6} \\ \sqrt{0.4} \end{pmatrix} \end{pmatrix}$$

Motivation produit tensoriel

$$\text{Qubit}_1 = \begin{pmatrix} \sqrt{0.3} \\ \sqrt{0.7} \end{pmatrix} \begin{matrix} \leftarrow \text{Proba } (0) \\ \leftarrow \text{Proba } (1) \end{matrix}, \quad \text{Qubit}_2 = \begin{pmatrix} \sqrt{0.6} \\ \sqrt{0.4} \end{pmatrix} \begin{matrix} \leftarrow \text{Proba } (0) \\ \leftarrow \text{Proba } (1) \end{matrix}$$

$$\text{Qubits}_{1,2} = \begin{pmatrix} \sqrt{0.3} \times \sqrt{0.6} \\ \sqrt{0.3} \times \sqrt{0.4} \\ \sqrt{0.7} \times \sqrt{0.6} \\ \sqrt{0.7} \times \sqrt{0.4} \end{pmatrix} \begin{matrix} \leftarrow \text{Proba } (0, 0) \\ \leftarrow \text{Proba } (0, 1) \\ \leftarrow \text{Proba } (1, 0) \\ \leftarrow \text{Proba } (1, 1) \end{matrix} = \begin{pmatrix} \sqrt{0.3} \\ \sqrt{0.7} \end{pmatrix} \otimes \begin{pmatrix} \sqrt{0.6} \\ \sqrt{0.4} \end{pmatrix} = \begin{pmatrix} \sqrt{0.3} \times \begin{pmatrix} \sqrt{0.6} \\ \sqrt{0.4} \end{pmatrix} \\ \sqrt{0.7} \times \begin{pmatrix} \sqrt{0.6} \\ \sqrt{0.4} \end{pmatrix} \end{pmatrix}$$



L'utilisation du produit tensoriel est (relativement) **naturelle** !

États non-séparables

Considérons $\Pr[\text{mesure} = 00] = \frac{1}{2}$, $\Pr[\text{mesure} = 11] = \frac{1}{2}$.

$$|\phi^+\rangle = \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 1/\sqrt{2} \end{pmatrix} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Corrélations $\implies$ impossible de décomposer $|\phi^+\rangle$ en $|\psi\rangle \otimes |\phi\rangle$.
L'état est **intriqué** (tenseur = indépendance).

Preuve. Si $|\phi^+\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$, alors $ad = 0$ et $ac \neq 0$ donc $d = 0$. Impossible : $bd \neq 0$.

Intrication

États non-séparables

Considérons $\Pr[\text{mesure} = 00] = \frac{1}{2}$, $\Pr[\text{mesure} = 11] = \frac{1}{2}$.

$$|\phi^+\rangle = \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 1/\sqrt{2} \end{pmatrix} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

} Paire de Bell C

Corrélations $\implies$ impossible de décomposer $|\phi^+\rangle$ en $|\psi\rangle \otimes |\phi\rangle$.
L'état est **intriqué** (tenseur = indépendance).

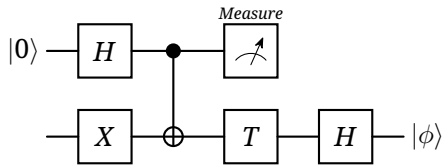
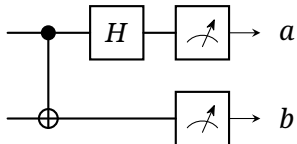
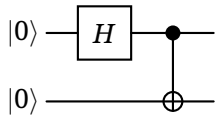
Preuve. Si $|\phi^+\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$, alors $ad = 0$ et $ac \neq 0$ donc $d = 0$. Impossible : $bd \neq 0$.

Portes universel

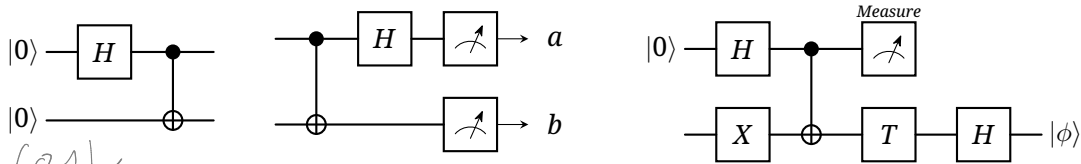
On peut réaliser n'importe quel circuit à partir des portes suivantes :

- $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
- $CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
- $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$
- Mesures dans la base calculatoire

Circuits universels



Circuits universels



$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$|0\rangle \xrightarrow{X} \xrightarrow{H} = ?$ Puis circuits plus hauts dans l'ordre

A $|0\rangle$

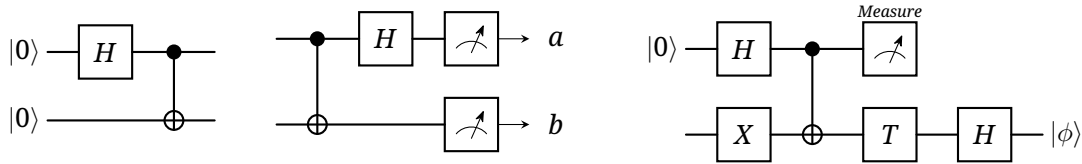
B $|1\rangle$

C $|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

D $|-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

?

Circuits universels



$|0\rangle \xrightarrow{X} \xrightarrow{H} = ?$? Puis circuits plus hauts dans l'ordre

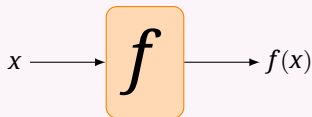
- A** $|0\rangle$
- B** $|1\rangle$
- C** $|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- D** $|-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ ✓

$$HX|0\rangle = H \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = H \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |-\rangle$$

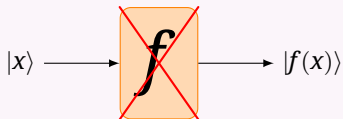
Circuits universels

Appliquer une fonction en superposition

Classiquement :



Quantiquement :

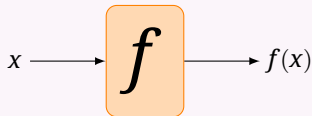


Problème : non unitaire, e.g. avec $f_0(x) = 0$ on aurait $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$.

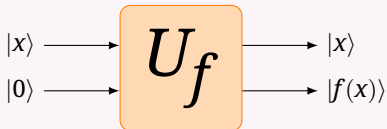
Circuits universels

Appliquer une fonction en superposition

Classiquement :



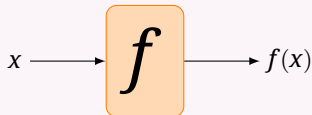
Quantiquement :



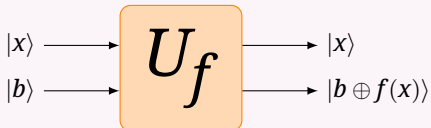
Circuits universels

Appliquer une fonction en superposition

Classiquement :



Quantiquement ($\oplus$ = XOR bit-à-bit):



Qubits

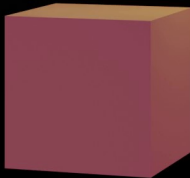
Applications

Qubits

Applications

- Shor's algorithm: factor numbers

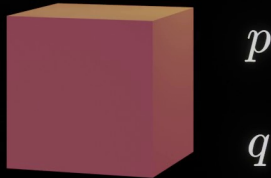
$$p \times q$$



Qubits

Applications

- Shor's algorithm: factor numbers



Qubits

Applications

- Shor's algorithm: factor numbers
- Grover: search efficiently an item



Qubits

Applications

- Shor's algorithm: factor numbers
- Grover: search efficiently an item



Qubits

Applications

- Shor's algorithm: factor numbers
- Grover: search efficiently an item
- ...





Informatique quantique

L'informatique quantique peut...

Détruire

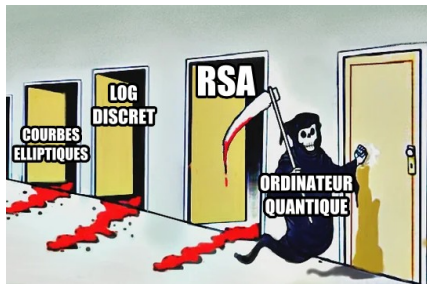


Algo de Shor = **casse toute la cryptographie**
(à clé publique) utilisée aujourd'hui sur internet
(RSA, courbes elliptiques)

Informatique quantique

L'informatique quantique peut...

Détruire



Algo de Shor = **casse toute la cryptographie**
(à clé publique) utilisée aujourd'hui sur internet
(RSA, courbes elliptiques)

Construire

- **Cryptographie post-quantique**
= cryptographie classique résistant aux ordinateurs quantiques
(réseaux euclidiens, codes, isogénies...)

Informatique quantique

L'informatique quantique peut...

Détruire



Algo de Shor = **casse toute la cryptographie**
(à clé publique) utilisée aujourd'hui sur internet
(RSA, courbes elliptiques)

Construire

- **Cryptographie post-quantique**
= cryptographie classique résistant aux ordinateurs quantiques
(réseaux euclidiens, codes, isogénies...)
- **Cryptographie quantique**
= entre ordinateur quantiques, sécurisé "à tout jamais"
(distribution quantique de clé QKD...)

Ordinateur quantique : la quête du Graal

Ordinateur quantique : acteurs et financements

Le Plan Quantique, ambitieux et attendu

Quelques investissements gouvernementaux dans les technologies quantiques autour du globe.

UE : Flagship Quantique
1 Md€ sur 10 ans
lancé en 2018

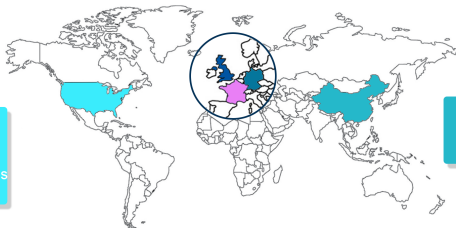
Royaume-Uni
1 Md£ sur 10 ans
lancé en 2014

France : Plan Quantique
1,8 Md€ sur 5 ans
lancé en 2021

Allemagne
650 M€ sur 5 ans
lancé en 2018
+ 2 Md€ en 2020

Etats-Unis
1,3 Md\$ sur 5 ans
lancé en 2018
+ 800 M\$ sur 2 ans
en mars 2020

Chine
10 Md€
lancé en 2015



© CNRS - Source : sites gouvernementaux, rapport Forteza et Olivier Ezratty



ALICE & BOB



VeriQloud



Ordinateur quantique : la quête du Graal

2019 : Google affirme avoir atteint la « **suprématie quantique** » (53 qubits)

Ordinateur quantique : la quête du Graal

2019 : Google affirme avoir atteint la « **suprématie quantique** » (53 qubits)

→  Calcul inutile !!!

Ordinateur quantique : la quête du Graal

2019 : Google affirme avoir atteint la « **suprématie quantique** » (53 qubits)

⇒ **Contestation par IBM !**

Ordinateur quantique : la quête du Graal

2019 : Google affirme avoir atteint la « **suprématie quantique** » (53 qubits)

⇒ **Contestation par IBM !**

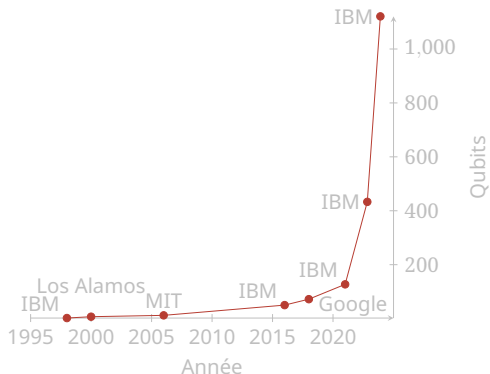


Comment vérifier
que le calcul n'est
pas accessible à des
ordinateurs classiques?
(sujet de recherche actif)

Ordinateur quantique : la quête du Graal

2019 : Google affirme avoir atteint la « **suprématie quantique** » (53 qubits)

⇒ **Contestation par IBM !**



Ordinateur quantique : le problème du bruit



10 QUBITS



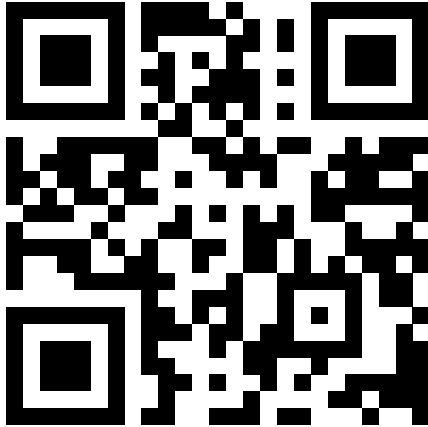
100 QUBITS



**1000 QUBITS
BRUITÉS**

Problème :
Très sensible au bruit !!!

Ordinateur quantique : le problème du bruit



Problème :
Très sensible au bruit !!!

⇒ **Solution :**
Correction d'erreurs (ECC)

Ordinateur quantique : le problème du bruit



Problème :
Très sensible au bruit !!!

⇒ **Solution :**
Correction d'erreurs (ECC)

Ordinateur quantique : le problème du bruit

Problème :

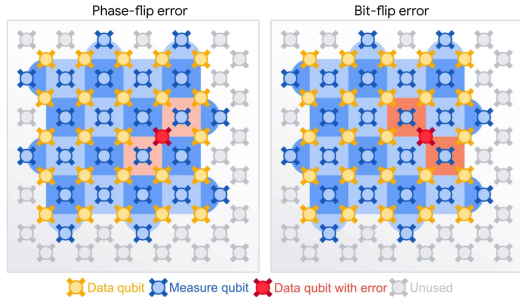
Très sensible au bruit !!!

⇒ Solution :

Correction d'erreurs (ECC)

Attention : pas facile !

(ECC = + de portes = + de bruit)



Ordinateur quantique : le problème du bruit

Problème :

Très sensible au bruit !!!

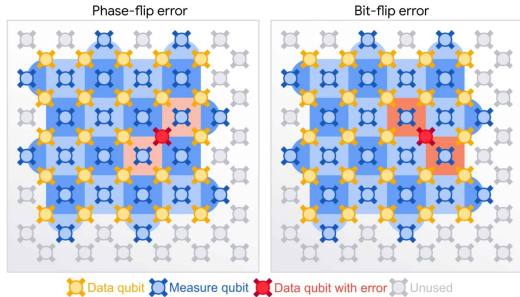
⇒ Solution :

Correction d'erreurs (ECC)

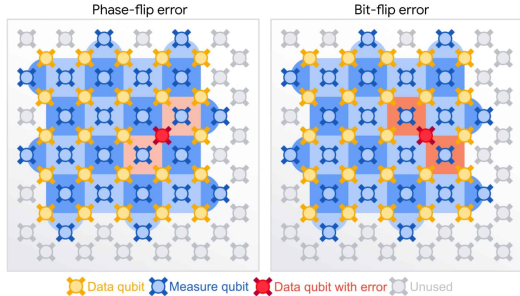
Attention : pas facile !

(ECC = + de portes = + de bruit)

⇒ **Threshold** theorem



Ordinateur quantique : le problème du bruit



Problème :
Très sensible au bruit !!!

⇒ **Solution :**
Correction d'erreurs (ECC)

Attention : pas facile !
(ECC = + de portes = + de bruit)

⇒ **Threshold** theorem

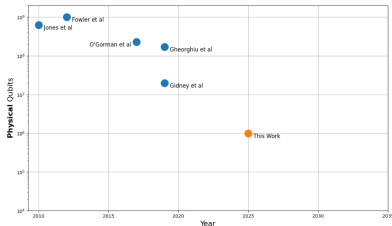
En pratique
2024 : Quantinuum/Microsoft =
qubits logiques > physiques
juin 2025 : démonstration par IBM
arXiv:2506.01779/arXiv:2506.03094

Améliorations matérielles & logicielles

Récentes améliorations importantes dans l'efficacité de Shor :

- Shor (1994) $\approx \tilde{O}(\log^2 N)$ **gates**, $\tilde{O}(\log N)$ **qubits**
- Regev (2024) $\approx \tilde{O}(\log^{3/2} N)$ quantum **gates** and **qubits** + polynomial classical post-processing
- Gidney (2024) *How to factor 2048 bit RSA integers with less than a million noisy qubits*

Assumptions: "a square grid of qubits with nearest neighbor connections, a uniform gate error rate of 0.1%, a surface code cycle time of 1 microsecond, and a control system reaction time of 10 microseconds."



- Ragavan, Vaikuntanathan (2026) Best of Shor + Regev: $\tilde{O}(\log^{3/2} N)$ quantum **gates** and $\tilde{O}(\log N)$ **qubits** + Noise-robust (use lattice to detect bad runs)

Ordinateur quantique : pourquoi s'inquiéter maintenant ?



S'il n'existe pas encore d'ordinateur quantique,
pourquoi s'inquiéter maintenant?

Ordinateur quantique : pourquoi s'inquiéter maintenant ?



?

S'il n'existe pas encore d'ordinateur quantique,
pourquoi s'inquiéter maintenant?

→ "Récolter maintenant, déchiffrer plus tard" !!



Ordinateur quantique : pourquoi s'inquiéter maintenant ?



Motivations



On ne peut donc **pas attendre...**

Problème : RSA/ECDSA/... bien plus étudiés que la cryptographie post-quantique ! (E.g. SIKE cassé !)



JAKE-CLARK.TUMBLR

imgflip.com

Motivations



On ne peut donc **pas attendre...**

Problème : RSA/ECDSA/... bien plus étudiés que la cryptographie post-quantique ! (E.g. SIKE cassé !)

- Création d'une **compétition internationale** NIST (Objectif : trouver les meilleurs chiffrements/signatures = efficaces & sécurisés)



JAKE-CLARK.TUMBLR

imgflip.com

Motivations



On ne peut donc **pas attendre...**

Problème : RSA/ECDSA/... bien plus étudiés que la cryptographie post-quantique ! (E.g. SIKE cassé !)



- Création d'une **compétition internationale** NIST (Objectif : trouver les meilleurs chiffrements/signatures = efficaces & sécurisés)
- Pour l'instant, **combiner** RSA/... & post-quantique?

Cryptographie post-quantique

Cryptographie clé publique/privée

Chiffrement clé privée



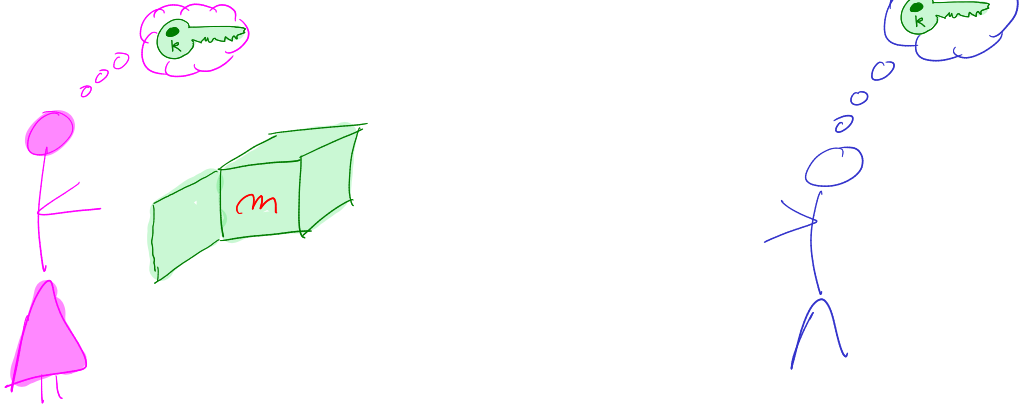
Cryptographie clé publique/privée

Chiffrement clé privée



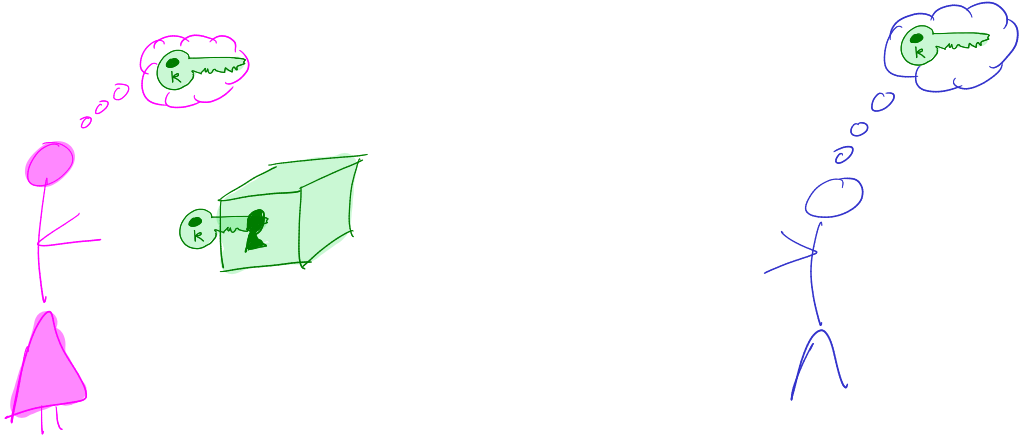
Cryptographie clé publique/privée

Chiffrement clé privée



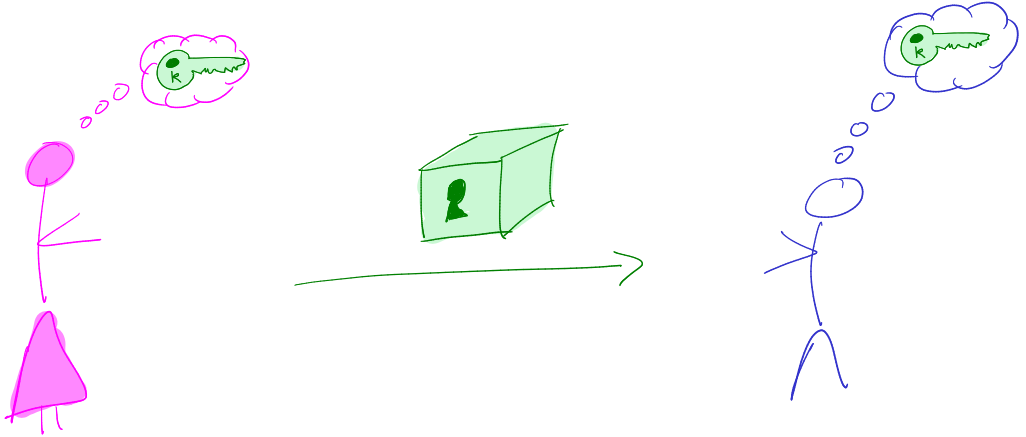
Cryptographie clé publique/privée

Chiffrement clé privée



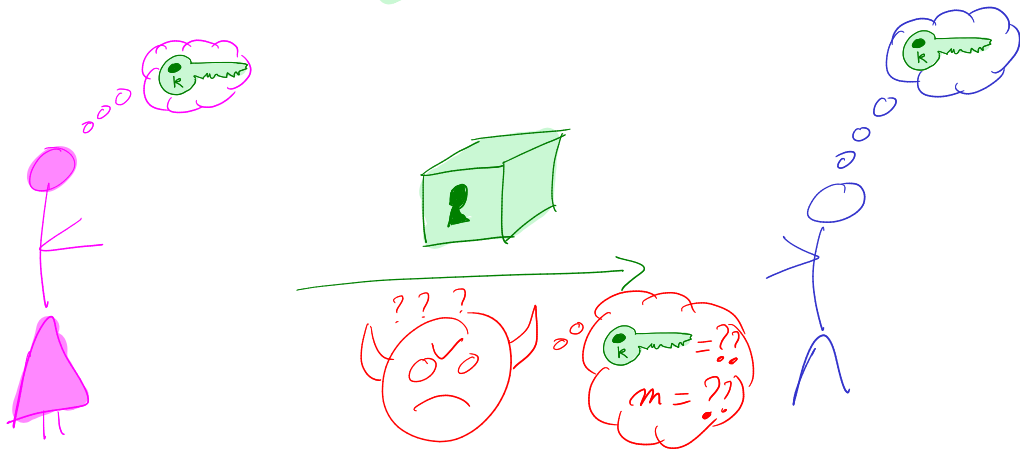
Cryptographie clé publique/privée

Chiffrement clé privée



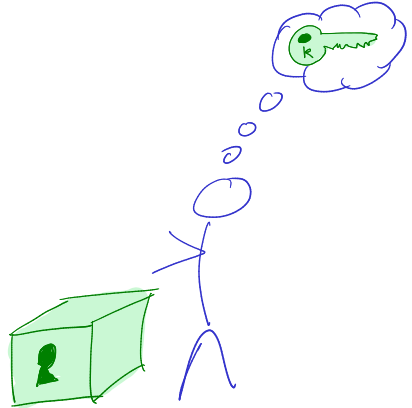
Cryptographie clé publique/privée

Chiffrement clé privée



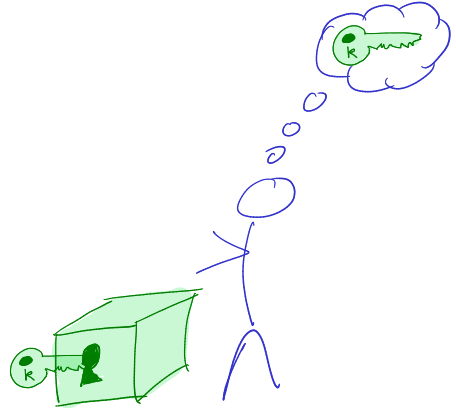
Cryptographie clé publique/privée

Chiffrement clé privée



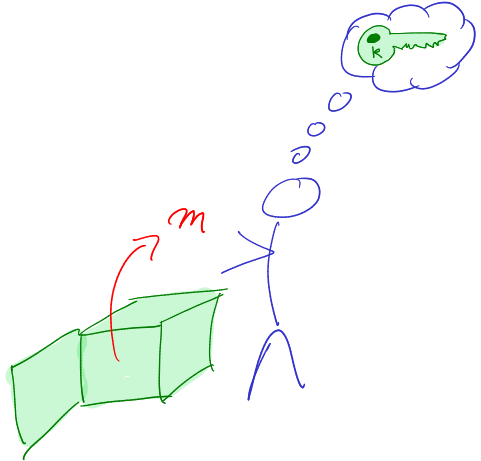
Cryptographie clé publique/privée

Chiffrement clé privée



Cryptographie clé publique/privée

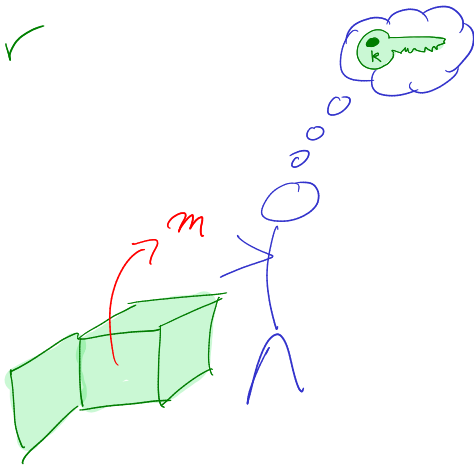
Chiffrement clé privée



Cryptographie clé publique/privée

Chiffrement clé privée

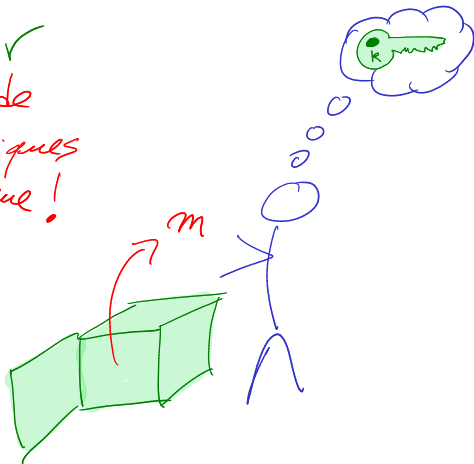
↳ Efficace ✓



Cryptographie clé publique/privée

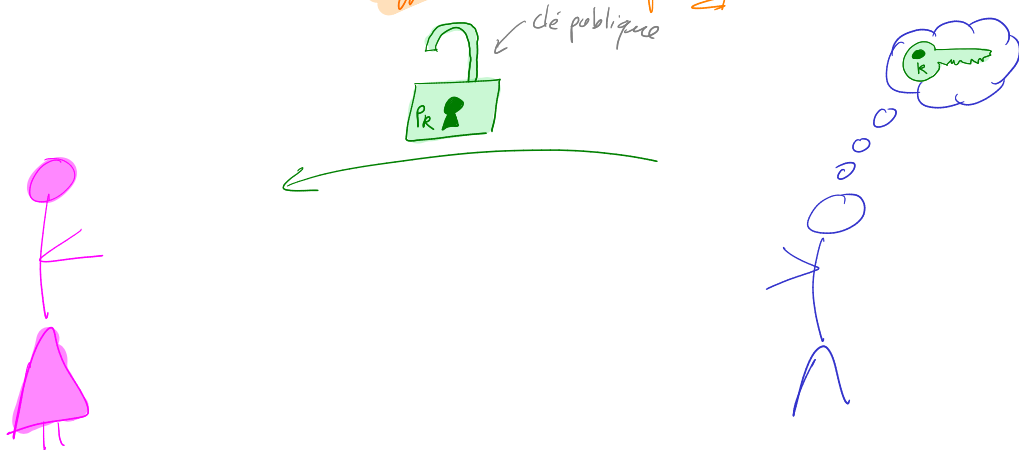
Chiffrement clé privée

↳ Efficace ✓
↳ Échange de
clés physiques
pas pratique!
☹️



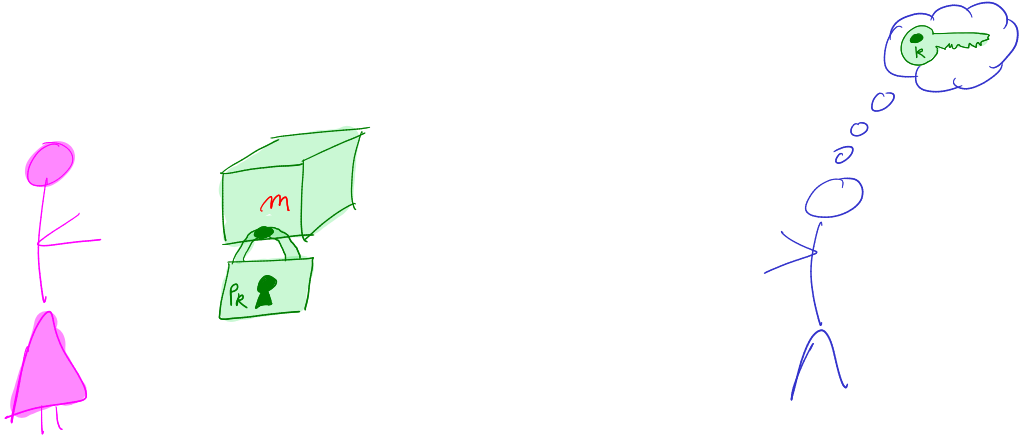
Cryptographie clé publique/privée

Chiffrement de public



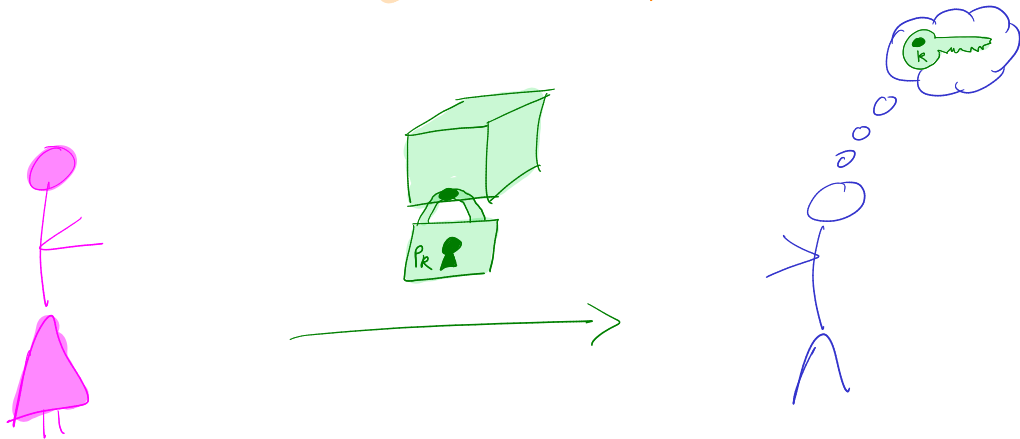
Cryptographie clé publique/privée

Chiffrement de public



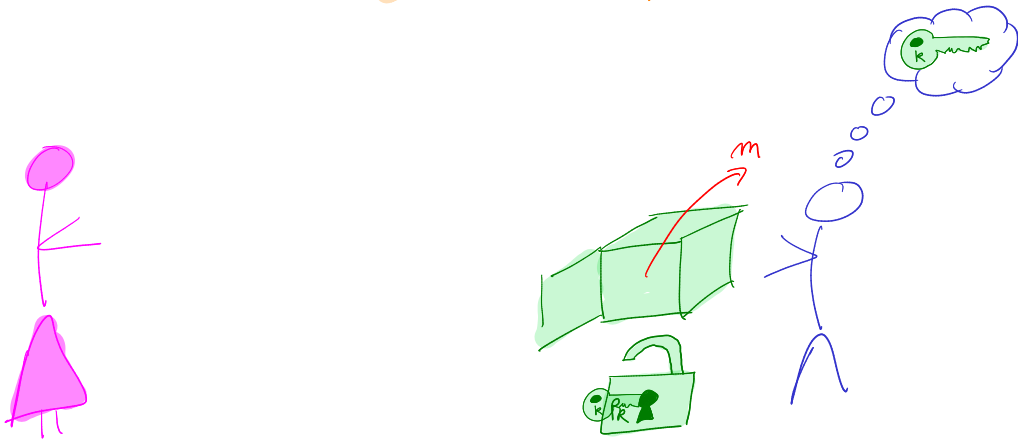
Cryptographie clé publique/privée

Chiffrement de public



Cryptographie clé publique/privée

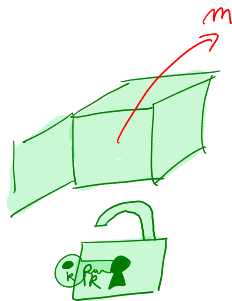
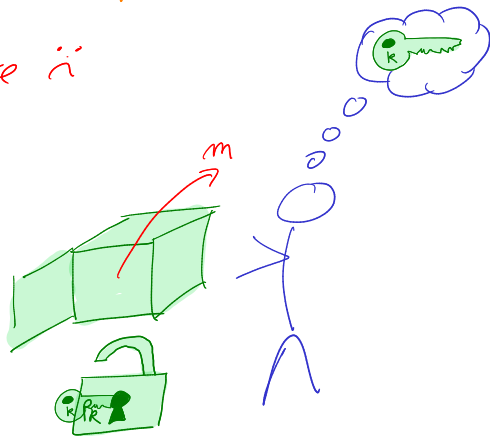
Chiffrement de public



Cryptographie clé publique/privée

Chiffrement de public

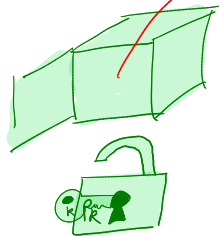
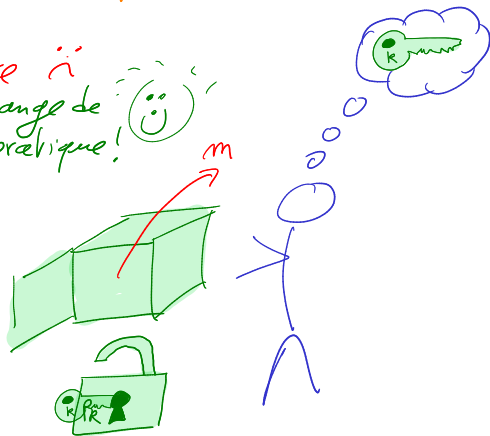
↳ moins efficace !!



Cryptographie clé publique/privée

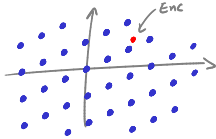
Chiffrement de public

↳ moins efficace !!
↳ pas d'échange de clés ! Très pratique ! (internet...)



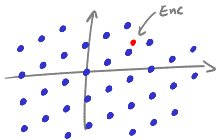
Famous post-quantum candidates

① Lattice-based Crypto

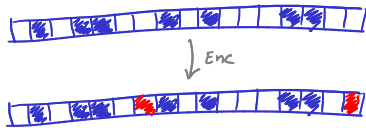


Famous post-quantum candidates

① Lattice-based Crypto

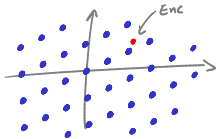


② Code-based Crypto

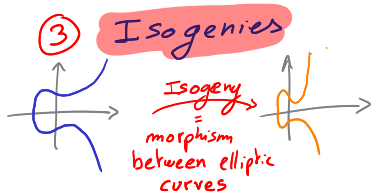
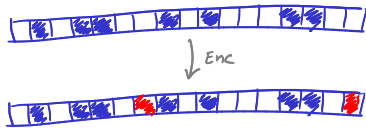


Famous post-quantum candidates

① Lattice-based Crypto

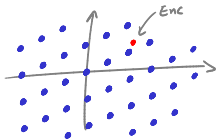


② Code-based Crypto

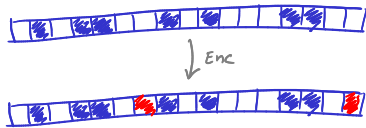


Famous post-quantum candidates

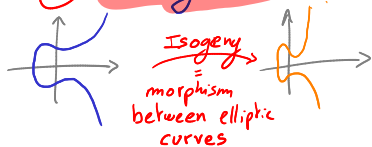
① Lattice-based Crypto



② Code-based Crypto



③ Isogenies

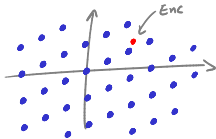


④ Multivariate Crypto

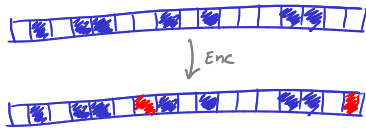
$$P_k := \begin{cases} \bullet 1 + x_1 + 2x_0x_3 \\ \bullet 4 + x_4 + 3x_1^2x_8 + x_9 \\ \bullet x_6 + x_2^3x_5 + x_7x_5 \end{cases} \xrightarrow{\text{Enc}} P_k(m)$$

Famous post-quantum candidates

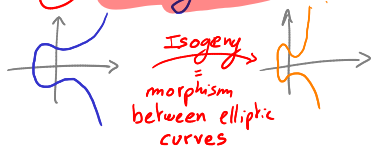
① Lattice-based Crypto



② Code-based Crypto



③ Isogenies



④ Multivariate Crypto

$$P_k := \begin{cases} \cdot 1 + x_1 + 2x_0x_3 \\ \cdot 4 + x_4 + 3x_1^2x_8 + x_9 \\ \cdot x_6 + x_2^3x_5 + x_3x_5 \end{cases} \xrightarrow{\text{Enc}} P_k(m)$$

⑤ + Symmetric crypto (incl. signatures)

Famous post-quantum candidates

① Lattice-based Crypto

- ✓ • studied extensively
- ✓ • efficient
- ✓ • simple
- ✓ • versatile (FHE...)
- ✓ • hard also on average !

③ Isogenies

- ✗ • SIDH broken $\Rightarrow$ lost confidence
- ✗ • complicated

② Code-based Crypto

- ✓ • simple
- ✗ • no worst case $\rightarrow$ average case reduction
- ✗ • FHE impossible

④ Multivariate Crypto

- ✗ • many candidates were broken $\Rightarrow$ lost confidence

⑤ + Symmetric crypto (incl. signatures)

Famous post-quantum candidates

① Lattice-based Crypto

- ✓ • studied extensively
- ✓ • efficient
- ✓ • simple
- ✓ • versatile (FHE...)
- ✓ • hard also on average !

③ Isogenies

- ✗ • SIDH broken $\Rightarrow$ lost confidence
- ✗ • complicated

② Code-based Crypto

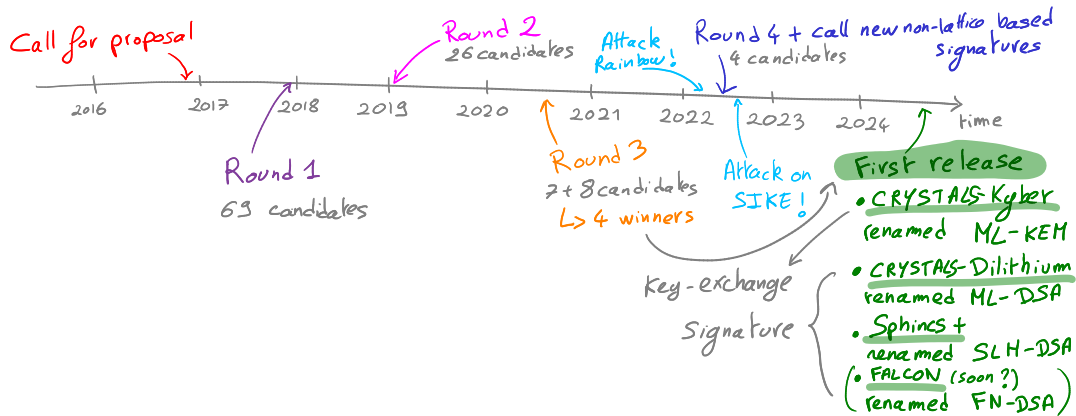
- ✓ • simple
- ✗ • no worst case $\rightarrow$ average case reduction
- ✗ • FHE impossible

④ Multivariate Crypto

- ✗ • many candidates were broken $\Rightarrow$ lost confidence

⑤ + Symmetric crypto (incl. signatures)

NIST : compétition post-quantique internationale



NIST : compétition post-quantique internationale

First release (2024)

Key-exchange (for encryption)

• CRYSTALS Kyber
renamed ML-KEM

Signature

• CRYSTALS Dilithium
renamed ML-DSA

• Sphincs+
renamed SLH-DSA

Hardness
Assumption

In
bytes,
Level 3

Lattice-based

$|pk|$: 1184
 $|sk|$: 2400
 $|cipher|$: 1088
 $|shared\ key|$: 32

Lattice-based

1952
4032
 $|signature|$: 3309

Hash-based

48

96

16224

Less efficient than ML-DSA
⇒ in case ML-DSA is broken

NIST : compétition post-quantique internationale

First release (2024)

Key-exchange (for encryption)

• CRYSTALS Kyber
renamed ML-KEM

Compare with ECDH with Curve 25519
(Not post-quantum!)

Hardness
Assumption

In
bytes,
Level 3

Lattice-based ✓

Pk :	1184	X
Sk :	2400	X
cipher :	1088	X
shared key :	32	X

Elliptic-curves X

32 ✓

32 ✓

64 (2x 32) ✓

32 ✓

NIST : compétition post-quantique internationale

First release (2024)

Key-exchange (for encryption)

• CRYSTALS Kyber
renamed ML-KEM

Compare with ECDH with Curve 25519
(Not post-quantum!)

Hardness
Assumption
In
bytes,
Level 3

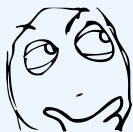
Lattice-based ✓

Pk :	1184	X
Sk :	2400	X
cipher :	1088	X
shared key :	32	X

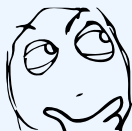
Elliptic-curves X

32	✓
32	✓
64 (2x 32)	✓
32	✓

Post-quantum
is less efficient
(but hopefully
more secure)



Est-ce grave si les systèmes post-quantiques sont moins efficaces ?



Est-ce grave si les systèmes post-quantiques sont moins efficaces ?

⇒ Souvent, pas vraiment car en pratique **chiffrement hybride**

(crypto clé publique seulement pour échanger la clé, puis crypto clé privée car + efficace)

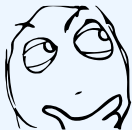
Migration vers le post-quantique : recommandations **officielles**

- USA : 16 janvier 2025 : décret 14144 de Joe Biden = transition avant 2030
- Commission Européenne/NIS :

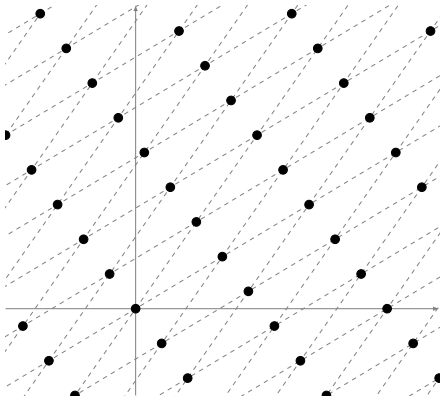
"All Member States should start transitioning to post-quantum cryptography by the end of 2026. At the same time, the protection of critical infrastructures should be transitioned to PQC **as soon as possible**, no later than **by the end of 2030**."

<https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography>

Le déploiement, c'est **maintenant** !



Mais alors, en pratique sur quoi exactement se basent les chiffrements post-quantique ?

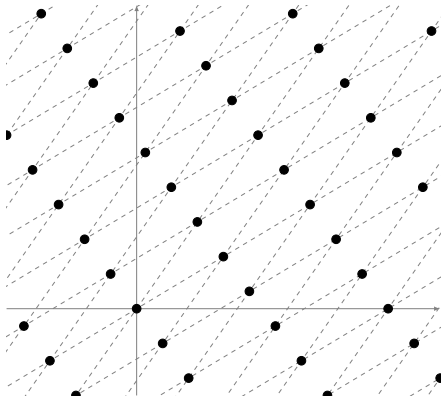


Learning With Errors (LWE)

Étant donné $\left(\mathbf{A}, \mathbf{y} \right)$, dire si $\mathbf{y}$ est

aléatoire ou $\mathbf{y} = \mathbf{A} \mathbf{s} + \mathbf{e}$, avec

$$\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{M \times N}, \quad \mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^N, \quad \mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}_q, \alpha q}^M.$$



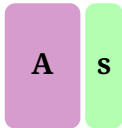
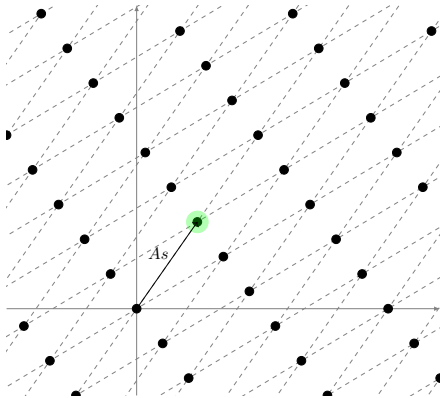
A

Learning With Errors (LWE)

Étant donné $\left(\begin{array}{c} \text{A} \\ \text{y} \end{array} \right)$, dire si y est

aléatoire ou $\text{y} = \text{A} \text{s} + \text{e}$, avec

$$\text{A} \xleftarrow{\$} \mathbb{Z}_q^{M \times N}, \text{ s} \xleftarrow{\$} \mathbb{Z}_q^N, \text{ e} \leftarrow \mathcal{D}_{\mathbb{Z}_q, \alpha q}^M.$$

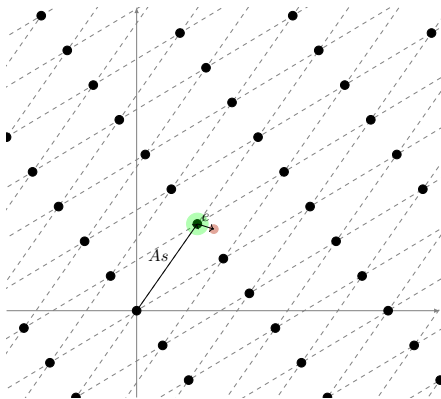


Learning With Errors (LWE)

Étant donné $\left(\begin{array}{c} \text{A} \\ \text{y} \end{array} \right)$, dire si y est

aléatoire ou $\text{y} = \text{A} \text{s} + \text{e}$, avec

$$\text{A} \xleftarrow{\$} \mathbb{Z}_q^{M \times N}, \text{ s} \xleftarrow{\$} \mathbb{Z}_q^N, \text{ e} \leftarrow \mathcal{D}_{\mathbb{Z}_q, \alpha q}^M.$$



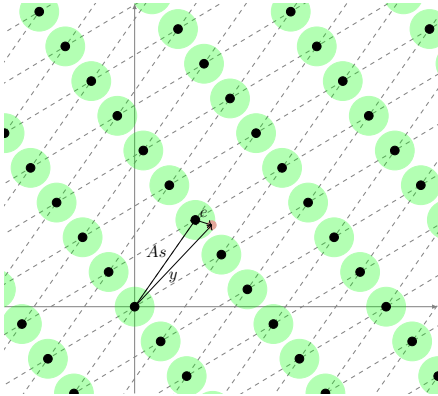
$$\mathbf{A} \mathbf{s} + \mathbf{e}$$

Learning With Errors (LWE)

Étant donné $\left(\mathbf{A}, \mathbf{y} \right)$, dire si $\mathbf{y}$ est

aléatoire ou $\mathbf{y} = \mathbf{A} \mathbf{s} + \mathbf{e}$, avec

$$\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{M \times N}, \mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^N, \mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}_q, \alpha q}^M.$$



$$\mathbf{A} \mathbf{s} + \mathbf{e}$$

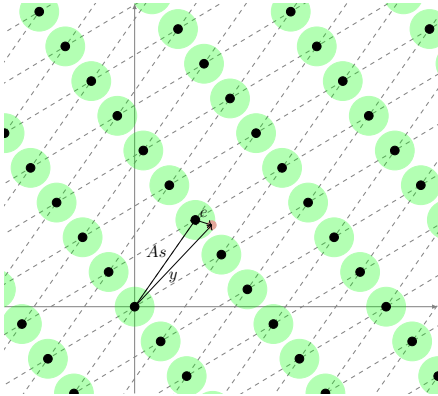
Learning With Errors (LWE)

Étant donné $(\mathbf{A}, \mathbf{y})$, dire si $\mathbf{y}$ est

aléatoire ou $\mathbf{y} = \mathbf{A} \mathbf{s} + \mathbf{e}$, avec

$$\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{M \times N}, \mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^N, \mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}_q, \alpha q}^M.$$

LWE



$$\mathbf{A} \mathbf{s} + \mathbf{e}$$

Learning With Errors (LWE)

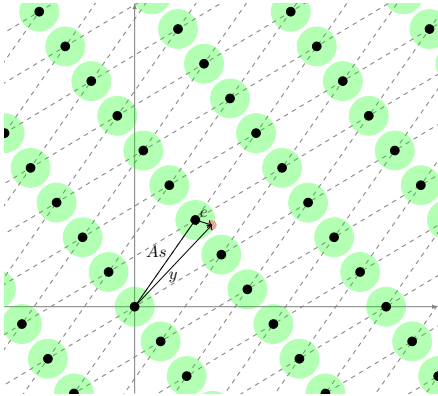
Étant donné $\left(\mathbf{A}, \mathbf{y} \right)$, dire si $\mathbf{y}$ est

aléatoire ou $\mathbf{y} = \mathbf{A} \mathbf{s} + \mathbf{e}$, avec

$$\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{M \times N}, \mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^N, \mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}_q, \alpha q}^M.$$

Clé publique

LWE



$$\mathbf{A} \mathbf{s} + \mathbf{e}$$

Learning With Errors (LWE)

Étant donné $(\mathbf{A}, \mathbf{y})$, dire si $\mathbf{y}$ est

aléatoire ou $\mathbf{y} = \mathbf{A} \mathbf{s} + \mathbf{e}$, avec

$$\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{M \times N}, \mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^N, \mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}_q, \alpha q}^M.$$

Clé publique

secret

Difficulté

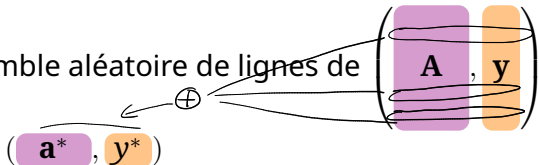
⇒ LWE est **dur** même pour des ordinateurs quantiques quand $\mathbf{e}$ est généré suivant une Gaussienne assez large:

2 versions:

- ratio de bruit polynomial (plus standard)
- ratio de bruit superpolynomial (plus petit ratio e/q = moins sécurisé)

LWE : chiffrement

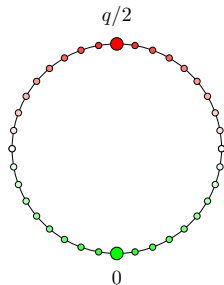
Pour chiffrer $m \in \{0, 1\}$:

- 1 Sommer un sous-ensemble aléatoire de lignes de $\begin{pmatrix} \mathbf{A} & \mathbf{y} \end{pmatrix}$ ("nouvelle ligne") pour obtenir un $\begin{pmatrix} \mathbf{a}^* & \mathbf{y}^* \end{pmatrix}$
- 

LWE : chiffrement

Pour chiffrer $m \in \{0, 1\}$:

- 1 Sommer un sous-ensemble aléatoire de lignes de $\begin{pmatrix} \mathbf{A} & \mathbf{y} \end{pmatrix}$ ("nouvelle ligne") pour obtenir un $(\mathbf{a}^*, \mathbf{y}^*)$
- 2 Renvoyer $(\mathbf{a}^*, \mathbf{y}^* + m \frac{q}{2})$

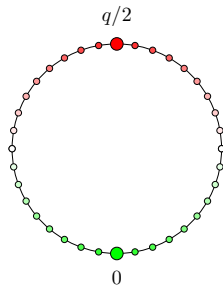


LWE : chiffrement

Pour chiffrer $m \in \{0, 1\}$:

- 1 Sommer un sous-ensemble aléatoire de lignes de $\begin{pmatrix} \mathbf{A} & \mathbf{y} \end{pmatrix}$ ("nouvelle ligne") pour obtenir un $(\mathbf{a}^*, \mathbf{y}^*)$
- 2 Renvoyer $(\mathbf{a}^*, \mathbf{y}^* + m \frac{q}{2})$

Sécurité : $y^* \approx \text{aléa}$
 $\rightarrow \text{et } \text{aléa} + \text{cle} = \text{aléa}$

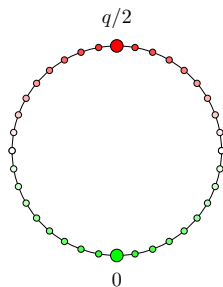


LWE : chiffrement

Pour chiffrer $m \in \{0, 1\}$:

- 1 Sommer un sous-ensemble aléatoire de lignes de $\begin{pmatrix} \mathbf{A} & \mathbf{y} \end{pmatrix}$ ("nouvelle ligne") pour obtenir un $(\mathbf{a}^*, \mathbf{y}^*)$
- 2 Renvoyer $(\mathbf{a}^*, \mathbf{y}^* + m \frac{\mathbf{q}}{2})$

Sécurité : $y^* \approx \text{aléa}$
 $\rightarrow \text{et } \text{aléa} + cke = \text{aléa}$
 $\rightarrow \text{info sur } m \text{ perdue !}$



LWE : chiffrement

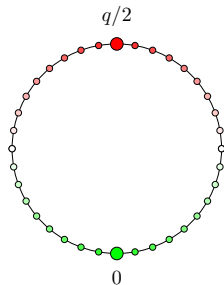
Pour chiffrer $m \in \{0, 1\}$:

- 1 Sommer un sous-ensemble aléatoire de lignes de $\begin{pmatrix} \mathbf{A} & \mathbf{y} \end{pmatrix}$ ("nouvelle ligne") pour obtenir un $(\mathbf{a}^*, \mathbf{y}^*)$

- 2 Renvoyer $(\mathbf{a}^*, \mathbf{y}^* + m \frac{q}{2})$

Dechiffres :

$$= \mathbf{a}^* s + \mathbf{e}^* + m \frac{q}{2}$$



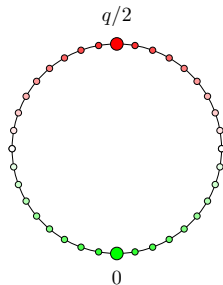
LWE : chiffrement

Pour chiffrer $m \in \{0, 1\}$:

- 1 Sommer un sous-ensemble aléatoire de lignes de $\begin{pmatrix} \mathbf{A} & \mathbf{y} \end{pmatrix}$ ("nouvelle ligne") pour obtenir un $(\mathbf{a}^*, \mathbf{y}^*)$
- 2 Renvoyer $(\mathbf{a}^*, \mathbf{y}^* + m \frac{q}{2})$

Déchiffrer :

$$= \underbrace{a^*}_{\text{connu}} s + \underbrace{e^*}_{\text{connu (clé privée)}} + m \frac{q}{2}$$



LWE : chiffrement

Pour chiffrer $m \in \{0, 1\}$:

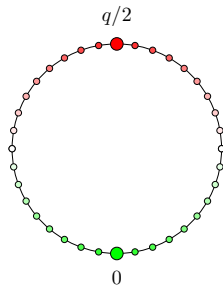
- 1 Sommer un sous-ensemble aléatoire de lignes de $\begin{pmatrix} \mathbf{A} & \mathbf{y} \end{pmatrix}$ ("nouvelle ligne") pour obtenir un $(\mathbf{a}^*, \mathbf{y}^*)$

- 2 Renvoyer $(\mathbf{a}^*, \mathbf{y}^* + m \frac{q}{2})$

Déchiffrer :

$$= \underbrace{\mathbf{a}^*}_{\text{connu}} s + \underbrace{e^*}_{\text{connu (clé privée)}} + m \frac{q}{2}$$

$\rightarrow$ simple d'avoir $e^* + m \frac{q}{2}$



LWE : chiffrement

Pour chiffrer $m \in \{0, 1\}$:

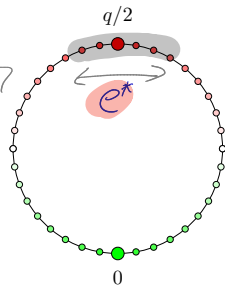
- 1 Sommer un sous-ensemble aléatoire de lignes de $\begin{pmatrix} \mathbf{A} & \mathbf{y} \end{pmatrix}$ ("nouvelle ligne") pour obtenir un $(\mathbf{a}^*, \mathbf{y}^*)$

- 2 Renvoyer $(\mathbf{a}^*, \mathbf{y}^* + m \frac{q}{2})$

Déchiffrer :

$$= \underbrace{\mathbf{a}^*}_{\text{connu}} s + \underbrace{e^*}_{\text{connu (clé privée)}} + m \frac{q}{2}$$

→ simple d'avoir $e^* + m \frac{q}{2}$
petit bruit



LWE : chiffrement

Pour chiffrer $m \in \{0, 1\}$:

- 1 Sommer un sous-ensemble aléatoire de lignes de $\begin{pmatrix} \mathbf{A} & \mathbf{y} \end{pmatrix}$ ("nouvelle ligne") pour obtenir un $(\mathbf{a}^*, \mathbf{y}^*)$

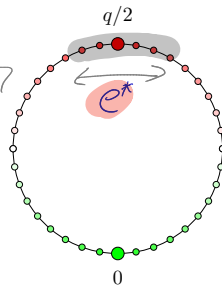
- 2 Renvoyer $(\mathbf{a}^*, \mathbf{y}^* + m \frac{q}{2})$

Déchiffrer :

$$= \underbrace{\mathbf{a}^*}_{\text{connu}} s + \underbrace{e^*}_{\text{connu (clé privée)}} + m \frac{q}{2}$$

→ simple d'avoir $e^* + m \frac{q}{2}$

petit bruit (pointing to e^*) *énorme bruit* (pointing to $m \frac{q}{2}$)



LWE : chiffrement

Pour chiffrer $m \in \{0, 1\}$:

- 1 Sommer un sous-ensemble aléatoire de lignes de $\begin{pmatrix} \mathbf{A} & \mathbf{y} \end{pmatrix}$ ("nouvelle ligne") pour obtenir un $(\mathbf{a}^*, \mathbf{y}^*)$

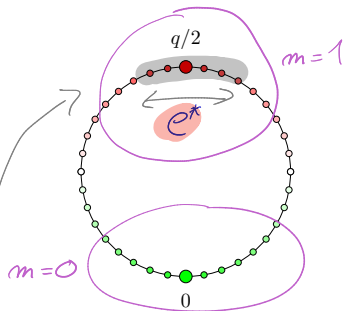
- 2 Renvoyer $(\mathbf{a}^*, \mathbf{y}^* + m \frac{q}{2})$

Déchiffrer :

$$= \underbrace{\mathbf{a}^*}_{\text{connu}} s + \underbrace{e^*}_{\text{connu (clé privée)}} + m \frac{q}{2}$$

→ simple d'avoir $e^* + m \frac{q}{2}$
petit bruit

énorme bruit



Questions post-quantique

TLS a introduit X25519MLKEM768 qui combine courbes elliptiques (ECDH) et ML-KEM. Est-ce une bonne idée ? **A** Oui **B** Non.

LWE peut-être utilisé pour : **A** Chiffrer **A** Signer **C** Les deux

Dans le problème LWE, le but est distinguer quelles distributions ($x \xleftarrow{\$} = x$ est tiré uniformément au hasard):

- A** $(A \xleftarrow{\$}, y \xleftarrow{\$})$ vs $(A \xleftarrow{\$}, A(s \xleftarrow{\$}) + (e \xleftarrow{\$}))$
B $(A \xleftarrow{\$}, y \xleftarrow{\$})$ vs $(A \xleftarrow{\$}, A(s \xleftarrow{\$}) + (e \leftarrow \mathcal{D}))$
C $(y \xleftarrow{\$})$ vs $(A(s \xleftarrow{\$}) + (e \xleftarrow{\$}))$
D $(y \xleftarrow{\$})$ vs $(A(s \xleftarrow{\$}) + (e \leftarrow \mathcal{D}))$

Soient $A = \begin{pmatrix} 3 & 3 \\ 5 & 1 \\ 8 & 5 \end{pmatrix}$, $y = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ (on travaille dans $\mathbb{Z}_{10}$). Chiffrer le message 1, en sélectionnant la première et dernière ligne de A .

- A** $((1 \ 8), (4))$ **B** $((1 \ 8), (9))$ **C** $((6 \ 9), (6))$ **D** $((6 \ 9), (1))$

Questions post-quantique

TLS a introduit X25519MLKEM768 qui combine courbes elliptiques (ECDH) et ML-KEM. Est-ce une bonne idée ? **A** Oui ✓ **B** Non.

LWE peut-être utilisé pour : **A** Chiffrer **A** Signer **C** Les deux

Dans le problème LWE, le but est distinguer quelles distributions ($x \xleftarrow{\$} = x$ est tiré uniformément au hasard):

- A** $(A \xleftarrow{\$}, y \xleftarrow{\$})$ vs $(A \xleftarrow{\$}, A(s \xleftarrow{\$}) + (e \xleftarrow{\$}))$
B $(A \xleftarrow{\$}, y \xleftarrow{\$})$ vs $(A \xleftarrow{\$}, A(s \xleftarrow{\$}) + (e \leftarrow \mathcal{D}))$
C $(y \xleftarrow{\$})$ vs $(A(s \xleftarrow{\$}) + (e \xleftarrow{\$}))$
D $(y \xleftarrow{\$})$ vs $(A(s \xleftarrow{\$}) + (e \leftarrow \mathcal{D}))$

Soient $A = \begin{pmatrix} 3 & 3 \\ 5 & 1 \\ 8 & 5 \end{pmatrix}$, $y = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ (on travaille dans $\mathbb{Z}_{10}$). Chiffrer le message 1, en sélectionnant la première et dernière ligne de A .

- A** $((1 \ 8), (4))$ **B** $((1 \ 8), (9))$ **C** $((6 \ 9), (6))$ **D** $((6 \ 9), (1))$

Questions post-quantique

TLS a introduit X25519MLKEM768 qui combine courbes elliptiques (ECDH) et ML-KEM. Est-ce une bonne idée ? **A** Oui ✓ **B** Non.

LWE peut-être utilisé pour : **A** Chiffrer **A** Signer **C** Les deux ✓

Dans le problème LWE, le but est distinguer quelles distributions ($x \xleftarrow{\$} = x$ est tiré uniformément au hasard):

- A** $(A \xleftarrow{\$}, y \xleftarrow{\$})$ vs $(A \xleftarrow{\$}, A(s \xleftarrow{\$}) + (e \xleftarrow{\$}))$
- B** $(A \xleftarrow{\$}, y \xleftarrow{\$})$ vs $(A \xleftarrow{\$}, A(s \xleftarrow{\$}) + (e \leftarrow \mathcal{D}))$
- C** $(y \xleftarrow{\$})$ vs $(A(s \xleftarrow{\$}) + (e \xleftarrow{\$}))$
- D** $(y \xleftarrow{\$})$ vs $(A(s \xleftarrow{\$}) + (e \leftarrow \mathcal{D}))$

Soient $A = \begin{pmatrix} 3 & 3 \\ 5 & 1 \\ 8 & 5 \end{pmatrix}$, $y = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ (on travaille dans $\mathbb{Z}_{10}$). Chiffrer le message 1, en sélectionnant la première et dernière ligne de A .

- A** $((1 \ 8), (4))$ **B** $((1 \ 8), (9))$ **C** $((6 \ 9), (6))$ **D** $((6 \ 9), (1))$

Questions post-quantique

TLS a introduit X25519MLKEM768 qui combine courbes elliptiques (ECDH) et ML-KEM. Est-ce une bonne idée ? **A** Oui ✓ **B** Non.

LWE peut-être utilisé pour : **A** Chiffrer **A** Signer **C** Les deux ✓

Dans le problème LWE, le but est distinguer quelles distributions ($x \xleftarrow{\$} = x$ est tiré uniformément au hasard):

- A** $(A \xleftarrow{\$}, y \xleftarrow{\$})$ vs $(A \xleftarrow{\$}, A(s \xleftarrow{\$}) + (e \xleftarrow{\$}))$
- B** $(A \xleftarrow{\$}, y \xleftarrow{\$})$ vs $(A \xleftarrow{\$}, A(s \xleftarrow{\$}) + (e \leftarrow \mathcal{D}))$ ✓
- C** $(y \xleftarrow{\$})$ vs $(A(s \xleftarrow{\$}) + (e \xleftarrow{\$}))$
- D** $(y \xleftarrow{\$})$ vs $(A(s \xleftarrow{\$}) + (e \leftarrow \mathcal{D}))$

Soient $A = \begin{pmatrix} 3 & 3 \\ 5 & 1 \\ 8 & 5 \end{pmatrix}$, $y = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ (on travaille dans $\mathbb{Z}_{10}$). Chiffrer le message 1, en sélectionnant la première et dernière ligne de A .

- A** $((1 \ 8), (4))$ **B** $((1 \ 8), (9))$ **C** $((6 \ 9), (6))$ **D** $((6 \ 9), (1))$

Questions post-quantique

TLS a introduit X25519MLKEM768 qui combine courbes elliptiques (ECDH) et ML-KEM. Est-ce une bonne idée ? **A** Oui ✓ **B** Non.

LWE peut-être utilisé pour : **A** Chiffrer **A** Signer **C** Les deux ✓

Dans le problème LWE, le but est distinguer quelles distributions ($x \xleftarrow{\$} = x$ est tiré uniformément au hasard):

- A** $(A \xleftarrow{\$}, y \xleftarrow{\$})$ vs $(A \xleftarrow{\$}, A(s \xleftarrow{\$}) + (e \xleftarrow{\$}))$
- B** $(A \xleftarrow{\$}, y \xleftarrow{\$})$ vs $(A \xleftarrow{\$}, A(s \xleftarrow{\$}) + (e \leftarrow \mathcal{D}))$ ✓
- C** $(y \xleftarrow{\$})$ vs $(A(s \xleftarrow{\$}) + (e \xleftarrow{\$}))$
- D** $(y \xleftarrow{\$})$ vs $(A(s \xleftarrow{\$}) + (e \leftarrow \mathcal{D}))$

Soient $A = \begin{pmatrix} 3 & 3 \\ 5 & 1 \\ 8 & 5 \end{pmatrix}$, $y = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ (on travaille dans $\mathbb{Z}_{10}$). Chiffrer le message 1, en sélectionnant la première et dernière ligne de A .

- A** $((1 \ 8), (4))$ **B** $((1 \ 8), (9))$ ✓ **C** $((6 \ 9), (6))$ **D** $((6 \ 9), (1))$

Échange quantique de clés

Cryptographie quantique

Cryptographie quantique = crypto basée sur les **lois de la physique**
(e.g. théorème non clonage)

Cryptographie quantique

Cryptographie quantique = crypto basée sur les **lois de la physique**
(e.g. théorème non clonage)

Objectifs : cryptographie impossible classiquement

- Sécurité **inconditionnelle**/everlasting security
(adversaire non borné calculatoirement/après le protocole)

Cryptographie quantique

Cryptographie quantique = crypto basée sur les **lois de la physique**
(e.g. théorème non clonage)

Objectifs : cryptographie impossible classiquement

- Sécurité **inconditionnelle**/everlasting security
(adversaire non borné calculatoirement/après le protocole)
- Utiliser des **hypothèses de sécurité moins fortes**
(MiniQCrypt, fonctions de hachage, Pseudo-Random States...)

Cryptographie quantique

Cryptographie quantique = crypto basée sur les **lois de la physique**
(e.g. théorème non clonage)

Objectifs : cryptographie impossible classiquement

- Sécurité **inconditionnelle**/everlasting security
(adversaire non borné calculatoirement/après le protocole)
- Utiliser des **hypothèses de sécurité moins fortes**
(MiniQCrypt, fonctions de hachage, Pseudo-Random States...)
- **Primitives impossibles** classiquement
(vérification de position, monnaie quantique unclonable...)

Cryptographie quantique

Cryptographie quantique = crypto basée sur les **lois de la physique**
(e.g. théorème non clonage)

Objectifs : cryptographie impossible classiquement

- Sécurité **inconditionnelle**/everlasting security
(adversaire non borné calculatoirement/après le protocole)
- Utiliser des **hypothèses de sécurité moins fortes**
(MiniQCrypt, fonctions de hachage, Pseudo-Random States...)
- **Primitives impossibles** classiquement
(vérification de position, monnaie quantique unclonable...)
- **Certifier le caractère quantique** d'un ordinateur

Cryptographie quantique

Cryptographie quantique = crypto basée sur les **lois de la physique**
(e.g. théorème non clonage)

Objectifs : cryptographie impossible classiquement

- Sécurité **inconditionnelle**/everlasting security
(adversaire non borné calculatoirement/après le protocole)
- Utiliser des **hypothèses de sécurité moins fortes**
(MiniQCrypt, fonctions de hachage, Pseudo-Random States...)
- **Primitives impossibles** classiquement
(vérification de position, monnaie quantique unclonable...)
- **Certifier le caractère quantique** d'un ordinateur
- Équivalents quantiques de protocoles classiques
(**calcul délégué** sécurisé/multipartite, vérification, ...)

Cryptographie quantique

Cryptographie quantique = crypto basée sur les **lois de la physique**
(e.g. théorème non clonage)

Objectifs : cryptographie impossible classiquement

- Sécurité **inconditionnelle**/everlasting security
(adversaire non borné calculatoirement/après le protocole)
- Utiliser des **hypothèses de sécurité moins fortes**
(MiniQCrypt, fonctions de hachage, Pseudo-Random States...)
- **Primitives impossibles** classiquement
(vérification de position, monnaie quantique unclonable...)
- **Certifier le caractère quantique** d'un ordinateur
- Équivalents quantiques de protocoles classiques
(**calcul délégué** sécurisé/multipartite, vérification, ...)
- **Preuves** de sécurité contre adversaires quantiques

Cryptographie quantique

Cryptographie quantique = crypto basée sur les **lois de la physique**
(e.g. théorème non clonage)

Objectifs : cryptographie impossible classiquement

- Sécurité **inconditionnelle**/everlasting security
(adversaire non borné calculatoirement/après le protocole)
- Utiliser des **hypothèses de sécurité moins fortes**
(MiniQCrypt, fonctions de hachage, Pseudo-Random States...)
- **Primitives impossibles** classiquement
(vérification de position, monnaie quantique unclonable...)
- **Certifier le caractère quantique** d'un ordinateur
- Équivalents quantiques de protocoles classiques
(**calcul délégué** sécurisé/multipartite, vérification, ...)
- **Preuves** de sécurité contre adversaires quantiques
- ...

Cryptographie quantique

Cryptographie quantique = crypto basée sur les **lois de la physique**
(e.g. théorème non clonage)

Objectifs : cryptographie impossible classiquement

Notre focus 1^{ère} partie

- **Sécurité inconditionnelle**/everlasting security
(adversaire non borné calculatoirement/après le protocole)
- Utiliser des **hypothèses de sécurité moins fortes**
(MiniQCrypt, fonctions de hachage, Pseudo-Random States...)
- **Primitives impossibles** classiquement
(vérification de position, monnaie quantique unclonable...)
- **Certifier le caractère quantique** d'un ordinateur
- Équivalents quantiques de protocoles classiques
(**calcul délégué** sécurisé/multipartite, vérification, ...)
- **Preuves** de sécurité contre adversaires quantiques
- ...

Cryptographie quantique

Cryptographie quantique = crypto basée sur les **lois de la physique**
(e.g. théorème non clonage)

Objectifs : cryptographie impossible classiquement

Notre focus 1^{ère} partie

- **Sécurité inconditionnelle**/everlasting security
(adversaire non borné calculatoirement/après le protocole)
- Utiliser des **hypothèses de sécurité moins fortes**
(MiniQCrypt, fonctions de hachage, Pseudo-Random States...)
- **Primitives impossibles** classiquement
(vérification de position, monnaie quantique unclonable...)
- **Certifier le caractère quantique** d'un ordinateur
- Équivalents quantiques de ~~protocoles classiques~~
(**calcul délégué sécurisé**/multipartite, vérification, ...)
- **Preuves** de sécurité contre adversaires quantiques
- ...

Focus de la 2^e partie

Cryptographie quantique

Cryptographie quantique = crypto basée sur les **lois de la physique**
(e.g. théorème non clonage)

Objectifs : cryptographie impossible classiquement

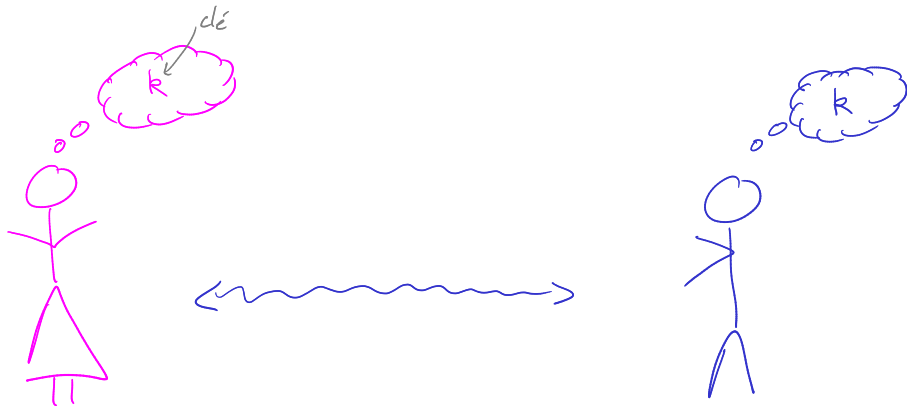
- **Sécurité inconditionnelle**/everlasting security
(adversaire non borné calculatoirement/après le protocole)
- Utiliser des **hypothèses de sécurité moins fortes**
(MiniQCrypt, fonctions de hachage, Pseudo-Random States...)
- **Primitives impossibles** classiquement
(vérification de position, monnaie quantique unclonable...)
- **Certifier le caractère quantique** d'un ordinateur
- Équivalents quantiques de ~~protocoles classiques~~
(calcul délégué sécurisé/multipartite, vérification, ...)
- **Preuves** de sécurité contre adversaires quantiques
- ...

Notre focus 1^{ère} partie

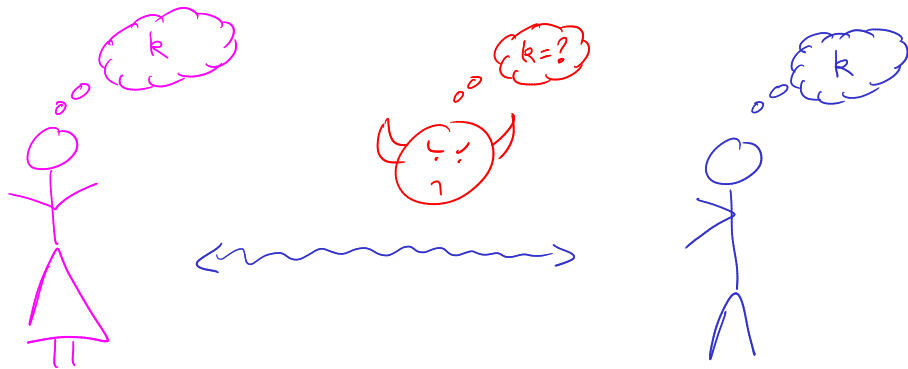
En lien avec

Focus de la 2^e partie

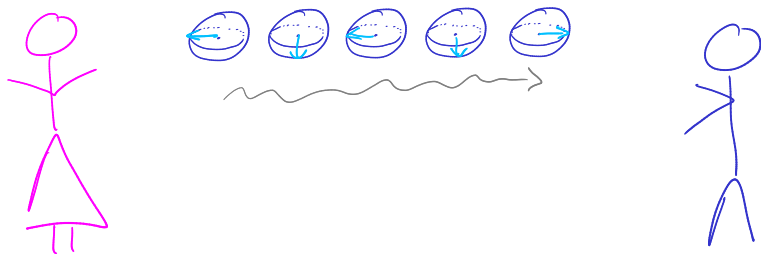
Exemple d'application : distribution quantique de clés (QKD)



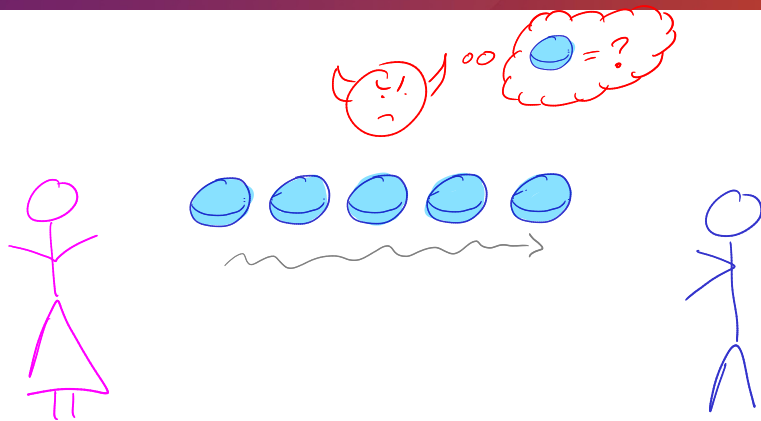
Exemple d'application : distribution quantique de clés (QKD)



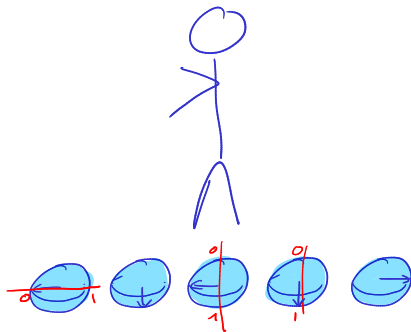
Exemple d'application : distribution quantique de clés (QKD)



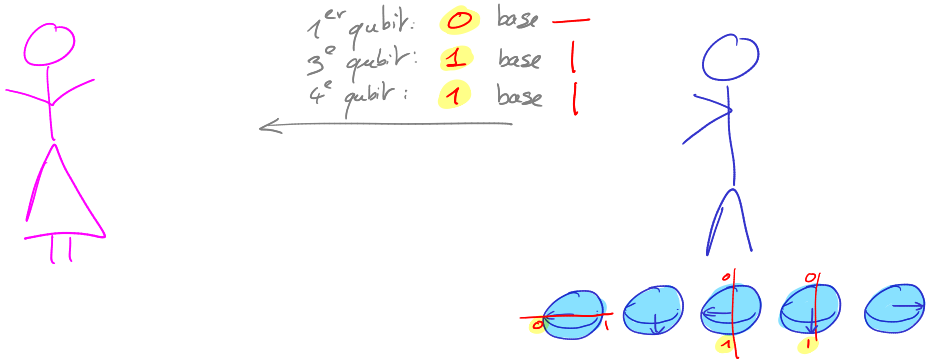
Exemple d'application : distribution quantique de clés (QKD)



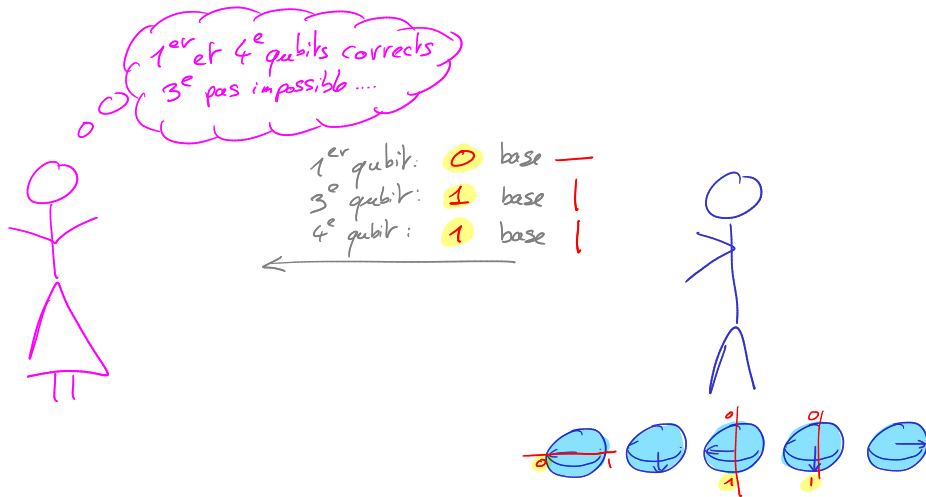
Exemple d'application : distribution quantique de clés (QKD)



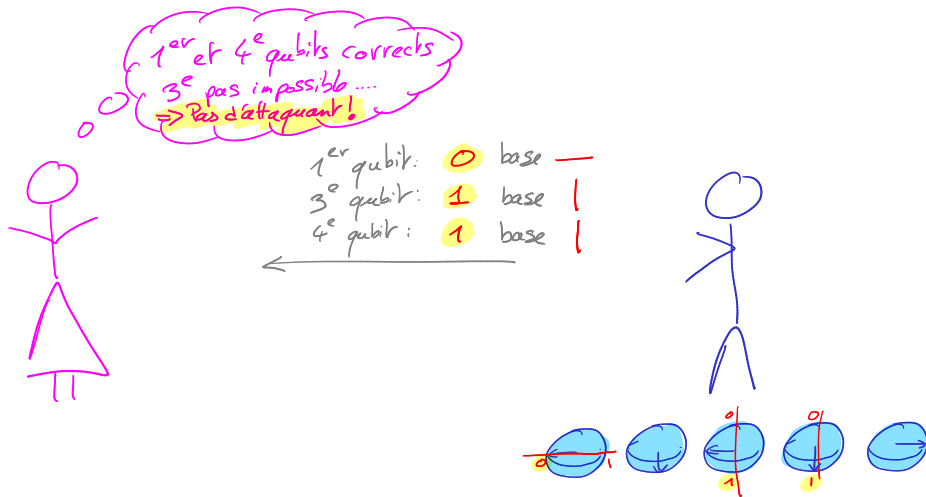
Exemple d'application : distribution quantique de clés (QKD)



Exemple d'application : distribution quantique de clés (QKD)



Exemple d'application : distribution quantique de clés (QKD)

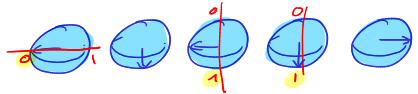


Exemple d'application : distribution quantique de clés (QKD)

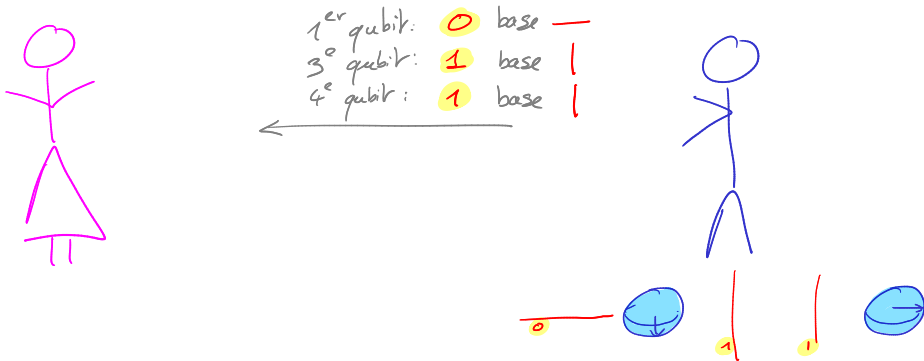


1^{er} qubit: 0 base —
3^e qubit: 1 base |
4^e qubit: 1 base |

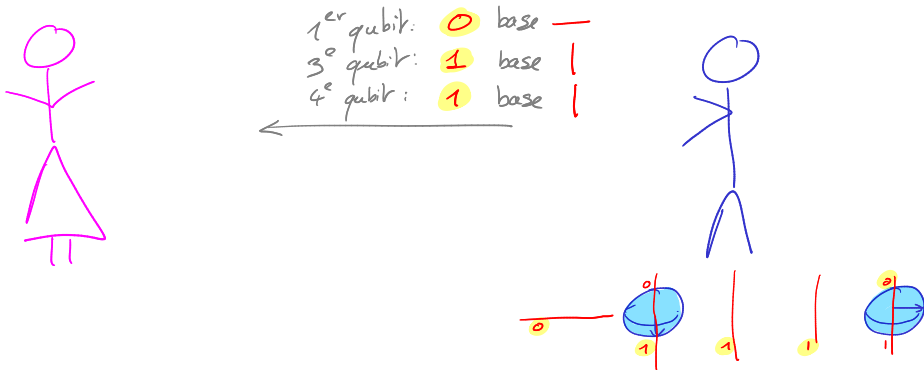
←



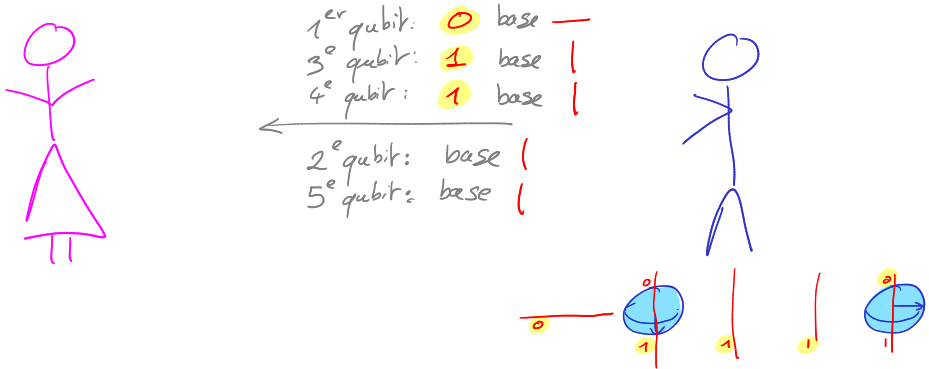
Exemple d'application : distribution quantique de clés (QKD)



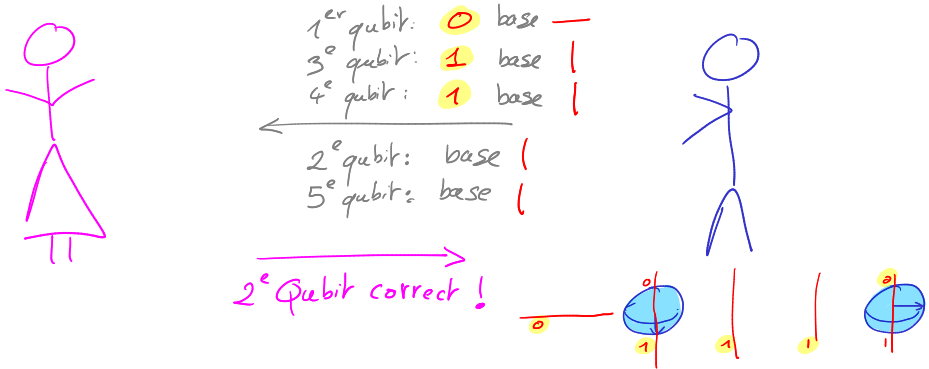
Exemple d'application : distribution quantique de clés (QKD)



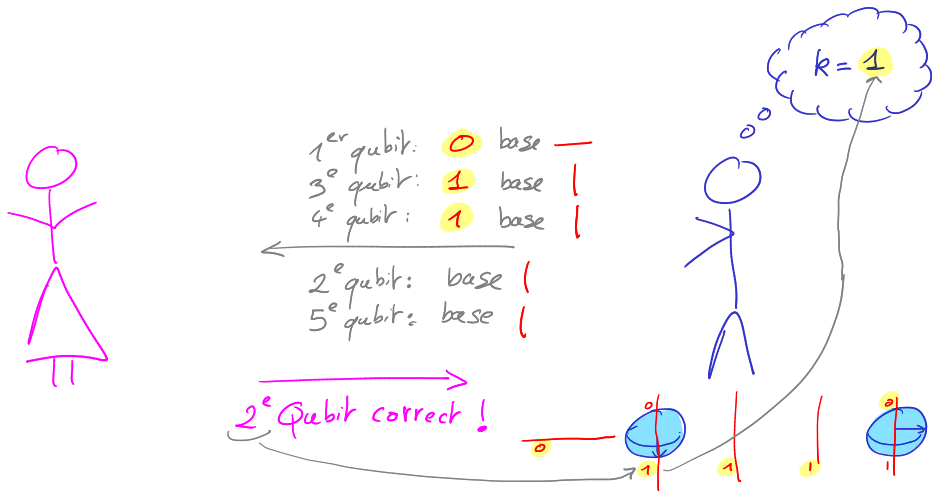
Exemple d'application : distribution quantique de clés (QKD)



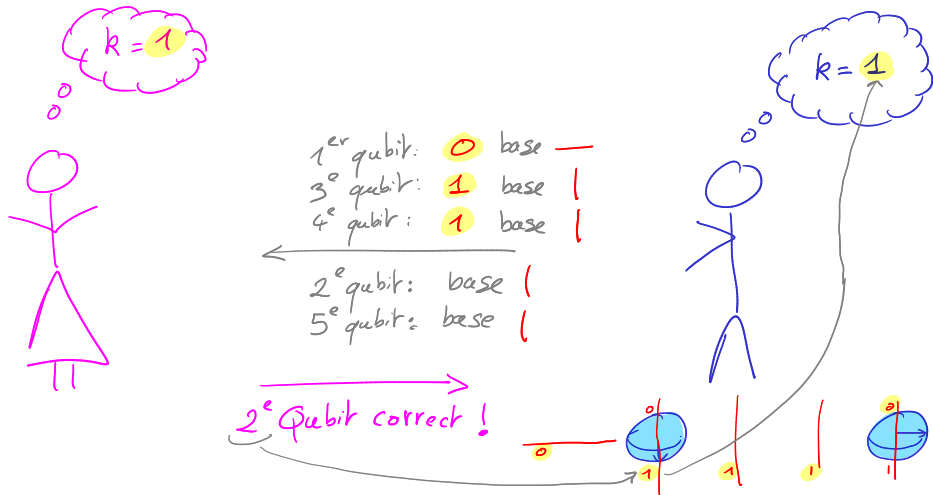
Exemple d'application : distribution quantique de clés (QKD)



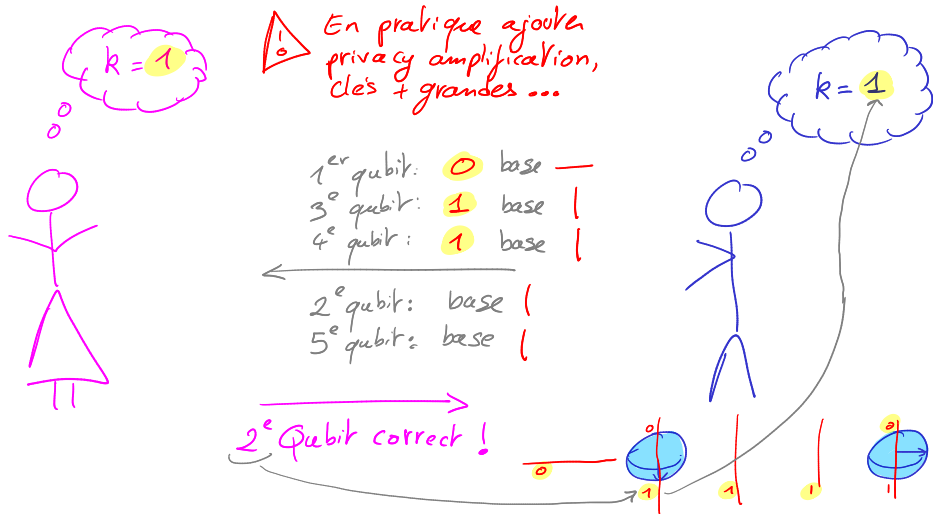
Exemple d'application : distribution quantique de clés (QKD)



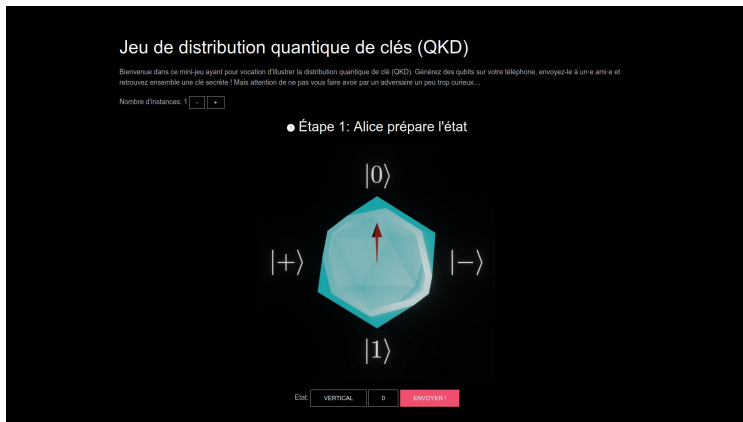
Exemple d'application : distribution quantique de clés (QKD)



Exemple d'application : distribution quantique de clés (QKD)



QKD : essayez par vous même !



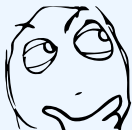
<https://leo-colisson.github.io/qkd-game/>

Limitations QKD

- QKD nécessite un canal **authentifié** (post-quantique)

Limitations QKD

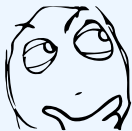
- QKD nécessite un canal **authentifié** (post-quantique)



Mais alors à quoi bon utiliser le quantique si on a besoin de post-quantique ?

Limitations QKD

- QKD nécessite un canal **authentifié** (post-quantique)

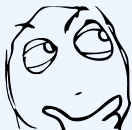


Mais alors à quoi bon utiliser le quantique si on a besoin de post-quantique ?

⇒ nécessite signature post-quantique **seulement durant le protocole**

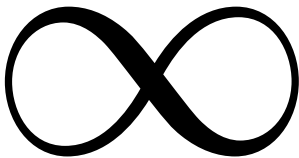
Limitations QKD

- QKD nécessite un canal **authentifié** (post-quantique)



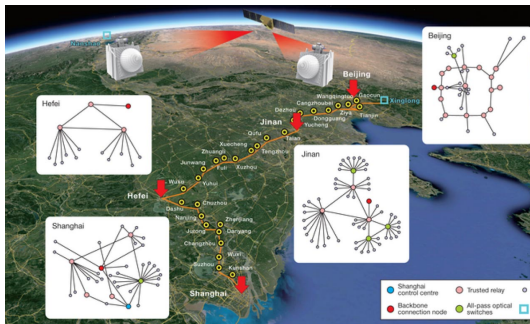
Mais alors à quoi bon utiliser le quantique si on a besoin de post-quantique ?

⇒ nécessite signature post-quantique **seulement durant le protocole**
⇒ même si signature cassée + tard = impossible de déchiffrer y compris avec une **puissance de calcul infinie** ! (**everlasting** security)



Limitations QKD

- Il faut un **internet quantique** (envoyer des photons uniques)
 - ⇒ via fibre faisable sur $\approx 100\text{km}$ + répéteur
(de confiance ou nécessite mémoire quantique = dur expérimentalement)
 - ⇒ satellites = bien plus efficace



Limitations QKD

- Attention également aux attaques par canaux auxiliaires (**side-channel attacks**)



Limitations QKD

- Attention également aux attaques par canaux auxiliaires (**side-channel attacks**)
⇒ protocoles **device independent** pour limiter ces attaques
+ combiner avec post-quantique



Clavis XG

High key transmission rate or extended range interconnection



- ④ Long range (90 to 150 km)
- ④ Standard key rate: typical 14'000 AES-256 Keys per hour @ 24 dB
- ④ Rackspace – Standard 19" 1U

[VIEW PRODUCT PAGE](#)



Quand pourra-t'on utiliser QKD ?

QKD en pratique

Clavis XG

High key transmission rate or extended range interconnection



- ① Long range (90 to 150 km)
- ① Standard key rate: typical 14'000 AES-256 Keys per hour @ 24 dB
- ① Rackspace – Standard 19" 1U

[VIEW PRODUCT PAGE](#)



Quand pourra-t'on utiliser QKD ?

⇒ **Maintenant, déjà en vente !**

QKD en pratique

Clavis XG
High key transmission rate or extended range interconnection



⌚ Long range (90 to 150 km)
⌚ Standard key rate: typical 14'000 AES-256 Keys per hour @ 24 dB
⌚ Rackspace – Standard 19" 1U

[VIEW PRODUCT PAGE](#)



Quand pourra-t'on utiliser QKD ?

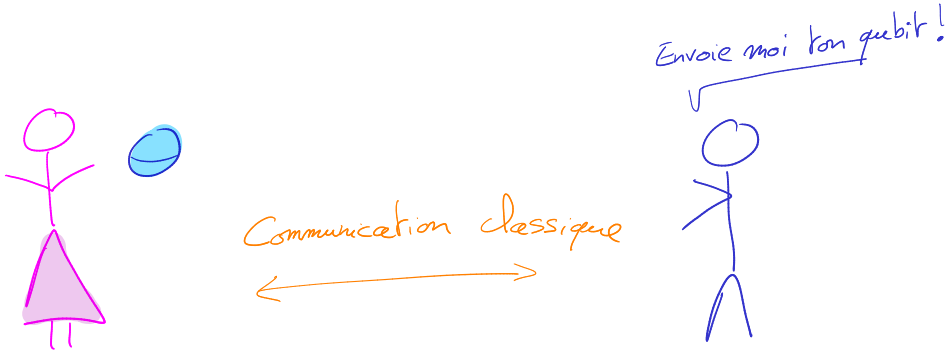
⇒ **Maintenant, déjà en vente !**

Attention : pas besoin d'un ordinateur quantique complet, mais :

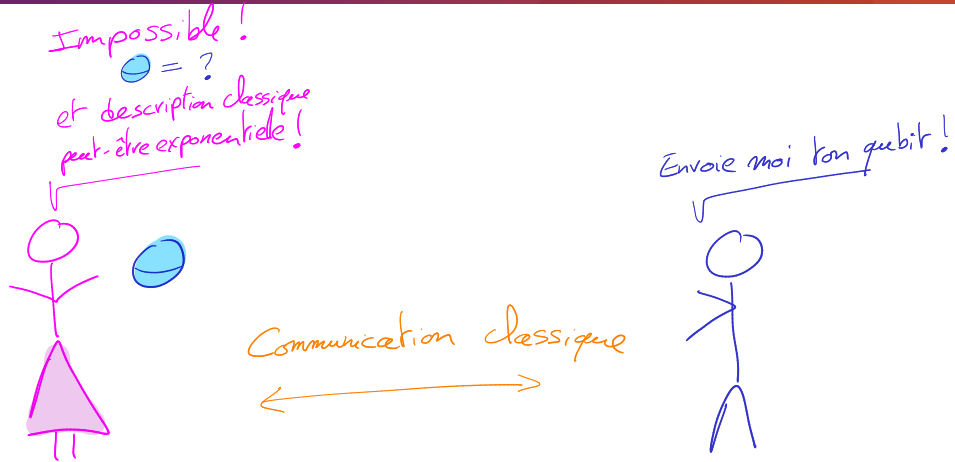
- reste difficile à utiliser sur de longues distances
- potentiellement sensible aux attaques canaux auxiliaires
- faible taux de clé $\approx 500\text{KB/h}$ ⇒ on utilise en pratique AES avec ces clés

Téléportation quantique

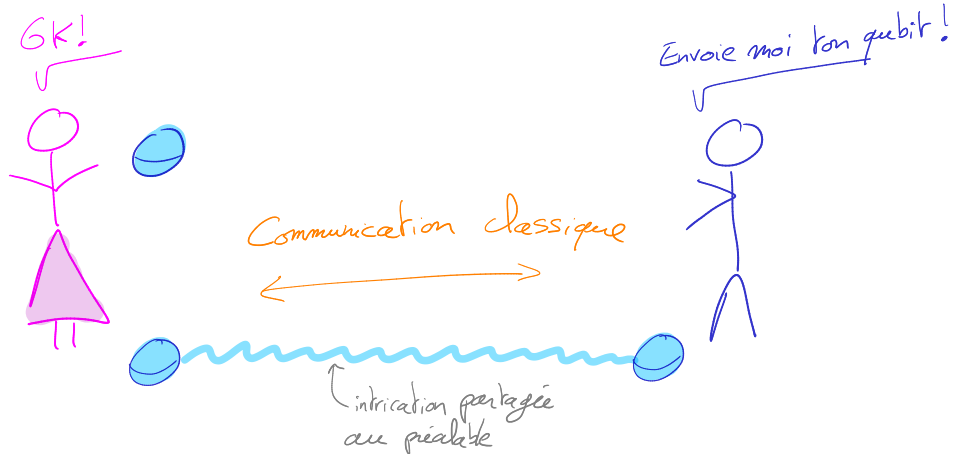
Téléportation quantique



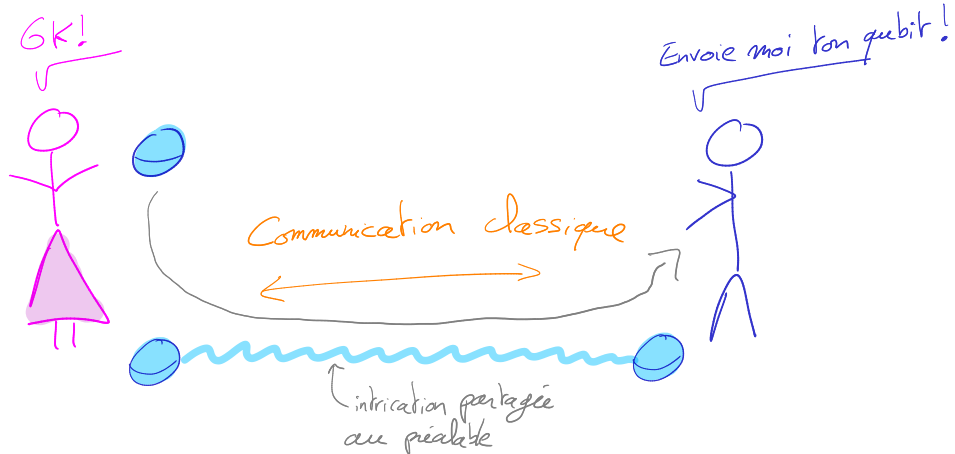
Téléportation quantique



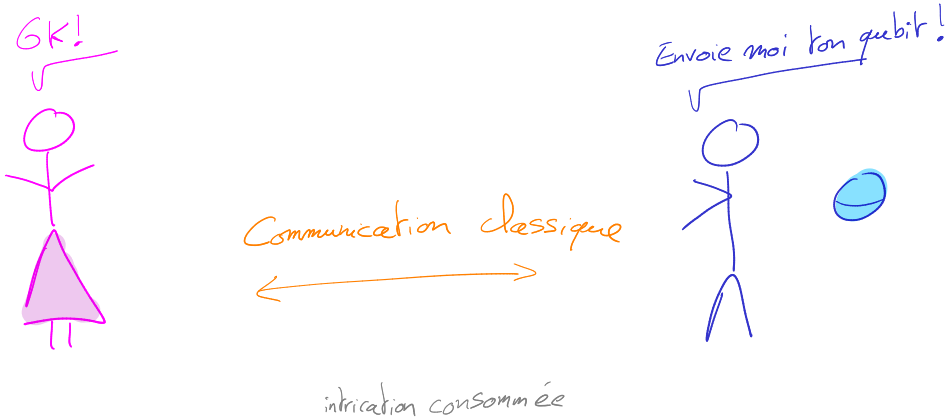
Téléportation quantique



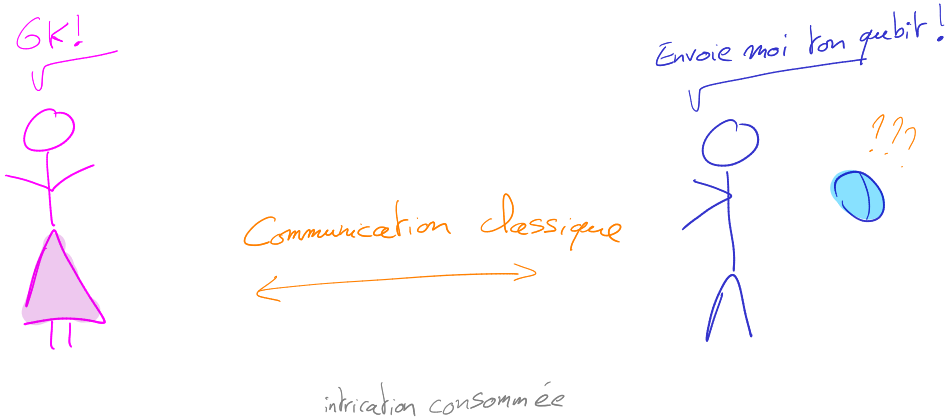
Téléportation quantique



Téléportation quantique



Téléportation quantique



Téléportation quantique



Communication classique
→
"Applique rotation $\frac{\pi}{2}$ "

intrication consommée



Téléportation quantique



Communication classique
→
"Applique rotation $\frac{\pi}{2}$ "

intrication consommée



Téléportation quantique

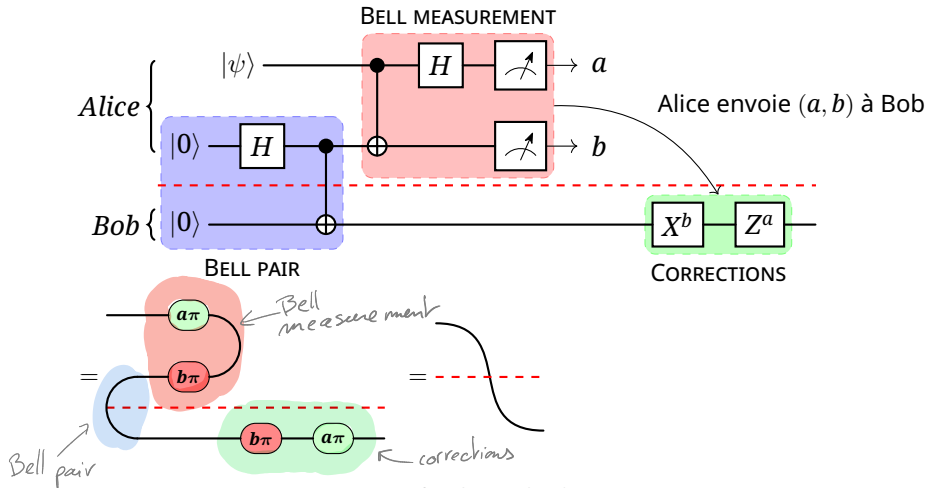


Communication classique
→
"Applique rotation $\frac{\pi}{2}$ "

intrication consommée



Téléportation quantique



Questions cryptographie quantique



La distribution quantique de clé (QKD) a-t-elle besoin de cryptographie post-quantique ? **A** Oui **B** Non.

La QKD est intéressante car elle est :



- A** Impossible à casser après le protocole
- B** Impossible à casser inconditionnellement
- C** Plus efficace



En présence d'intrication mais avec une communication classique, Alice ne peut transmettre que des états quantiques dont elle connaît la description.

- A** Vrai
- B** Faux

Questions cryptographie quantique



La distribution quantique de clé (QKD) a-t-elle besoin de cryptographie post-quantique ? **A** Oui  **B** Non.

La QKD est intéressante car elle est :



- A** Impossible à casser après le protocole
- B** Impossible à casser inconditionnellement
- C** Plus efficace



En présence d'intrication mais avec une communication classique, Alice ne peut transmettre que des états quantiques dont elle connaît la description.

- A** Vrai
- B** Faux

Questions cryptographie quantique



La distribution quantique de clé (QKD) a-t-elle besoin de cryptographie post-quantique ? **A** Oui ✓ **B** Non.

La QKD est intéressante car elle est :



- A** Impossible à casser après le protocole ✓
- B** Impossible à casser inconditionnellement
- C** Plus efficace



En présence d'intrication mais avec une communication classique, Alice ne peut transmettre que des états quantiques dont elle connaît la description.

- A** Vrai
- B** Faux

Questions cryptographie quantique



La distribution quantique de clé (QKD) a-t-elle besoin de cryptographie post-quantique ? **A** Oui ✓ **B** Non.

La QKD est intéressante car elle est :



- A** Impossible à casser après le protocole ✓
- B** Impossible à casser inconditionnellement
- C** Plus efficace



En présence d'intrication mais avec une communication classique, Alice ne peut transmettre que des états quantiques dont elle connaît la description.

- A** Vrai
- B** Faux ✓

Calcul délégué quantique à l'aveugle









































Measurement-based quantum computing (MBQC)

R. Raussendorf and H. Briegel, "*A one-way quantum computer*", PRL, 2001

R. Raussendorf, D. Browne, and H. Briegel, "Measurement-based quantum computation with cluster states", PRA, 2003

V. Danos and E. Kashefi, "Determinism in the one-way model", PRA, 2006



Measurement-based quantum computing (MBQC)

R. Raussendorf and H. Briegel, "*A one-way quantum computer*", PRL, 2001

R. Raussendorf, D. Browne, and H. Briegel, "Measurement-based quantum computation with cluster states", PRA, 2003

V. Danos and E. Kashefi, "Determinism in the one-way model", PRA, 2006



Measurement-based quantum computing (MBQC)

R. Raussendorf and H. Briegel, "*A one-way quantum computer*", PRL, 2001

R. Raussendorf, D. Browne, and H. Briegel, "Measurement-based quantum computation with cluster states", PRA, 2003

V. Danos and E. Kashefi, "Determinism in the one-way model", PRA, 2006



U



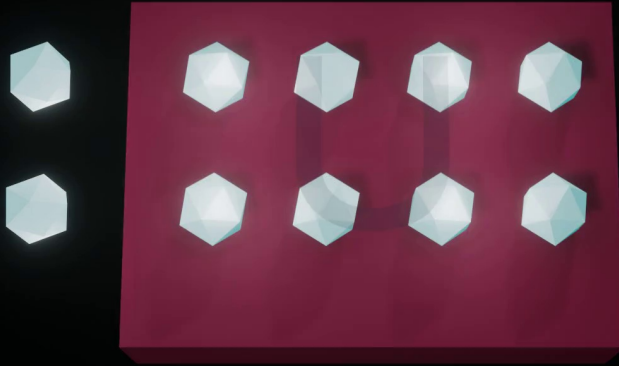
N

Measurement-based quantum computing (MBQC)

R. Raussendorf and H. Briegel, "A one-way quantum computer", PRL, 2001

R. Raussendorf, D. Browne, and H. Briegel, "Measurement-based quantum computation with cluster states", PRA, 2003

V. Danos and E. Kashefi, "Determinism in the one-way model", PRA, 2006

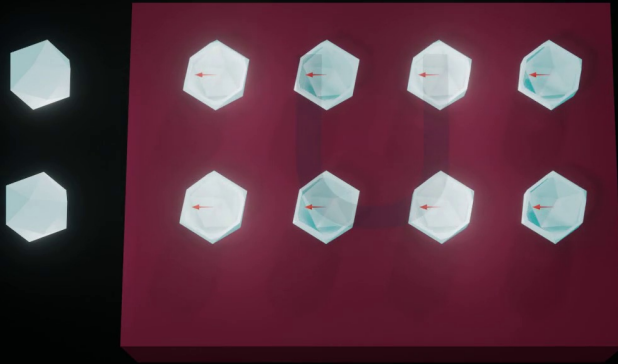


Measurement-based quantum computing (MBQC)

R. Raussendorf and H. Briegel, "A one-way quantum computer", PRL, 2001

R. Raussendorf, D. Browne, and H. Briegel, "Measurement-based quantum computation with cluster states", PRA, 2003

V. Danos and E. Kashefi, "Determinism in the one-way model", PRA, 2006

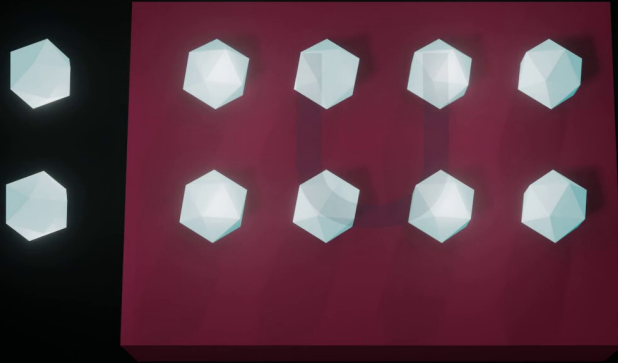


Measurement-based quantum computing (MBQC)

R. Raussendorf and H. Briegel, "A one-way quantum computer", PRL, 2001

R. Raussendorf, D. Browne, and H. Briegel, "Measurement-based quantum computation with cluster states", PRA, 2003

V. Danos and E. Kashefi, "Determinism in the one-way model", PRA, 2006

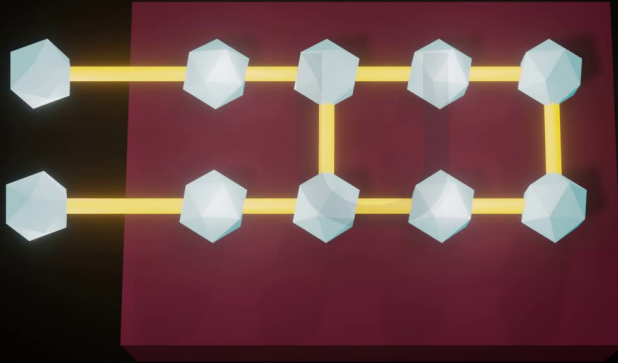


Measurement-based quantum computing (MBQC)

R. Raussendorf and H. Briegel, "A one-way quantum computer", PRL, 2001

R. Raussendorf, D. Browne, and H. Briegel, "Measurement-based quantum computation with cluster states", PRA, 2003

V. Danos and E. Kashefi, "Determinism in the one-way model", PRA, 2006

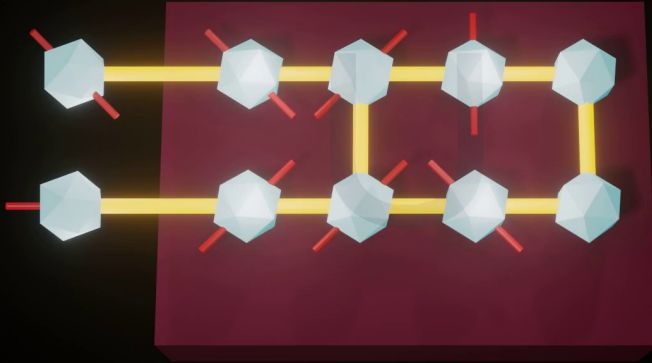


Measurement-based quantum computing (MBQC)

R. Raussendorf and H. Briegel, "A one-way quantum computer", PRL, 2001

R. Raussendorf, D. Browne, and H. Briegel, "Measurement-based quantum computation with cluster states", PRA, 2003

V. Danos and E. Kashefi, "Determinism in the one-way model", PRA, 2006

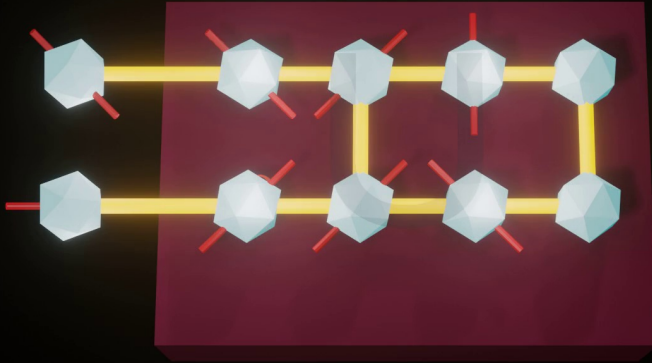


Measurement-based quantum computing (MBQC)

R. Raussendorf and H. Briegel, "A one-way quantum computer", PRL, 2001

R. Raussendorf, D. Browne, and H. Briegel, "Measurement-based quantum computation with cluster states", PRA, 2003

V. Danos and E. Kashefi, "Determinism in the one-way model", PRA, 2006

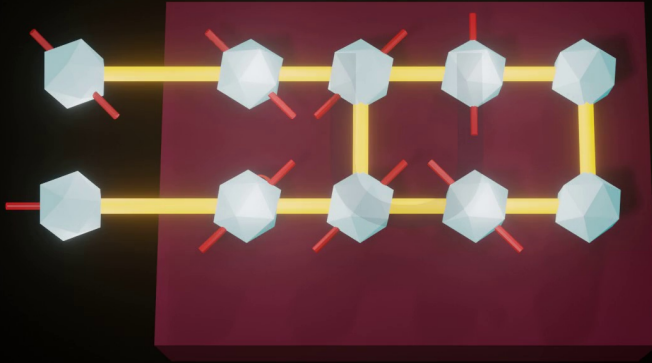


Measurement-based quantum computing (MBQC)

R. Raussendorf and H. Briegel, "A one-way quantum computer", PRL, 2001

R. Raussendorf, D. Browne, and H. Briegel, "Measurement-based quantum computation with cluster states", PRA, 2003

V. Danos and E. Kashefi, "Determinism in the one-way model", PRA, 2006



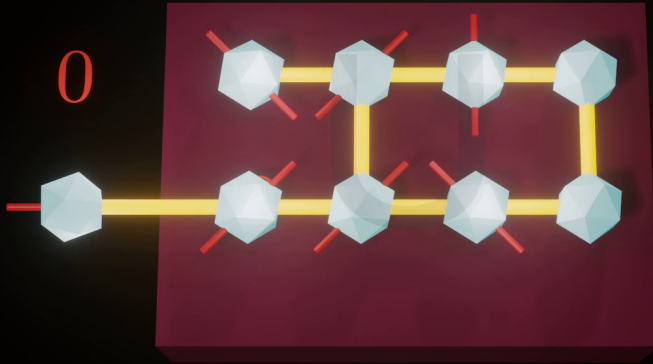
$$\theta \in \{0, \frac{\pi}{4}, \dots, 7\frac{\pi}{4}\}$$

Measurement-based quantum computing (MBQC)

R. Raussendorf and H. Briegel, "A one-way quantum computer", PRL, 2001

R. Raussendorf, D. Browne, and H. Briegel, "Measurement-based quantum computation with cluster states", PRA, 2003

V. Danos and E. Kashefi, "Determinism in the one-way model", PRA, 2006



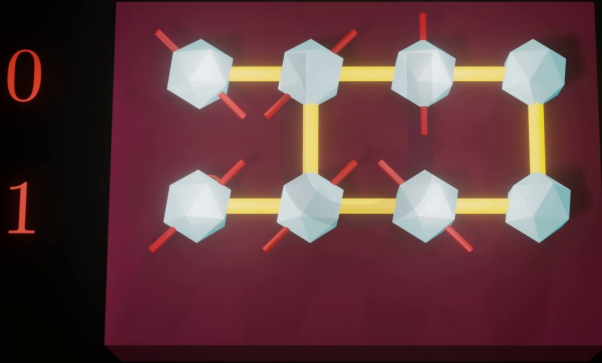
$$\theta \in \{0, \frac{\pi}{4}, \dots, 7\frac{\pi}{4}\}$$

Measurement-based quantum computing (MBQC)

R. Raussendorf and H. Briegel, "A one-way quantum computer", PRL, 2001

R. Raussendorf, D. Browne, and H. Briegel, "Measurement-based quantum computation with cluster states", PRA, 2003

V. Danos and E. Kashefi, "Determinism in the one-way model", PRA, 2006



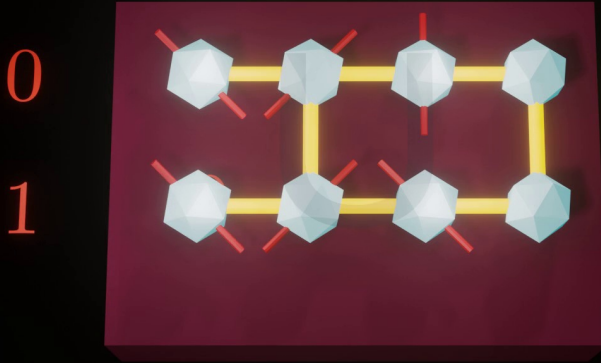
$$\theta \in \{0, \frac{\pi}{4}, \dots, 7\frac{\pi}{4}\}$$

Measurement-based quantum computing (MBQC)

R. Raussendorf and H. Briegel, "A one-way quantum computer", PRL, 2001

R. Raussendorf, D. Browne, and H. Briegel, "Measurement-based quantum computation with cluster states", PRA, 2003

V. Danos and E. Kashefi, "Determinism in the one-way model", PRA, 2006



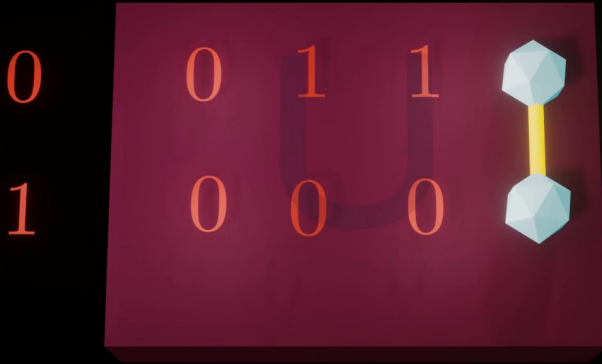
$$\theta \in \{0, \frac{\pi}{4}, \dots, 7\frac{\pi}{4}\}$$

Measurement-based quantum computing (MBQC)

R. Raussendorf and H. Briegel, "A one-way quantum computer", PRL, 2001

R. Raussendorf, D. Browne, and H. Briegel, "Measurement-based quantum computation with cluster states", PRA, 2003

V. Danos and E. Kashefi, "Determinism in the one-way model", PRA, 2006



$$\theta \in \{0, \frac{\pi}{4}, \dots, 7\frac{\pi}{4}\}$$

Universal blind quantum computing (UBQC)

A. Broadbent, J. Fitzsimons, E. Kashefi, "*Universal blind quantum computation*", FOCS, 2009



Universal blind quantum computing (UBQC)

A. Broadbent, J. Fitzsimons, E. Kashefi, "*Universal blind quantum computation*", FOCS, 2009



Universal blind quantum computing (UBQC)

A. Broadbent, J. Fitzsimons, E. Kashefi, "*Universal blind quantum computation*", FOCS, 2009



Universal blind quantum computing (UBQC)

A. Broadbent, J. Fitzsimons, E. Kashefi, "*Universal blind quantum computation*", FOCS, 2009



Universal blind quantum computing (UBQC)

A. Broadbent, J. Fitzsimons, E. Kashefi, "*Universal blind quantum computation*", FOCS, 2009



Universal blind quantum computing (UBQC)

A. Broadbent, J. Fitzsimons, E. Kashefi, "*Universal blind quantum computation*", FOCS, 2009



Universal blind quantum computing (UBQC)

A. Broadbent, J. Fitzsimons, E. Kashefi, "*Universal blind quantum computation*", FOCS, 2009



Universal blind quantum computing (UBQC)

A. Broadbent, J. Fitzsimons, E. Kashefi, "*Universal blind quantum computation*", FOCS, 2009



Universal blind quantum computing (UBQC)

A. Broadbent, J. Fitzsimons, E. Kashefi, "*Universal blind quantum computation*", FOCS, 2009



Universal blind quantum computing (UBQC)

A. Broadbent, J. Fitzsimons, E. Kashefi, "*Universal blind quantum computation*", FOCS, 2009



Universal blind quantum computing (UBQC)

A. Broadbent, J. Fitzsimons, E. Kashefi, "*Universal blind quantum computation*", FOCS, 2009



Universal blind quantum computing (UBQC)

A. Broadbent, J. Fitzsimons, E. Kashefi, "*Universal blind quantum computation*", FOCS, 2009



Universal blind quantum computing (UBQC)

A. Broadbent, J. Fitzsimons, E. Kashefi, "*Universal blind quantum computation*", FOCS, 2009



Universal blind quantum computing (UBQC)

A. Broadbent, J. Fitzsimons, E. Kashefi, "*Universal blind quantum computation*", FOCS, 2009



Universal blind quantum computing (UBQC)

A. Broadbent, J. Fitzsimons, E. Kashefi, "*Universal blind quantum computation*", FOCS, 2009



Universal blind quantum computing (UBQC)

A. Broadbent, J. Fitzsimons, E. Kashefi, "*Universal blind quantum computation*", FOCS, 2009

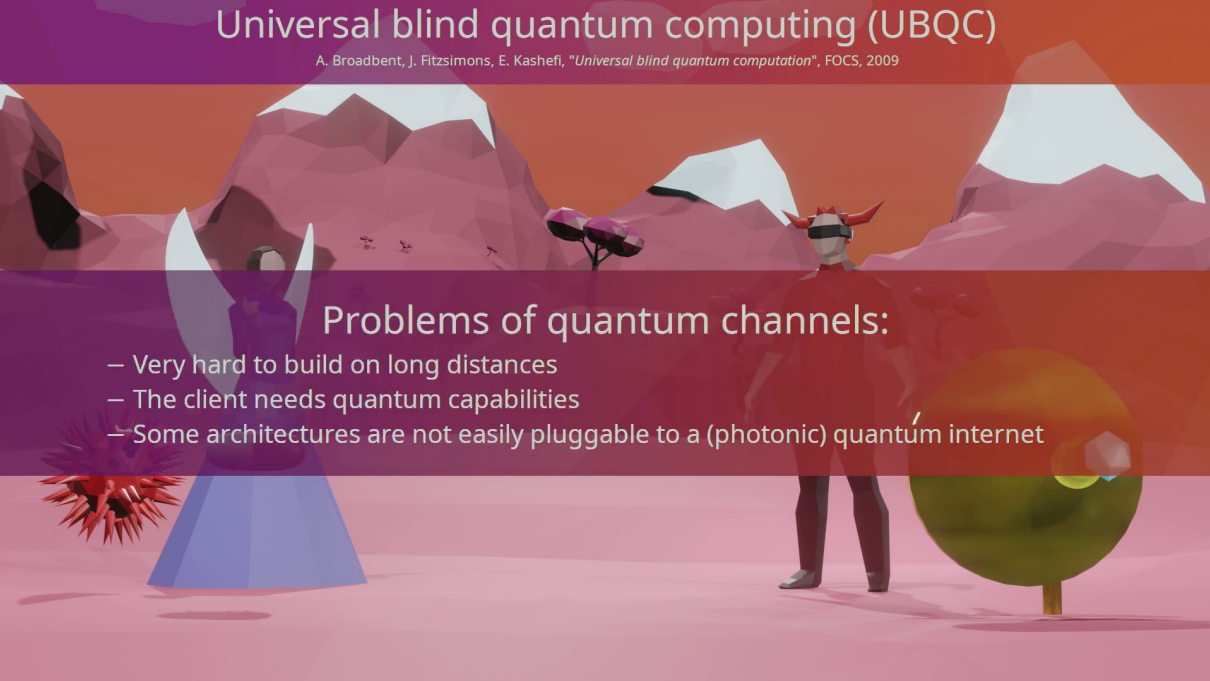


Universal blind quantum computing (UBQC)

A. Broadbent, J. Fitzsimons, E. Kashefi, "*Universal blind quantum computation*", FOCS, 2009

Problems of quantum channels:

- Very hard to build on long distances
- The client needs quantum capabilities
- Some architectures are not easily pluggable to a (photonic) quantum internet





Is it possible to do delegated blind quantum computing (and more) with purely classical clients?

QFactory



QFactory



QFactory



QFactory



QFactory



QFactory



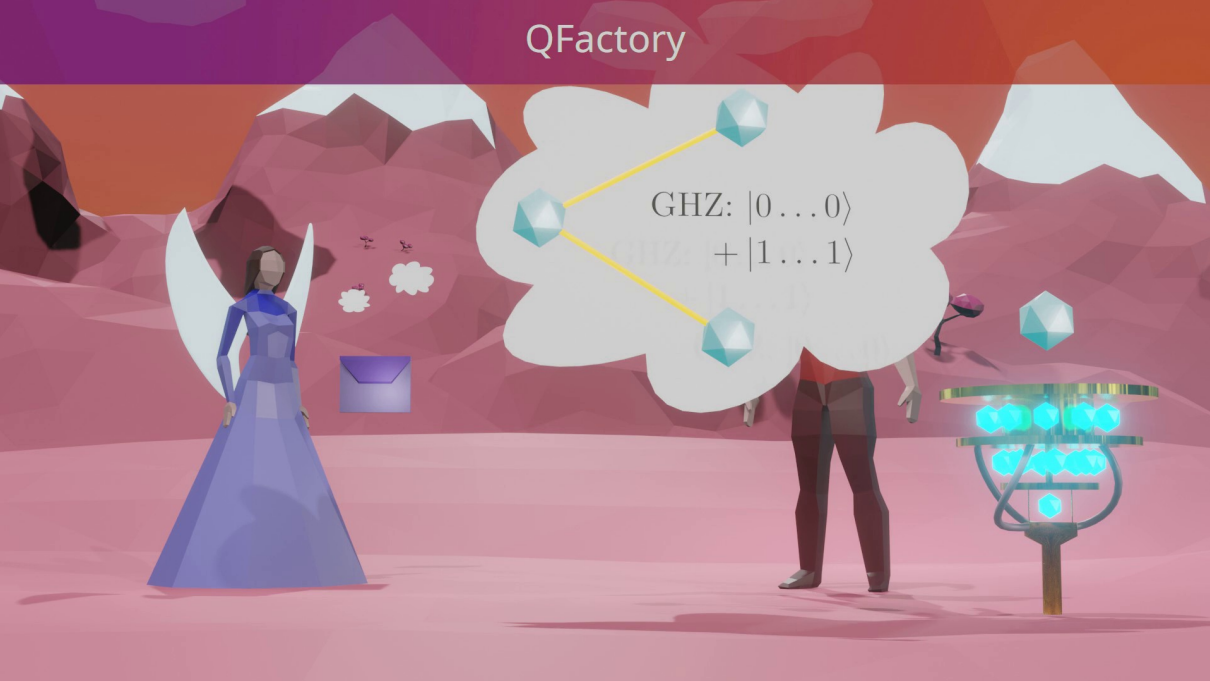
QFactory



QFactory

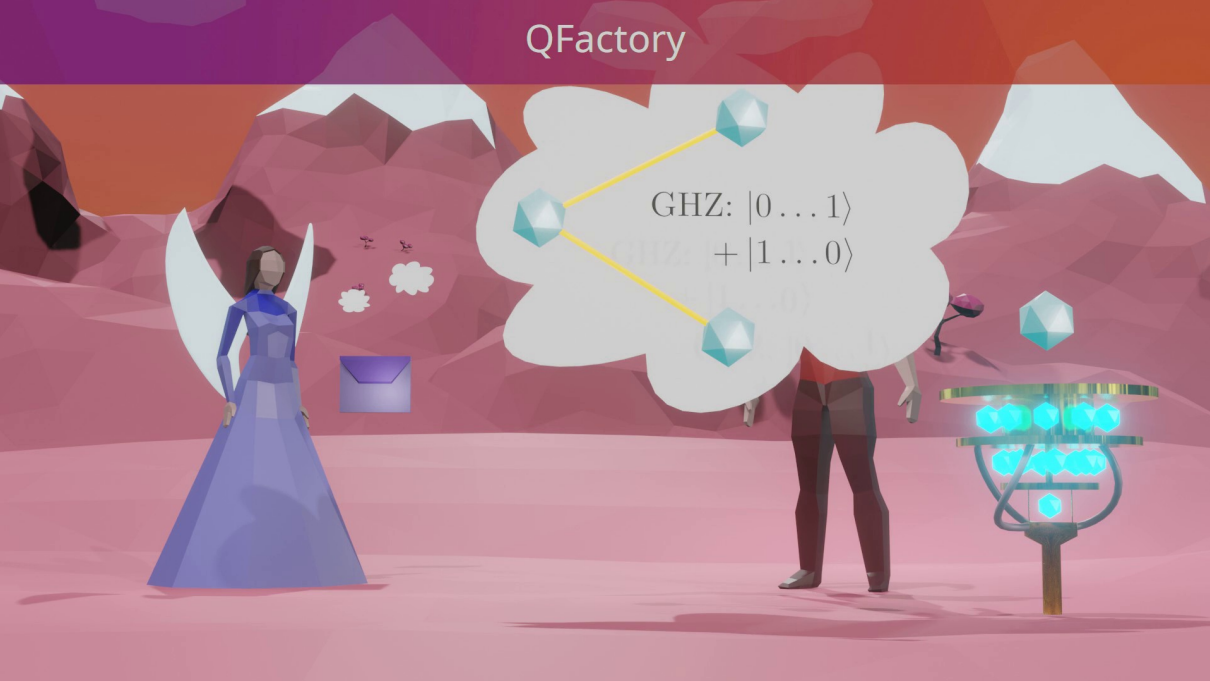


QFactory

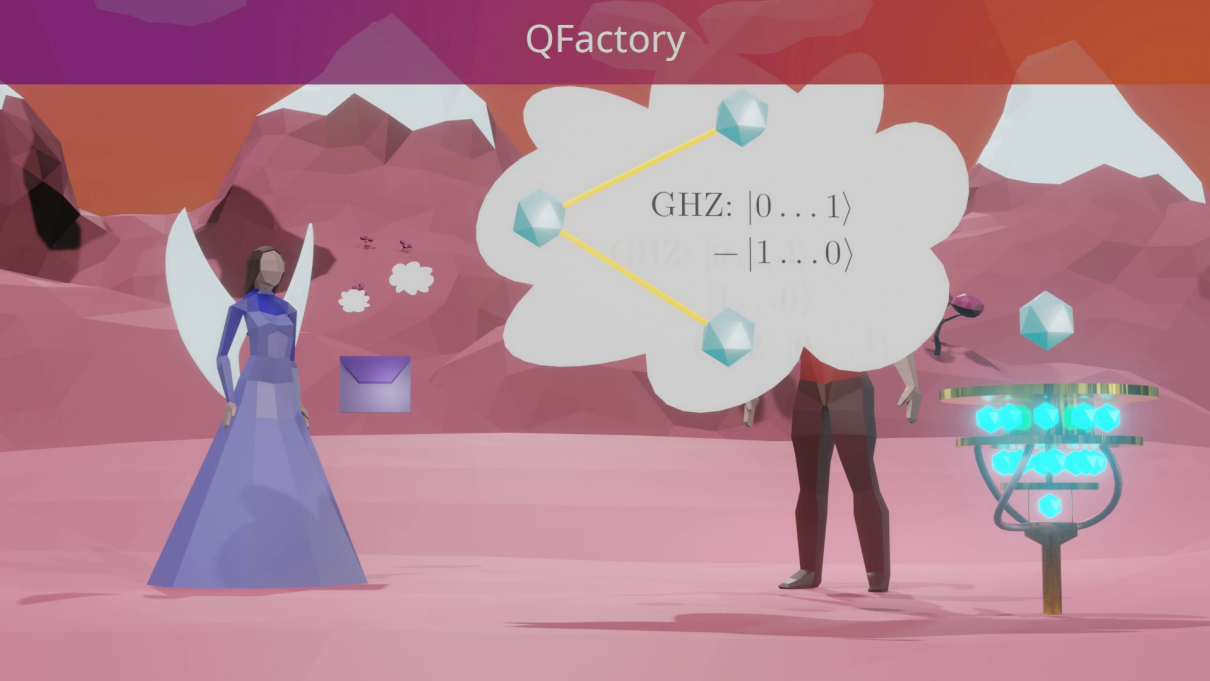


GHZ: $|0 \dots 0\rangle$
+ $|1 \dots 1\rangle$

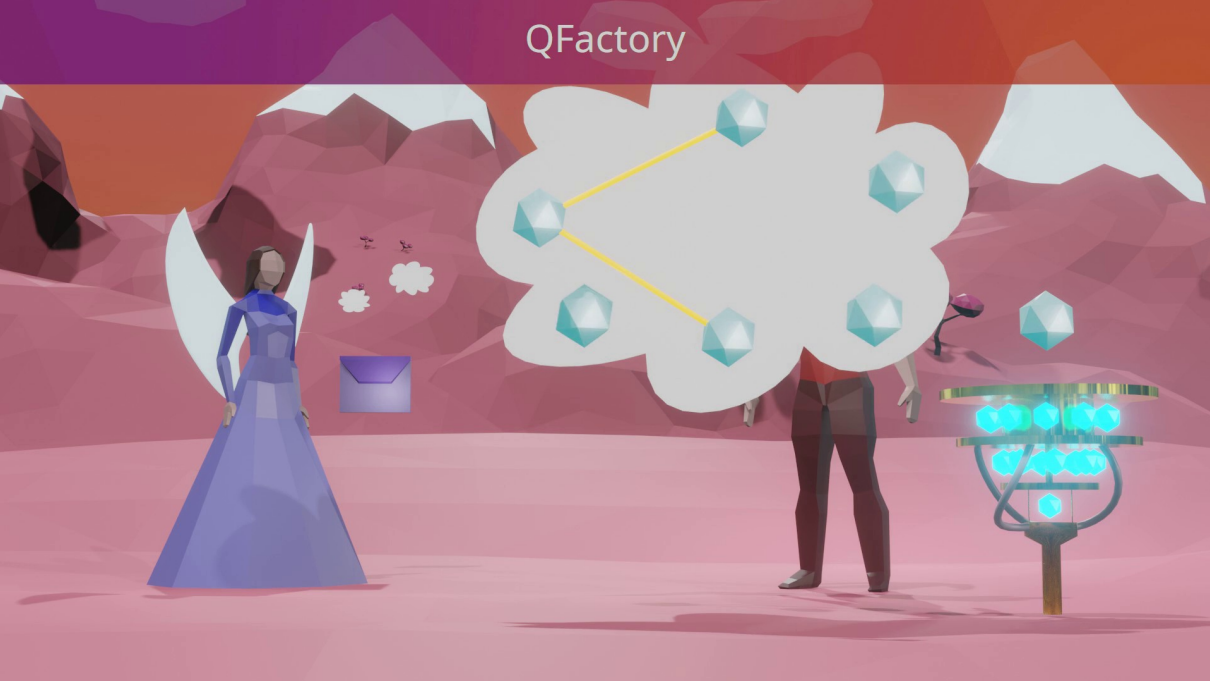
QFactory


$$\text{GHZ: } |0 \dots 1\rangle + |1 \dots 0\rangle$$

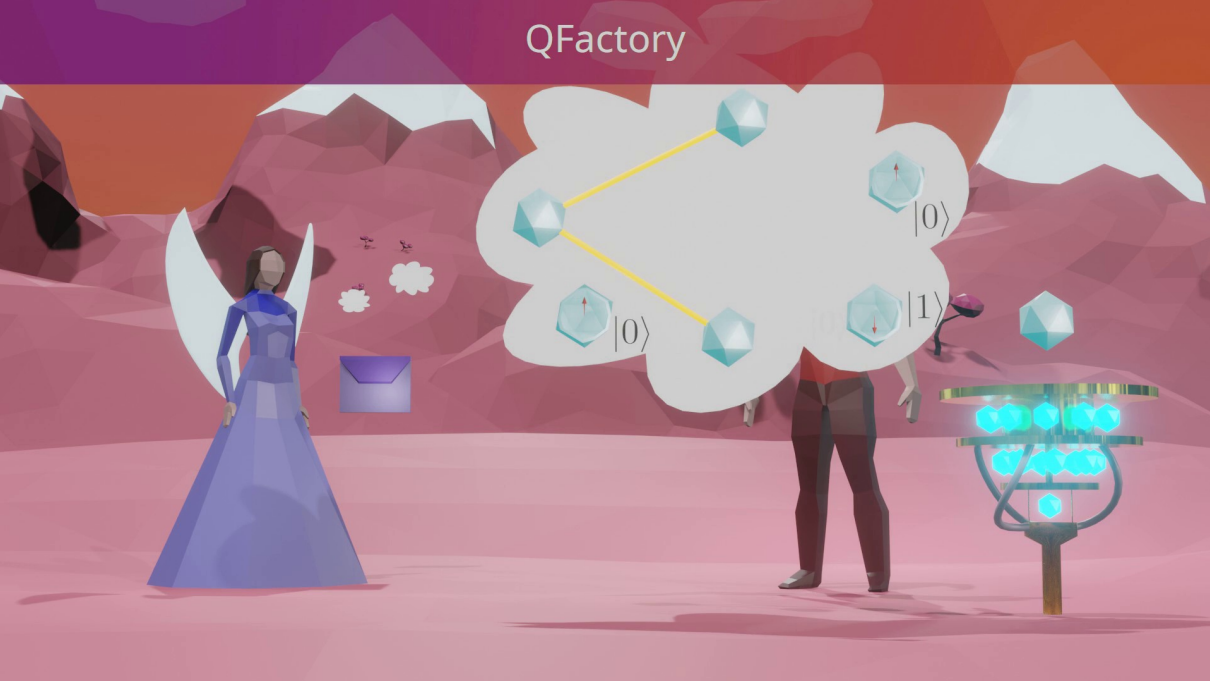
QFactory


$$\text{GHZ: } |0 \dots 1\rangle \\ - |1 \dots 0\rangle$$

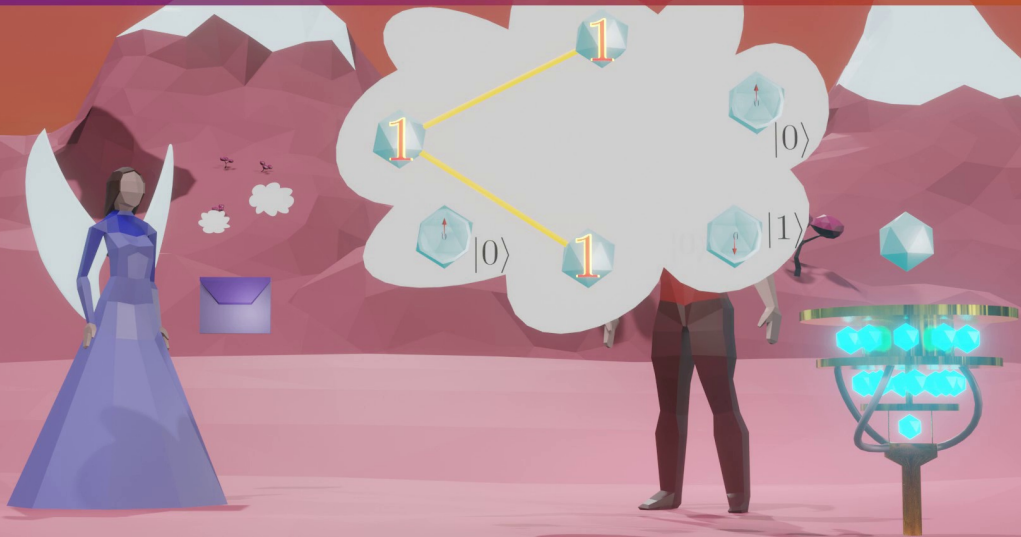
QFactory



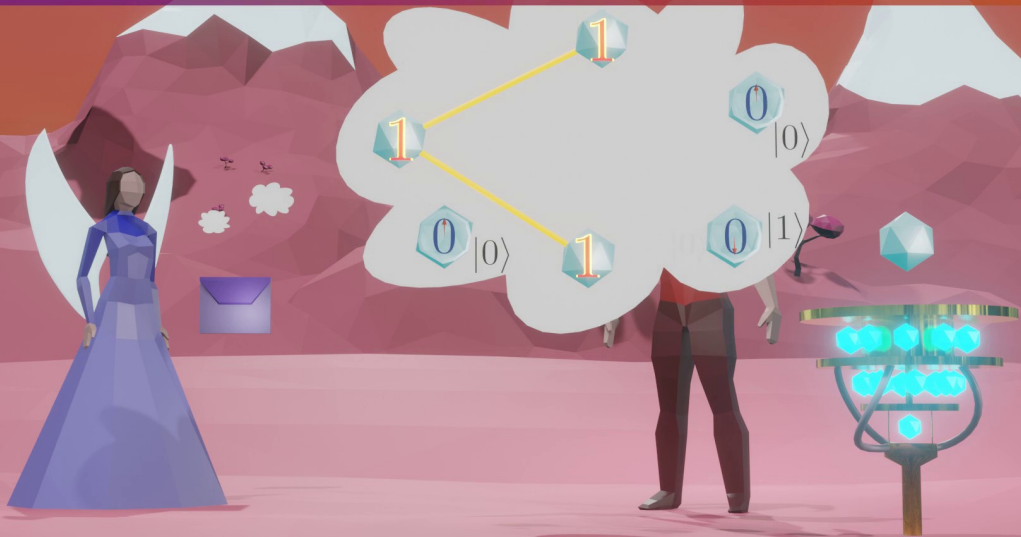
QFactory



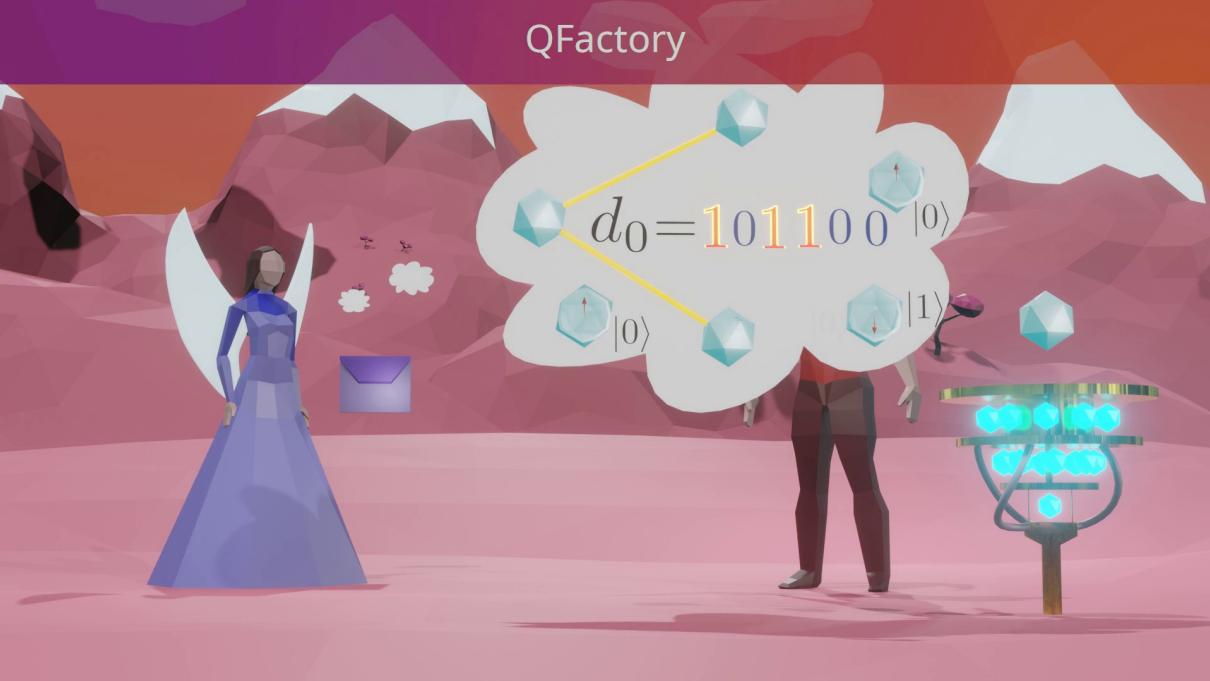
QFactory



QFactory



QFactory

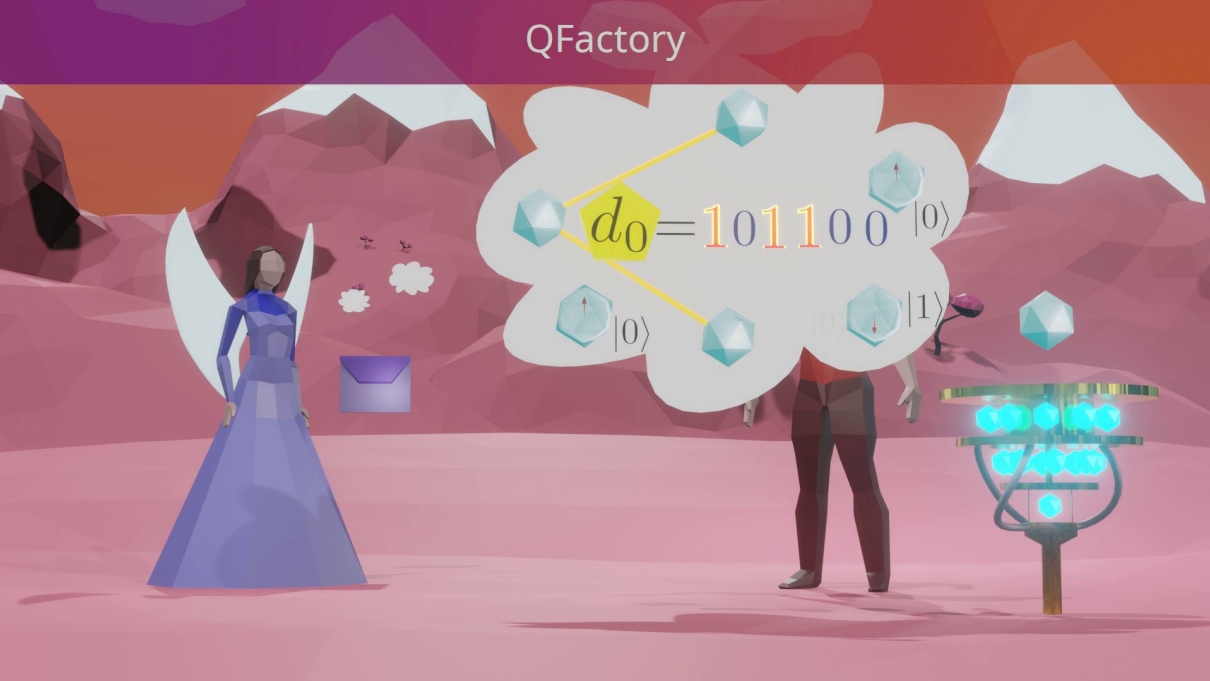


$d_0 = 101100 |0\rangle$

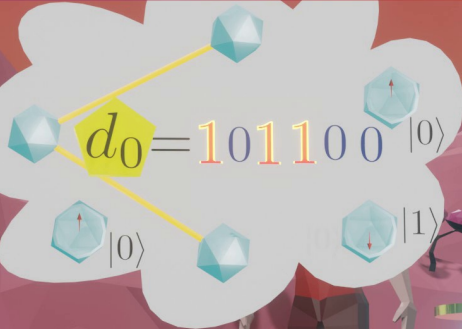
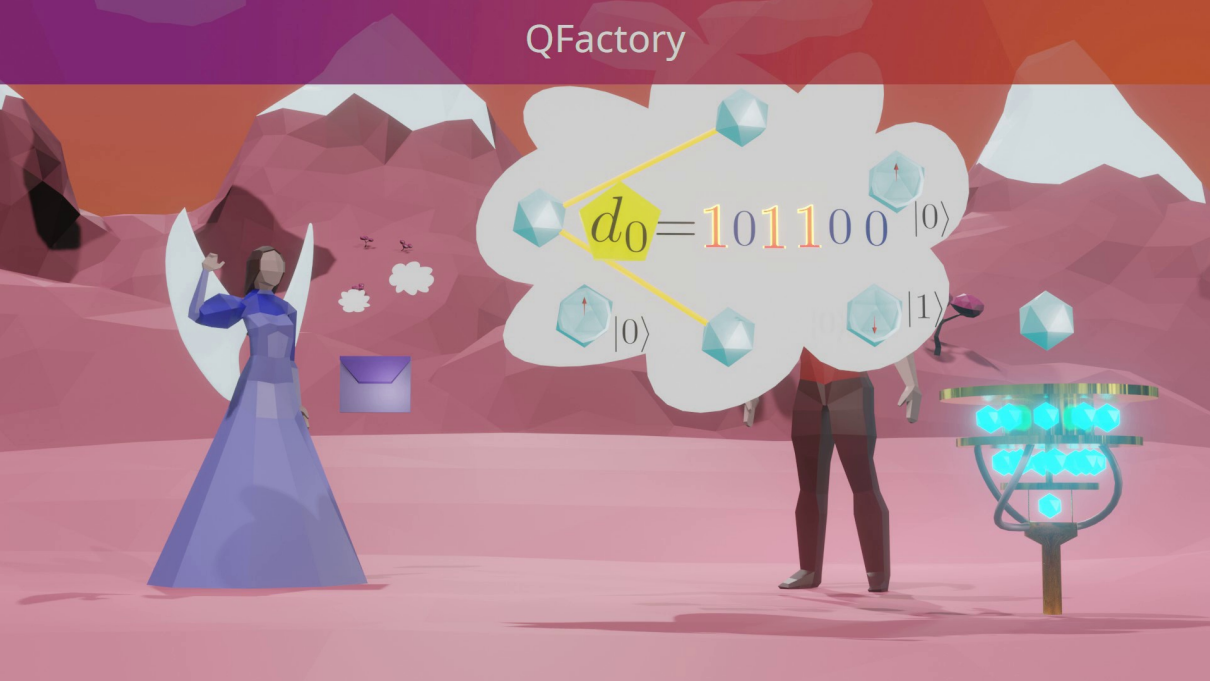
$|0\rangle$

$|1\rangle$

QFactory



QFactory



QFactory



QFactory: cryptographic requirements



QFactory: cryptographic requirements

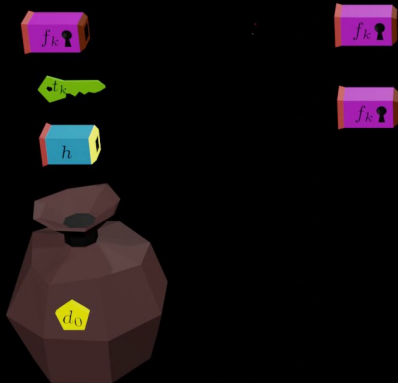


QFactory: cryptographic requirements



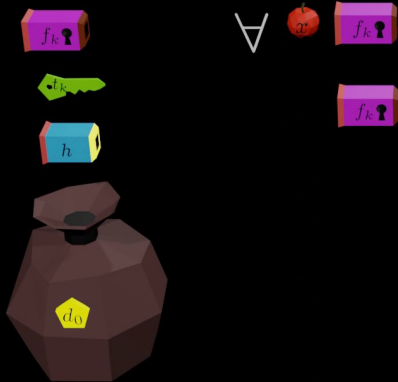
QFactory: cryptographic requirements

– 2-to-1



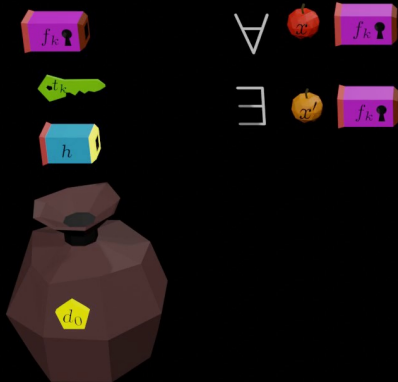
QFactory: cryptographic requirements

– 2-to-1



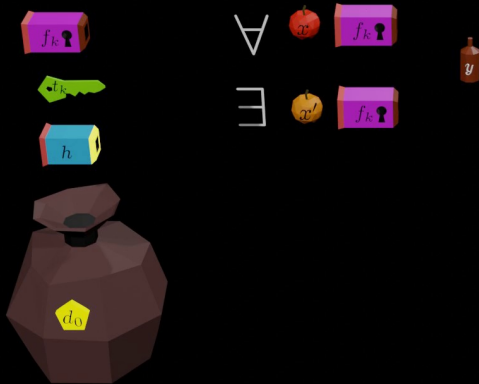
QFactory: cryptographic requirements

– 2-to-1



QFactory: cryptographic requirements

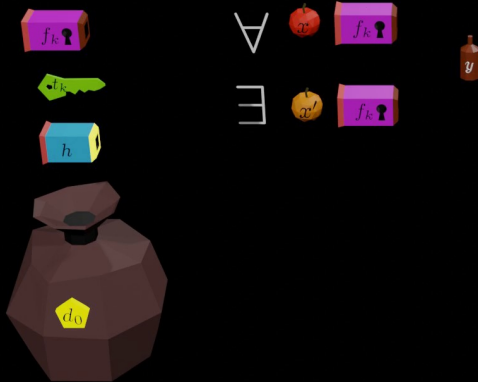
– 2-to-1



QFactory: cryptographic requirements

– 2-to-1

– Trapdoor



QFactory: cryptographic requirements

– 2-to-1

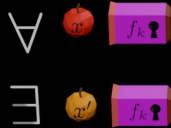


– Trapdoor



QFactory: cryptographic requirements

– 2-to-1



– Trapdoor



QFactory: cryptographic requirements

– 2-to-1



– Trapdoor

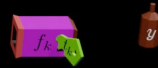


QFactory: cryptographic requirements

– 2-to-1



– Trapdoor



QFactory: cryptographic requirements

– 2-to-1



– Trapdoor



QFactory: cryptographic requirements

– 2-to-1



$\forall$



$\exists$



– Trapdoor



– XOR property

QFactory: cryptographic requirements

– 2-to-1



$\forall$



$\exists$



– Trapdoor



– XOR property



QFactory: cryptographic requirements

– 2-to-1



$\forall$



$\exists$



– Trapdoor



– XOR property



QFactory: cryptographic requirements

– 2-to-1



$\forall$



$\exists$



– Trapdoor



– XOR property



QFactory: cryptographic requirements

– 2-to-1



$\forall$



$\exists$



– Trapdoor

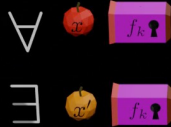


– XOR property



QFactory: cryptographic requirements

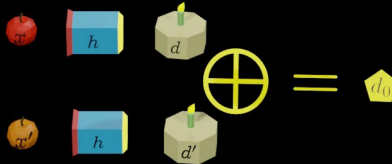
– 2-to-1



– Trapdoor



– XOR property



QFactory: cryptographic requirements

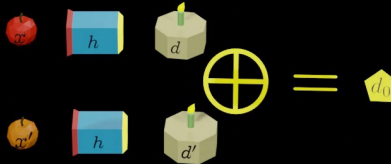
– 2-to-1



– Trapdoor



– XOR property



– Hardcore bit

Given

QFactory: cryptographic requirements

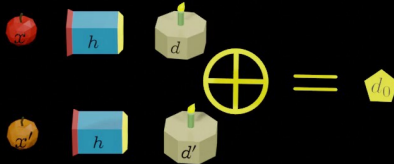
– 2-to-1



– Trapdoor



– XOR property



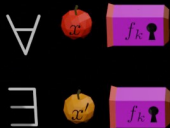
– Hardcore bit

Given 



QFactory: cryptographic requirements

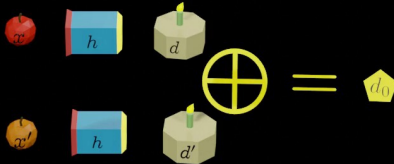
– 2-to-1



– Trapdoor



– XOR property



– Hardcore bit

Given 



QFactory: the protocol



QFactory: the protocol



QFactory: the protocol



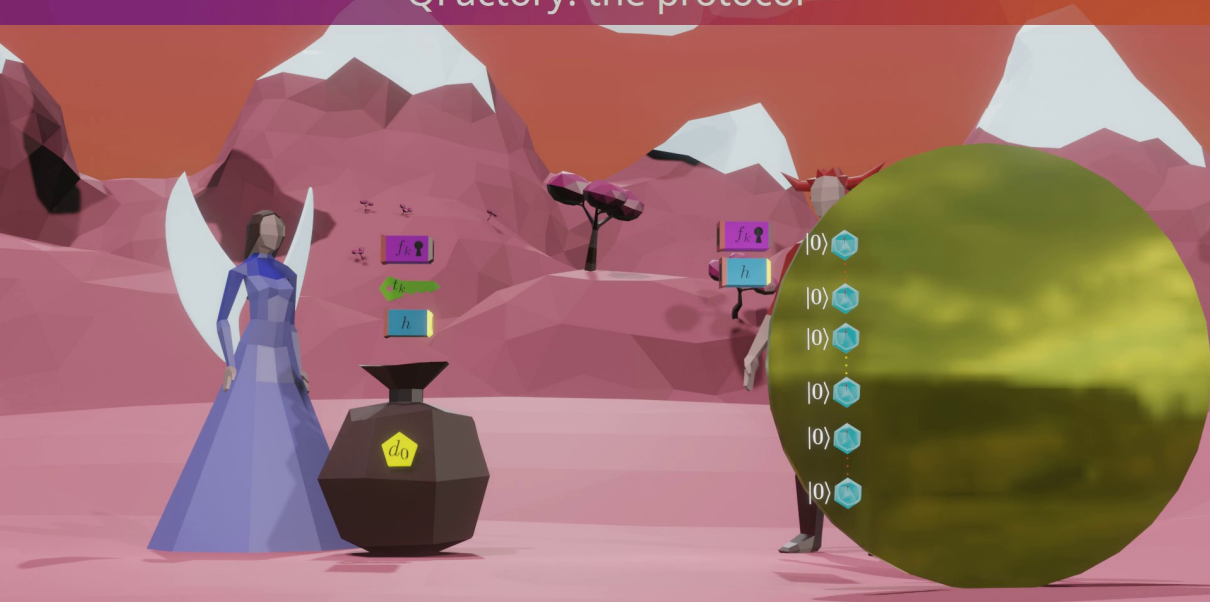
QFactory: the protocol



QFactory: the protocol

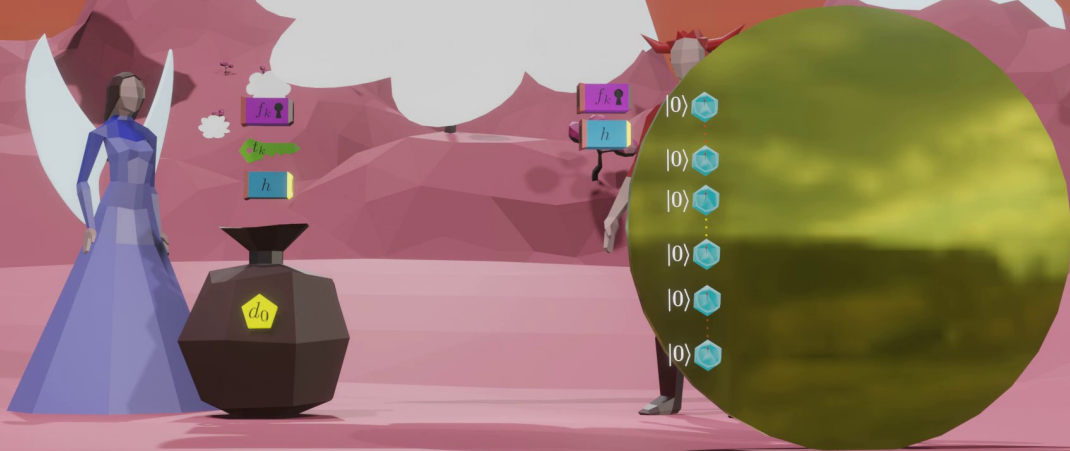


QFactory: the protocol



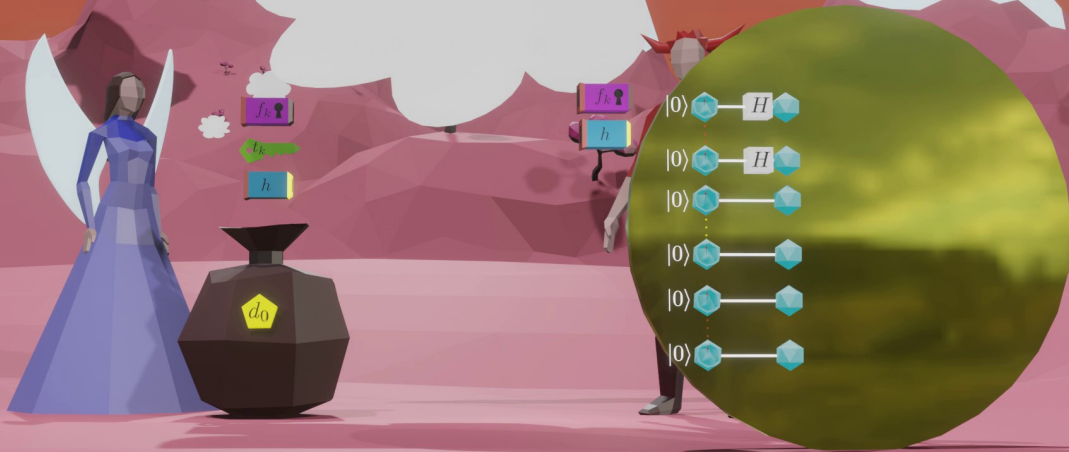
QFactory: the protocol

$$|0 \dots 0\rangle |0 \dots 0\rangle |0 \dots 0\rangle$$



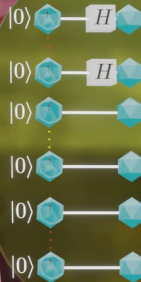
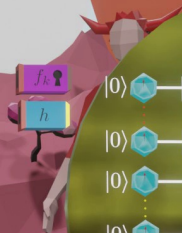
QFactory: the protocol

$$|0 \dots 0\rangle |0 \dots 0\rangle |0 \dots 0\rangle$$



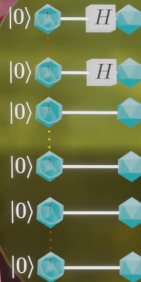
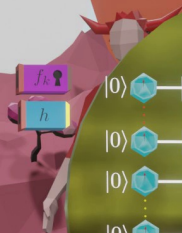
QFactory: the protocol

$$\sum_x |0 \dots 0\rangle |0 \dots 0\rangle |0 \dots 0\rangle$$



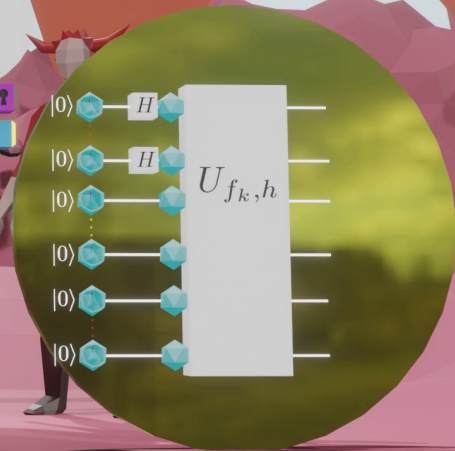
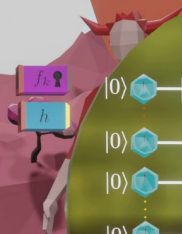
QFactory: the protocol

$$\sum_x |x\rangle |0 \dots 0\rangle |0 \dots 0\rangle$$



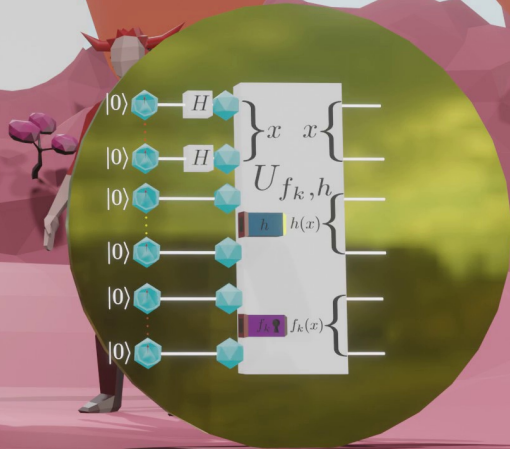
QFactory: the protocol

$$\sum_x |x\rangle |0 \dots 0\rangle |0 \dots 0\rangle$$



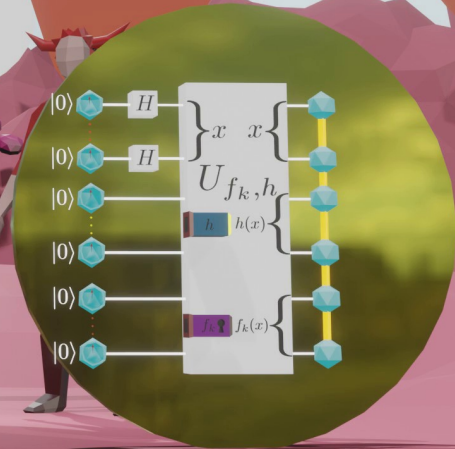
QFactory: the protocol

$$\sum_x |x\rangle |0 \dots 0\rangle |0 \dots 0\rangle$$



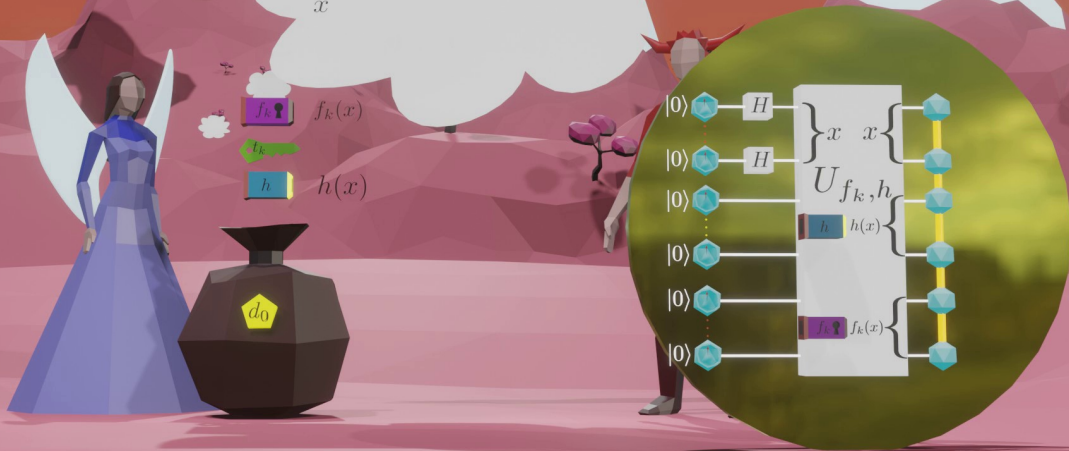
QFactory: the protocol

$$\sum_x |x\rangle |0 \dots 0\rangle |0 \dots 0\rangle$$



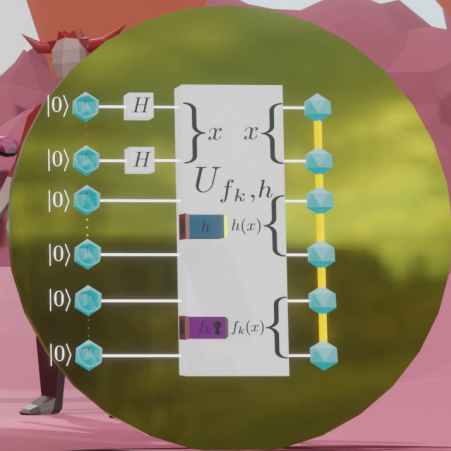
QFactory: the protocol

$$\sum_x |x\rangle |0 \dots 0\rangle |0 \dots 0\rangle$$



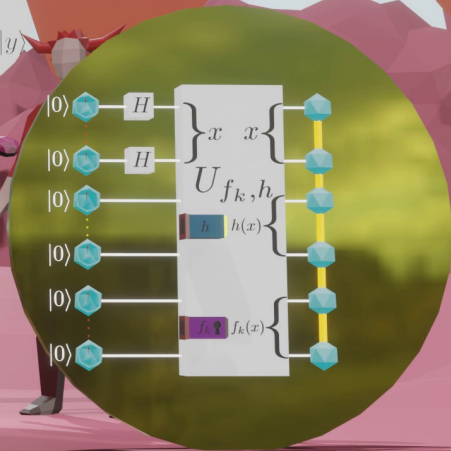
QFactory: the protocol

$$\sum_x |x\rangle |h(x)\rangle |f_k(x)\rangle$$



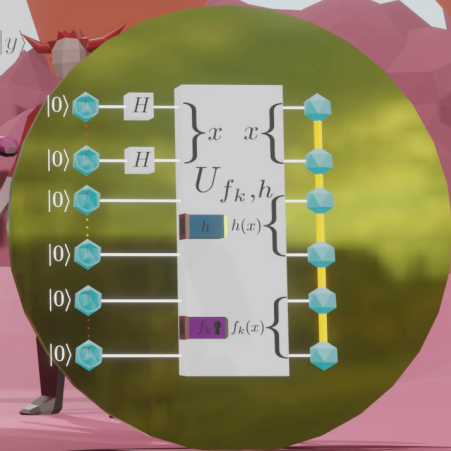
QFactory: the protocol

$$\sum_x |x\rangle |h(x)\rangle |f_k(x)\rangle = \sum_y (|\text{apple}\rangle |h(x)\rangle + |\text{orange}\rangle |h(x')\rangle) |y\rangle$$



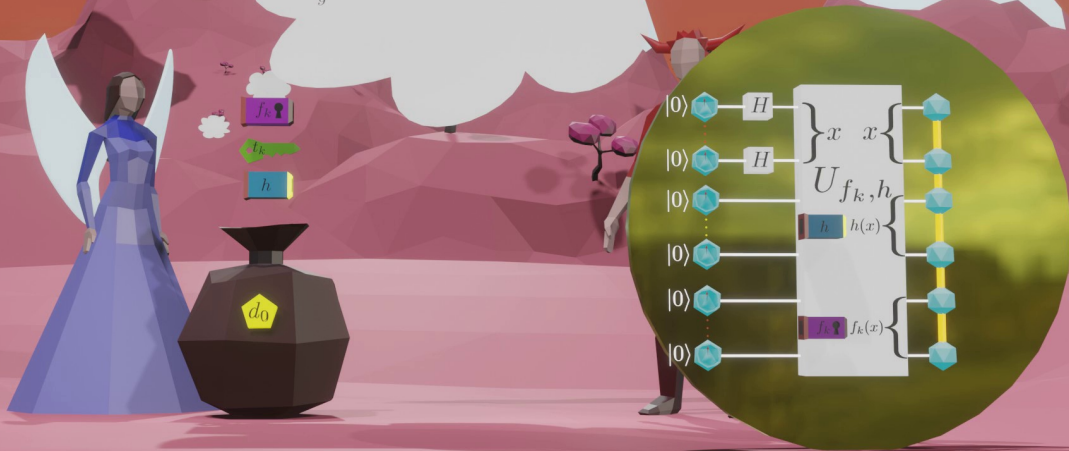
QFactory: the protocol

$$\sum_x |x\rangle |h(x)\rangle |f_k(x)\rangle = \sum_y (|x\rangle |h(x)\rangle + |x'\rangle |h(x')\rangle) |y\rangle$$



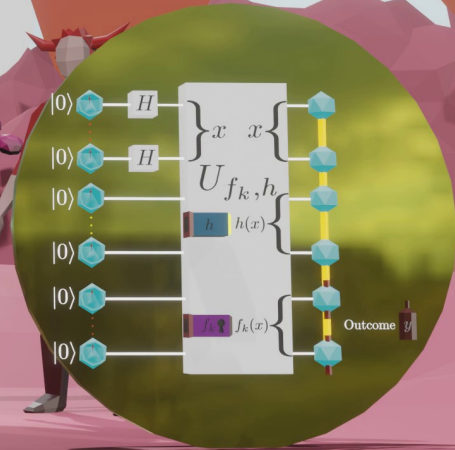
QFactory: the protocol

$$\sum_y (|x\rangle |h(x)\rangle + |x'\rangle |h(x')\rangle) |y\rangle$$



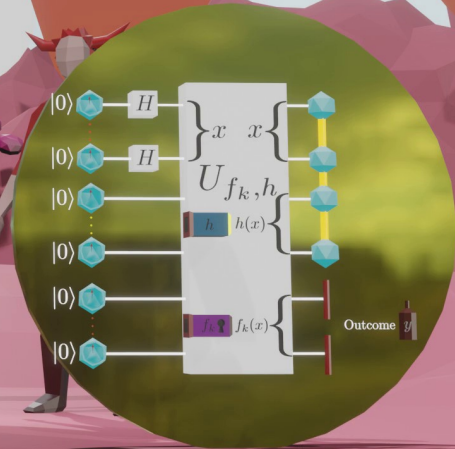
QFactory: the protocol

$$\sum_y (|x\rangle |h(x)\rangle + |x'\rangle |h(x')\rangle) |y\rangle$$



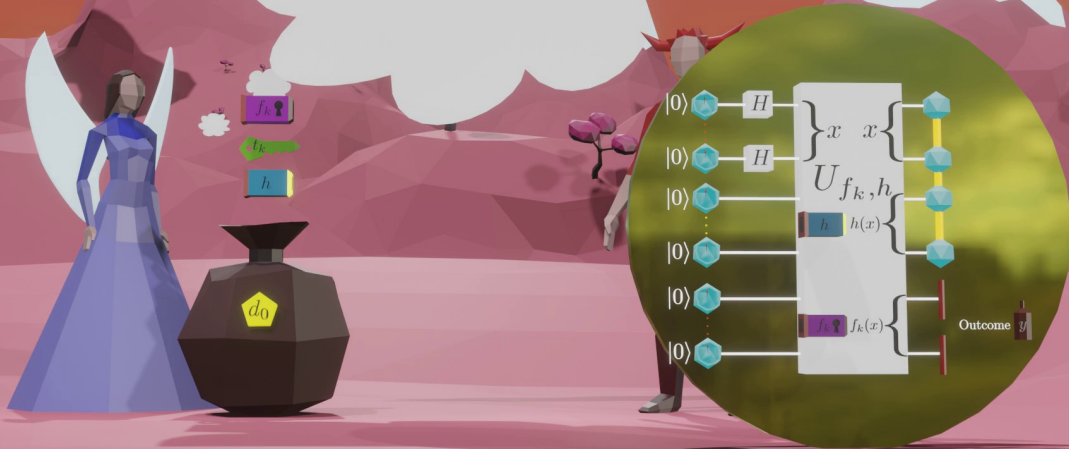
QFactory: the protocol

$$\sum_y (|x\rangle |h(x)\rangle + |x'\rangle |h(x')\rangle) |y\rangle$$



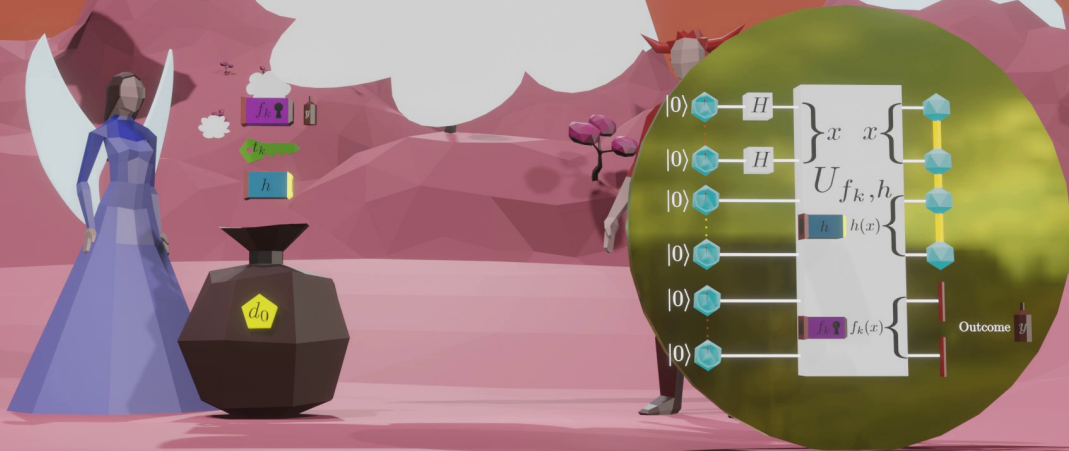
QFactory: the protocol

$$(|x\rangle |h(x)\rangle + |x'\rangle |h(x')\rangle) |y\rangle$$



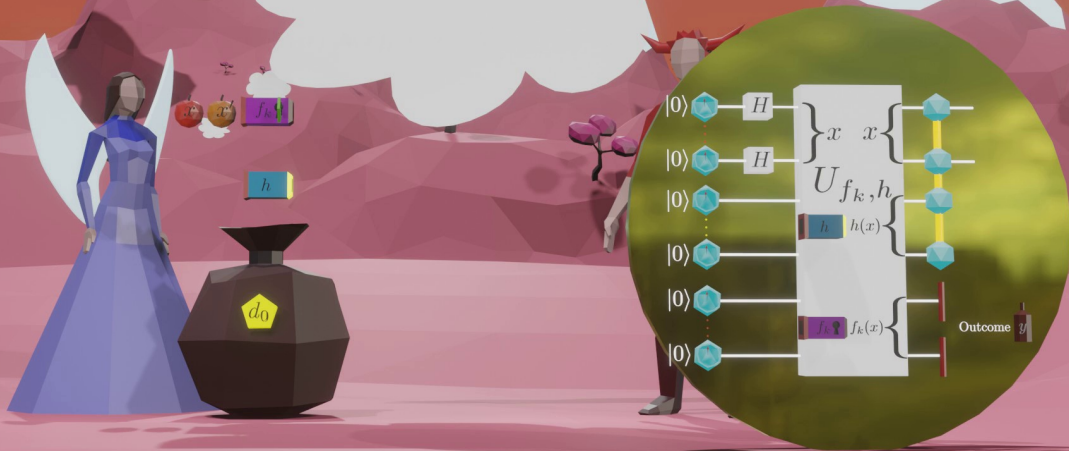
QFactory: the protocol

$$(|x\rangle |h(x)\rangle + |x'\rangle |h(x')\rangle) |y\rangle$$



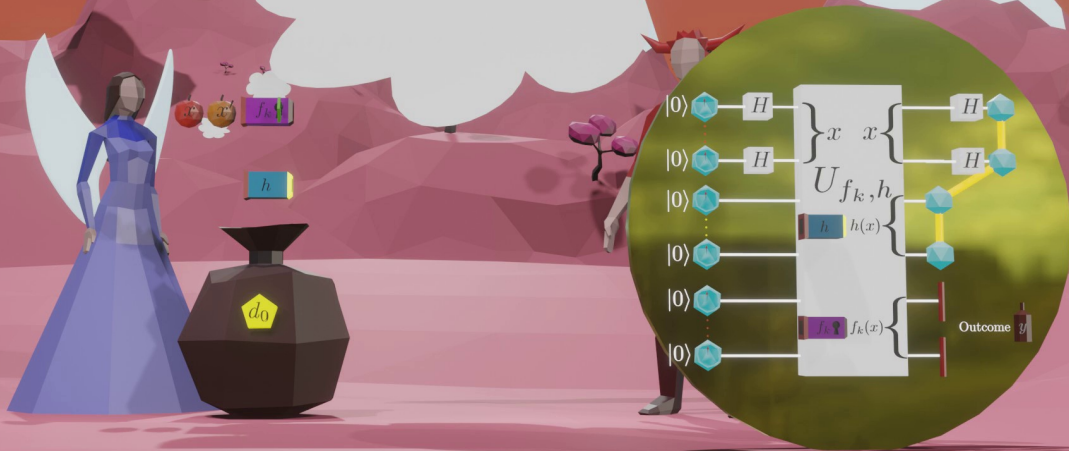
QFactory: the protocol

$$(|x\rangle |h(x)\rangle + |x'\rangle |h(x')\rangle) |y\rangle$$



QFactory: the protocol

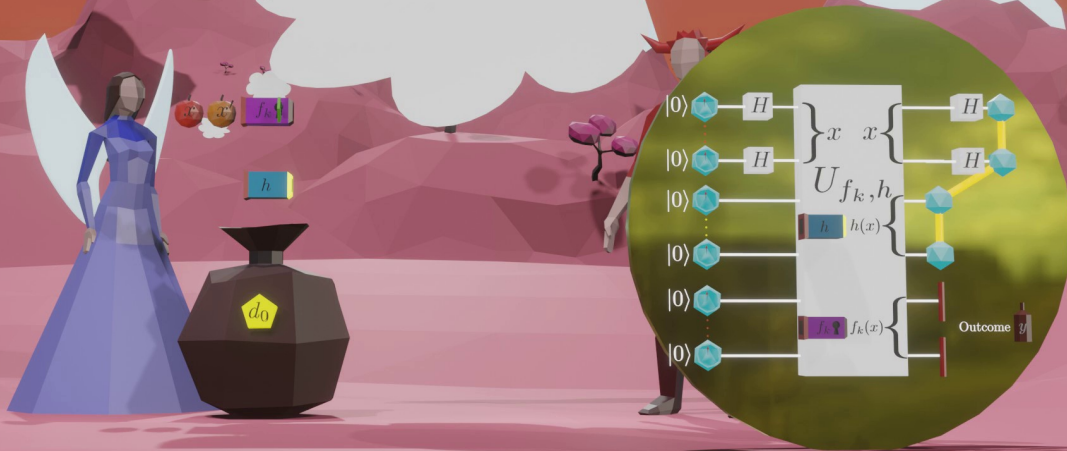
$$(|x\rangle |h(x)\rangle + |x'\rangle |h(x')\rangle) |y\rangle$$



QFactory: the protocol

$$(|x\rangle |h(x)\rangle + |x'\rangle |h(x')\rangle) |y\rangle$$

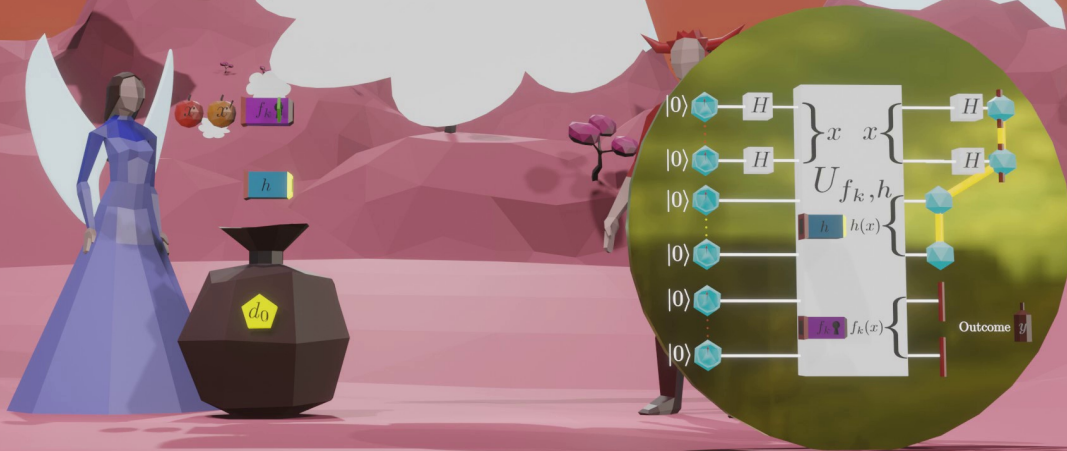
$$\rightsquigarrow \sum_b (-1)^{x \cdot b} |b\rangle |h(x)\rangle + (-1)^{x' \cdot b} |b\rangle |h(x')\rangle$$



QFactory: the protocol

$$(|x\rangle |h(x)\rangle + |x'\rangle |h(x')\rangle) |y\rangle$$

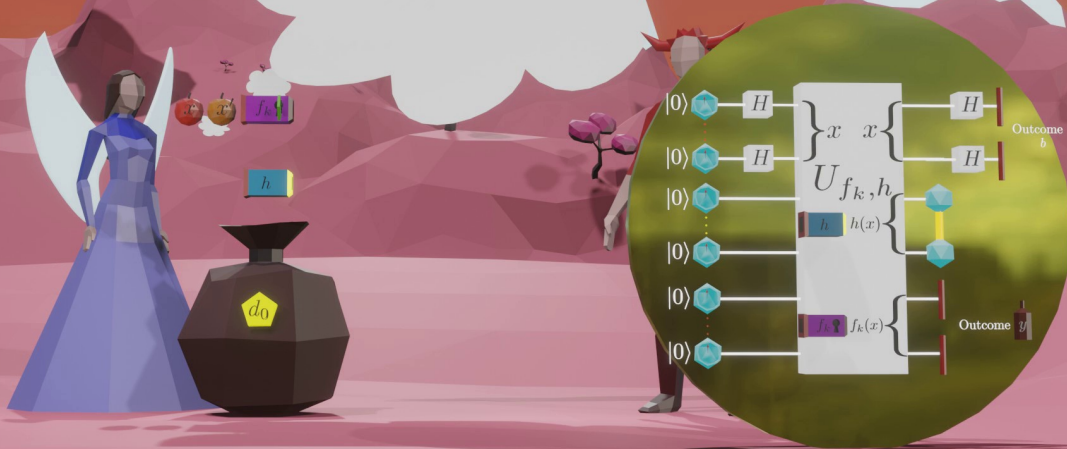
$$\rightsquigarrow \sum_b (-1)^{x \cdot b} |b\rangle |h(x)\rangle + (-1)^{x' \cdot b} |b\rangle |h(x')\rangle$$



QFactory: the protocol

$$(|x\rangle |h(x)\rangle + |x'\rangle |h(x')\rangle) |y\rangle$$

$$\rightsquigarrow \sum_b (-1)^{x \cdot b} |b\rangle |h(x)\rangle + (-1)^{x' \cdot b} |b\rangle |h(x')\rangle$$

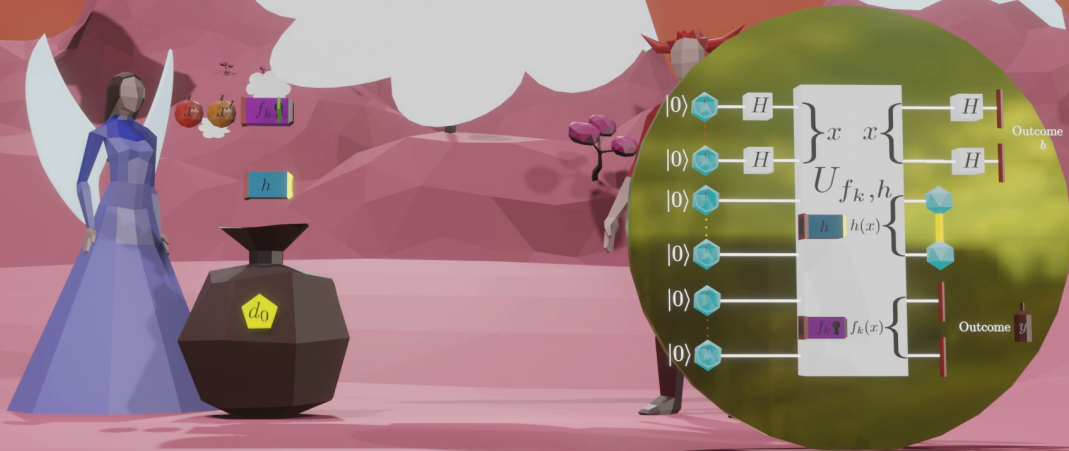


QFactory: the protocol

$$(|x\rangle |h(x)\rangle + |x'\rangle |h(x')\rangle) |y\rangle$$

$$\rightsquigarrow$$

$$(-1)^{x \cdot b} |b\rangle |h(x)\rangle + (-1)^{x' \cdot b} |b\rangle |h(x')\rangle$$

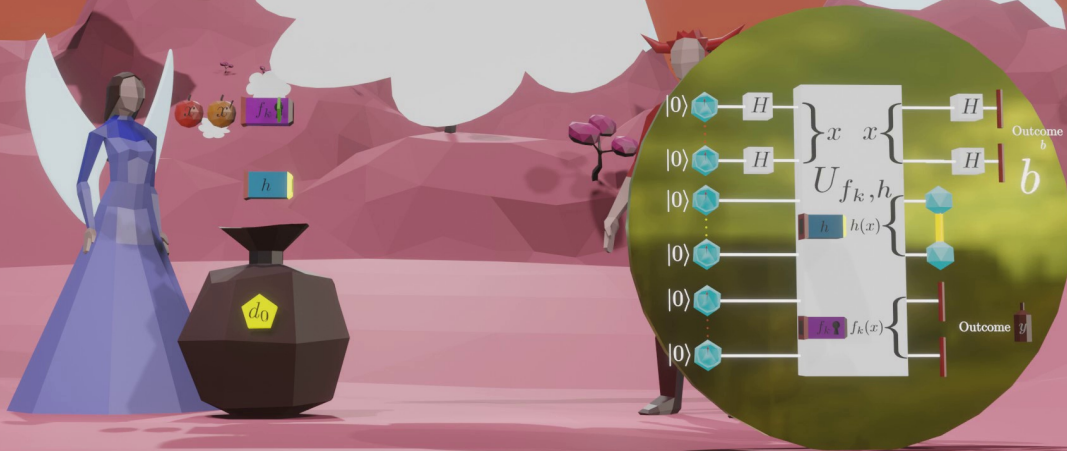


QFactory: the protocol

$$(|x\rangle |h(x)\rangle + |x'\rangle |h(x')\rangle) |y\rangle$$

$$\rightsquigarrow$$

$$(-1)^{x \cdot b} |b\rangle |h(x)\rangle + (-1)^{x' \cdot b} |b\rangle |h(x')\rangle$$

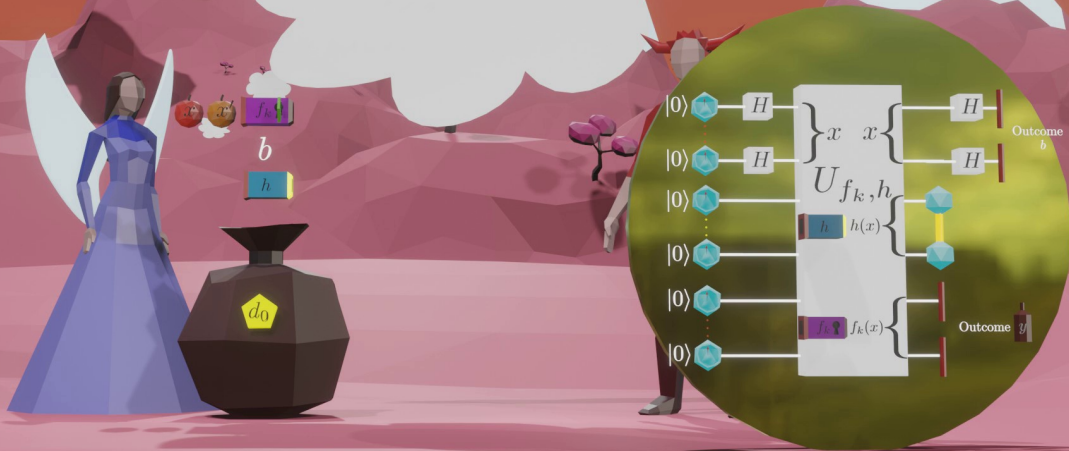


QFactory: the protocol

$$(|x\rangle |h(x)\rangle + |x'\rangle |h(x')\rangle) |y\rangle$$

$$\rightsquigarrow$$

$$(-1)^{x \cdot b} |b\rangle |h(x)\rangle + (-1)^{x' \cdot b} |b\rangle |h(x')\rangle$$

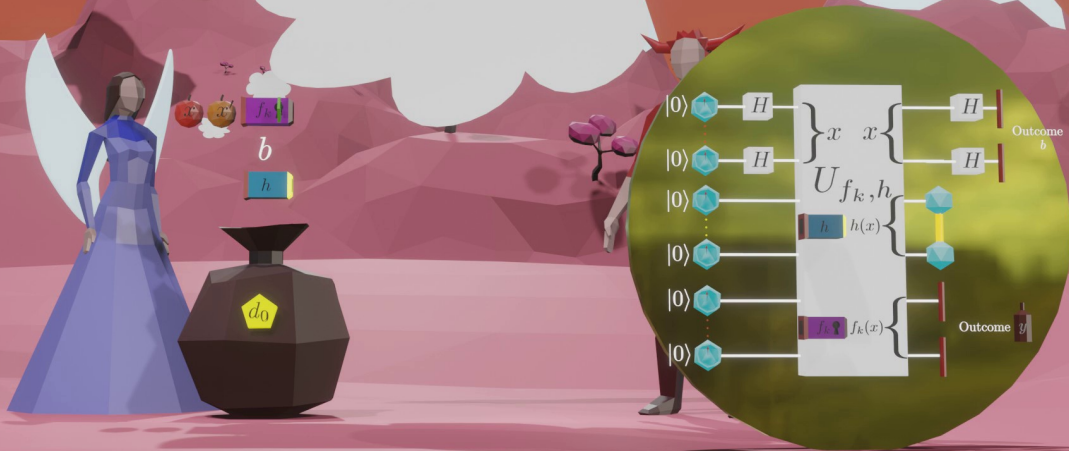


QFactory: the protocol

$$(|x\rangle |h(x)\rangle + |x'\rangle |h(x')\rangle) |y\rangle$$

$$\rightsquigarrow$$

$$|b\rangle |h(x)\rangle + (-1)^{(x \oplus x') \cdot b} |b\rangle |h(x')\rangle$$

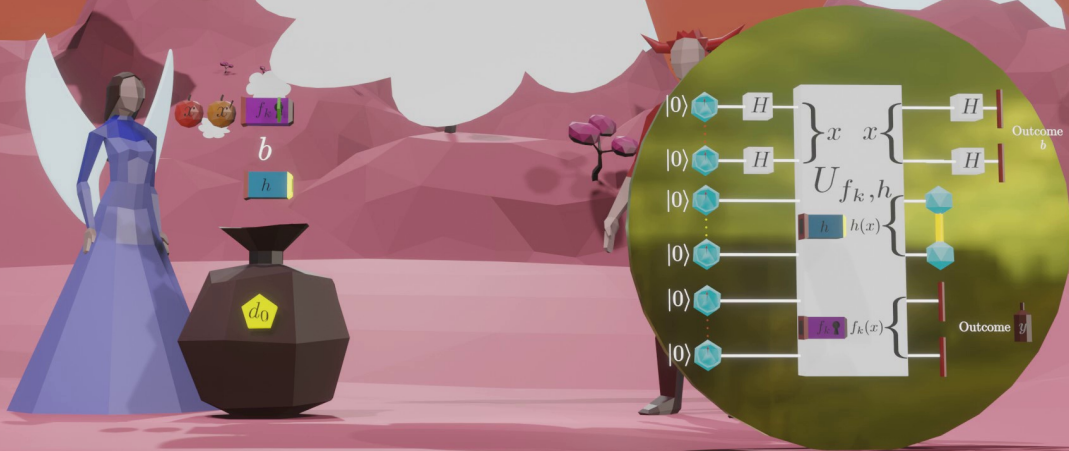


QFactory: the protocol

$$(|x\rangle |h(x)\rangle + |x'\rangle |h(x')\rangle) |y\rangle$$

$$\rightsquigarrow$$

$$|h(x)\rangle + (-1)^{(x \oplus x') \cdot b} |h(x')\rangle$$

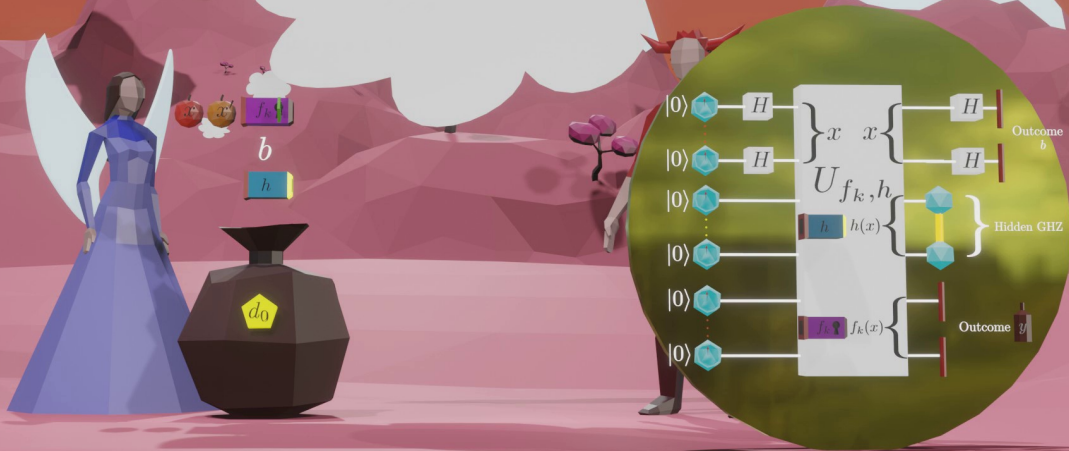


QFactory: the protocol

$$(|x\rangle |h(x)\rangle + |x'\rangle |h(x')\rangle) |y\rangle$$

$$\rightsquigarrow$$

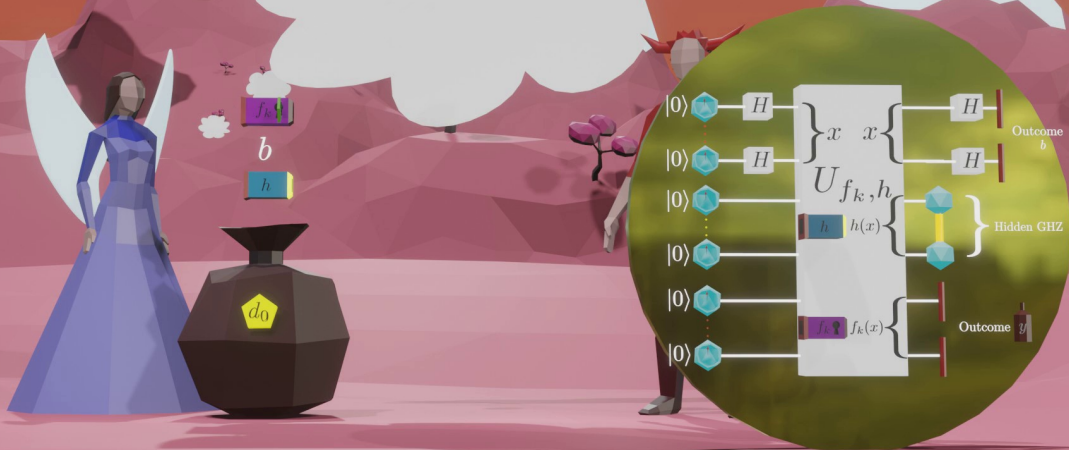
$$|h(x)\rangle + (-1)^{(x \oplus x') \cdot b} |h(x')\rangle$$



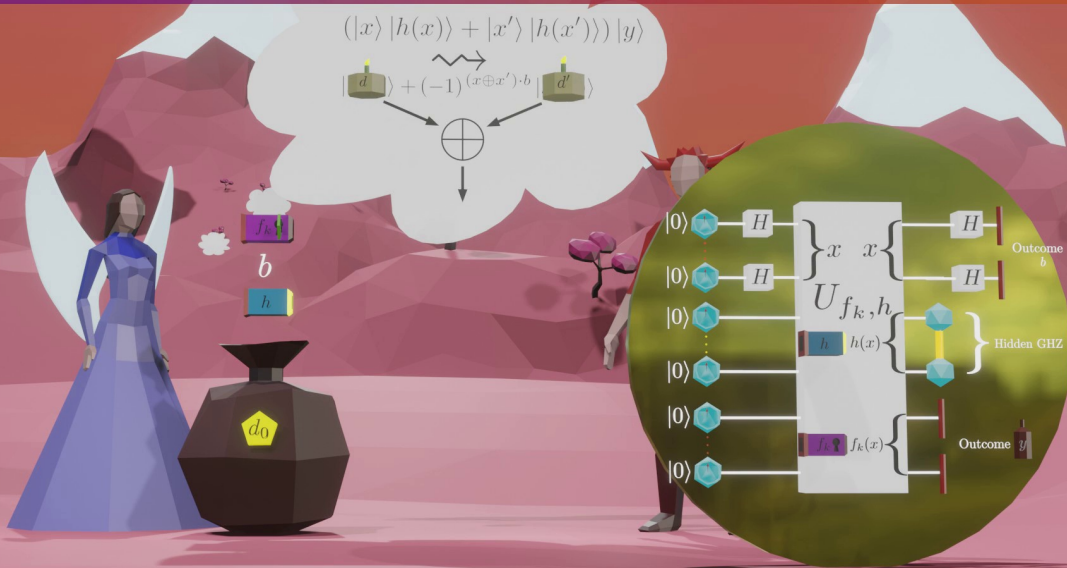
QFactory: the protocol

$$(|x\rangle |h(x)\rangle + |x'\rangle |h(x')\rangle) |y\rangle$$

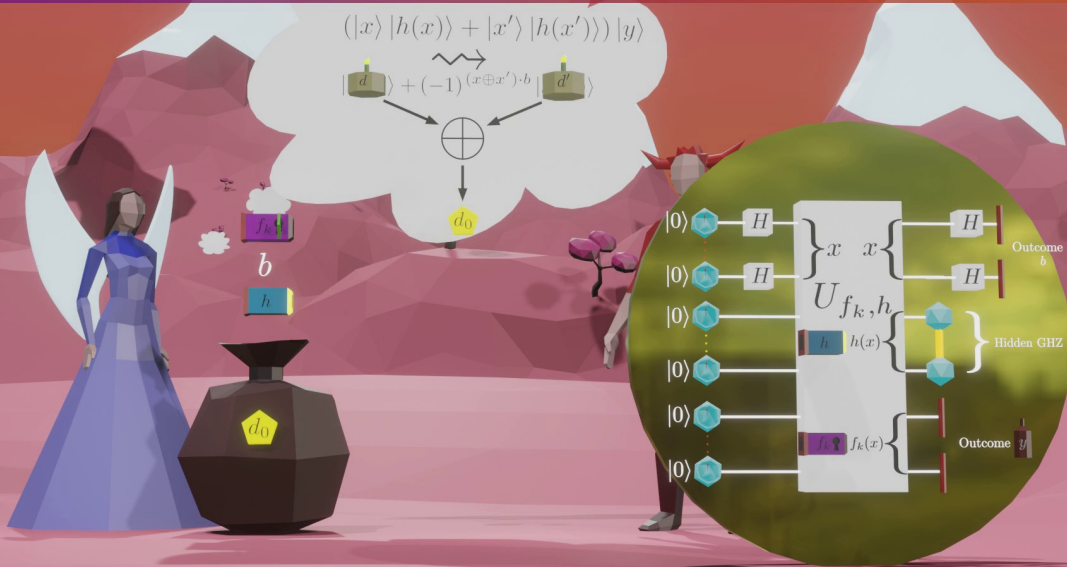
$$|d\rangle + (-1)^{(x \oplus x') \cdot b} |d'\rangle$$



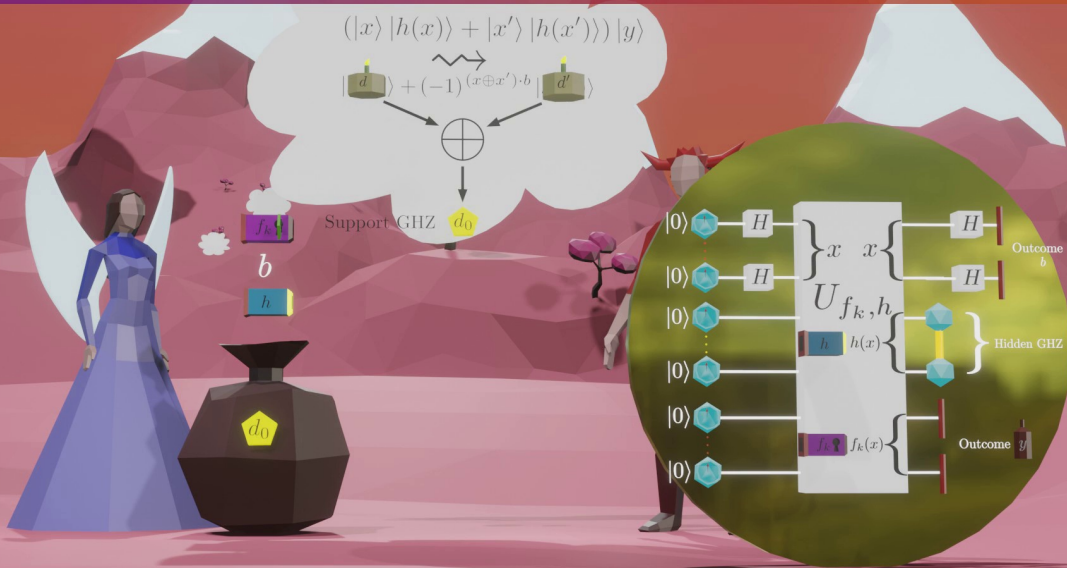
QFactory: the protocol



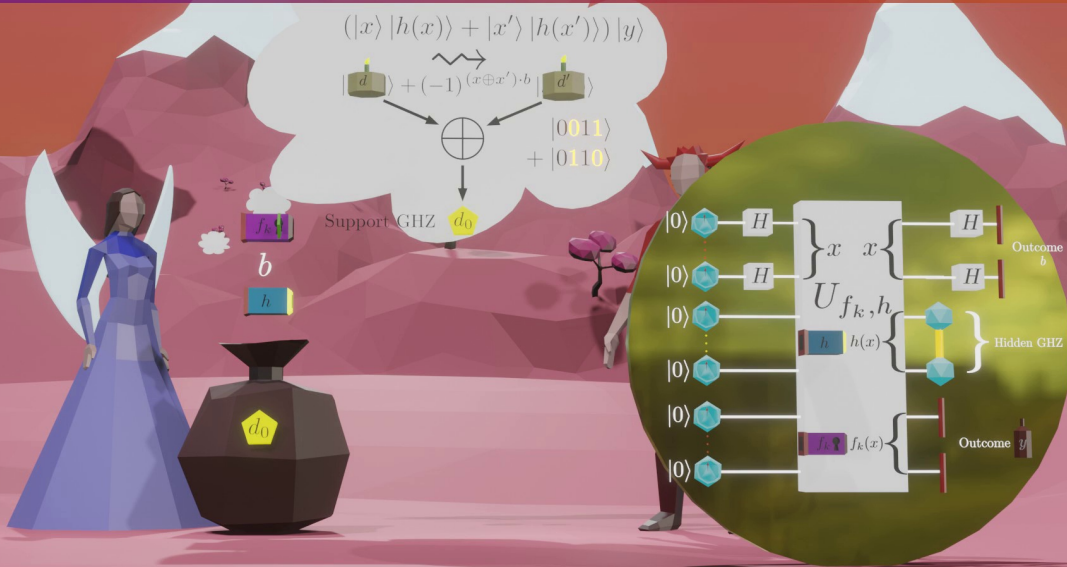
QFactory: the protocol



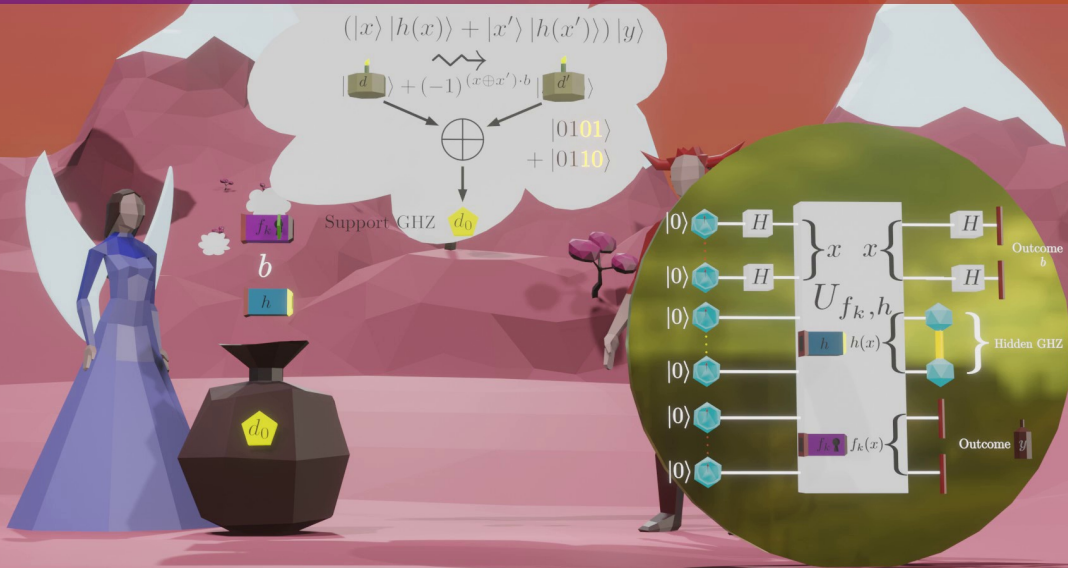
QFactory: the protocol



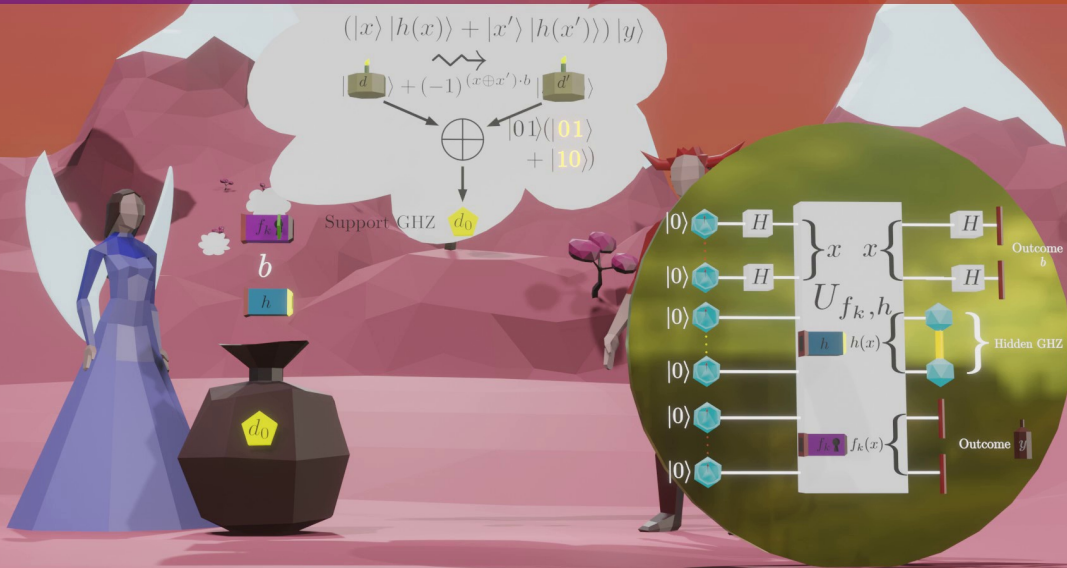
QFactory: the protocol



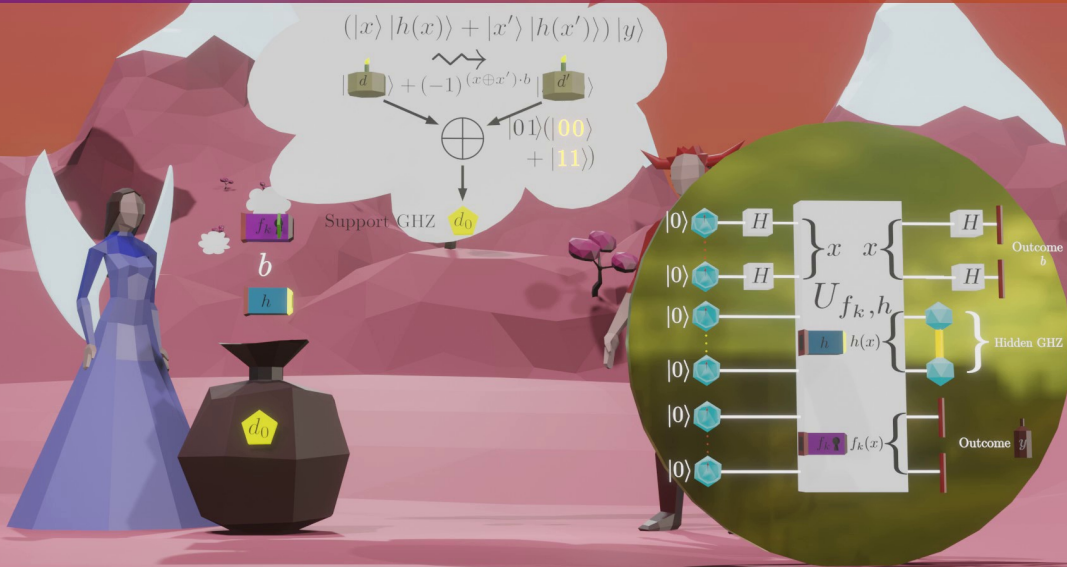
QFactory: the protocol



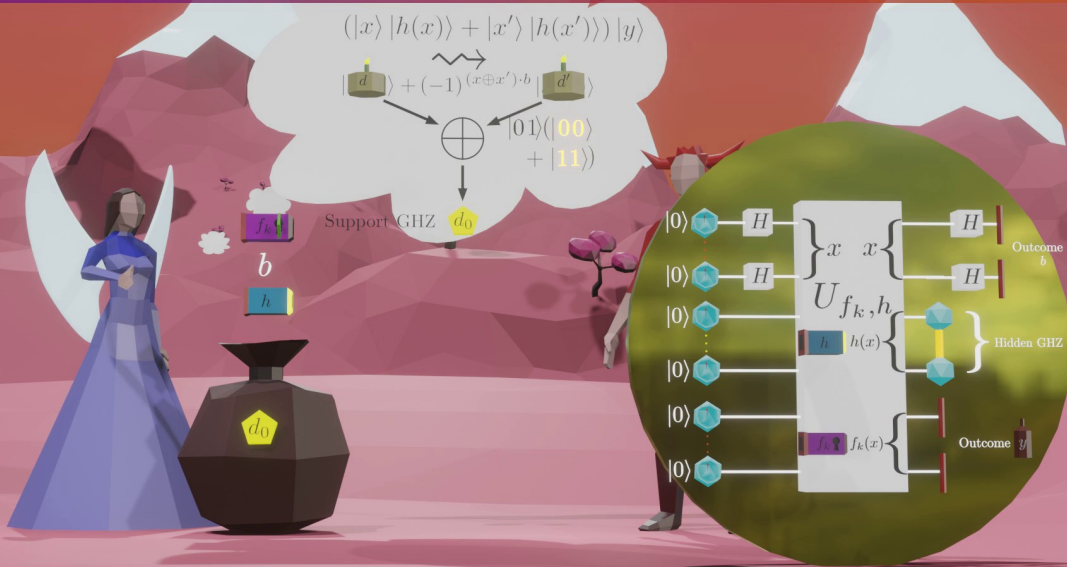
QFactory: the protocol



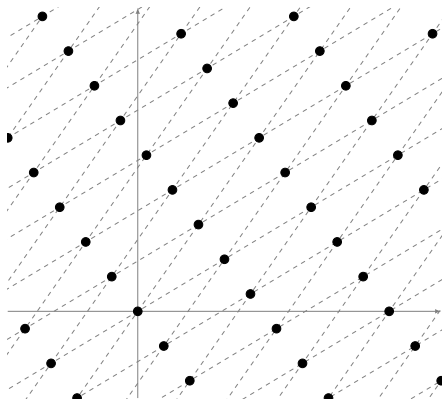
QFactory: the protocol



QFactory: the protocol



Construction de la fonction : LWE



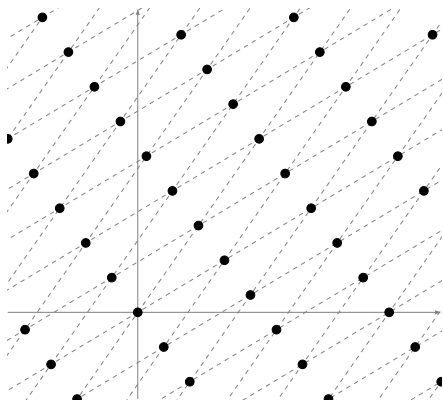
Learning With Errors (LWE)

Étant donné $\left(\mathbf{A}, \mathbf{y} \right)$, dire si $\mathbf{y}$ est

aléatoire ou $\mathbf{y} = \mathbf{A} \mathbf{s} + \mathbf{e}$, avec

$$\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{M \times N}, \mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^N, \mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}_q, \alpha q}^M.$$

Construction de la fonction : LWE



A

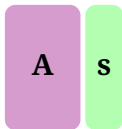
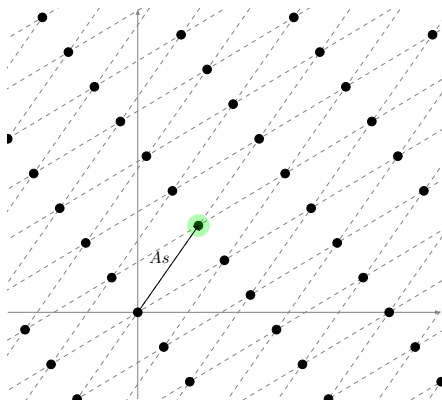
Learning With Errors (LWE)

Étant donné $\left(\begin{array}{c} \mathbf{A} \\ \mathbf{y} \end{array} \right)$, dire si $\mathbf{y}$ est

aléatoire ou $\mathbf{y} = \mathbf{A} \mathbf{s} + \mathbf{e}$, avec

$$\mathbf{A} \leftarrow \mathbb{Z}_q^{M \times N}, \mathbf{s} \leftarrow \mathbb{Z}_q^N, \mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}_q, \alpha q}^M.$$

Construction de la fonction : LWE



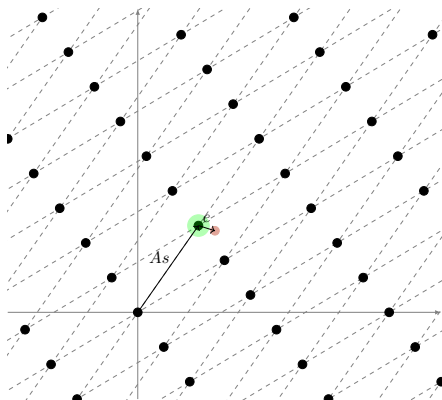
Learning With Errors (LWE)

Étant donné $\left(\begin{array}{c} \text{A} \\ \text{y} \end{array} \right)$, dire si y est

aléatoire ou $\text{y} = \text{A} \text{s} + \text{e}$, avec

$$\text{A} \xleftarrow{\$} \mathbb{Z}_q^{M \times N}, \text{ s} \xleftarrow{\$} \mathbb{Z}_q^N, \text{ e} \leftarrow \mathcal{D}_{\mathbb{Z}_q, \alpha q}^M.$$

Construction de la fonction : LWE



$$\mathbf{A} \mathbf{s} + \mathbf{e}$$

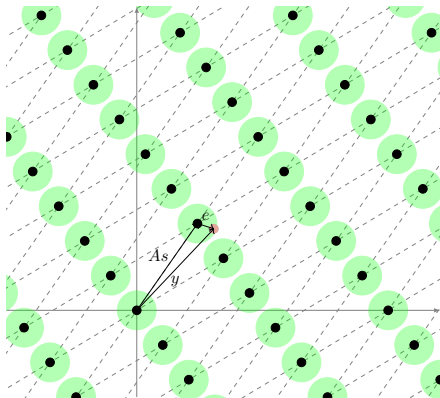
Learning With Errors (LWE)

Étant donné $\left(\mathbf{A}, \mathbf{y} \right)$, dire si $\mathbf{y}$ est

aléatoire ou $\mathbf{y} = \mathbf{A} \mathbf{s} + \mathbf{e}$, avec

$$\mathbf{A} \leftarrow \mathbb{Z}_q^{M \times N}, \mathbf{s} \leftarrow \mathbb{Z}_q^N, \mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}_q, \alpha q}^M.$$

Construction de la fonction : LWE



$$\mathbf{A} \mathbf{s} + \mathbf{e}$$

Learning With Errors (LWE)

Étant donné $(\mathbf{A}, \mathbf{y})$, dire si $\mathbf{y}$ est

aléatoire ou $\mathbf{y} = \mathbf{A} \mathbf{s} + \mathbf{e}$, avec

$$\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{M \times N}, \mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^N, \mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}_q, \alpha q}^M.$$

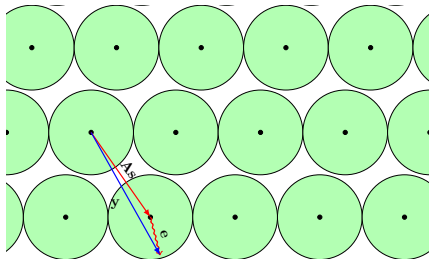
Construction de la fonction : porte dérobée

Porte dérobée [MP12]

$\left(\begin{array}{c} \text{A} \\ \text{R} \end{array} \right) \leftarrow \text{Gen}(1^\lambda), \text{ A } \text{ semble aléatoire, mais } \text{R} \text{ peut-}$
 $\text{être utilisée pour obtenir } \left(\begin{array}{c} \text{s} \\ \text{e} \end{array} \right) \text{ à partir de } \text{y} := \text{A} \text{ s} + \text{e}.$

[MP12] D. Micciancio and C. Peikert, "Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller", EUROCRYPT, 2012

Construction de la fonction



Première étape : porte dérobée

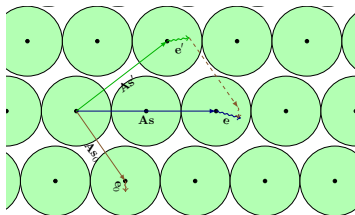
Génère $\left(\begin{array}{c} \text{A} \\ \text{R} \end{array} \right)$ avec [MP12].

La fonction suivante a une porte dérobée

$$f_{\text{A}} \left(\begin{array}{c} \text{s} \\ \text{e} \end{array} \right) := \text{A} \text{ s} + \text{e}$$

Injective si e est assez petit

Construction de la fonction



2e étape : 2-vers-1

Génère A , s_0 et e_0 :

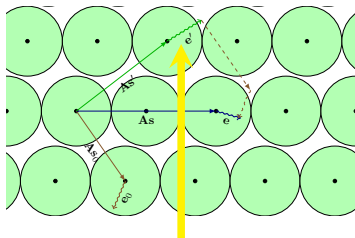
$$y_0 := A s_0 + e_0$$



$$f_{A, y_0} \left(\begin{matrix} s \\ e \\ c \end{matrix} \right) := A s + e + c \times y_0$$

$$\Rightarrow f_{A, y_0} \left(\begin{matrix} s \\ e \\ 0 \end{matrix} \right) = f_{A, y_0} \left(\begin{matrix} s - s_0 \\ e - e_0 \\ 1 \end{matrix} \right)$$

Construction de la fonction



Pas toujours 2 préimages :-(

2e étape : 2-vers-1

Génère A , s_0 et e_0 :

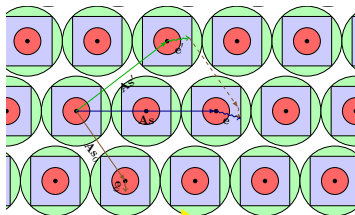
$$y_0 := A s_0 + e_0$$



$$f_{A, y_0} \left(\begin{pmatrix} s \\ e \\ c \end{pmatrix} \right) := A s + e + c \times y_0$$

$$\Rightarrow f_{A, y_0} \left(\begin{pmatrix} s \\ e \\ 0 \end{pmatrix} \right) = f_{A, y_0} \left(\begin{pmatrix} s - s_0 \\ e - e_0 \\ 1 \end{pmatrix} \right)$$

Construction de la fonction



$e_0 + \text{petit}, e$ dans un hypercube
(superposition efficace)

2e étape : 2-vers-1

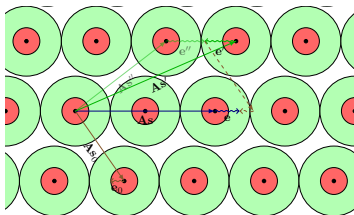
Génère A , s_0 et e_0 :

$$y_0 := A s_0 + e_0$$



$$\begin{aligned} f_{A, y_0} \left(\begin{pmatrix} s \\ e \\ c \end{pmatrix} \right) &:= A s + e + c \times y_0 \\ \Rightarrow f_{A, y_0} \left(\begin{pmatrix} s \\ e \\ 0 \end{pmatrix} \right) &= f_{A, y_0} \left(\begin{pmatrix} s - s_0 \\ e - e_0 \\ 1 \end{pmatrix} \right) \end{aligned}$$

Construction de la fonction



2e étape : 2-vers-1

Génère A , s_0 et e_0 :

$$y_0 := A s_0 + e_0$$



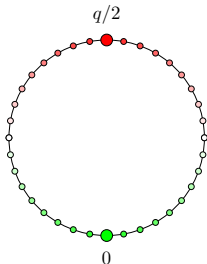
$$f_{A, y_0} \left(\begin{matrix} s \\ e \\ c \end{matrix} \right) := A s + e + c \times y_0$$

$$\Rightarrow f_{A, y_0} \left(\begin{matrix} s \\ e \\ 0 \end{matrix} \right) = f_{A, y_0} \left(\begin{matrix} s - s_0 \\ e - e_0 \\ 1 \end{matrix} \right)$$

Construction de la fonction

3e étape : propriété du XOR

Génère A , s_0 et e_0 :



$$y_0 := \begin{matrix} A_u \\ A_l \end{matrix} \begin{matrix} s_0 \\ e_{0,u} \\ e_{0,l} \end{matrix} + \frac{q}{2} \begin{matrix} 0 \\ d_0 \end{matrix}$$



$$h(x) \oplus h(x') = d_0$$

$$f_{A, y_0} \left(\begin{matrix} s \\ e \\ c \\ d \end{matrix} \right) := \begin{matrix} A_u \\ A_l \end{matrix} \begin{matrix} s \\ e_u \\ e_l \end{matrix} + c \times y_0 + \frac{q}{2} \begin{matrix} 0 \\ d \end{matrix} \quad h \left(\begin{matrix} s \\ e \\ c \\ d \end{matrix} \right) = d$$

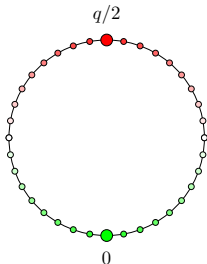
Construction de la fonction

3e étape : propriété du XOR

Génère A , s_0 et e_0 :

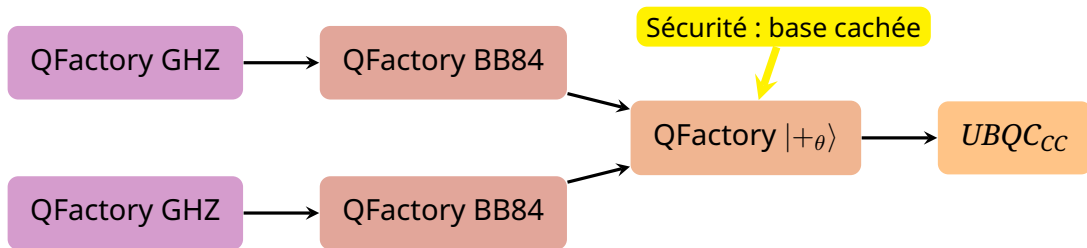
$$y_0 := \begin{matrix} A_u \\ A_l \end{matrix} \begin{matrix} s_0 \\ s_l \end{matrix} + \begin{matrix} e_{0,u} \\ e_{0,l} \end{matrix} + \frac{q}{2} \begin{matrix} 0 \\ d_0 \end{matrix}$$

$$f_{A, y_0} \left(\begin{matrix} s \\ e \end{matrix}, c, d \right) := \begin{matrix} A_u \\ A_l \end{matrix} \begin{matrix} s \\ s_l \end{matrix} + \begin{matrix} e_u \\ e_l \end{matrix} + c \times y_0 + \frac{q}{2} \begin{matrix} 0 \\ d \end{matrix} \quad h \left(\begin{matrix} s \\ e \end{matrix}, c, d \right) = d$$



Sécurité : $As+e$ indistinguishable d'un vecteur aléatoire

LWE ratio de bruit superpolynomial



LWE ratio de bruit polynomial

Astuce pour utiliser les rounds avortés et les combiner pour obtenir un BB84, mais nécessite une conjecture

Questions cryptographie quantique



Dans le calcul délégué à l'aveugle, le serveur peut renvoyer un résultat faux au client : **A** Oui **B** Non



Dans le calcul délégué à l'aveugle, un serveur avec une puissance de calcul infinie peut casser le protocole : **A** Vrai **B** Faux



Le Measurement Based Quantum Computing (MBQC) est :

- A** Une méthode pour cacher les calculs
- B** Une méthode pour cacher les calculs avec un client classique
- C** Une méthode pour faire des calculs quantiques avec des portes simples à réaliser

Questions cryptographie quantique



Dans le calcul délégué à l'aveugle, le serveur peut renvoyer un résultat faux au client : ☐ A Oui ☒ B Non



Dans le calcul délégué à l'aveugle, un serveur avec une puissance de calcul infinie peut casser le protocole : ☐ A Vrai ☐ B Faux



Le Measurement Based Quantum Computing (MBQC) est :

- ☐ A Une méthode pour cacher les calculs
- ☐ B Une méthode pour cacher les calculs avec un client classique
- ☐ C Une méthode pour faire des calculs quantiques avec des portes simples à réaliser

Questions cryptographie quantique



Dans le calcul délégué à l'aveugle, le serveur peut renvoyer un résultat faux au client : ☐ A Oui ☒ ☐ B Non



Dans le calcul délégué à l'aveugle, un serveur avec une puissance de calcul infinie peut casser le protocole : ☐ A Vrai ☒ B Faux



Le Measurement Based Quantum Computing (MBQC) est :

- ☐ A Une méthode pour cacher les calculs
- ☐ B Une méthode pour cacher les calculs avec un client classique
- ☐ C Une méthode pour faire des calculs quantiques avec des portes simples à réaliser

Questions cryptographie quantique



Dans le calcul délégué à l'aveugle, le serveur peut renvoyer un résultat faux au client : **A** Oui  **B** Non



Dans le calcul délégué à l'aveugle, un serveur avec une puissance de calcul infinie peut casser le protocole : **A** Vrai **B** Faux 



Le Measurement Based Quantum Computing (MBQC) est :

- A** Une méthode pour cacher les calculs
- B** Une méthode pour cacher les calculs avec un client classique
- C** Une méthode pour faire des calculs quantiques avec des portes simples à réaliser 

Conclusion

Conclusion

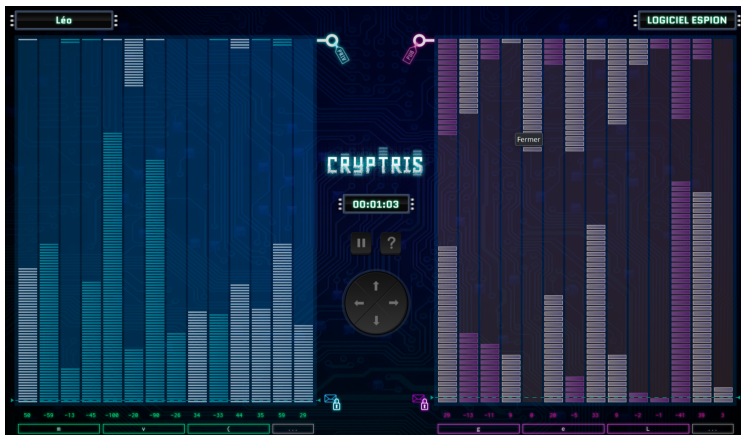
- Ordinateur quantique **casse tous les chiffrements**/signatures utilisés à l'heure actuelle sur internet
- Remplacement par **cryptographie post-quantique** (PQC, cf. standardisation NIST) d'ici 2030
- La cryptographie quantique permet d'avoir des garanties encore plus fortes (en combinaison avec PQC) = sécurité "inconditionnelle", mais encore de nombreuses difficultés pour une adoption large
- + offre de nouveaux protocoles impossibles classiquement (aléa certifié...)

Aller plus loin

- Nombreuses autres applications :
 - **Aléa certifié** (éviter/limiter backdoors)
 - ⇒ Magic Square
 - ⇒ déjà en vente ! <https://www.quantinuum.com/products-solutions/quantum-origin>
 - Monnaie quantique infalsifiable
 - Vérification de position, calcul délégué/multipartite...
- Device independent (DI)
- Certification de caractère quantique
- Sécurité des cryptomonnaies : signatures, mais également PoW
- Preuves de sécurité
- ...

Aller plus loin : tester LWE

Pour comprendre **pourquoi LWE est difficile**, essayez de **jouer** à <https://inriamecsci.github.io/cryptris/>!



A low-poly illustration featuring an angel on the left and a devil on the right, standing in a desert landscape. The angel is a woman with large white wings, wearing a long blue dress. The devil is a man with red horns and a red suit. The background consists of reddish-brown mountains with white snow-capped peaks, a few small trees, and a bright orange sky. The text "Thank you!" is centered in the foreground.

Thank you!

A low-poly illustration featuring an angel and a devil in a desert landscape. The angel, on the left, is a woman with large white wings, wearing a long blue dress. The devil, on the right, is a man with red horns and a red suit. They stand on a pinkish ground with shadows. The background consists of jagged, low-poly mountains in shades of red and orange, some with white snow. Small, stylized trees and flying insects are scattered in the mid-ground. The sky is a solid orange-red color with a few white, blocky clouds. The text "Thank you!" is centered in the lower half of the image.

Thank you!