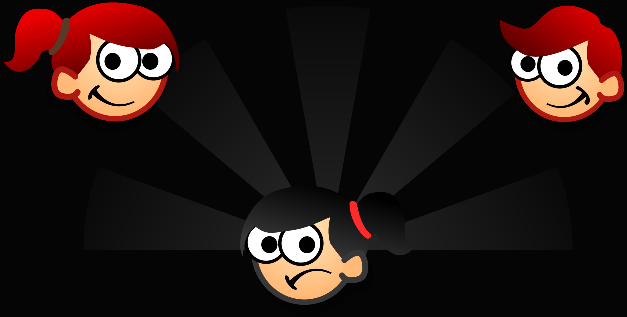
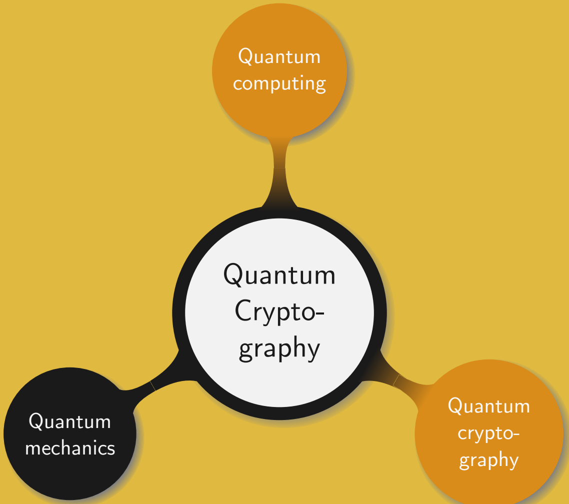


Introduction to Cryptography

9. Quantum Cryptography

Manuel – Summer 2021

Chapter organisation



Quantum mechanics

Basics on quantum mechanics:

- Physics at the atomic and subatomic levels
- Accurate and precise theory
- The state of the system is not given by a physical observation
- Impossible to know exactly the state of the system
- Probabilistic predictions can be made

Formalism

Mathematical formulation:

- Every system is associated with a separable Hilbert space H
- A state of the system is represented by a unit vector in H
- The *Ket A* denoted $|A\rangle$ represents the column vector $A = a_1|e_1\rangle + a_2|e_2\rangle + \cdots + a_n|e_n\rangle$, where $|e_1\rangle, \ldots, |e_n\rangle$ form a basis for H

$$|A\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

- The *Bra B* denoted $\langle B|$ is the conjugate transpose of $|B\rangle$

$$\langle B| = \begin{pmatrix} b_1^* & b_2^* & \cdots & b_n^* \end{pmatrix}$$

Formalism

Mathematical formulation:

- The *inner product* of B and A is

$$\langle B|A\rangle = b_1^* a_1 + b_2^* a_2 + \cdots + b_n^* a_n$$

- The *outer product* of A and B is the tensor product of A and B and is denoted

$$|A\rangle\langle B| = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \otimes \begin{pmatrix} b_1^* & b_2^* & \cdots & b_n^* \end{pmatrix} = \begin{pmatrix} a_1 b_1^* & a_1 b_2^* & \cdots & a_1 b_n^* \\ a_2 b_1^* & a_2 b_2^* & \cdots & a_2 b_n^* \\ \vdots & \vdots & \ddots & \vdots \\ a_n b_1^* & a_n b_2^* & \cdots & a_n b_n^* \end{pmatrix}$$

- An *observable* quantity is represented by an Hermitian matrix M

Quantum Principles

Basic ideas behind quantum physics:

- M can be unitarily diagonalized
- The possible outcomes of M are its eigenvectors
- Its eigenvectors $|\phi_i\rangle$, $1 \leq i \leq n$, generate an orthogonal basis
- Any vector $|\psi\rangle$ can be written as a *superposition* of the $|\phi_i\rangle$
$$|\psi\rangle = c_1|\phi_1\rangle + \cdots + c_n|\phi_n\rangle$$
- A measurement of M results in $|\phi_i\rangle$ with probability $|c_i|^2$
- Two quantum objects, whose states can only be described with reference to each other, are said to be *entangled*

Example

For $|A\rangle = \begin{pmatrix} 1/2 \\ 1/2 \\ 1/2 \\ 1/2 \end{pmatrix}$, $\langle A|A\rangle = \begin{pmatrix} 1/2 & 1/2 & 1/2 & 1/2 \end{pmatrix} \cdot \begin{pmatrix} 1/2 \\ 1/2 \\ 1/2 \\ 1/2 \end{pmatrix} = 1$, and

$$\begin{aligned} |A\rangle\langle A| &= \begin{pmatrix} 1/2 \\ 1/2 \\ 1/2 \\ 1/2 \end{pmatrix} \otimes \begin{pmatrix} 1/2 & 1/2 & 1/2 & 1/2 \end{pmatrix} \\ &= \begin{pmatrix} 1/4 & 1/4 & 1/4 & 1/4 \\ 1/4 & 1/4 & 1/4 & 1/4 \\ 1/4 & 1/4 & 1/4 & 1/4 \\ 1/4 & 1/4 & 1/4 & 1/4 \end{pmatrix}. \end{aligned}$$

Example

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

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

Given two particles which can collapse in the states 0 or 1, the four possible outcomes are $|00\rangle,\ |01\rangle,\ |10\rangle,\ |11\rangle$.

The general state of the two particles is given by the superposition

$$|\psi\rangle = a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle, \text{ with } \sum_{i=0}^{3} |a_i|^2 = 1.$$

Some states might be written as a product of states for each particle. For instance

$$\frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right).$$

However in some other cases, such as $\frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$, it cannot be factorized. The particles are then said to be entangled.

EPR paradox

Einstein Podolsky Rosen paper (1935):

- Two particles interact and get entangled
- They form a system which remains in this superposition until a measurement is performed
- The two particles travel far from each other

For instance if a measurement is realised on the first particle from the previous example (9.8) and the outcome is $|0\rangle$ then the second particle must be in state $|1\rangle$.

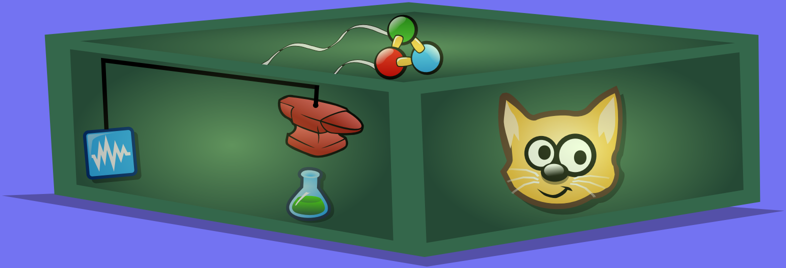
This idea conflicts with the theory of relativity which states that nothing can travel faster than the speed of light. In fact the measurement of $|0\rangle$ on the first particle implies probability 1 of getting $|1\rangle$ whatever the distance between the two particles.

Schrödinger’s cat

Basic idea: create a system where a radioactive atom is “entangled with a cat”. If the atom decays and emit radiation some poison is released and the cat dies.

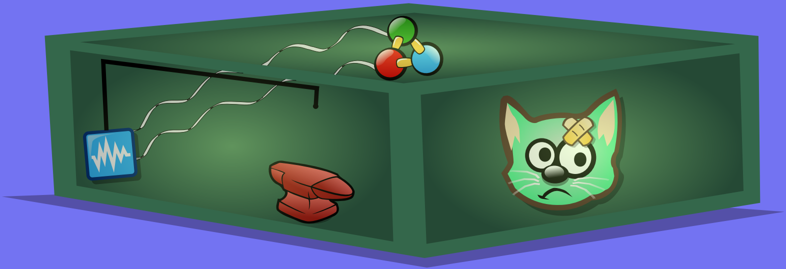
Schrödinger's cat

Basic idea: create a system where a radioactive atom is "entangled with a cat". If the atom decays and emit radiation some poison is released and the cat dies.



Schrödinger's cat

Basic idea: create a system where a radioactive atom is "entangled with a cat". If the atom decays and emit radiation some poison is released and the cat dies.



Schrödinger's cat

Basic idea: create a system where a radioactive atom is "entangled with a cat". If the atom decays and emit radiation some poison is released and the cat dies.

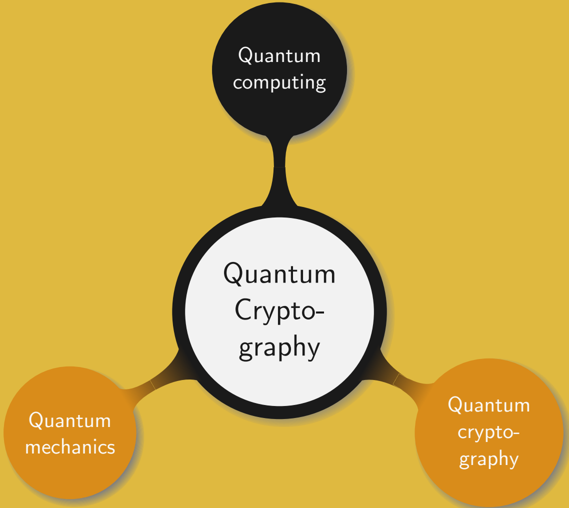
Quantum teleportation

High level idea:

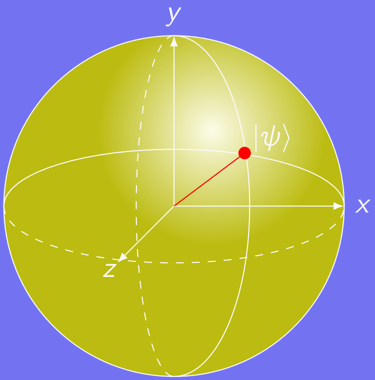
- Alice and Bob meet to construct an EPR pair (A, B), Alice takes A and Bob B
- Alice wants to share quantum information on a particle C with Bob
- Alice creates an EPR pair (A, C) such that A, B, and C are now entangled
- Alice measures A such that B collapses in a state that “resembles” the state of C
- Using a classical channel Alice sends the state of A to Bob
- When Bob knows the state of A he can easily work out the state C is in

Experiencing quantum mechanics

Chapter organisation



Bit vs. Qubit

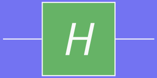


- A *qubit* is to a quantum computer, what a bit is to a classical computer
- A qubit can be in any superposition of the states $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- Several entangled qubits taken together form a *register*
- A *quantum gate* is a unitary transform on a fixed number of qubits
- A *quantum circuit* is a set of quantum gates linked together

Quantum gates

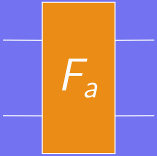
Hadamard transform:

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



Inverse the phase of the third state in a superposition of two qubits:

$$F_a = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

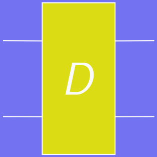


More generally $F_a|x\rangle = \begin{cases} -|a\rangle & \text{if } x = a \\ |x\rangle & \text{otherwise} \end{cases}$

Quantum gates

Diffusion transform for a superposition of two qubits:

$$D = \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$$

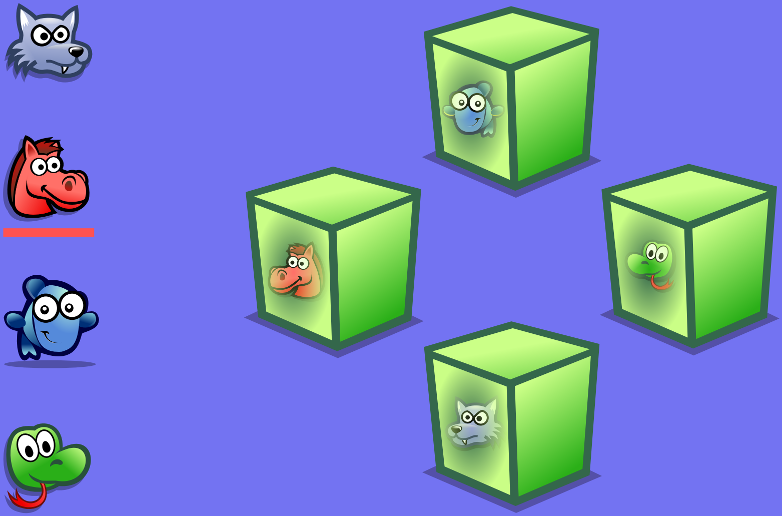


Calling the initial superposition of n states $|\psi_0\rangle$ it is generalized as

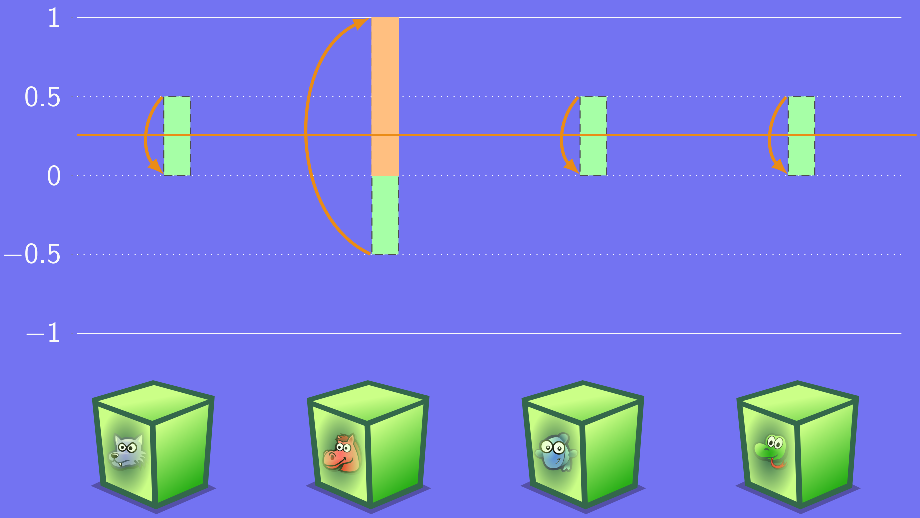
$$D = 2|\psi_0\rangle\langle\psi_0| - I_n,$$

where I_n is the identity matrix of dimension n.

A quantum search



Grover's algorithm



Finding the horse

For the sake of simplicity we define *wolf* $= |00\rangle$, *horse* $= |01\rangle$, *fish* $= |10\rangle$, and *snake* $= |11\rangle$. Therefore only two qubits are needed.

We start with the superposition

$$\frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right) = \frac{1}{2}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}.$$

This is achieved by setting the two qubits to $|0\rangle$ an applying an Hadamard transform to each of them:

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}.$$

Finding the horse

Then applying the transform F_{horse} yields

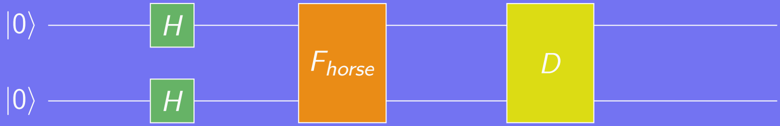
$$\frac{1}{2}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & -1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1\\1\\1\\1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1\\-1\\1\\1\end{pmatrix}.$$

Finally after applying D we get

$$\frac{1}{4}\begin{pmatrix}-1 & 1 & 1 & 1\\ 1 & -1 & 1 & 1\\ 1 & 1 & -1 & 1\\ 1 & 1 & 1 & -1\end{pmatrix}\begin{pmatrix}1\\-1\\1\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}.$$

Quantum circuit

In the case of four elements this can be represented using the following quantum circuit.



This can easily be extended to a set of n elements, by using a register of $\log_2 n$ qubits. Hadamard transforms are applied to get the superposition

$$|s\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle.$$

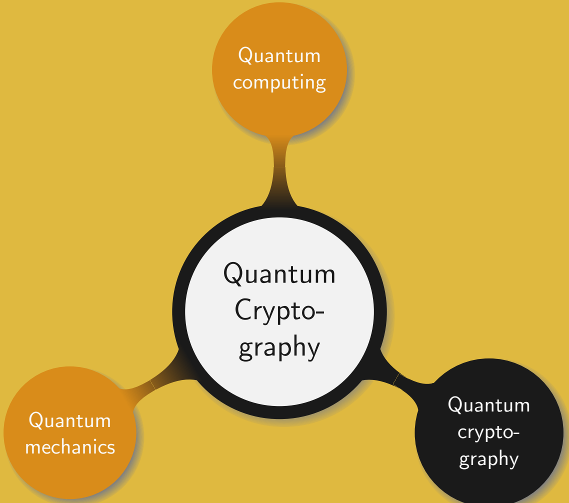
The horse can be found by repetitively applying the F_{horse} and D transforms $O(\sqrt{n})$ times.

Quantum computing and cryptography

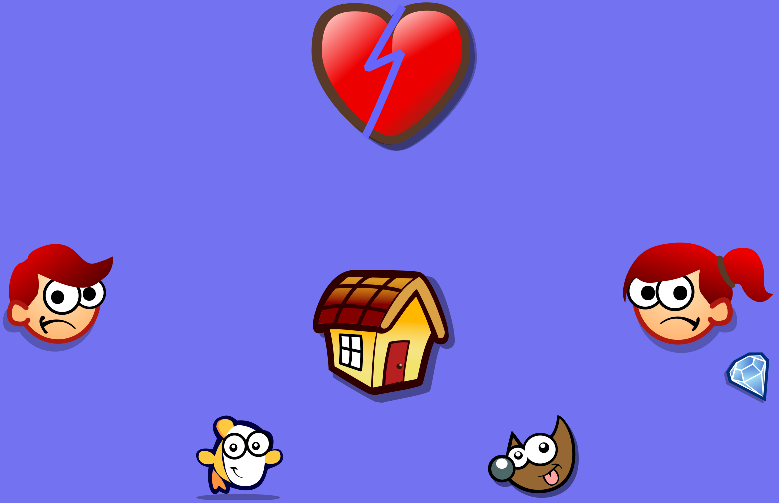
A few additional remarks:

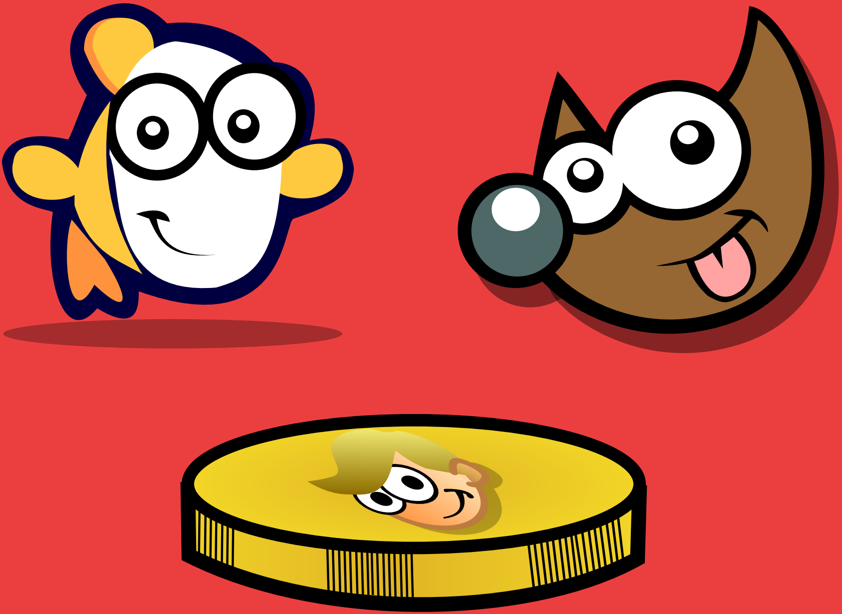
- Grover's algorithm can be used to find collisions in $\mathcal{O}(n^{1/3})$ queries
- Quantum algorithms solving the RSA and the DLP in polynomial time exist
- The actual record, established in 2012, is $56153 = 233 \cdot 241$
- Several hard problems in multivariate and lattice cryptography cannot be solved in polynomial time on a quantum computer

Chapter organisation



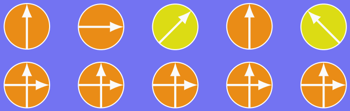
The true story of Alice and Bob

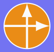




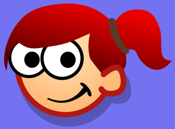
Quantum bit commitment

3 Commit to b by choosing a basis for the measurements

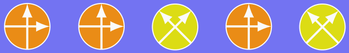


4 Send to Alice with $b =$ 

1 0 1 1 1

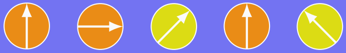


1 Pick n elements in $\{0, 1\}$ and n basi at random

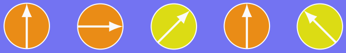


1 0 0 1 1

2 Send to Bob



5 Only verify qubits in base b



1 0 1

Security

Security of the protocol:

- Alice generates the 0,1 and the basis but has no idea on b, so she cannot cheat
- If Bob has access to a large quantum memory he can copy the qubits, measure them in a basis and their copy in the other basis
- Qubits are very hard to store, so it is a fair assumption to assume that Bob cannot store the n qubits
- As a measurement destroys the information he cannot measure again in another basis and as such he cannot cheat

Bit commitment

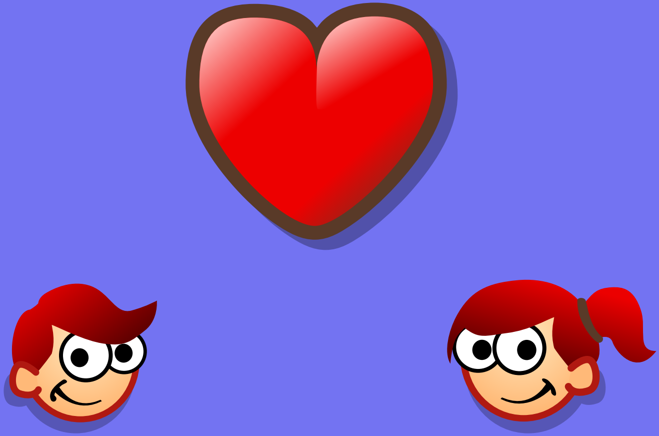
Bit commitment protocols are very simple, and can easily be realised without the help of quantum cryptography.

Example. Simple bit commitment protocol:

- Bob generates a 100-bit long string
- He appends his bit b and another 100-bit long string
- He sends the hash of the 201-bit long string to Alice
- To reveal b Bob sends the 201-bit long string

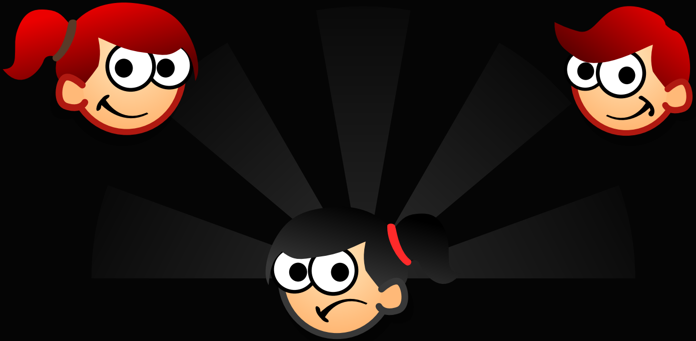
The end...

While figuring out a bit commitment protocol Alice and Bob forgot why they wanted to get a divorce and they fell in love again...



Key points

- For two particles what does it mean to be entangled?
- What is a qubit?
- What is the advantage of quantum computing over classical computing?
- What is a bit commitment protocol?



Thank you!