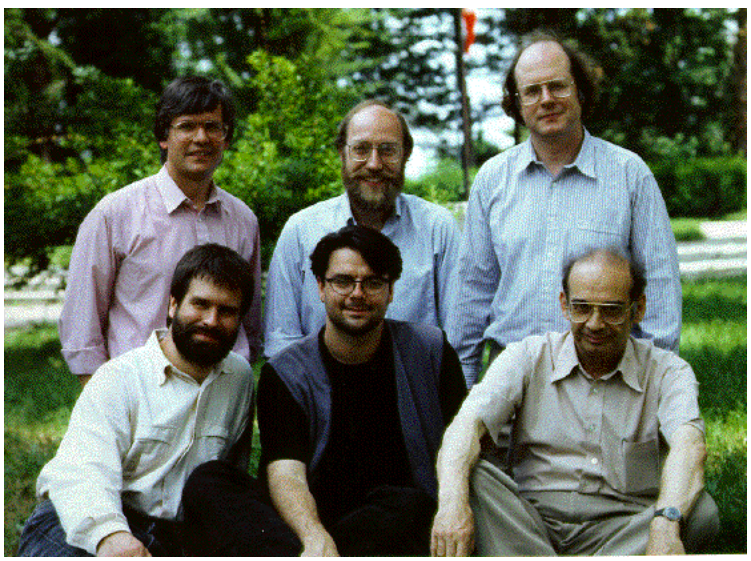


RICHARD JOSZA, WILLIAM K WOOTTERS, CHARLES BENNETT,
GILLES BRASSARD, CLAUDE CREPEAU, ASHER PERES

RECALL:

$$\text{EPR pair} = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Let us try to rewrite in basis $|v\rangle, |u\rangle$ where $u \perp v$

Let $v = \alpha|0\rangle + \beta|1\rangle$. [where $|\alpha|^2 + |\beta|^2 = 1$]

Then u (in order to be orthogonal to v) must be:

$$u = \beta|0\rangle - \alpha|1\rangle$$

$$\frac{1}{\sqrt{2}}|vv\rangle + \frac{1}{\sqrt{2}}|uu\rangle$$

$$= \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) + \frac{1}{\sqrt{2}}(\beta|0\rangle - \alpha|1\rangle)(\beta|0\rangle - \alpha|1\rangle)$$

$$= \frac{1}{\sqrt{2}}(\alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle)$$

$$+ \frac{1}{\sqrt{2}}(\beta^2|00\rangle - \alpha\beta|01\rangle - \alpha\beta|10\rangle + \alpha^2|11\rangle)$$

$$= \frac{1}{\sqrt{2}}((\alpha^2+\beta^2)|00\rangle + (\alpha^2+\beta^2)|11\rangle)$$

$$= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Bob walks away from Alice...

Alice & Bob share entanglement.

Bob walks away from Alice with his particle.

What is the state of Bob's particle?

It is the mixed state, obtained by imagining an expmt where Alice measured her particle.

Suppose Alice measures in the $\{|0\rangle, |1\rangle\}$ basis.

$$\Pr[\text{Alice sees "0"}] = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$$

Bob's particle also collapses to $|0\rangle$

$$\Pr[\text{Alice sees "1"}] = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$$

Bob's particle also collapses to $|1\rangle$

So, what is Bob's state?

* (In-class exercise)
* What if Alice measured in the $\{|+\rangle, |-\rangle\}$ basis?

Your particle is identical in the following 3 games!

---

1. Challenger | You

Toss a random coin

If heads, set $|\psi\rangle = |0\rangle$

If tails, set $|\psi\rangle = |1\rangle$

$|\psi\rangle$ →

---

2. Challenger | You

Toss a random coin

If heads, set $|\psi\rangle = |+\rangle$

If tails, set $|\psi\rangle = |-\rangle$

$|\psi\rangle$ →

---

3. Challenger | You

Prepare EPR pair

Register B →

Why is this cryptographically useful?

Intuition:

Alice	Eve

Sample

$|\psi\rangle \leftarrow \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$

Send $|\psi\rangle$ →

Eve cannot output

$|\psi\rangle \otimes |\psi\rangle$

(i.e. 2 copies of $|\psi\rangle$)

[Importantly, Eve cannot even tell whether

$|\psi\rangle$ is a computational basis state or

a Hadamard basis state]

Quantum Money

Main goal of money/currency:
avoid double spending

Since unknown quantum states cannot be cloned, so can possibly use them as banknotes!

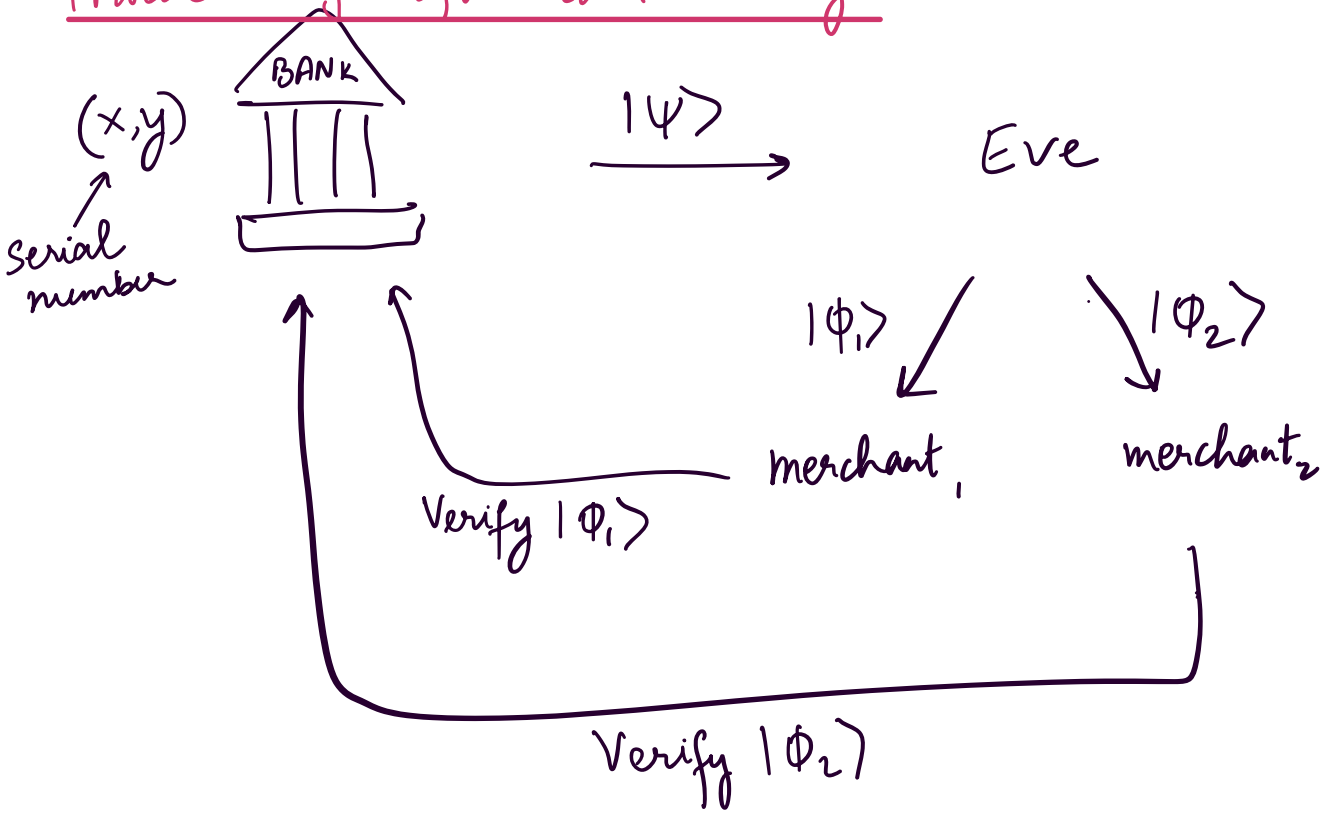
Suppose a mint only wanted to produce/circulate a single banknote.

Pick 2 bits (x, y)

Prepare $|\psi\rangle$ as follows

If xy	$\|\psi\rangle$
00	$\|0\rangle$
10	$\|1\rangle$
01	$\|+\rangle$
11	$\|-\rangle$

Private-key Quantum Money



To Verify $|\phi\rangle$, Bank measures $|\phi\rangle$ in basis y.

If outcome is x, accept. Else, reject.

Theorem: $\Pr[\text{Mint accepts } |\phi_1\rangle, |\phi_2\rangle] \leq \frac{3}{4}$

If you use n-qubit banknotes, this probability becomes $\left(\frac{3}{4}\right)^n$.

Can now release more banknotes!

This is called Wiesner money.

Classroom exercise:

Suppose each time you query bank on $|\phi\rangle$, it returns $|\phi\rangle$ along with Y/N. Using repeated queries to Bank, can you clone $|\psi\rangle$?

This happens because a Y/N answer leaks information about the serial number.

Public-Key Quantum Money

Mint outputs $(\sigma, |\psi\rangle)$

σ: serial number

$|\psi\rangle$: note

Anybody (including merchants themselves) can verify a banknote.

The previous scheme fails when σ is released so it is not a public-key scheme.

Quantum Key Distribution

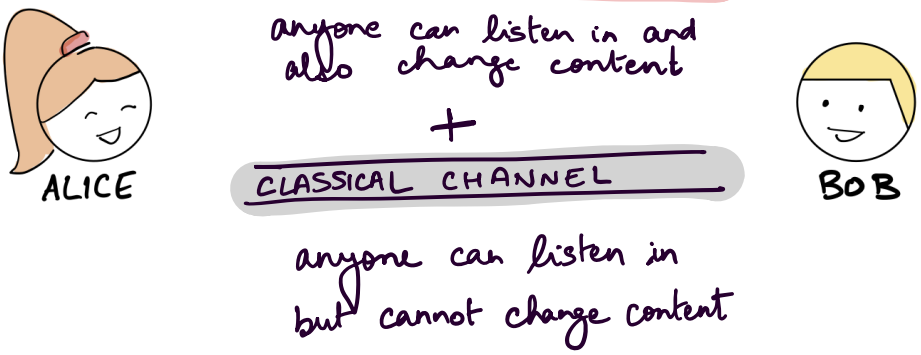
Agree on a common, shared key.

Classically, this is impossible unless you assume that eavesdropper cannot solve certain hard mathematical problems.

Quantumly, no such assumptions needed!

Can agree on such a key simply based on the laws of quantum mechanics!

QKD : THE SETTING



Classroom exercise :

Some naïve solutions ?