Hybrid Quantum Key Distribution

Dr hab. Magdalena Stobińska, prof. UW
www.stobinska-group.eu

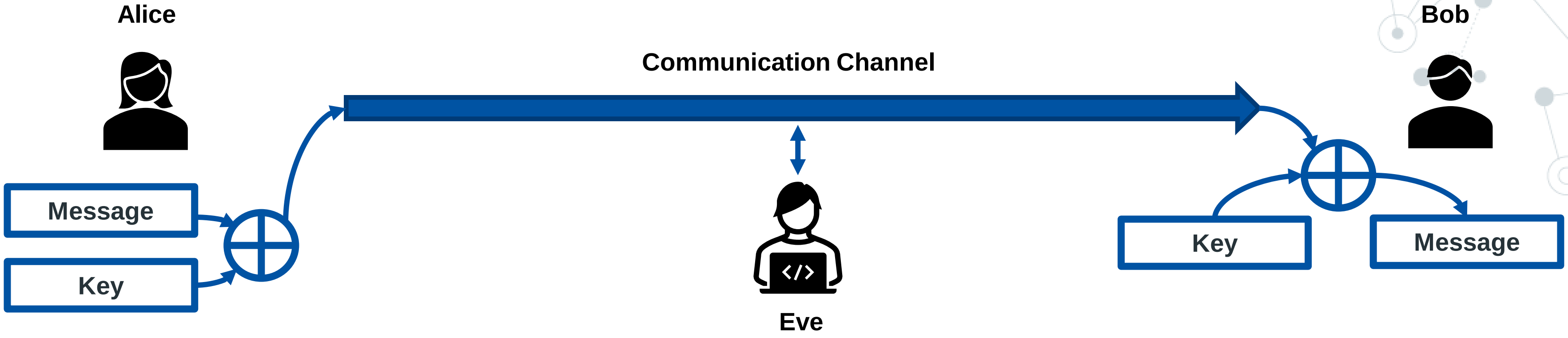
Baby Steps Beyond the Horizon

Będlewo, 2 September 2022

Agenda

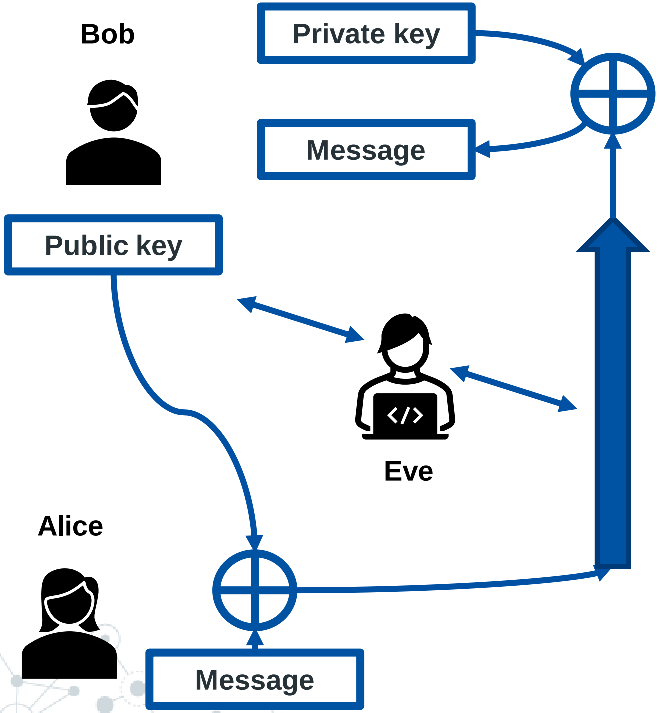
- Introduction - Classical Cryptography
- Quantum Cryptography
- Post-Quantum Cryptography
- Hybrid Quantum-Classical Cryptography

Classical cryptography



- The “Holy Grail” is **information-theoretical security** (unconditional). It can be achieved with one-time-pad (OTP) method, **if Alice and Bob share a long random one-time key that is kept secret from Eve**.
- Key distribution (KD) problem: how to distribute the key in the presence of Eve?
- All conventional KD schemes that rely on classical physics and mathematics can provide only **computational security**.

Classical Cryptography. Key Distribution Problem



- Public Key Infrastructure (PKI)
uses asymmetric encryption,
with separate public and private keys.

- PKI is based on Rivest–Shamir–Adleman (RSA) algorithm [Rivest et al., Comm. ACM **21**, 120 (1978)]: relies on **hardness of prime factorization.**

- Shor's algorithm: prime factorization on a **quantum computer in polynomial time**
[Shor, IEEE FOCS, 124 (1994)].

Classical Cryptography. Quantum Computer Threat

Therefore, since the hardness of most PKI is based on integer factorization and discrete logarithm problems that are difficult or intractable for conventional computers.

Recently, in 2020, the factoring of RSA-250 was announced, an RSA number of 250 decimal digits or 829 bits, as well as solved a discrete logarithm of the same size. New records of this type are constantly being refreshed as the performance of computer hardware increases over time.

Quantum-Safe Encryption

In the era of quantum computing, there are two kinds of reliable information security mechanisms

Approach	Based on	Pros	Cons
Quantum cryptography	Laws of physics, e.g. no-cloning theorem	• **Information-theoretical security**	• Does not replicate all functionality of PKI • Requires a new infrastructure (a quantum network)
Post-quantum cryptography	New algorithms, e.g. McEliece code-based cryptography	• Compatible with existing PKI schemes • High key rates	• Computational security • **Resistant only to currently known attacks**

Both approaches are complementary and could be combined for higher security.

Quantum Cryptography

Alice and Bob can employ quantum information, and in particular entanglement (though not necessarily), to solve the key exchange problem for good.

Quantum key distribution (QKD) protocols can be devised that are invulnerable to any attack allowed by the laws of physics, either now or in the future!

This is the key difference to the classical cryptography where the security is based solely on the limited computational powers of an eavesdropper.

What is quantum information?

- It is represented by a **physical state of a quantum system**.
- Governed by the laws of quantum world (physics).
- **Basic unit:** *a quantum bit (**qubit**)*, encoded in a two-level quantum system:
  - A normalized vector in a 2-dimensional Hilbert space $\mathbb{C}^2$, spanned by two orthonormal basis vectors (states), in literature denoted as:

    $$\begin{bmatrix}1\\0\end{bmatrix} \equiv |0\rangle \quad \text{and} \quad \begin{bmatrix}0\\1\end{bmatrix} \equiv |1\rangle.$$

  - A linear combination of $|0\rangle$ and $|1\rangle$ is called **quantum superposition**

    $$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$ α, β – complex numbers.

  - n qubit basis states can form tensor product basis states in 2^n-dimensional Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \equiv \mathbb{C}^{2\otimes n}$.
  - **Example - 2 qubits:** $|0\rangle \otimes |0\rangle \equiv |00\rangle, |0\rangle \otimes |1\rangle \equiv |01\rangle, |1\rangle \otimes |0\rangle \equiv |10\rangle, |1\rangle \otimes |1\rangle \equiv |11\rangle$.

Qubit

- $|\psi\rangle \in \mathbb{C}^2$ and $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is a normalized vector thus,

$$\boxed{|\alpha|^2 + |\beta|^2 = 1.}$$

- Statistical interpretation of measurement results: $|\psi\rangle$ has probability $|\alpha|^2$ of the value 0 and $|\beta|^2$ of 1.

- **Example:** a horizontally polarized photon

  linear basis: $|H\rangle \equiv |0\rangle, \qquad |V\rangle \equiv |1\rangle$

  circular basis: $|R\rangle = \frac{|H\rangle + i|V\rangle}{\sqrt{2}}, \quad |L\rangle = \frac{|H\rangle - i|V\rangle}{\sqrt{2}}$

$$|H\rangle = \frac{|R\rangle + |L\rangle}{\sqrt{2}}$$

The no-cloning theorem

Theorem: It is impossible to perfectly clone an unknown quantum state using a unitary operator [Wootters, Zurek, Nature **299**, 802 (1982)].

Proof: $|\psi\rangle_A, |\varphi\rangle_A \in \mathbb{C}^{2\otimes n}$ – states (data) of source A to copy, $|s\rangle_B \in \mathbb{C}^{2\otimes n}$ – state of target B,
(a.a.) U – unitary operator, $U^\dagger U = \mathbb{1}$, that performs copying from A to B.

$$|\psi\rangle_A \otimes |s\rangle_B \overset{U}{\rightarrow} U|\psi\rangle_A \otimes |s\rangle_B = |\psi\rangle_A \otimes |\psi\rangle_B,$$

$$|\varphi\rangle_A \otimes |s\rangle_B \overset{U}{\rightarrow} U|\varphi\rangle_A \otimes |s\rangle_B = |\varphi\rangle_A \otimes |\varphi\rangle_B.$$

Hilbert space is equipped with inner product that is denoted like this: $\langle\psi|\varphi\rangle$.
Taking the inner product of these two equations gives

$$\langle\psi|\langle s|\underbrace{U^\dagger U}_{\mathbb{1}}|s\rangle|\varphi\rangle = \langle\psi|\langle\psi|\varphi\rangle|\varphi\rangle$$

$$\langle\psi|\varphi\rangle = \langle\psi|\varphi\rangle^2$$

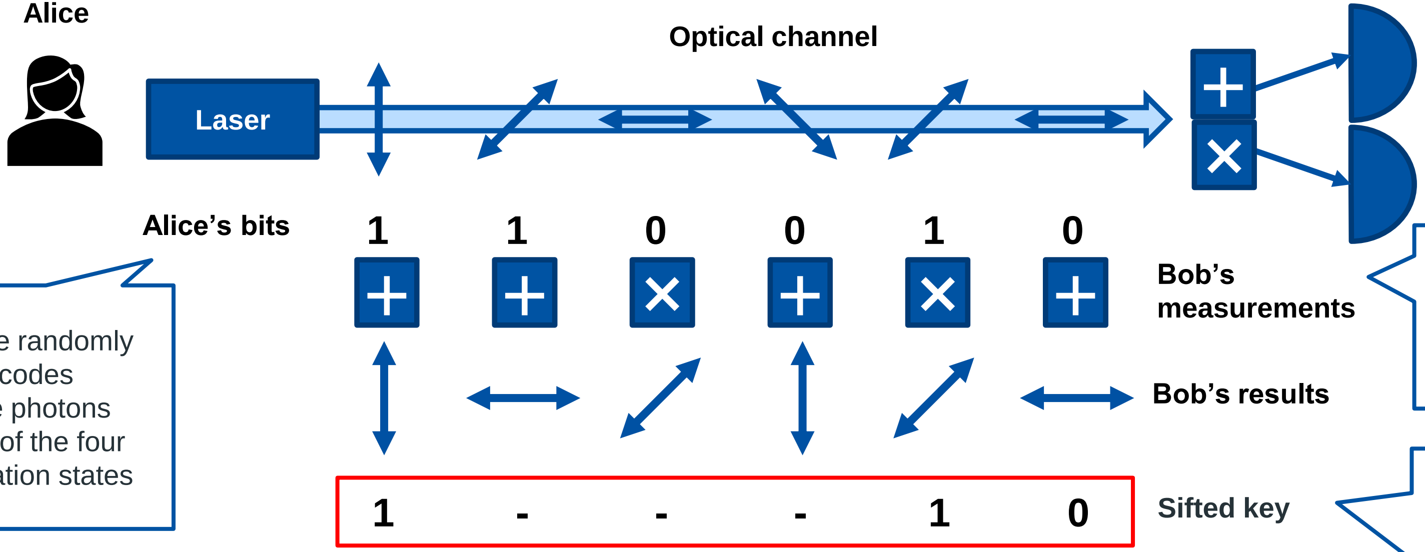
$$x = x^2 \quad \Rightarrow \quad x = 0 \vee x = 1 \quad \Rightarrow \quad \langle\psi|\varphi\rangle = 0 \vee |\psi\rangle = |\varphi\rangle$$

so either states $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal or identical.

The no-cloning theorem is the basis for quantum cryptography

Quantum Key Distribution: BB84 Protocol

[Bennett, Brassard, IEEE ICCSSP, 175 (1984)]



Alice

Laser

Optical channel

Bob

Alice's bits 1 1 0 0 1 0

Bob's measurements

Bob's results

Sifted key 1 - - - 1 0

(1) Alice randomly encodes single photons in one of the four polarization states

(2) Bob randomly chooses one of the two bases (linear or circular)

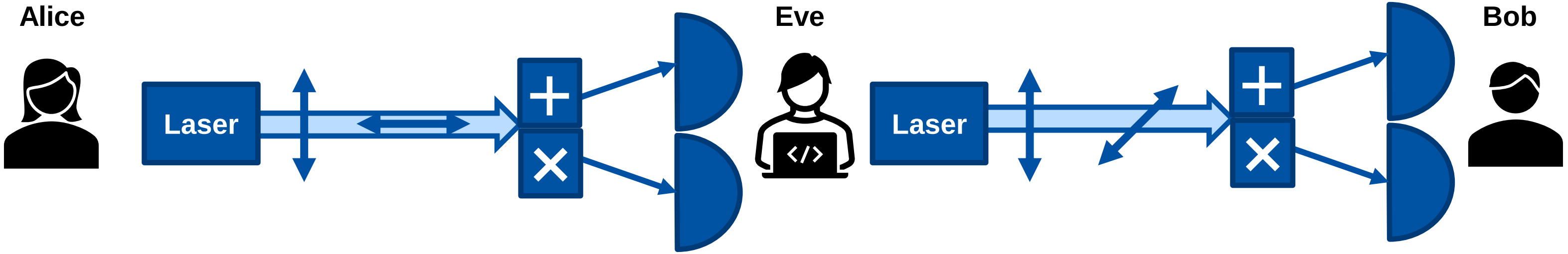
(3) Alice and Bob publicly announce their basis choices

(4) Alice and Bob discard the polarization data encoded in different bases

(5) Alice and Bob compare random samples of their sifted key bits to compute **Quantum Bit Error Rate** (QBER). If it is too high, then Eve may have interfered and they should abort.

QKD. Information gain as a disturbance

- What if Eve attacks the quantum channel?
  Let’s consider the simplest eavesdropping strategy: the intercept-resend attack.



- Let us focus on those cases when Alice and Bob happen to use the same basis since they will throw away the rest.
- Eve can guess the correct basis only 50% times. Thus, Eve’s attack will introduce 50% QBER for half of the total bits, and total of 25% QBER.

QKD. Fiber Implementation by Toshiba

In 2018 Toshiba (Cambridge) proposed **Twin-Field (TF)-QKD** protocol, which enables efficient quantum communications over hundreds of kms [Nature **557**, 400 (2018)].

They demonstrated QKD for **240 km** fiber link and in 2021, for **555- and 600-km** link [Nat. Photon. **15**, 530 (2021)]

Achieved key rates:

- 300 kbit/sec for 120 km,
- 1.77 bit/sec for 555 km,
- 0.778 bit/sec for 600 km.

QKD. Satellite-Based by China

In 2016 **China** launched its **Micius** satellite and demonstrated the first entanglement distribution between the ground stations separated by 1200 km. [Science **356**, 1140 (2017)]. An experiment linking China and Austria with "quantum-encrypted" video call (7,600 km) was conducted in 2018.

In 2020 this satellite was used for the first QKD over **1100 km**. Achieved bit rate was **0.21 bits/sec** [Nature **582**, 501 (2020)].

In 2021 it became a part of 4,600 km-long quantum Chinese network [Nature **589**, 214 (2021)], involving free-space and fiber networks.

Protocol: Entanglement-based QKD (BBM92)

Post-Quantum Cryptography (PQC)

In 2016, NIST published a report on PQC20 anticipating that a quantum computer is likely to be built by 2030 that breaks 2000-bit RSA in a few hours and therefore renders the current public-key infrastructure insecure.

As a result, in the same year, **NIST** initiated the *“Post-Quantum Cryptography Standardization”* process by announcing a call for proposals of quantum-resistant cryptographic primitives including public-key encryption, digital signature, and key exchange algorithms.

This process is expected to release the standardization documents by 2024.

PQC.

Post-Quantum Cryptography, despite its name, has nothing in common with Quantum Mechanics. It is based on problems that are *believed* to be computationally-hard and that are not threatened by the Shor's algorithm (that is beyond the integer factorization problem, the discrete logarithm problem or the elliptic-curve discrete logarithm problem). Therefore, PQC can offer only the computational security.

There are several different types of PQC, out of which the following two are the most popular:

- **Lattice-based PQC** (rely on lattices over vector space $\mathbb{Q}^n$ or free modules $\mathbb{Z}^n$)
- **Code-based PQC** (rely on error-correcting codes)

PQC. Learning With Errors Problem

Learning with errors (LWE) *problem*

This is the computational problem of inferring a linear n-ary function f over a finite ring from given samples $y_i = f\ (x_i)$ some of which may be erroneous.

The LWE problem is conjectured to be hard to solve and the best-known algorithms require $O(2^n)$ operations (exponential time and computer memory) to tackle it.

It gives rise to e.g. public-key encryption, and identity-based encryption.

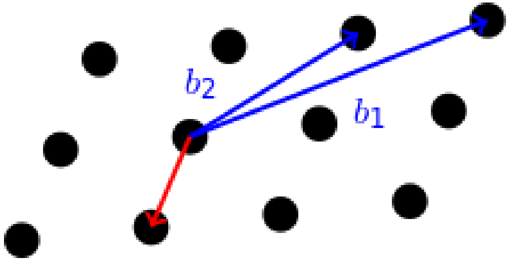
PQC. Shortest Vector Problem

Shortest vector problem (SVP)

For a given lattice L, a basis of a vector space V and a norm N (often L^2) one must find the shortest non-zero vector in V, as measured by N, in L.

Solving of this problem also consumes time exponentially $O(2^n)$.

SVP find its applications in public key cryptosystems.



Hybrid Quantum-Classical Cryptography

This is the idea of the hybrid cryptography approach stems from the following problem.

Although QKD can provide information theoretically secure key exchange even in the era of quantum computers, it requires authentication of its classical channel! The authentication is executed by exchanging the “seed” keys, which distribution is still an open problem.

On the other hand, there already exists a mature PKI that if combined with a PQC algorithm may elevate its security level and offer a Shor-resistant computational security solution.

By combining a short-term security of a PQC algorithm we may achieve a long-term security of the keys distributed by QKD that is Shor’s algorithm-proof.

Hybrid Cryptography. Implementation

The group of Jan-Wei Pan in China has recently experimentally demonstrated the first example of the hybrid cryptographic approach [npj Quantum Information **7**, 67 (2021)].

QKD was based on a *BB84-type of protocol* with polarization encoding, that was amended by a PQC authentication.

Their result has demonstrated an additional benefit. Usually, for a QKD network of n users, it is required to exchange $\frac{1}{2}n(n-1)$ pairs of symmetric keys to realize pairwise interconnection.

In contrast, in this new approach, with the help of a PKI and PQC, each user only needs to apply for one digital certificate from a certificate authority (CA) to achieve an efficient and secure authentication for QKD. This reduces the connectivity load from $\mathrm{O}(n^2)$ to $\mathrm{O}(n)$.

Hybrid Cryptography. The Idea

Although PQC can be used for both encryption and authentication and is believed to be secure against Shor algorithm, *PQC is still not an information theoretically secure method*, and *it is still an open question whether PQC is secure* against other classical or quantum algorithm except for Shor algorithm.

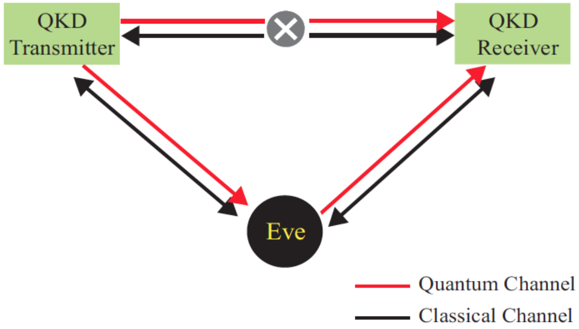
Therefore, it is reasonable to assume that *PQC is good for short-term security* (e.g. authentication) but not for long-term security (e.g. key for coding information).

Hybrid Cryptography.

Authentication Problem in QKD

QKD includes the quantum channel that transmits photons and the classical channel used in post data processing. The unconditional security of QKD does not require the classical channel to be confidential but requires it to be *authenticated.* Otherwise, a man in-the-middle attack will occur.

As a middleman, Eve pretends to be a legitimate party. She cuts off the quantum channel, reconnects the legitimate parties, and carries out the man-in-the-middle attack.



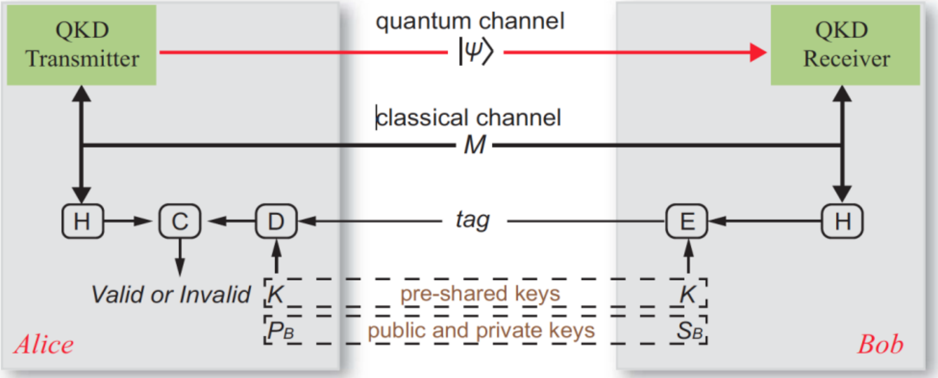
Hybrid Cryptography.

Authentication via Pre-Shared Key

The current secure authentication method is to pre-share a small amount of symmetric seed keys and encrypt (sign) and decrypt (verify) the hash value of classical messages.

- The QKD transmitter sends quantum signals |ψ⟩ through a quantum channel to the QKD receiver, and they carry out data processing via a classical channel by exchanging classical messages (M).

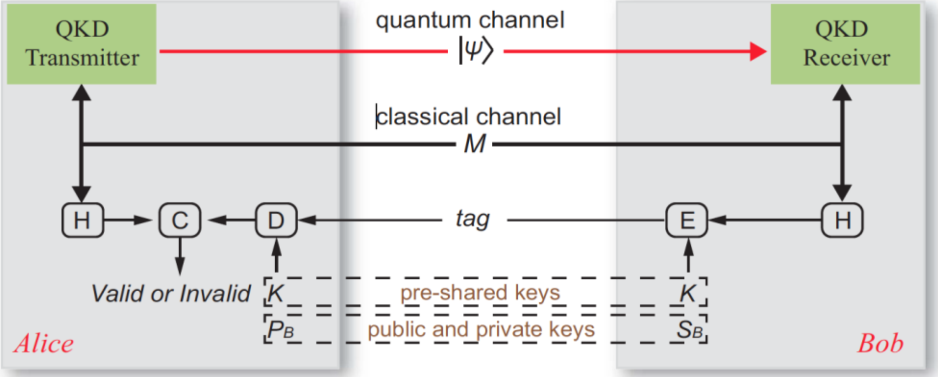
- To authenticate the classical messages, Alice and Bob each generate a digest using a hash function (H), which is the SM3 hash algorithm in this experiment.



Hybrid Cryptography.

Authentication via Pre-Shared Key

- Then, Bob encrypts (E) his digest with a pre-shared key (K) or Bob's private key (SB) and subsequently sends the tag to Alice.
- After receiving the tag, Alice decrypts (D) it with the same pre-shared key (K) or Bob's public key (PB) and compares (C) the result with her own digest. If the two are the same, the authentication is successful. otherwise, the authentication fails.



The figure shows that Alice authenticates Bob's identity. In the experiment, two-way authentication was implemented.

Hybrid Cryptography.

Authentication via Pre-Shared Key

This method can guarantee the *information theoretical secure* authentication, but only in principle, not in practice.

It also allows us to connect any two users in the network. However, it is not scalable. If the number of users in the network is n, then the number of pre-shared key pairs m is

$$m = C_n^2 = \frac{1}{2}n(n-1).$$

Symmetric keys are generally pre-shared face to face. When the number of users is relatively large, the burden of pre-sharing keys is heavy and inefficient. For example, if $n = 100$, then $m = 4950$.

Hybrid Cryptography.

Authentication via Pre-Shared Key

At the same time, each user needs to store the authentication key pairs with all other users.

The storage, synchronization and management of so many key pairs will increase the complexity and security risk of the network. One solution is to use a *trusted relay* to form a *star-type network*, each user connects and pre-shares one key pair only with the trusted relay, but this reduces the interconnection between users.

Moreover, when new users join a QKD network, they need to pre-share symmetric keys with the trusted relay or the original users on demand. If the new user’s QKD task is urgent, it may be too late to distribute the authentication key pairs.

Hybrid Cryptography.

Authentication via PQC+PKI

Another type of secure authentication method is to use the post-quantum public key algorithm and public key infrastructure.

Each user receives a digital certificate signed by a trusted certification center, which contains his/her identity, public key and other items required by the PKI standard.

For a network of n users, the number of digital certificates issued is n. If a new user joins the QKD network, he/she needs to obtain *only one* digital certificate. Therefore, the authentication based on the public key algorithm can solve the problems of pre-sharing symmetric keys.

Hybrid Cryptography.

Authentication via PQC+PKI

As long as the PQC algorithm is secure during the authentication process, the security of this round of authentication and the key generated by QKD can be guaranteed.

Even if the PQC algorithm is cracked in the future, the security of the previous authentication and keys will not be affected. Thus, we need to assume only the short-term security of PQC.

This is different from using the PQC algorithm for confidentiality or key distribution, which requires long-term security of the PQC algorithm.

Hybrid Cryptography. PQC Algorithm

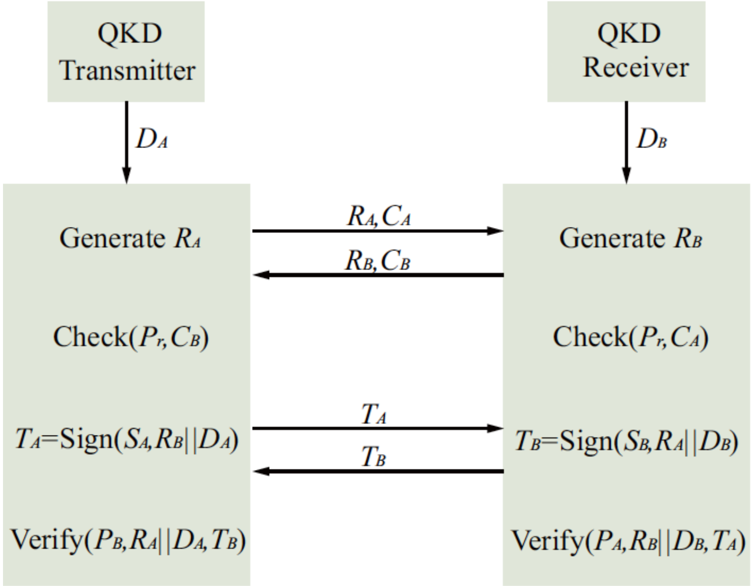
The PQC algorithm used was *Aigis-Sig*, an efficient lattice-based digital signature scheme from variants of the *learning with errors* (LWE) and *short integer solutions* (SIS) *problems*.

It has been shown that these two problems are at least as hard as some worst-case lattice problems for certain parameter choices. Therefore, the post-quantum security of Aigis-Sig algorithm is based on the conjectured quantum resistance of the underlying lattice problems. Furthermore, it has not been found that quantum algorithms have substantial advantages (beyond polynomial speedup) over classical ones in solving lattice problems.

Hybrid Cryptography. PQC Authentication

- Alice and Bob exchange their own certificates (C_A, C_B) and random nonce (R_A, R_B) with each other.

- Then, they use the public key of certificate authority (Pr) to verify that the other public key belongs to its identity and use the PQC algorithm to sign the message digest (D_A, D_B) and the nonce under their own private keys (S_A, S_B) to generate signatures (T_A, T_B).

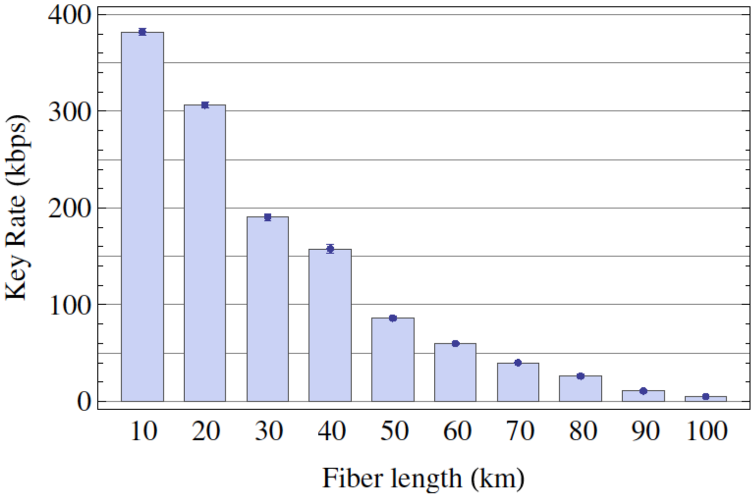


- Afterwards, they use the confirmed public keys of the other to verify the correctness of the received signatures. Because only the legitimate party has the corresponding private key, it can be confirmed that the message is signed legally.

Hybrid Cryptography.
QKD Network Authentication

In the experiment the application of PQC in the QKD point-to-point link was realized with fiber distances from 10 to 100 km.

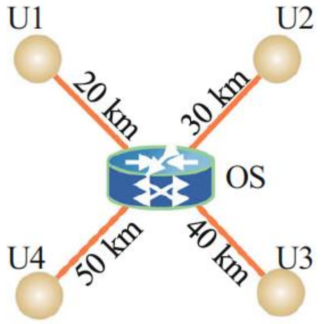
The secure key rate decreases exponentially with the fiber length, which is consistent with the theoretical expectation for the BB84 protocol (*not all QKD protocols suffer from this unfavorable key rate-distance scaling problem*).



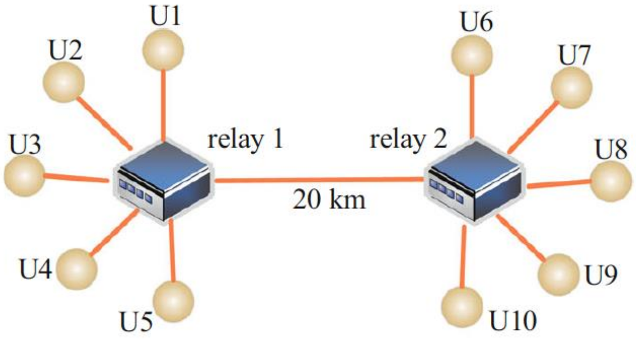
Hybrid Cryptography. QKD Networks

QKD networks can generally be divided into two types

- **All-pass network.** Here users are connected by optical switches (OSs). To achieve an arbitrary connection between users, and each user must have a QKD transmitter and a receiver.



- **Trusted relay network.** It simulates the metropolitan area networks. A user must first connect to its closest trusted relay, next the relay talks to the other relay, and only then the second relay connects to the other end user.

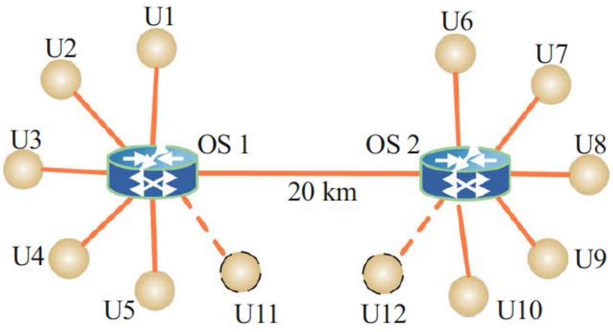


Hybrid Cryptography.

QKD Network + PQC Authentication

◎ If pre-shared key authentication is used, for the relay network, new users need to pre-share keys with the relay, and can perform QKD only with the relay, and not with other users. This reduces the interconnectivity.

◎ For the all-pass network, each new user needs to pre-share 10 pairs of symmetric keys with 10 original users and 1 pair of keys between the two new users. A total of 21 pairs of keys need to be pre-shared to achieve a connection between any two users.



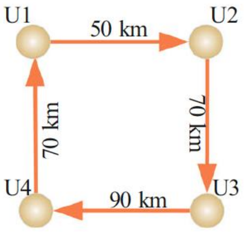
◎ If PQC authentication is adopted, trusted relays can be replaced with OSs. Each new user needs to apply for only one digital certificate, and a total of two digital certificates is sufficient to realize the connection of any two users. This greatly increases the accessibility of the network and the interconnection for new users.

Hybrid Cryptography.

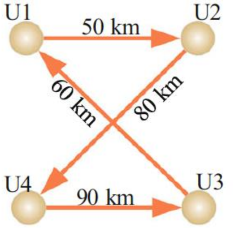
QKD Network + PQC Authentication

In the experiment, the all-pass network realized:

a ring connection



and a cross connection



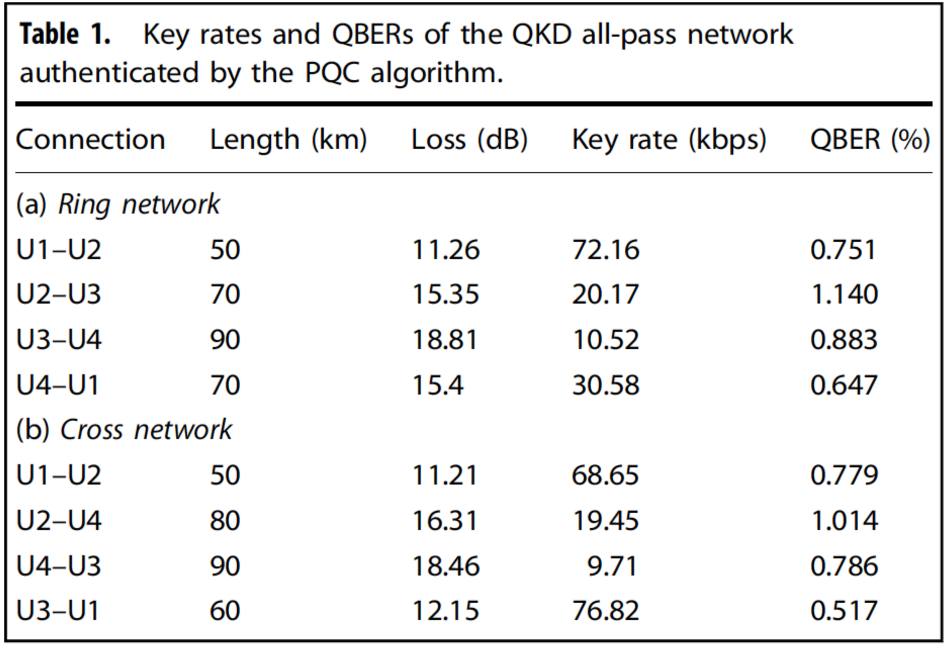


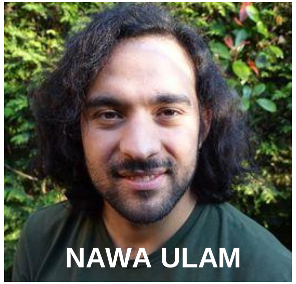
Table 1. Key rates and QBERs of the QKD all-pass network authenticated by the PQC algorithm.

Connection	Length (km)	Loss (dB)	Key rate (kbps)	QBER (%)
(a) *Ring network*				
U1–U2	50	11.26	72.16	0.751
U2–U3	70	15.35	20.17	1.140
U3–U4	90	18.81	10.52	0.883
U4–U1	70	15.4	30.58	0.647
(b) *Cross network*				
U1–U2	50	11.21	68.65	0.779
U2–U4	80	16.31	19.45	1.014
U4–U3	90	18.46	9.71	0.786
U3–U1	60	12.15	76.82	0.517

European Funds
Smart Growth

FNP Foundation for Polish Science

European Union
European Regional Development Fund



This place for your photo
☺

MARIE CURIE ACTIONS

Ministerstwo Edukacji i Nauki

NAWA
NARODOWA AGENCJA WYMIANY AKADEMICKIEJ

Thanks!

Any questions? Drop me a line!

magdalena.stobinska@gmail.com

www.stobinska-group.eu