Quantum Cryptography

Quantum Key Distribution

CPS

07-05-2025

chrysoula.vlachou@tecnico.ulisboa.pt

Quantum Computation

Church-Turing thesis

Can quantum computers solve problems that classical computers cannot?

Extended Church-Turing thesis

Quantum computers can achieve at most an exponential speedup over classical

Quantum Turing Machine*

Turing machines fail to capture all physically realizable computing devices

Welcome to the dark side...

Quantum algorithms

Shor's for factoring and Grover's for unstructured base search

Find the prime factors of $n-$bit integer N

Classical

$$\exp\left(\Theta(n^{1/3}\log^{2/3} n)\right) \text{ steps}$$

Quantum

$$O\left(n^2 \log n \log\log n\right) \text{ steps}$$

Efficient

Given a set of N elements $X = x_1, x_2, \ldots, x_N$ and a boolean function $f : X \to \{0,1\}$, find $x^* \in X$ such that $f(x^*) = 1$.

Classical

$O(N)$ queries

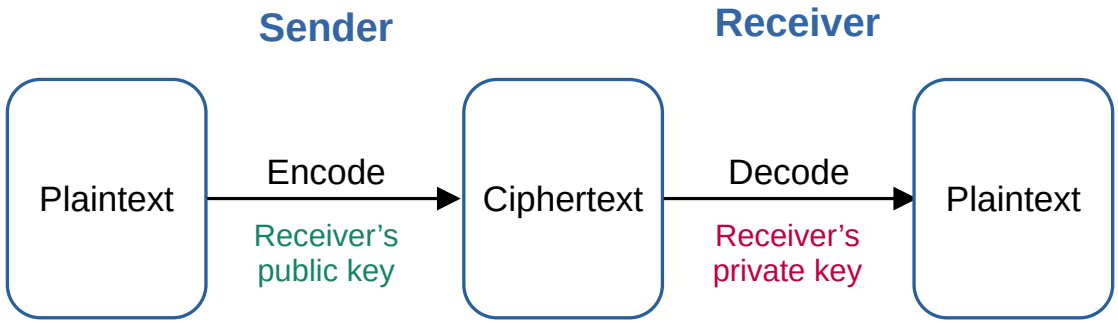
Quantum

$O(\sqrt{N})$ queries

Quadratic speedup

Asymmetric encryption

Public-key cryptography (key exchange, signatures)



Shor's algorithm solves efficiently...

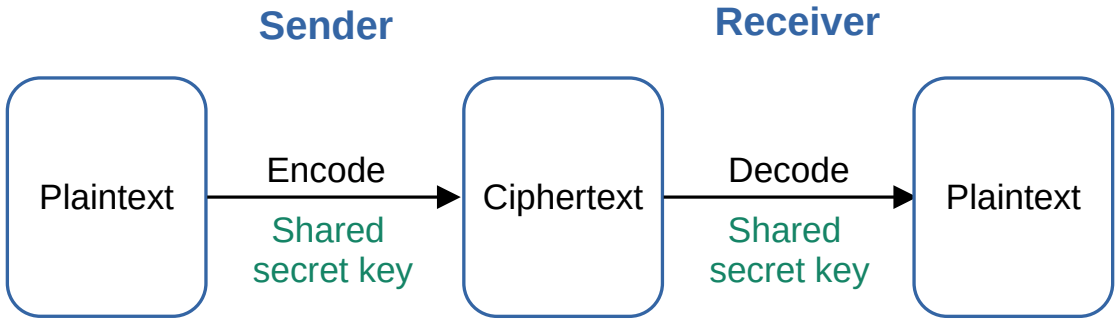
- Integer factorization
- Discrete logarithm
- Elliptic-curve discrete logarithm

...breaking

- RSA cryptosystem
- Finite-field and elliptic-curve Diffie-Hellman key exchange

Solution: Post-quantum cryptography

Symmetric encryption and hashing



Grover's algorithm for brute force attacks

Solution: Double key size

e.g. AES and ChaCha20 with 256-bit keys are practically quantum-safe (same as classical for 128-bit keys)

SHA-256 pre-image safe

Quantum cryptanalytic attacks

...Ongoing research...

- AES seems secure
- Other ciphers need to be updated
- Hash functions: collision resistance attacks

Solution: Checking, updating and removing obsolete systems

Threats and solutions

Q-Day

Harvest Now, Decrypt Later

Solutions

- Post-quantum cryptography
- Crypto-transition and agility
- **Quantum cryptography**

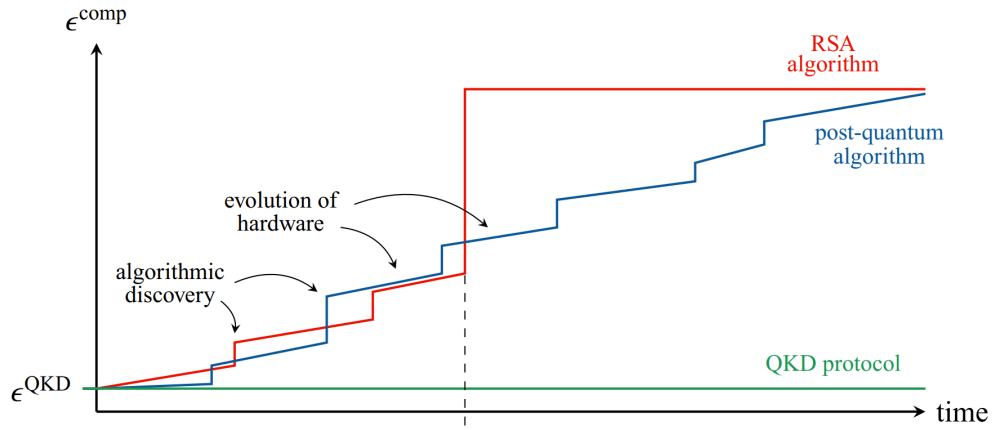
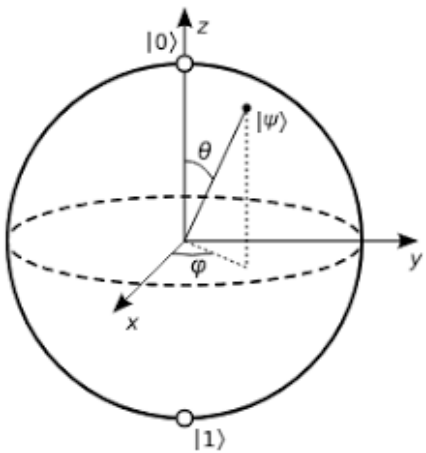


Figure from R. Renner and R. Wolf, AIAA Journal 61:5, pp. 1895-1910, 2023.

Postulates of Quantum Mechanics

I: State space (information encoding)

The state of a closed quantum system is described by a unit vector in a complex Hilbert space.



Qubit: $|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \in \mathbb{C}^2; \langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1.$

Basis in $\mathbb{C}^2$: $\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\} \equiv \{|0\rangle, |1\rangle\}.$

Superposition: $|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha|0\rangle + \beta|1\rangle.$

*1 bit of information in the qubit

Postulates of Quantum Mechanics

II: Evolution (information processing)

The evolution of a closed quantum system is described by a unitary operator on the respective Hilbert space.

$$|\psi'\rangle = U\,|\psi\rangle\,,$$

where $U^\dagger U = UU^\dagger = I$ and $U^\dagger$: transpose and complex conjugate.

Matrix representation in $\mathbb{C}^2$:

$$U = \begin{bmatrix} \alpha & \beta \\ -e^{i\phi}\beta^* & e^{i\phi}\alpha^* \end{bmatrix},$$

where $|\alpha|^2 + |\beta|^2 = 1$ and ϕ is the relative phase between α, β.

Postulates of Quantum Mechanics

III: Measurements (information "readout")

Quantum measurements are described by a collection $\{M_m\}$ of Hermitian operators[1] *acting on the respective Hilbert space.*

Example: Projection of $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ on $\{|0\rangle, |1\rangle\}$

$$M_0 = |0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \text{ and } M_1 = |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Completeness[2]**:** $M_0^\dagger M_0 + M_1^\dagger M_1 = M_0 + M_1 = I$.

Probability of getting outcome 0 and post-measurement state:[3]

$$p(0) = \langle\psi| M_0^\dagger M_0 |\psi\rangle = |\alpha|^2 \text{ and } |\psi_0'\rangle = \frac{M_0|\psi\rangle}{|\alpha|} = \frac{\alpha}{|\alpha|}|0\rangle.$$

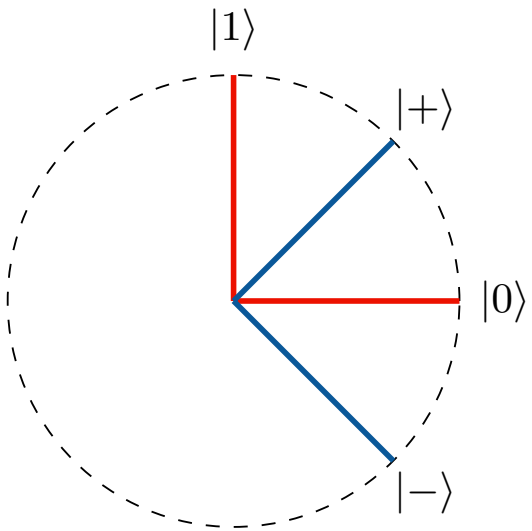
---

[1] Real eigenvalues

[2] Probabilities sum to 1.

[3] Analogously, $p(1) = |\beta|^2$ and $|\psi_1'\rangle = \frac{\beta}{|\beta|}|1\rangle$.

Mutually unbiased bases (MUBs) and uncertainty



Computational basis

$$\mathbf{C} = \{|0\rangle, |1\rangle\}$$

Diagonal basis

$$\mathbf{D} = \{|+\rangle, |-\rangle\}$$

(also a basis in $\mathbb{C}^2$)

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

Mutually unbiased*

$$|\langle 0|+\rangle|^2 = |\langle 0|-\rangle|^2 =$$

$$|\langle 1|+\rangle|^2 = |\langle 1|-\rangle|^2 = \frac{1}{2}$$

*Projection on one: maximum uncertainty about outcome on the other

Postulates of Quantum Mechanics

IV: Composite Systems (registers)

The state space of a composite quantum system is the tensor product of the component physical systems.

Example: Composite system in $\mathbb{C}^2 \otimes \mathbb{C}^2$

Computational basis:

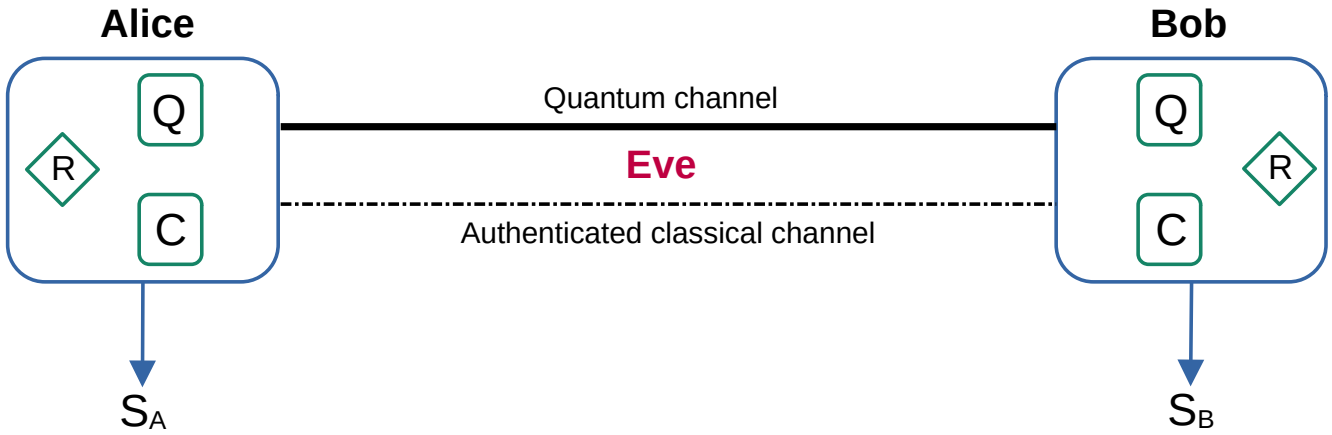
$$\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\} \equiv \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}.$$

Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|\phi\rangle = \gamma|0\rangle + \delta|1\rangle$.

$$|\psi\rangle \otimes |\phi\rangle = \alpha\cdot\gamma|00\rangle + \alpha\cdot\delta|01\rangle + \beta\cdot\gamma|10\rangle + \beta\cdot\delta|11\rangle = \begin{bmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{bmatrix}.$$

Quantum Key Distribution

Two legitimate collaborating parties, Alice and Bob, securely establish a shared secret key in the presence of an adversary, Eve



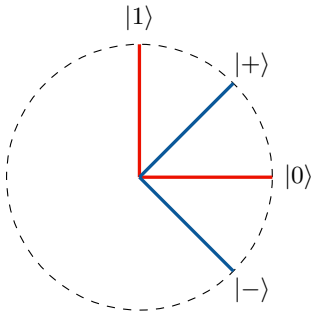
Information-theoretic security

Assumption: Classical authenticated channel

Use: Encryption using a (classical) symmetric cipher, e.g. OTP

The BB84 protocol

Quantum part



Bit encoding	**C**	**D**
0	$\|0\rangle$	$\|+\rangle$
1	$\|1\rangle$	$\|-\rangle$

Alice's bit	0	0	1	0	1	0	1	0	1	...
Alice's basis	**D**	**C**	**D**	**C**	**D**	**C**	**C**	**D**	**D**	...
Qubit sent	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	...
Bob's basis	**C**	**C**	**C**	**C**	**D**	**D**	**D**	**D**	**D**	...
Bob's outcome	?	$\|0\rangle$	?	$\|0\rangle$	$\|-\rangle$	?	?	$\|+\rangle$	$\|-\rangle$	...
Sifted key bit*	–	0	–	0	1	–	–	0	1	...

***Communication through the classical authenticated channel for sifting**

The BB84 protocol

Classical post-processing

- **Parameter estimation**

  Announcing results for a subset of rounds to get an estimate of the error rate of the strings, from which they derive a bound on the information that Eve could have gained.[4] If the error rate is higher than a previously determined threshold, Alice and Bob abort the protocol.[5]

- **Error correction**

  Protocol making the strings identical; checking success by comparing hashes of the bit strings.

- **Privacy amplification**

  Removing Eve's information on the key and producing the final key (shorter). Bounding accurately Eve's knowledge during parameter estimation is crucial, otherwise she will still have knowledge on the final key.

---

[4] Perfect devices and no Eve: the results should coincide after sifting.

[5] Eve has too much information on the key.

Correctness and Security

Conditioned on not aborting

Protocol outputs (S_A, S_B)

$$\epsilon^{\text{QKD}} = \epsilon_{\text{correct}} + \epsilon_{\text{secure}}$$

$\epsilon_{\text{correct}}$: probability that $S_A \neq S_B$

ϵ_{secret}: probability that Eve has some information on (S_A, S_B)

Success: pair of identical secret keys (S_A, S_B)
Failure: insecure (S_A, S_B)

Information-theoretic security

protocol fails with *negligible* probability

Eve guesses correctly **all** bases: $P = 2^{-n}$, n: number of rounds

Performance: Secret key rate (number of secret key bits generated per round)

Why is QKD secure?

I: Information gain vs state disturbance

Eve intercepts, measures and resends the qubit to Bob

1. Eve doesn't know the basis*
   Measuring in the wrong basis gives no information
2. Every informative measurement disturbs the qubit
   The more info she gains the more she changes the qubit

*Solution: A machine measuring in both bases
Uncertainty principle: Such machines do not exist for MUBs
For generating a key, always choose MUBs

More information: higher probability of getting detected

Why is QKD secure?

II: The no-cloning theorem

Making copies of the qubits?

Measuring in both bases without disturbing

Theorem. Let H be a Hilbert space. Then, there is no unitary operator U on $H \otimes H$, such that for all normalized $|\psi\rangle_1$ and $|a\rangle_2$ it satisfies:

$$U\left(|\psi\rangle_1 \otimes |a\rangle_2\right) = |\psi\rangle_1 \otimes |\psi\rangle_2 .$$

Proof. For contradiction, let such a U exist, and let $|\psi\rangle , |\phi\rangle \in H$. Then,

$$U\left(|\psi\rangle_1 \otimes |a\rangle_2\right) = |\psi\rangle_1 \otimes |\psi\rangle_2 \text{ and } U\left(|\phi\rangle_1 \otimes |a\rangle_2\right) = |\phi\rangle_1 \otimes |\phi\rangle_2 .$$

Consider the inner product $\langle\psi|\phi\rangle$, and recall that $\langle a|a\rangle = 1$ and $U^\dagger U = I$. Then,

$$\langle\psi|\phi\rangle \langle a|a\rangle = \left(\langle\psi|_1 \otimes \langle a|_2\right) |U^\dagger U| \left(|\phi\rangle_1 \otimes |a\rangle_2\right) = \left(\langle\psi|_1 \otimes \langle\psi|_2\right) \left(|\phi\rangle_1 \otimes |\phi\rangle_2\right) = \langle\psi|\phi\rangle^2$$

But $|\langle\psi|\phi\rangle| = |\langle\psi|\phi\rangle|^2 \Rightarrow |\langle\psi|\phi\rangle| = 0$ or 1; not true for arbitrary $|\psi\rangle , |\phi\rangle$.

Eve cannot make copies of the qubits

To gain information she has to measure and disturb the ones that Alice sends to Bob

Recap

Features with no classical analogue giving advantage to quantum Crypto

Structure of the state space and uncertainty
Superposition

Uncertainty principle
Implies restrictions on *joint measurability*

Information gain vs disturbance
The more information we gain from the measurement of a qubit, the more it is altered

No-cloning theorem
Perfectly cloning an unknown qubit is impossible

Quantum Money

Is that all?

Enter.....entanglement

"Spooky action at a distance"

Separable registers

$$|\psi_A \psi_B\rangle = \frac{|00\rangle + |01\rangle}{\sqrt{2}} = \frac{|0\rangle \otimes (|0\rangle + |1\rangle)}{\sqrt{2}}$$

Entangled registers

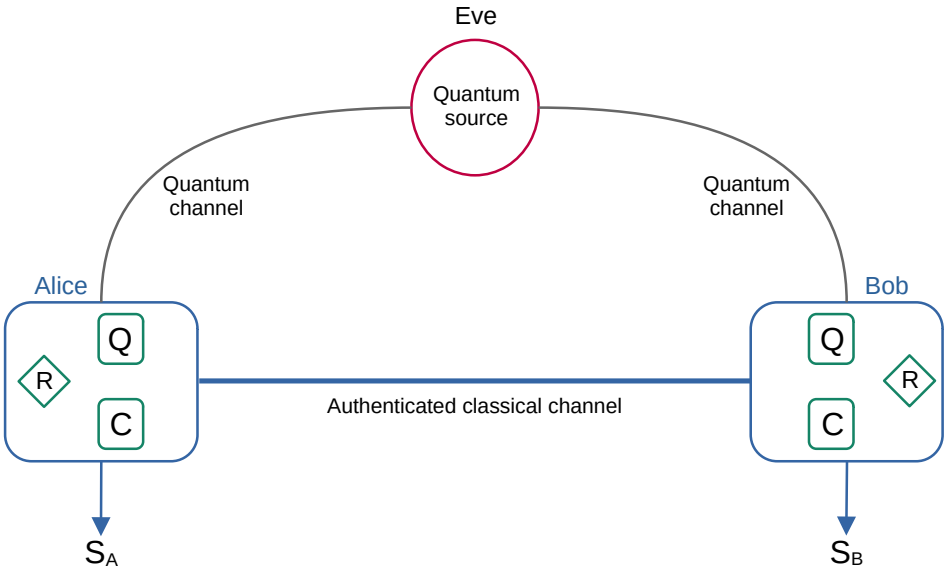
$$|\phi_A \phi_B\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Alice and Bob measure their individual qubits in the same basis: they obtain the same results; they can use them to generate a shared secret key

Entanglement is a *resource* for QKD

Entanglement-based ≡ prepare-and-measure protocols

Advantage: untrusted source



- **Quantum part**
  State distribution and measurements
- **Classical post-processing**

Protocols for *certifying* and *quantifying* entanglement

Monogamy of entanglement

When two qubits are *maximally* entangled, neither of them can be entangled to another

Beyond the untrusted source...

Device-independent QKD

Quantum secure communications with QKD

Light and mirrors for information-theoretical security[6]

No need for quantum computers

Research on QKD today

- Search for more robust and efficient protocols
- From asymptotic to finite-size security
- Improving classical post-processing of raw data
- Making security proofs protocol-independent and attack-independent
- Improving (semi-) device-independent and semi-quantum protocols
- Practical attacks (quantum hacking)
- Hardware development, improvement and cost reduction
- Standardization of components and security proofs

[6] Establishing private information-theoretically secure communication channels

Going quantum beyond QKD

- Quantum conference key agreement
- Quantum secure multi-party computation
- Device-independent cryptography (semi-)
- Semi-quantum cryptography
- Quantum random number generation

....Cryptography beyond quantum mechanics....

Sticking around and moving forward

- To learn the basics
  Quantum Computation and Quantum Information, M. A. Nielsen and I. L. Chuang, Cambridge University Press.

- To program IBM's "quantum computer"
  `https://www.ibm.com/quantum/qiskit`

- QKD
  `https://arc.aiaa.org/doi/10.2514/1.J062267`

- Quantum cryptography beyond QKD
  `https://arxiv.org/abs/2411.08877`