Quantum Cryptography

Anna Pappa

16 February 2017

Cyber technologies are everywhere

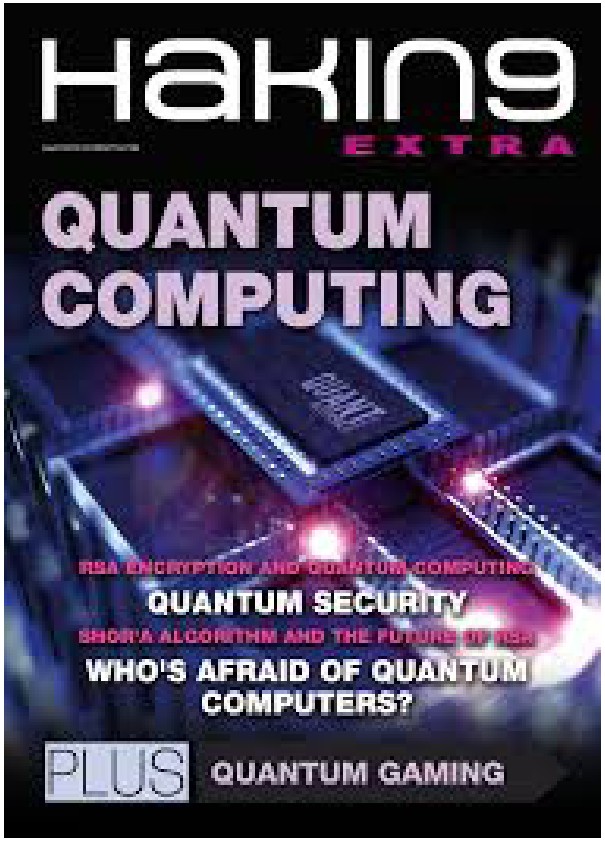
Goal: Secure and efficient network of untrusted agents and devices who transmit information, perform distributed computational tasks, delegate computation to large-scale servers, etc.

Security threats are everywhere

- Broken Cryptosystems
- Hacking attacks
- Malicious software
- Side-channel attacks

Quantum Computers: A new threat

- A quantum computer can break RSA [Shor94]
- A quantum computer can break Elliptic curves [Shor94]



Quantum Computers: A new opportunity

Harnessing the power of quantum mechanical effects

- Faster computations
- Efficient algorithms
- Improved security

Towards a solution: Quantum-safe infrastucture

Post-quantum cryptography: Classical cryptosystems resistant against quantum attacks

- Lattice-based cryptography
- Multivariate polynomials
- ...

Quantum cryptography: Cryptosystems that use quantum technologies

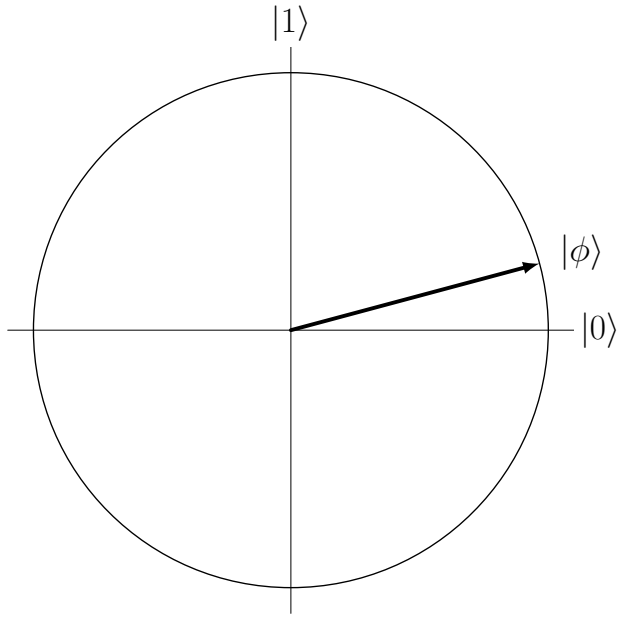
- Quantum Key Distribution
- Quantum signatures
- ...

The qubit

- Unit vector in a two-dimensional complex vector space

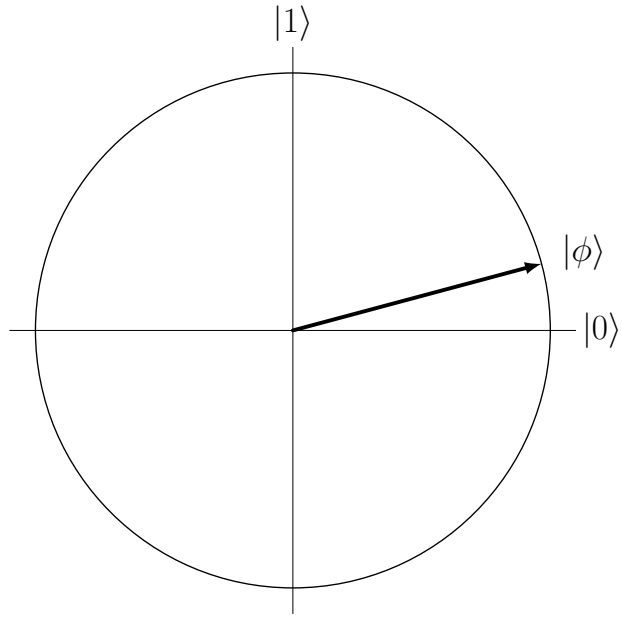
Linear superposition of two states (ex: $|0\rangle$ and $|1\rangle$):

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle, \text{ where } \alpha, \beta \in \mathcal{C} \text{ and } |\alpha|^2 + |\beta|^2 = 1$$



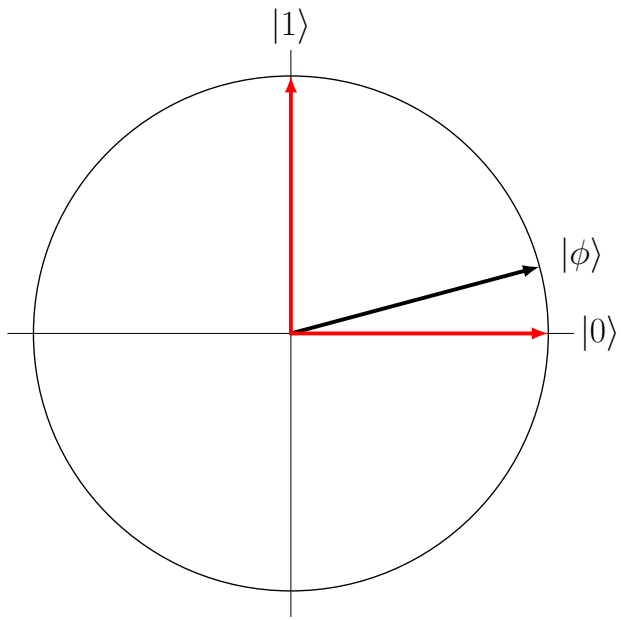
Properties of quantum states

- An unknown state cannot be copied



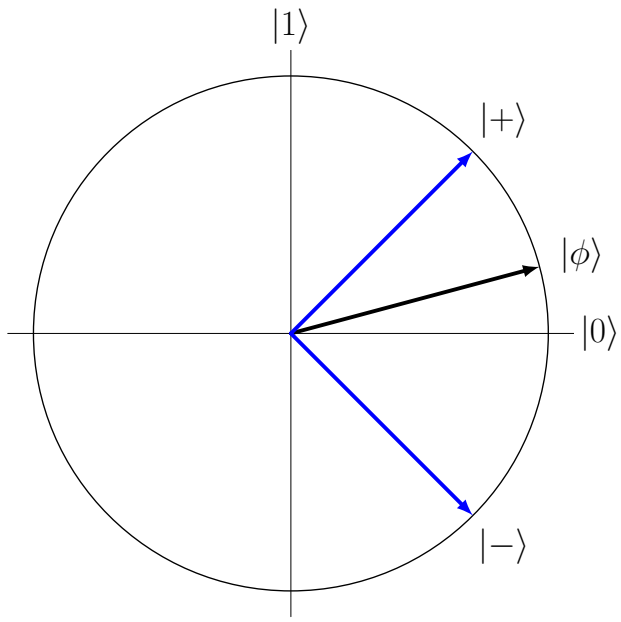
Properties of quantum states

- An unknown state cannot be copied
- After the measurement, the state collapses to one of the basis states



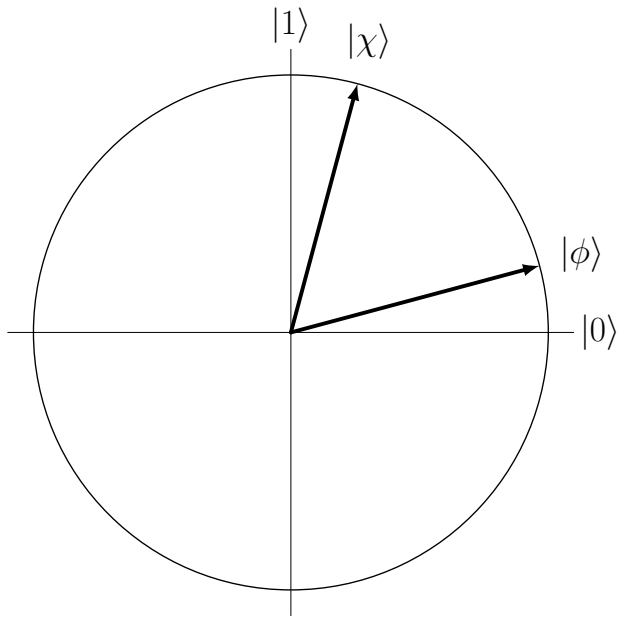
Properties of quantum states

- An unknown state cannot be copied
- After the measurement, the state collapses to one of the basis states



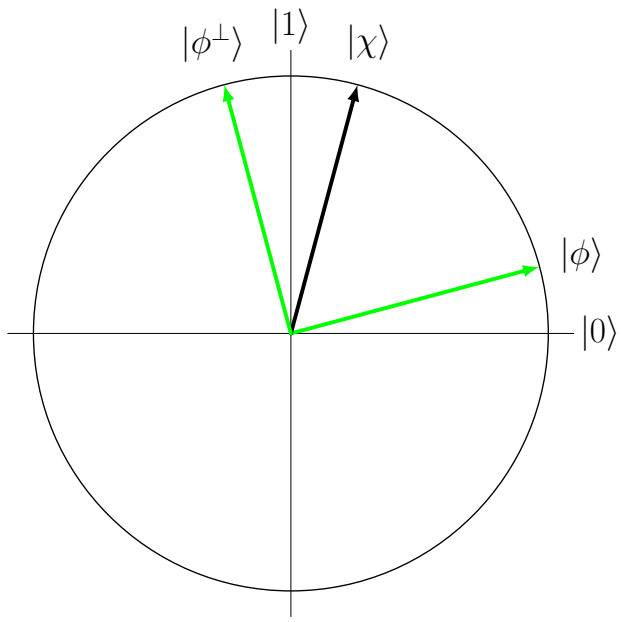
Properties of quantum states

- An unknown state cannot be copied
- After the measurement, the state collapses to one of the basis states
- There is no way to perfectly distinguish between two non-orthogonal states



Properties of quantum states

- An unknown state cannot be copied
- After the measurement, the state collapses to one of the basis states
- There is no way to perfectly distinguish between two non-orthogonal states



Quantum Key Distribution

quantum

classical

channel

channel

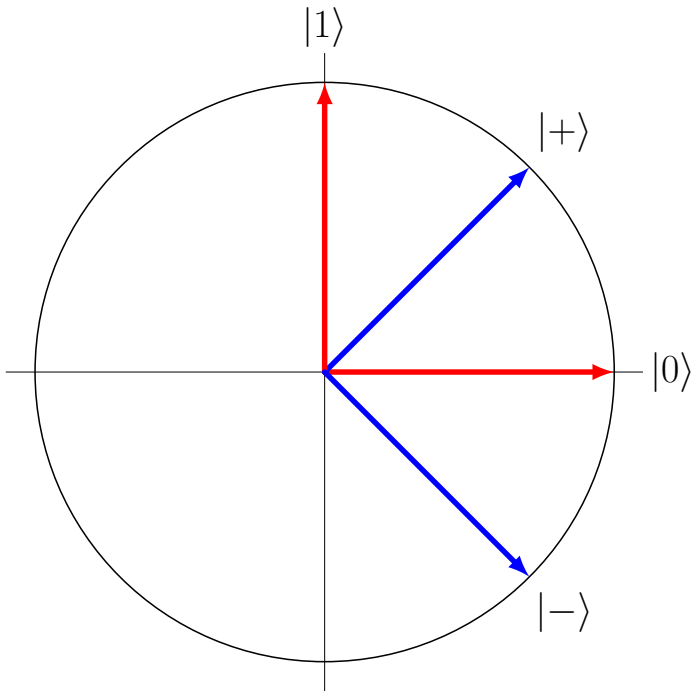
The goal is to establish a secret key between Alice and Bob

The BB84 protocol

The protocol uses the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

We define the measurement bases:

$$\begin{aligned} \mathcal{B}_0 &= \{|0\rangle, |1\rangle\} \\ \mathcal{B}_1 &= \{|+\rangle, |-\rangle\} \end{aligned}$$



The BB84 protocol

1. Alice chooses random states from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and sends them to Bob.
2. For each one, Bob chooses $\mathcal{B}_0$ or $\mathcal{B}_1$ and measures.
3. They announce the bases of the states and keep the ones they agree on ($\approx 50\%$).
4. They announce the bits of half of the remaining states. If they agree, then the remaining bits are the secret key.

The BB84 protocol

1. Alice chooses random states from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and sends them to Bob.
2. For each one, Bob chooses $\mathcal{B}_0$ or $\mathcal{B}_1$ and measures.
3. They announce the bases of the states and keep the ones they agree on ($\approx 50\%$).
4. They announce the bits of half of the remaining states. If they agree, then the remaining bits are the secret key.

The BB84 protocol

1. Alice chooses random states from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and sends them to Bob.
2. For each one, Bob chooses $\mathcal{B}_0$ or $\mathcal{B}_1$ and measures.
3. They announce the bases of the states and keep the ones they agree on ($\approx 50\%$).
4. They announce the bits of half of the remaining states. If they agree, then the remaining bits are the secret key.

The BB84 protocol

1. Alice chooses random states from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and sends them to Bob.
2. For each one, Bob chooses $\mathcal{B}_0$ or $\mathcal{B}_1$ and measures.
3. They announce the bases of the states and keep the ones they agree on ($\approx 50\%$).
4. They announce the bits of half of the remaining states. If they agree, then the remaining bits are the secret key.

The BB84 protocol - Security

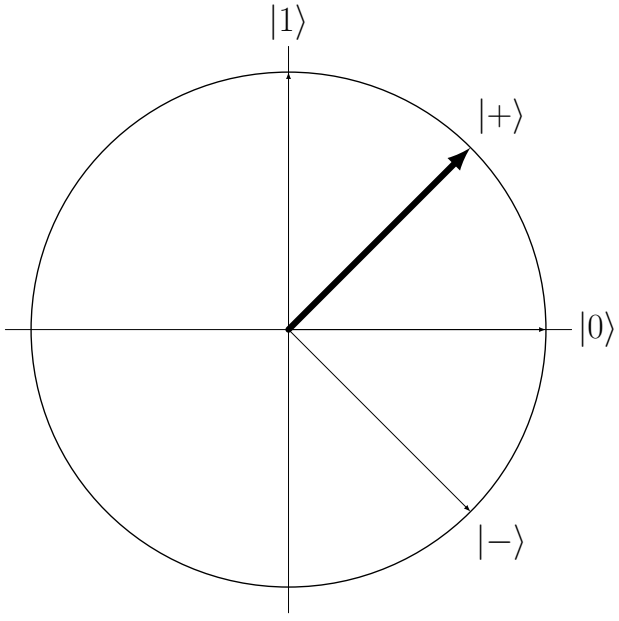
- Eve cannot clone the state and wait for the bases announcement to measure.
- If Eve measures the states, she disrupts them.

The BB84 protocol - Security

- Eve cannot clone the state and wait for the bases announcement to measure.
- If Eve measures the states, she disrupts them.

The BB84 protocol - Security

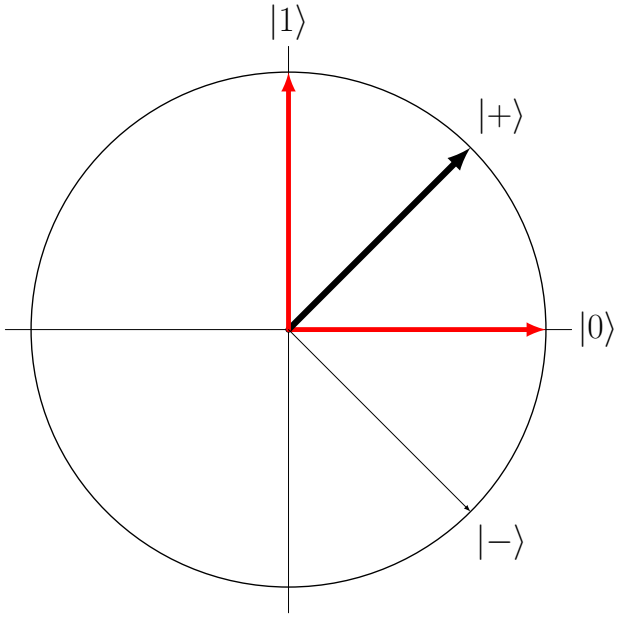
Eve picks a basis, measures the qubit and sends the result to Bob.



The BB84 protocol - Security

Eve picks a basis, measures the qubit and sends the result to Bob.

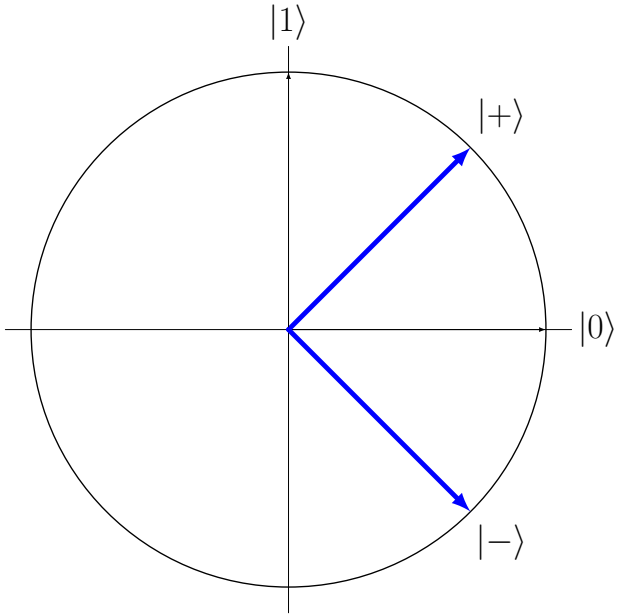
- If Bob and Alice choose different bases, they disregard the bit



The BB84 protocol - Security

Eve picks a basis, measures the qubit and sends the result to Bob.

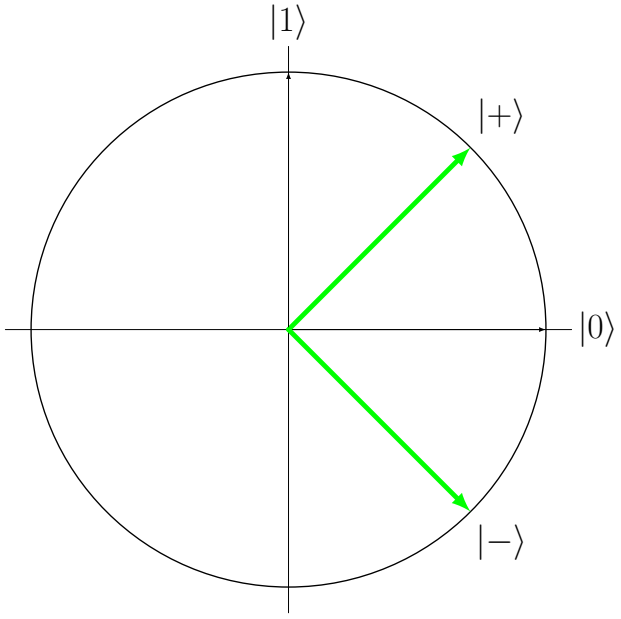
- If Bob and Alice choose different bases, they disregard the bit
- If all three choose the same basis, Eve is not detected



The BB84 protocol - Security

Eve picks a basis, measures the qubit and sends the result to Bob.

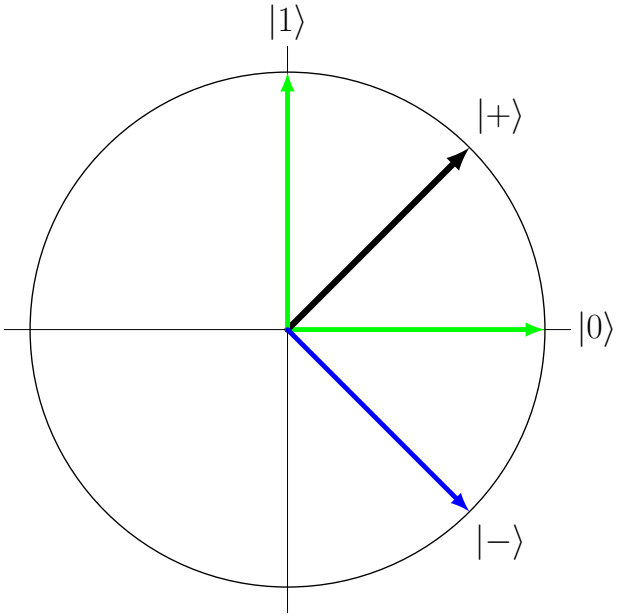
- If Bob and Alice choose different bases, they disregard the bit
- If all three choose the same basis, Eve is not detected



The BB84 protocol - Security

Eve picks a basis, measures the qubit and sends the result to Bob.

- If Bob and Alice choose different bases, they disregard the bit
- If all three choose the same basis, Eve is not detected
- If Bob and Alice choose the same basis but Eve picks a different one, then with 50% she will get caught.



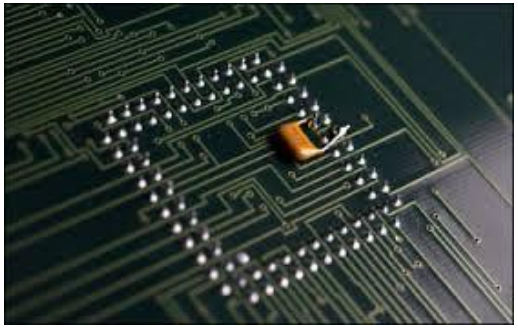
QKD in practice

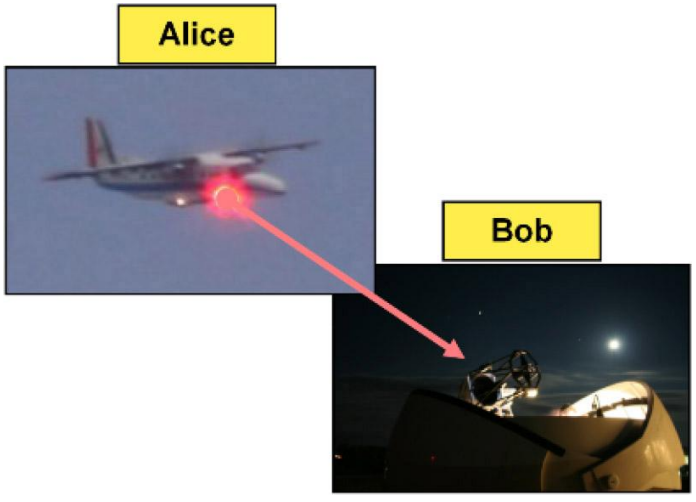
- All practical implementations have **errors** due to system imperfections.
- These should be considered as originating from Eve

Goal: To bound the information leakage as a function of the error rate

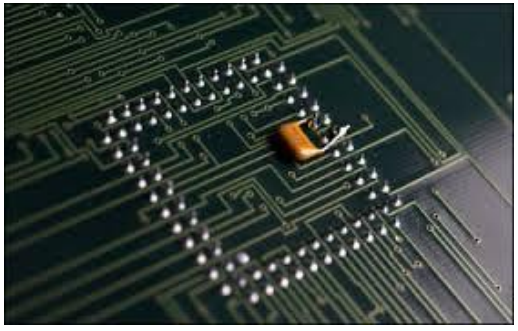
Error correction + Privacy amplification

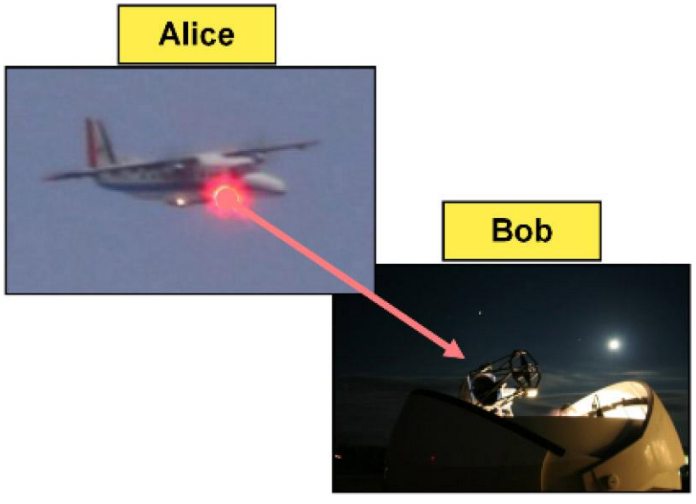
Implementations





Implementations

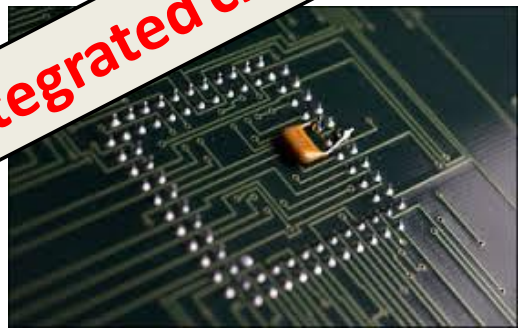


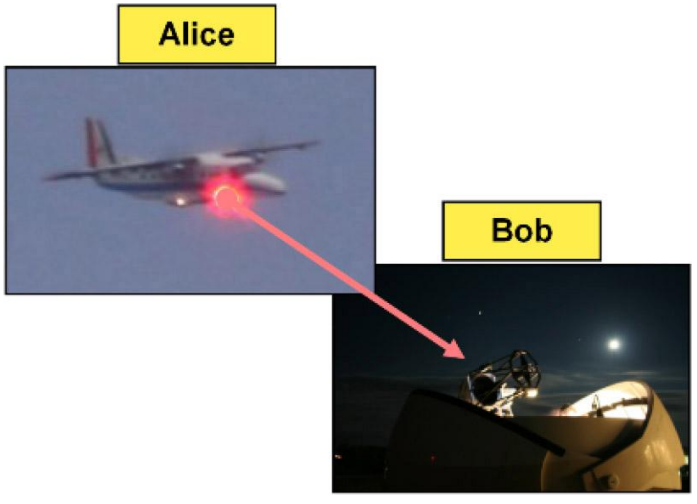


Implementations

Hundreds of kms

Integrated chips

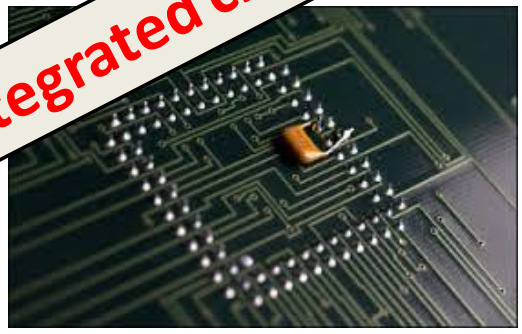




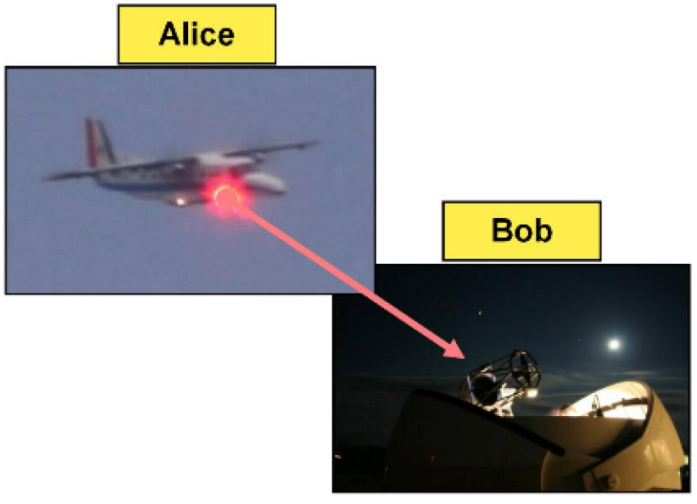
Implementations

Hundreds of kms

Integrated chips



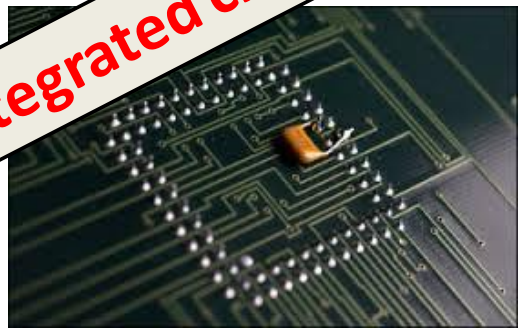
Commercial devices



Implementations

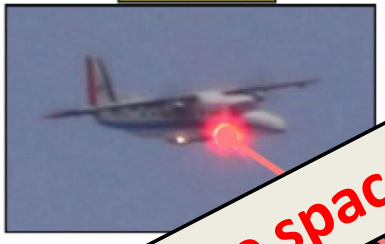
Hundreds of kms

Integrated chips



Commercial devices

Alice



Free space

Bob

Cryptography with distrustful participants

Quantum Networks: Secure and efficient networks of quantum and classical untrusted agents who communicate, perform distributed tasks, delegate computation to large-scale servers, etc.

Primitives: Bit commitment
Oblivious transfer
Coin Flipping

Can quantum mechanics help in this setting?

Coin Flipping

communication

channel

Why do we need it?

1. Bit commitment
2. Leader election and zero-knowledge protocols
3. Secure identification

Coin Flipping with bias ϵ

- If Alice and Bob are honest then

$$\Pr[c = 0] = \Pr[c = 1] = \frac{1}{2}$$

- If Alice cheats and Bob is honest then

$$p_*^A := \max_A \{\Pr[c = 0], \Pr[c = 1]\} \leq \frac{1}{2} + \epsilon$$

- If Bob cheats and Alice is honest then

$$p_*^B := \max_B \{\Pr[c = 0], \Pr[c = 1]\} \leq \frac{1}{2} + \epsilon$$

Coin Flipping with bias ϵ

- If Alice and Bob are honest then

$$\Pr[c = 0] = \Pr[c = 1] = \frac{1}{2}$$

- If Alice cheats and Bob is honest then

$$p_*^A := \max_A\{\Pr[c = 0], \Pr[c = 1]\} \leq \frac{1}{2} + \epsilon$$

- If Bob cheats and Alice is honest then

$$p_*^B := \max_B\{\Pr[c = 0], \Pr[c = 1]\} \leq \frac{1}{2} + \epsilon$$

The **cheating probability** of the CF protocol is $p_* = \max\{p_*^A, p_*^B\}$.

Coin flipping with information-theoretic security

Impossibility of classical CF	$p_c = 1$
Impossibility of perfect quantum CF (May97,LC98)	$p_q > 1/2$
Several non-perfect protocols (ATVY00, SR02, Amb04)	$p_q \leq 3/4$
Kitaev's SDP proof (2003)	$p_q \geq 1/\sqrt{2}$
Chailloux, Kerenidis (2009)	$p_q \approx 1/\sqrt{2}$

Coin flipping with information-theoretic security

Impossibility of classical CF	$p_c = 1$
Impossibility of perfect quantum CF (May97,LC98)	$p_q > 1/2$
Several non-perfect protocols (ATVY00, SR02, Amb04)	$p_q \leq 3/4$
Kitaev's SDP proof (2003)	$p_q \geq 1/\sqrt{2}$
Chailloux, Kerenidis (2009)	$p_q \approx 1/\sqrt{2}$

Quantum Cryptography in practice

Common problems :

- Ideally single photon sources (but in practice coherent states or entangled pairs)
- System transmission losses and noise, imperfections of detectors
- Quantum memories

Quantum Cryptography in practice

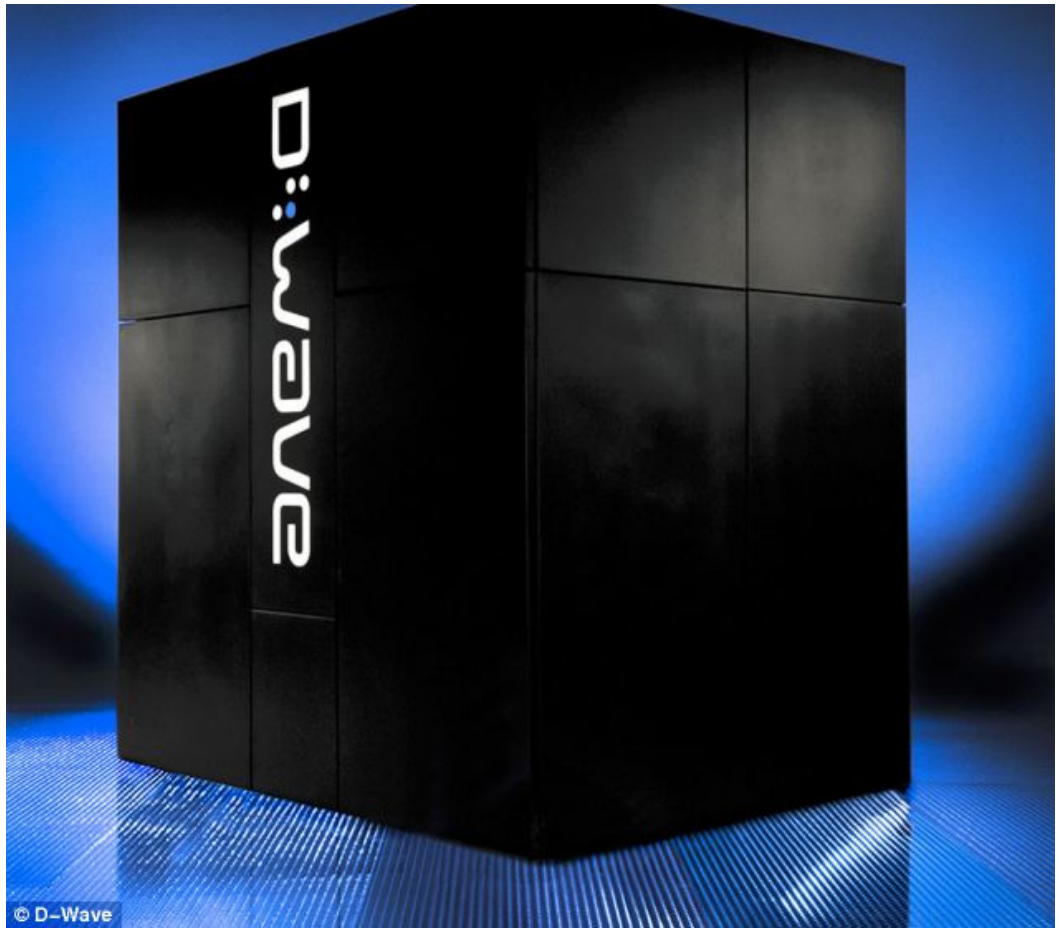
Common problems :

- Ideally single photon sources (but in practice coherent states or entangled pairs)
- System transmission losses and noise, imperfections of detectors
- Quantum memories

Implementations :

- QKD over 2.000km between Shanghai and Beijing
- Coin Flipping over 15km of optical fibre using commercial platform.

How can we verify a quantum computer?



Verification of computation

Computationally restricted, honest client

Verification of computation

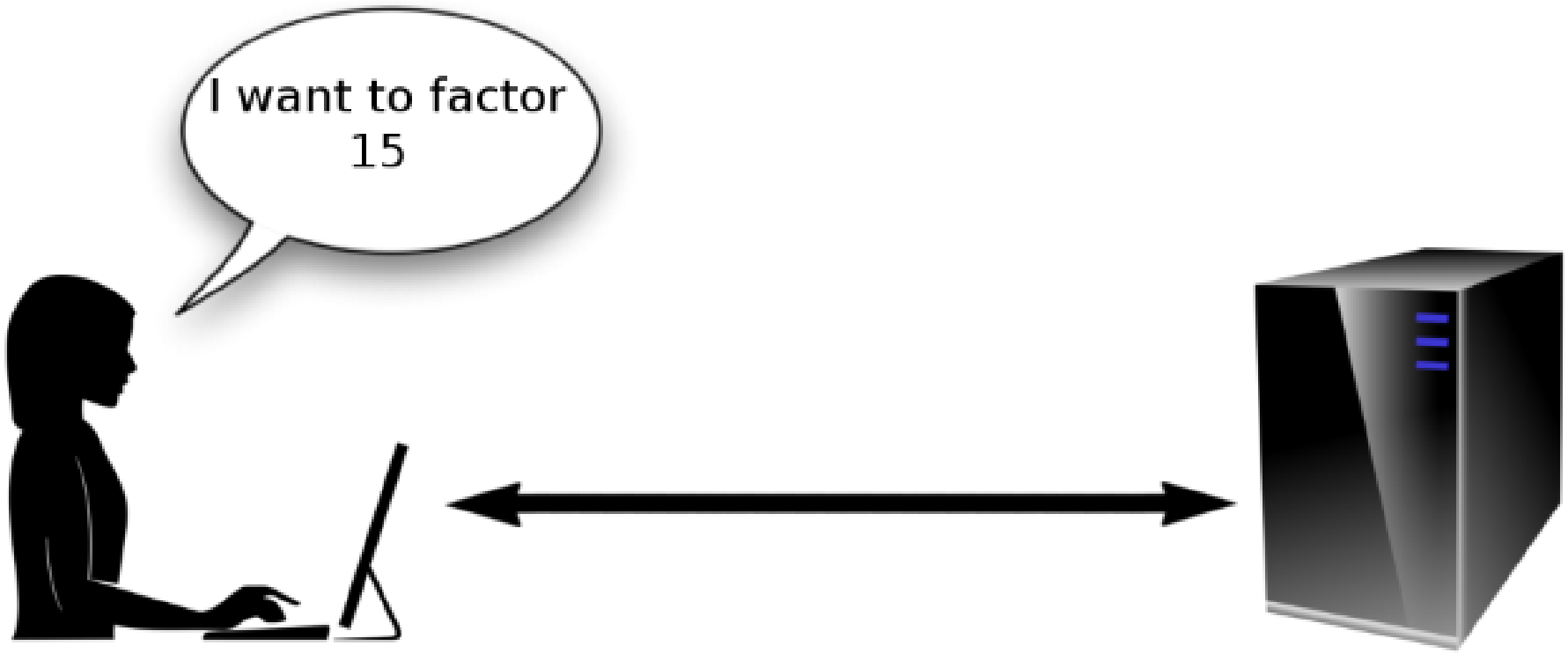
Wants to run difficult computation by delegating it to...

Verification of computation

Computationally powerful, (dishonest) server

Verification of computation

They interact through classical/quantum channel



Verification of computation

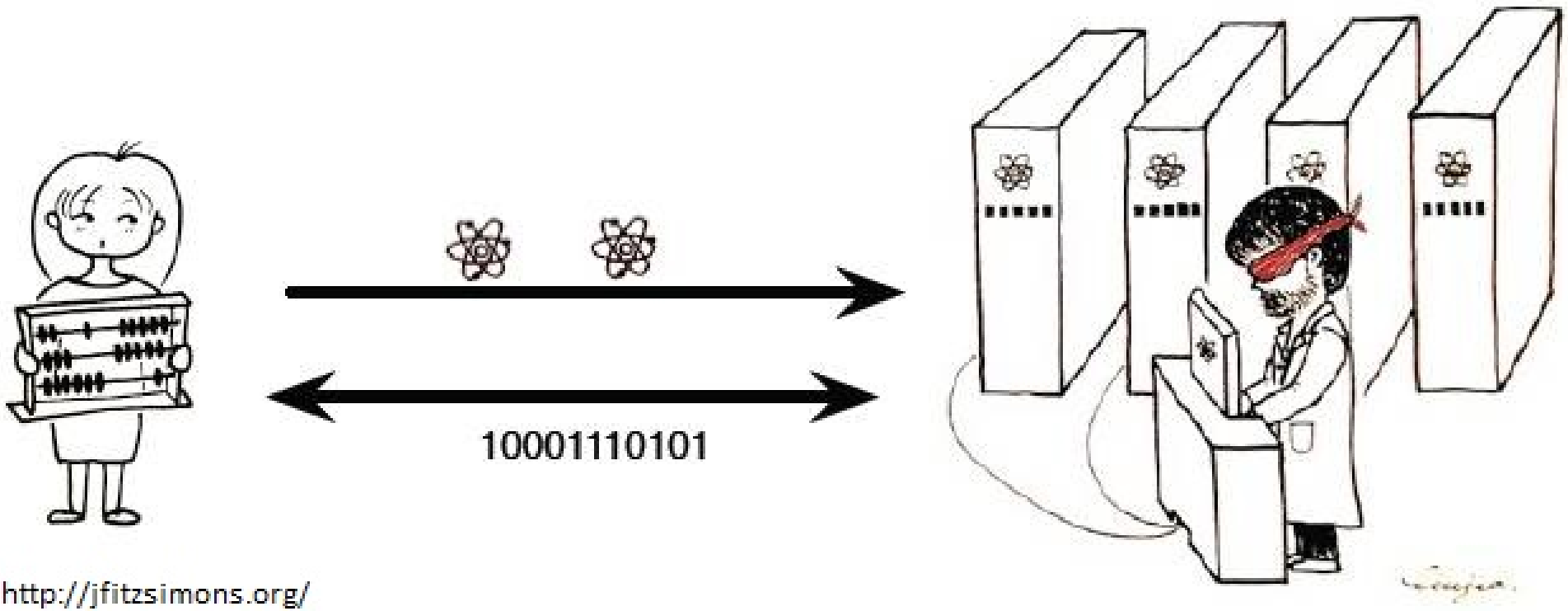
Completeness (probability of accepting correct outcome)

Verification of computation

Soundness (probability of accepting incorrect outcome)

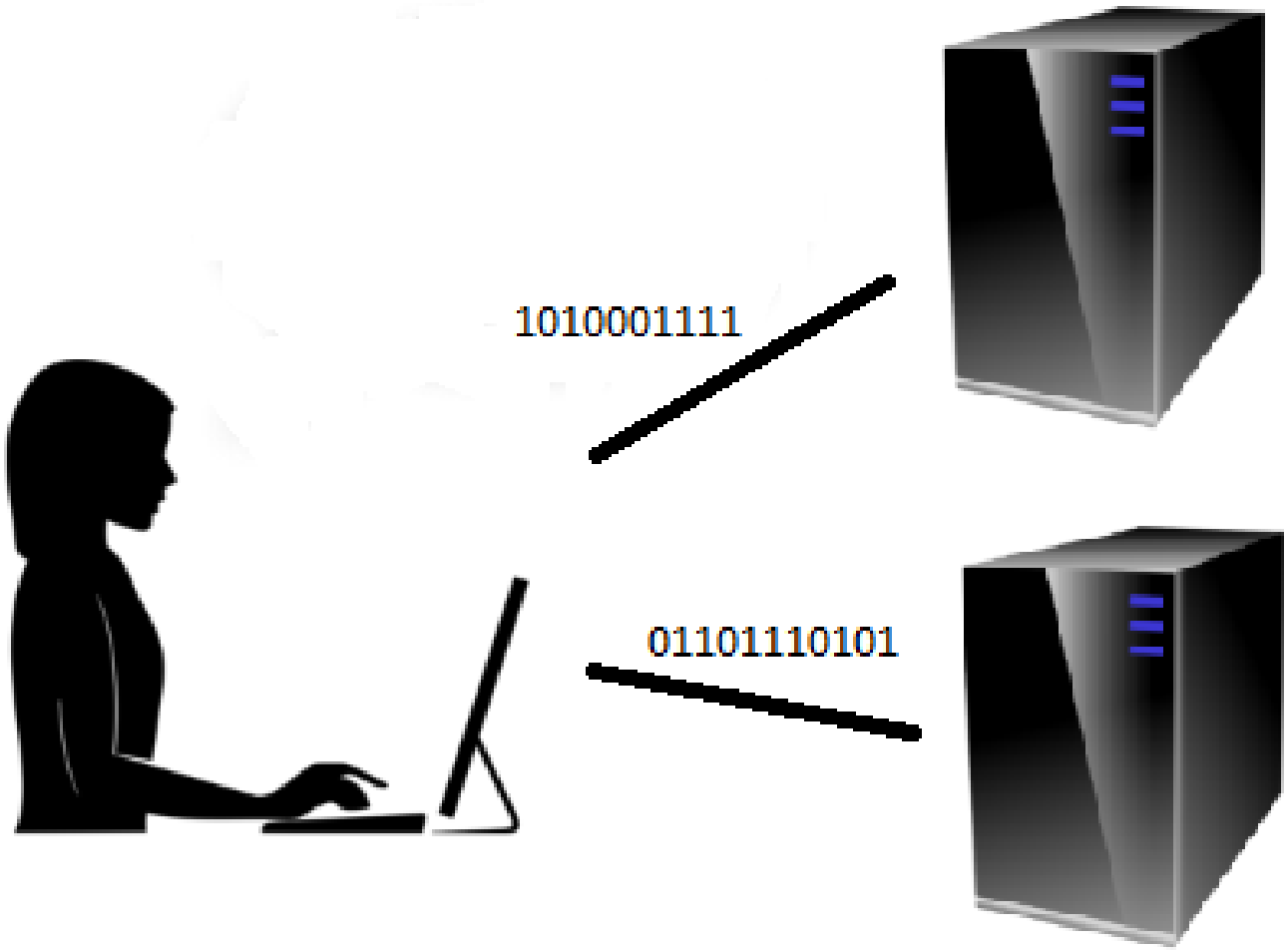
Different models

Universal Blind Quantum Computing [Broadbent, Fitzsimons, Kashefi]



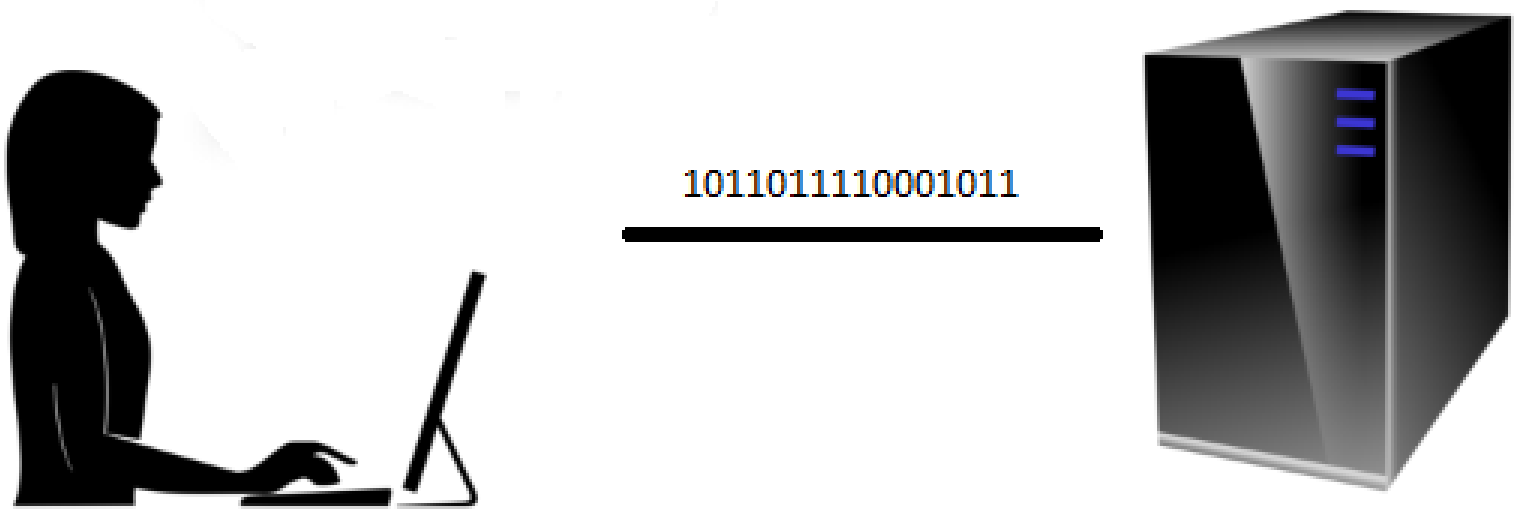
Different models

Multi-server protocol [Reichardt, Unger, Vazirani]



Open question

Classical Verifier



Current Topics in Quantum Cryptography

Security proofs

- Proofs are usually *ad hoc* depending on particular settings, and therefore not easy to extent/generalise
- Solution: Use of classical cryptographic tools (e.g. simulatability, composability) to formulate proofs.

Current Topics in Quantum Cryptography

Restricted models

- Security is treated similarly to classical cryptography
- Adversaries are limited by their equipment
  - Bounded storage
  - Noisy storage
  - ...

Current Topics in Quantum Cryptography

Quantum Hacking

- Side channels due to deviations between security proofs and real implementations allow additional leakage of information
- Solutions:
  1. Exhaustive search for side channels, characterization, counter measures
  2. Device Independence

Should we start caring about Quantum Cryptography?

YES!!!

- European Flagship for Quantum Technologies
- EPSRC Quantum Technology Hubs (UK)
- QuTech (Delft), UCLQ (UK), PCQC (France), Perimeter (Canada)
- Industrial interest (Google, Lockheed Martin, IBM)