Cybersecurity Management
T10 – Quantum Security

2025-2026

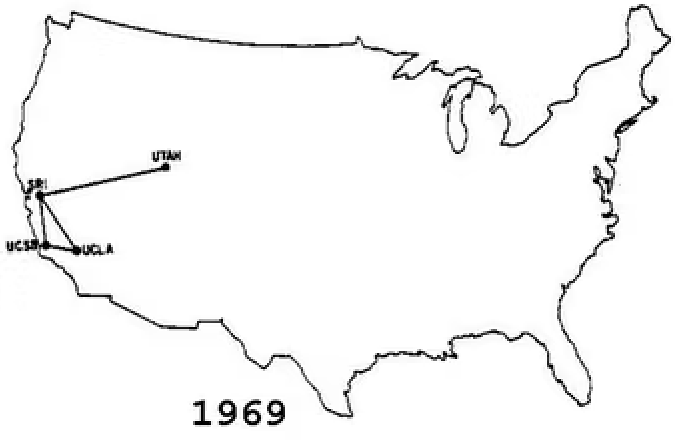
Prof. Marc Ruiz

marc.ruiz-ramirez@upc.edu

Quantum – Where we are?

Like at the birth of the Internet…

29 October 1969
LOGIN
We typed the L and asked on the phone: “Did you see the L?”
“ Yes, we see the L”
We typed the O and asked on the phone: “Did you see the O?
“ Yes, we see the O”
Then we typed G and the System actually crashed



Taking from the talk of Stephanie Wehner

Warm start

- https://www.youtube.com/watch?v=90za6mazNps

Classical vs Qubit

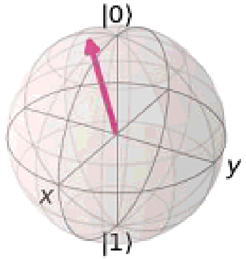
Classical

0

1

Quantum

0+1

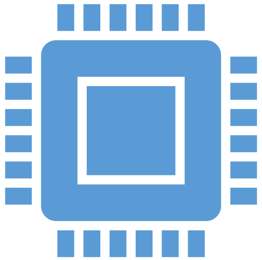


$$|\Psi\rangle_{a_0} = \alpha\,|0\rangle_{a_0} + \beta\,|1\rangle_{a_0}$$

With 275 qubits, we can represent more basis states than the number of atoms in the observable universe

2^{275}

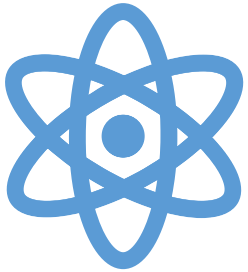
Quantum Technologies



Quantum computing

Speed-up tasks

- Quantum database search (Grover's algorithm)
- Quantum prime number factorization (Shor’s algorithm)

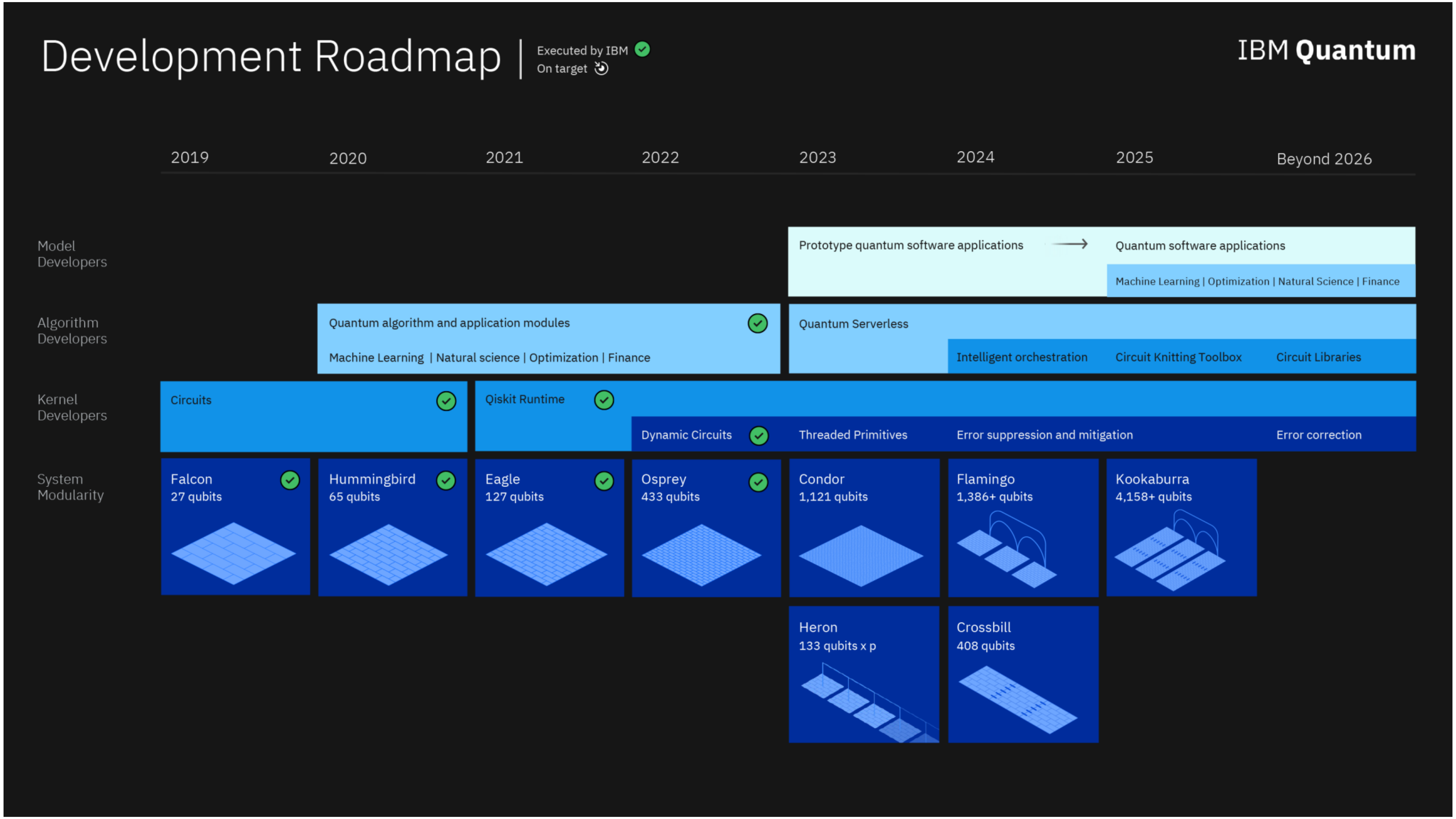


Quantum communication

Secure communication

Efficiency

Quantum Computing – Where we are?



Applications of Quantum Communication

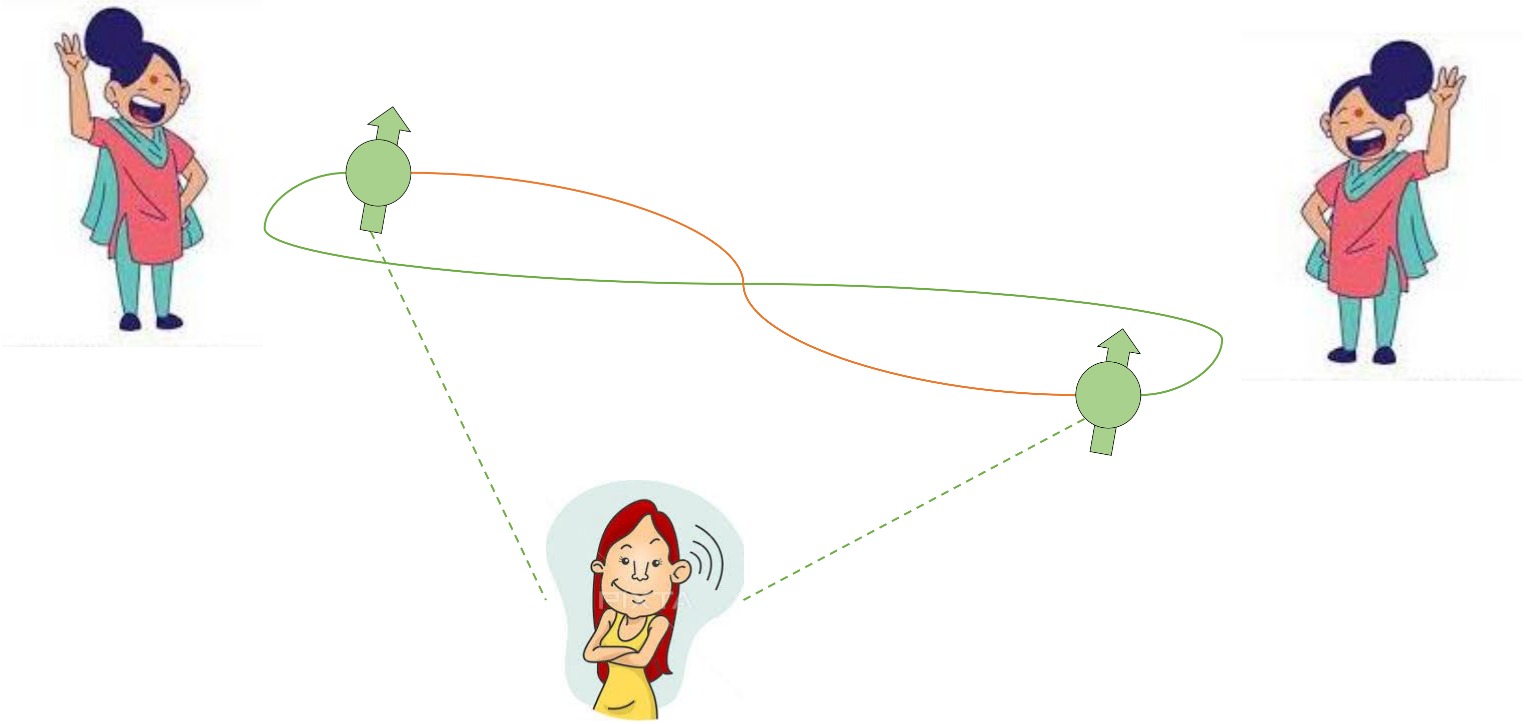
- Secure Communication
- Secure Quantum Computing in the cloud
- Secure Identification
- Clock Synchronization
- Position Verification
- Online Games

No-Cloning theorem

- The no-cloning theorem states that it is impossible to create an independent and identical copy of an arbitrary unknown quantum state

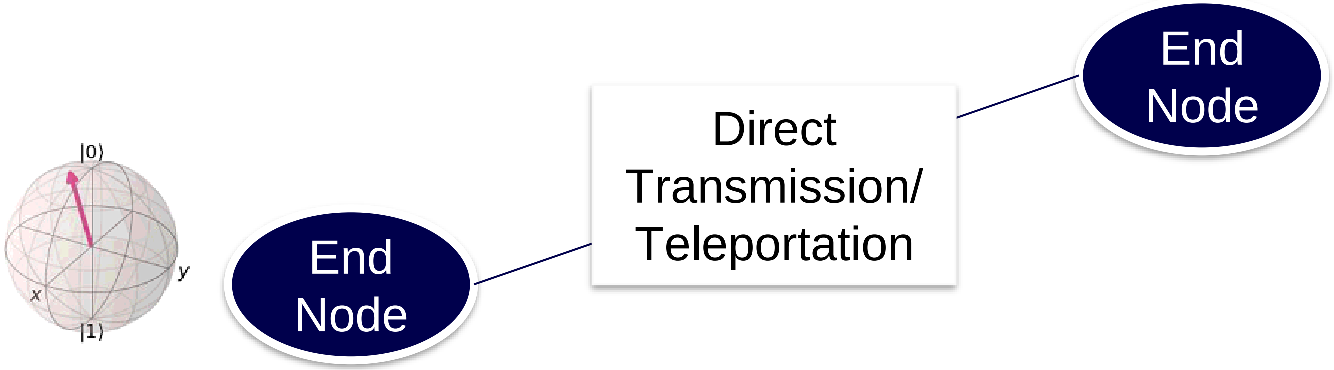
Entanglement

It strongly correlates two particles, that measurement of one can tell the measurement result of the other, even if they are far apart.



https://youtu.be/nkLPsJPxad0

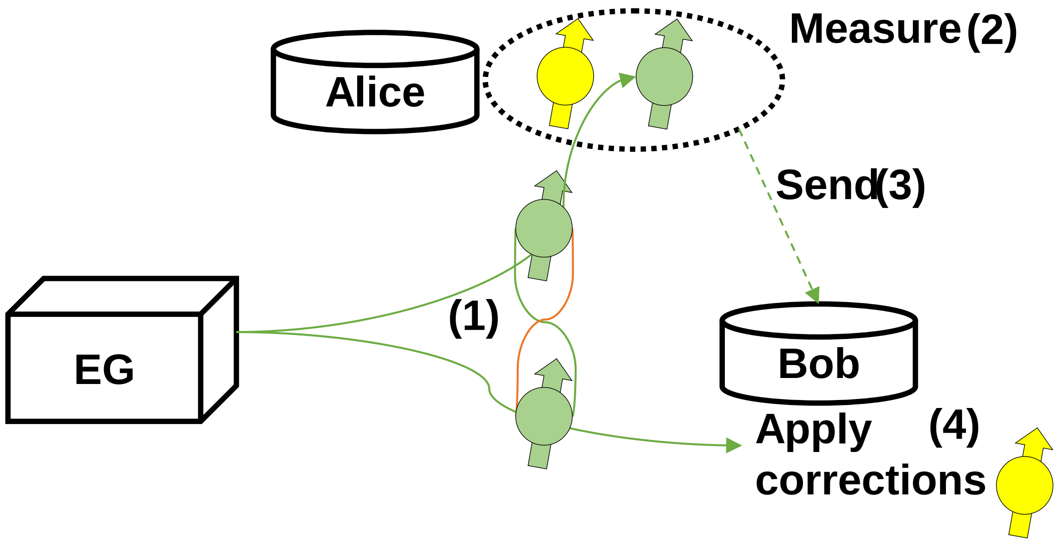
Methods of qubit transmission



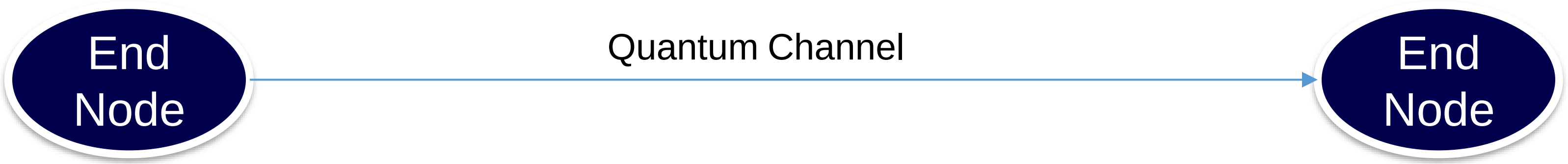
Direct Transmission: Using Quantum Channel
Teleportation: Take advantage of two classical bits and an entangled qubit pair and avoid using quantum channel

Teleportation Protocol

- Alice prepares the state, she wants to send.
- An entanglement is created and shared between Alice and Bob.
- Alice performs measurement.
- Alice sends the measurement results to Bob.
- Bob applies gates according to results



Challenges of direct transmission



Transmission Losses

- Losses in transmission media

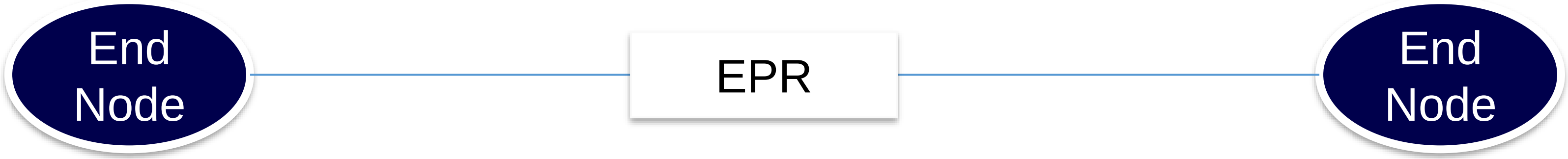
Decoherence

- Interaction with environment

No cloning theorem

- Qubits can’t be copied

Challenges of teleportation



Transmission Losses

- Losses in transmission media

Decoherence

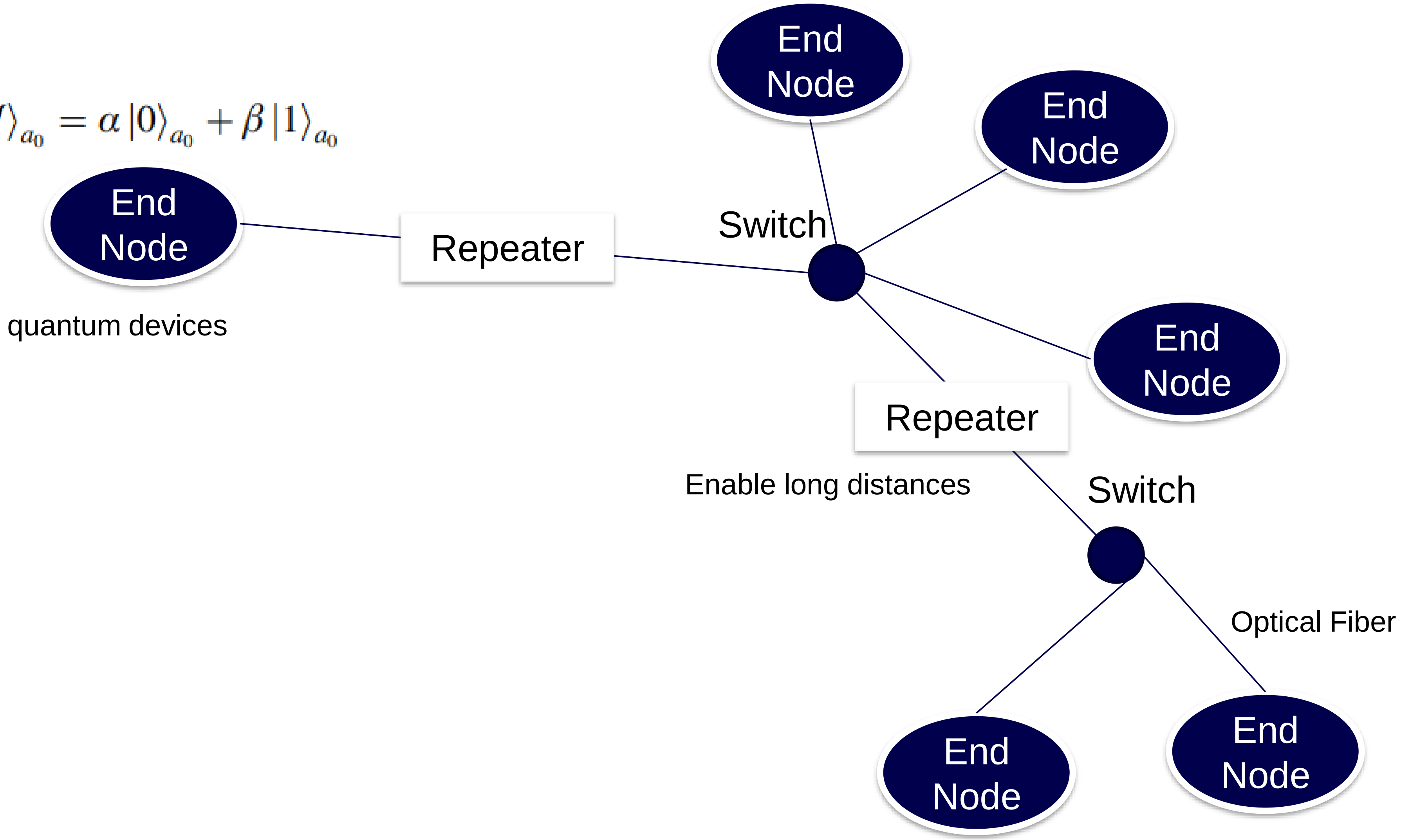
- Interaction with environment

Source fidelity

- Quality of generated entanglement pairs

Quantum Network

$$|\Psi\rangle_{a_0} = \alpha\,|0\rangle_{a_0} + \beta\,|1\rangle_{a_0}$$



Takeaways

Qubits are very fragile and are prone to many losses.

So, we don't transmit Qubits over long distances

We can use entanglement assistance to teleport the qubit without transmitting the qubit through a quantum channel.

But entanglement pairs are also qubits, so we can't send the pair over long distances too.

So, we generate multiple entanglement pairs, and through teleportation perform entanglement swapping to enable long-distance entanglement distribution.

Quantum Key Distribution

“The” encryption: One Time Pad

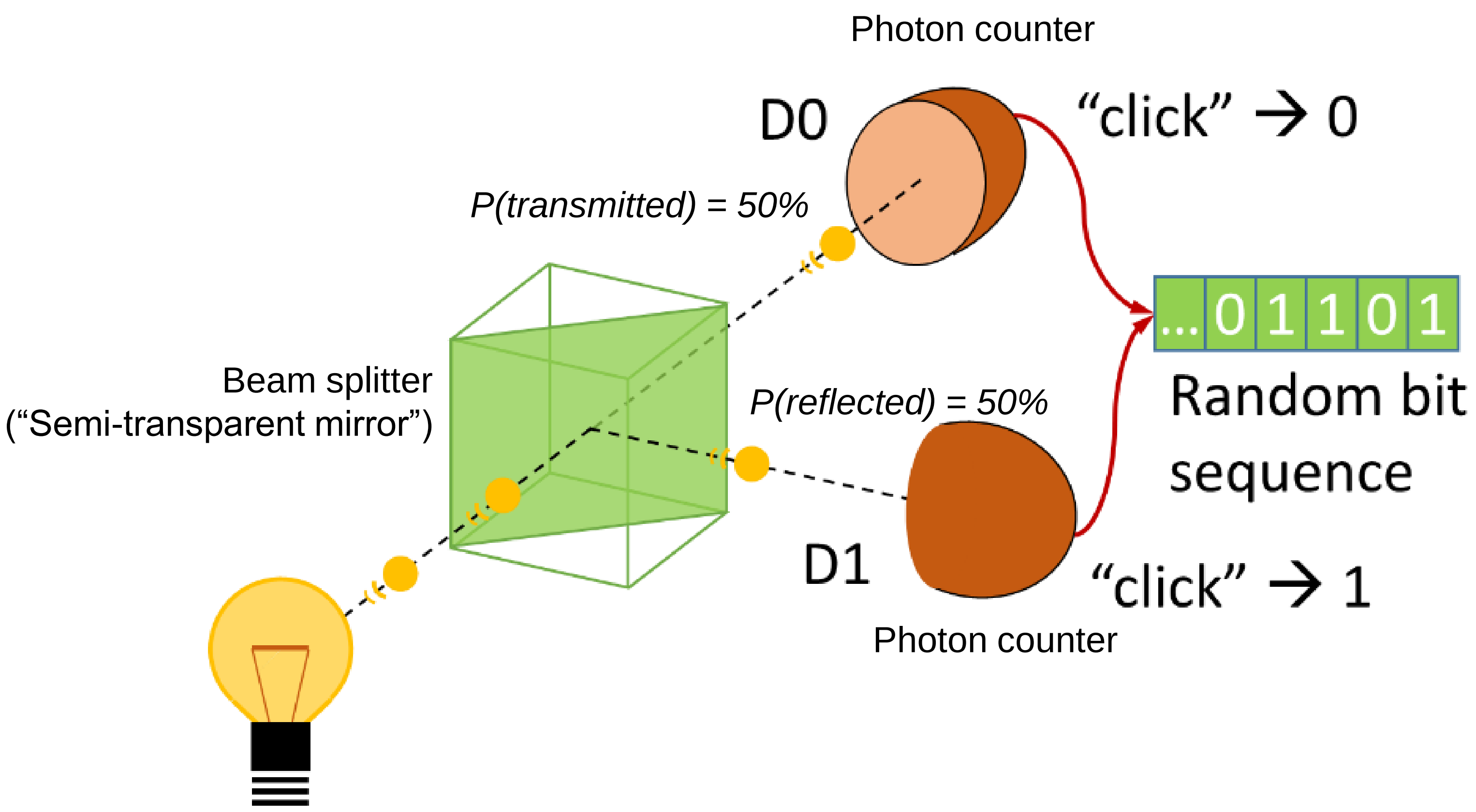
Text	1	1	0	0	1	1	0	1
$\oplus$								
Key	0	1	0	1	1	0	1	0
Cyphertext	1	0	0	1	0	1	1	1

XOR	0	1
0	0	1
1	1	0

- **Proven security if:**
  - Length text = Length key
  - Key is used one time only
  - Key is generated **randomly**

Quantum Random Number Generators (QRNG) can do this!!!

QRNG

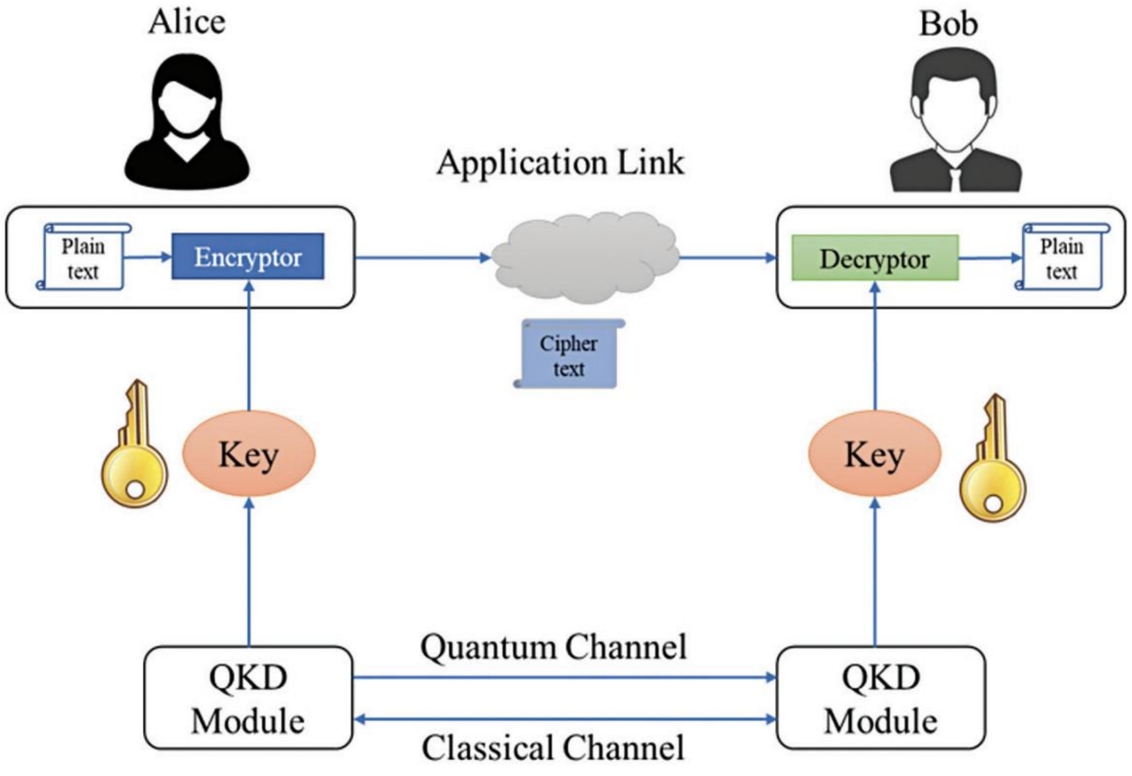


Currently, they achieve low rates: ~4 Mb/s

https://idquantique.com

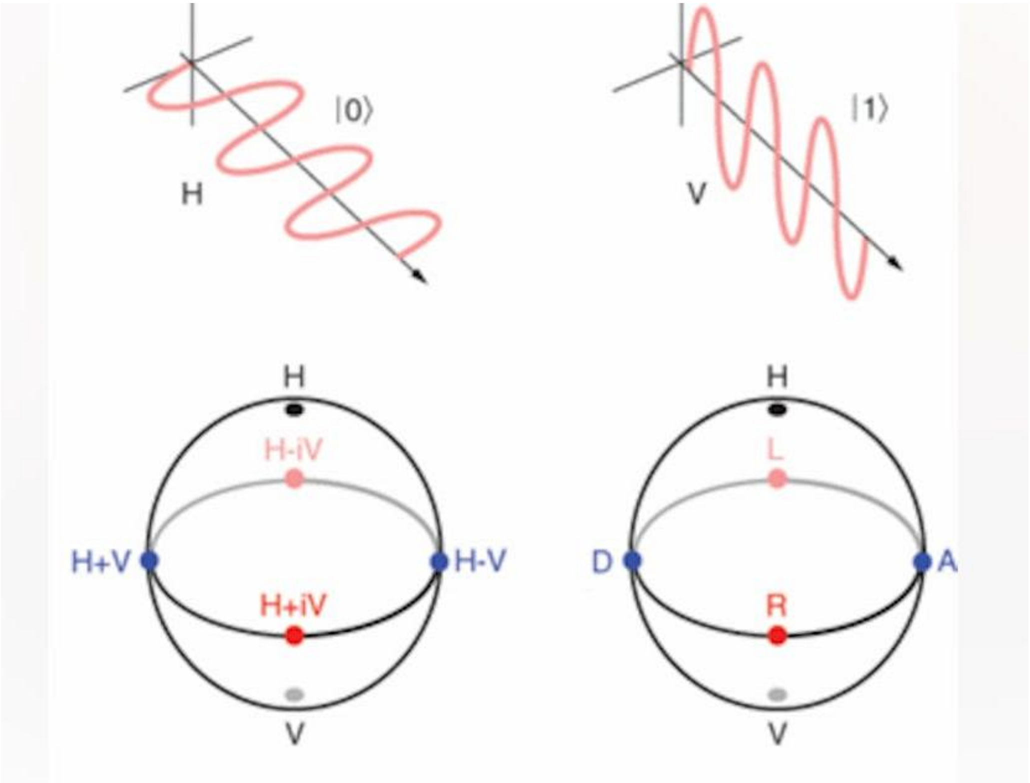
Quantum Key Distribution (QKD)

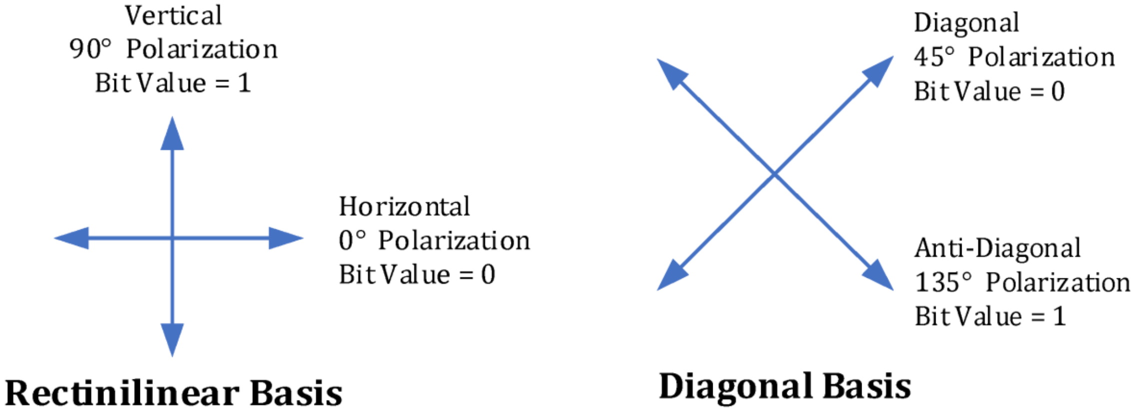
- It enables two parties to produce a shared random **secret key** known only to them, which can then be used to encrypt and decrypt messages
- The two communicating users can detect the presence of any third party trying to gain knowledge of the key (**eavesdropping**)
- Qubits are coded into quantum particles (photons), e.g., using polarization
- Any measurement by an eavesdropper will alter qubit state (photon polarization) and this perturbation is going to be detected
- However other sources of noise (no eavesdropping) can introduce perturbations



https://www.youtube.com/watch?v=Hm2Nmw_gnMQ

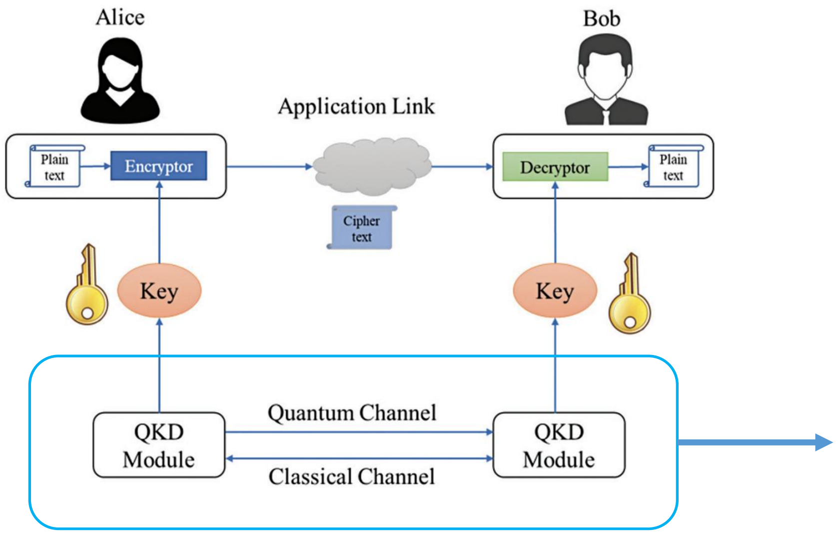
Encoding qubits as photons

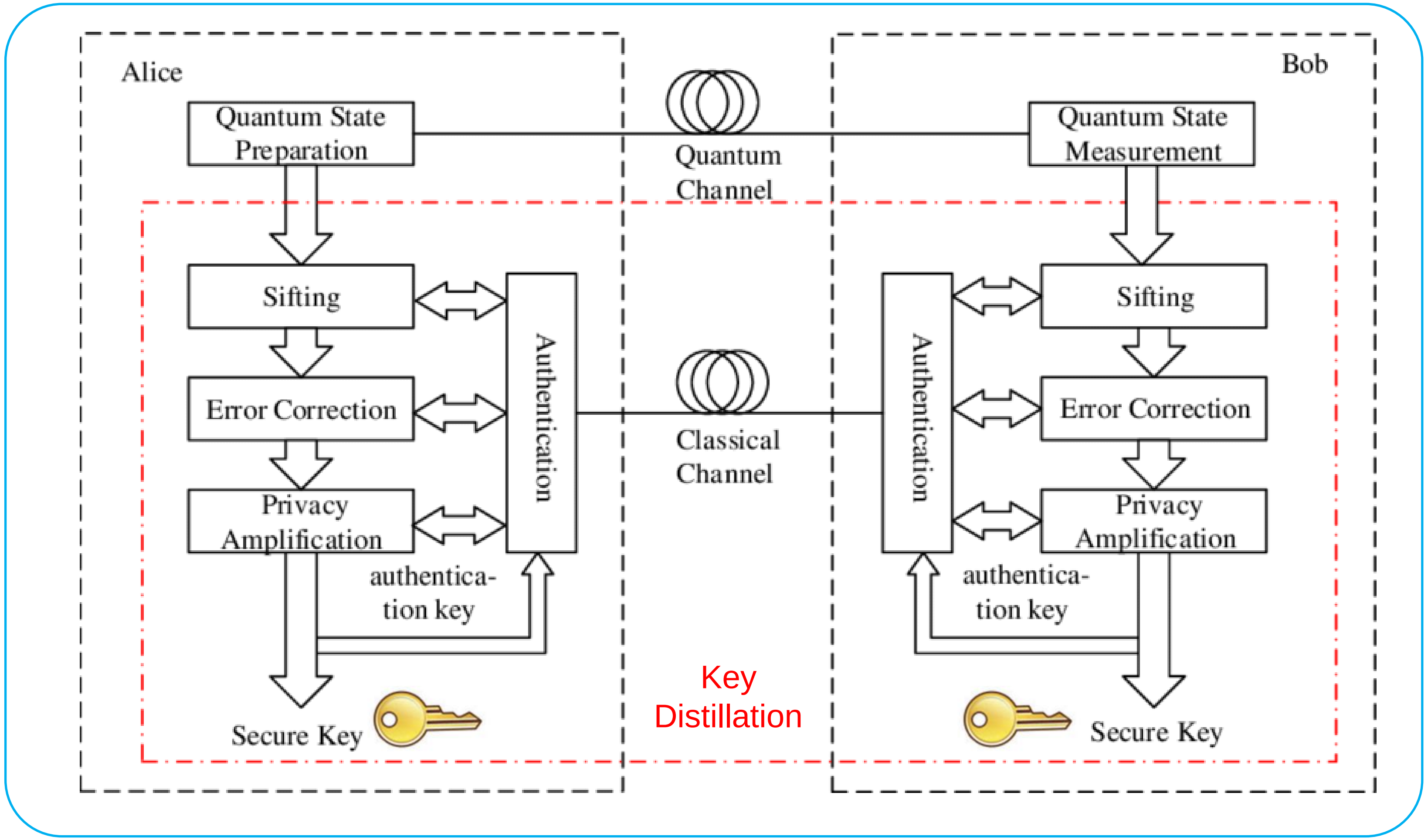




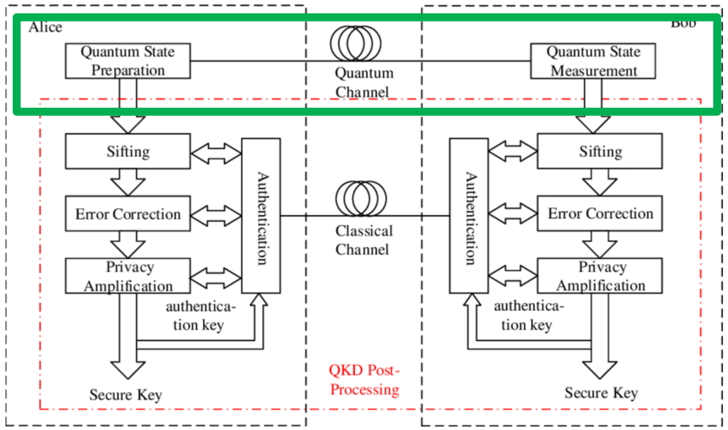
BB84 Protocol

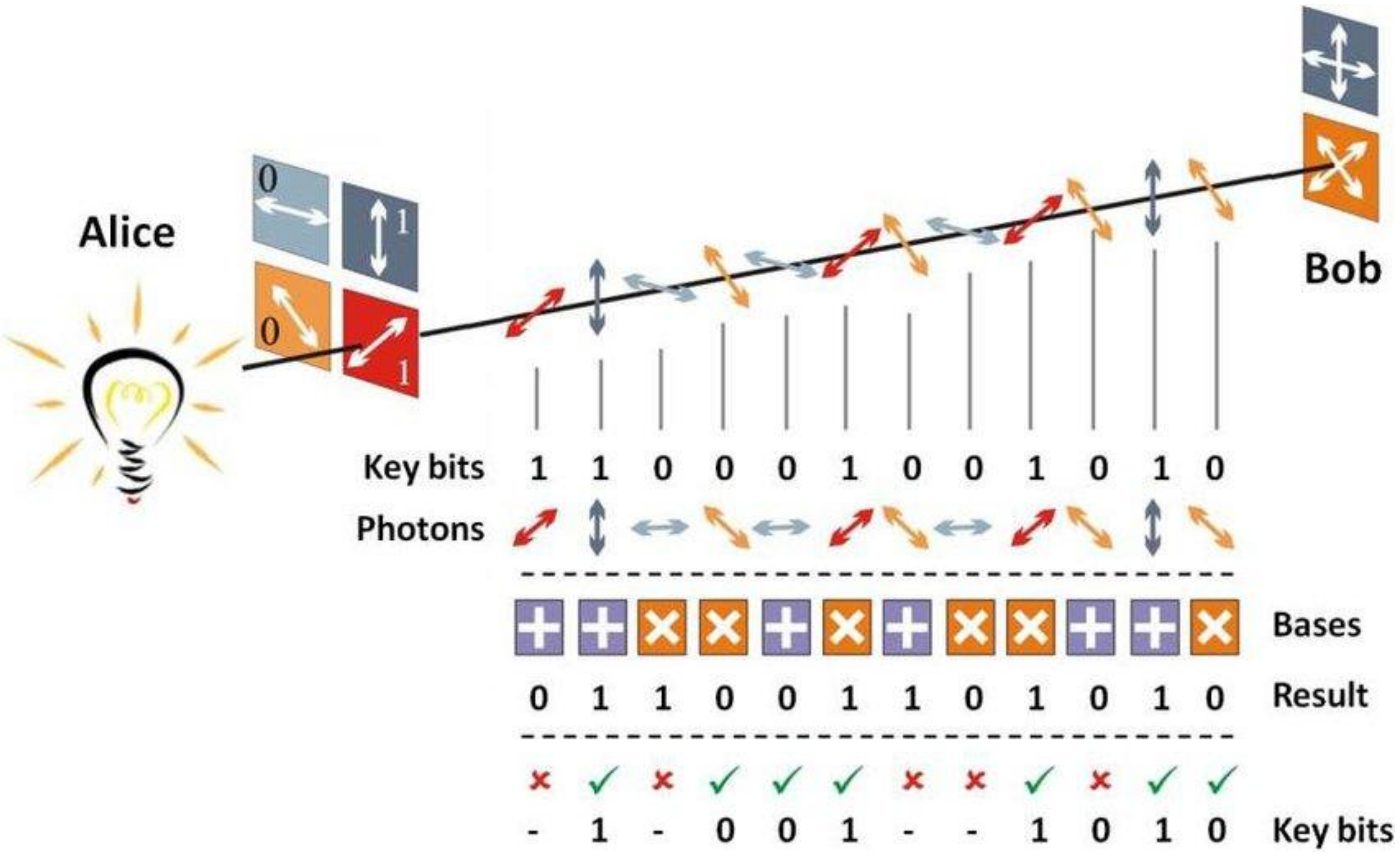
- Oldest protocol, works for polarization-encoded QKD systems
- Several phases:
  - Distribution
  - Sifting
  - Error estimation and correction
  - Privacy amplification



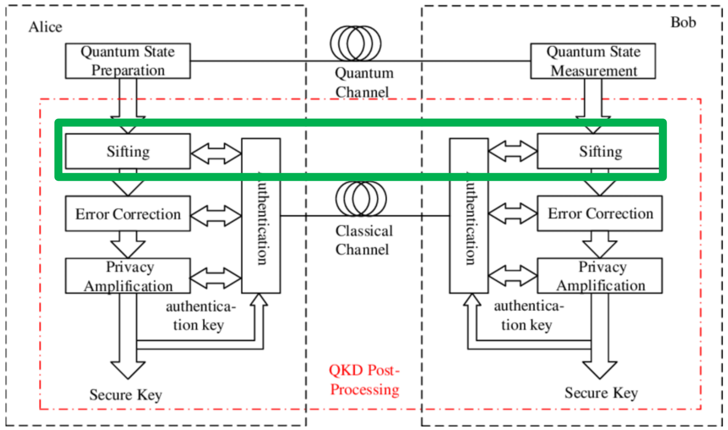


BB84 - Distribution



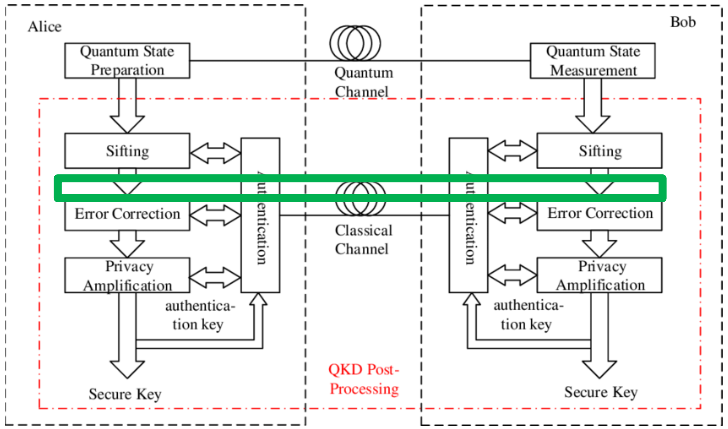


BB84 – Key sifting



Alice's selected basis	+	x	x	+	x	+	+	+	x	+	x	x
Alices's selected states	↑	↗	↗	→	↘	→	↑	↑	↗	→	↘	↘
Alice's raw-key	1	0	0	0	1	0	1	1	0	0	1	1
Bob's selected basis	+	+	x	+	x	X	+	+	x	+	+	x
Bob's measured states	↑	→	↗		↘	↘	↑	↑	↗	→		↘
Bob's raw-key	1	0	0		1	1	1	1	0	0		1
Alice's sifted-key	1		0		1		1	1	0	0		1
Bob's sifted-key	1		0		1		1	1	0	0		1

BB84 – Error estimation



Alice's selected basis	+	x	x	+	x	+	+	+	x	+	x	x
Alices's selected states	↑	↗	↗	→	↘	→	↑	↑	↗	→	↘	↘
Alice's raw-key	1	0	0	0	1	0	1	1	0	0	1	1
Bob's selected basis	+	+	x	+	x	X	+	+	x	+	+	x

Without eavesdropping

Bob's measured states	↑	→	↗		↘	↘	↑	↑	↗	→		↘
Bob's raw-key	1	0	0		1	1	1	1	0	0		1
Alice's sifted-key	1		0		1		1	1	0	0		1
Bob's sifted-key	1		0		1		1	1	0	0		1

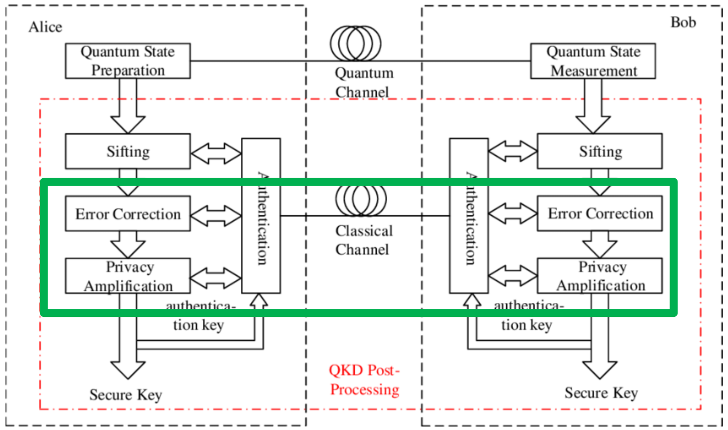
With eavesdropping

Bob's measured states	↑	→	↗		$\underline{\nearrow}$	↘	↑	↑	↗	$\underline{\uparrow}$		↘
Bob's received bits	1	0	0		0	1	1	1	0	1		1
Alice's sifted-key	1		0		1		1	1	0	0		1
Bob's sifted-key	1		0		0		0	1	0	1		1

A sample is chosen, shared, and if **errors > 10%**, it is assumed that there is **eavesdropping** and the key is **discarded**

https://www.youtube.com/watch?v=2kdRuqvIaww

BB84 – Last steps



- Error correction
  - Aka, information reconciliation
  - Needed to correct the rest of bits that were not discarded during error estimation
  - Using a cascade protocol, Bob can correct errors exposing (leaking) a minimum amount of bits through the classical channels
  - Eavesdropper can get significant information about keys in this phase
  - Process ends with identical Alice and Bob secret keys

- Privacy amplification
  - Using a hash function, a secret key of length *n* is transformed into a shorter one of length $m<<n$
  - In this way, potential information retrieved by eavesdropper is cancelled.

Some numbers

Obtained with https://www.qkdsimulator.com

Initial Configuration							
Property Qubit Count	Basis choice bias delta	Eve basis choice bias delta	Eavesdropping	Eavesdropping rate	Error estimation sampling rate	Biased error estimation	Error tolerance
1000	0.5	0.5	0	0.1	0.2	0	0.11

Statistics and Overview

Property	Value
Initial number of qubits	1000
Final key length	343
Raw key mismatch before error correction	0.0
Raw key mismatch after error correction	0
Information leakage (Total number of disclosed bits)	52
Overall key cost for authentication	256
Key length before error correction	415
Bit error probability	0.0
Bits leaked during error correction	20

Some numbers

Obtained with https://www.qkdsimulator.com

Initial Configuration

Property Qubit Count	Basis choice bias delta	Eve basis choice bias delta	Eavesdropping	Eavesdropping rate	Error estimation sampling rate	Biased error estimation	Error tolerance
1000	0.5	0.5	1	0.2	0.2	0	0.11

Statistics and Overview

Property	Value
Initial number of qubits	1000
Final key length	234
Raw key mismatch before error correction	0.0438
Raw key mismatch after error correction	0
Information leakage (Total number of disclosed bits)	166
Overall key cost for authentication	256
Key length before error correction	420
Bit error probability	0.0405
Bits leaked during error correction	134

Commercial QKD

- IDquantique

IDQ Random Number Generation | Quantum-Safe Security | Quantum Sensing | What's New | Resources | About IDQ

Home | Quantum-Safe Security | Products | Clavis XG QKD System

Back to products

Clavis XG QKD System

Quantum Key Distribution for production environments requiring high key transmission rate or extended range interconnection

- Long range (up to 150 km)
- High key rate (>100 kb/s)
- Complex network topologies (ring, hub and spoke, meshed, star)
- Controlled and monitored centrally
- Interoperability with major Ethernet and OTN encryptors

DOWNLOAD BROCHURE

VIEW USE CASES

HOW TO BUY

Local SME on Quantum

- LuxQuanta -> Continuous Variable QKD

LUXQUANTA

Solutions | About us | Resources | News | Careers | Contact us

LuxQuanta® Continuous Variable Quantum Key Distribution system

Adding quantum security to optical networks

LuxQuanta Continuous Variable Quantum Key Distribution (CV-QKD) systems are ideal for distributing highly secure keys in metropolitan networks, integrating this technology into existing optical fiber links and coexisting with conventional telecommunication technologies.

Contact us for more information

Built with mature telecommunication components

Easy network integration

High performance at metro distances

Reduced system and implementation cost

A clear path to future scalability via full photonic integration

Recent research

JOURNAL OF LIGHTWAVE TECHNOLOGY, VOL. 40, NO. 13, JULY 1, 2022 4119

Cost-Effective ML-Powered Polarization-Encoded Quantum Key Distribution

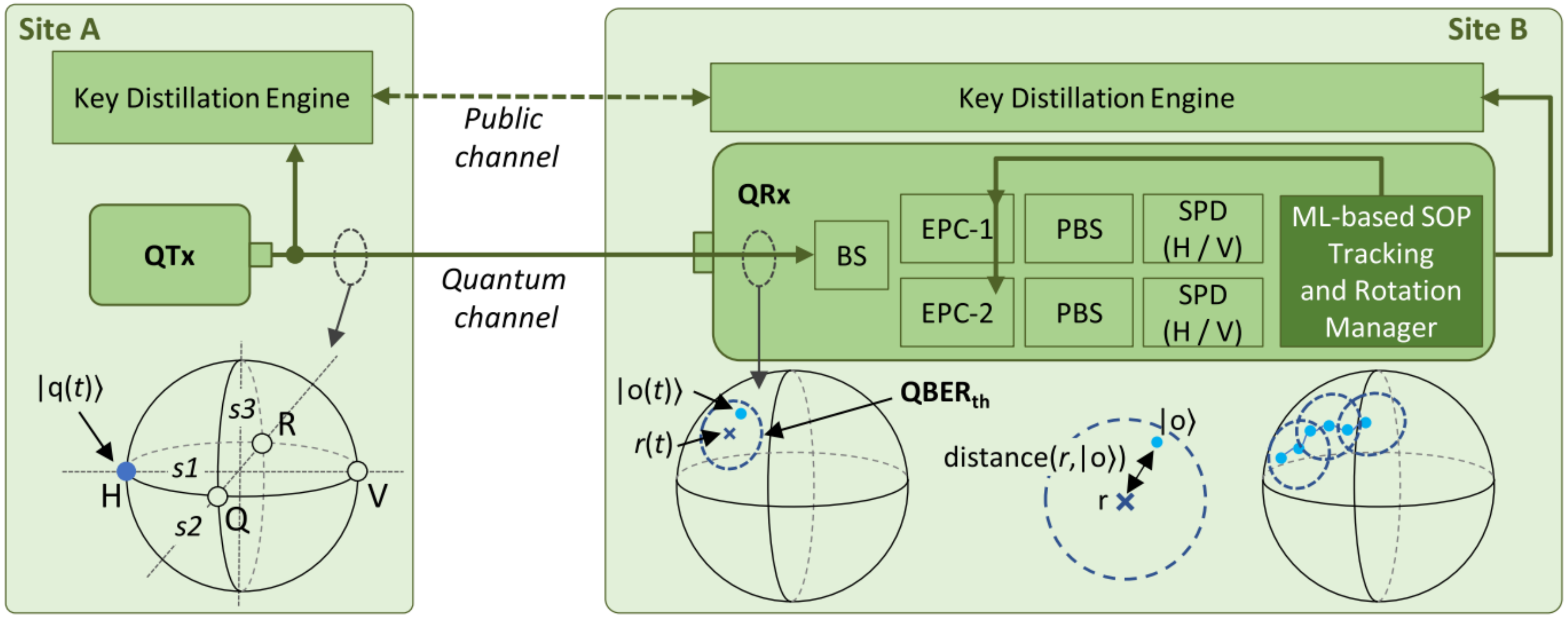
Morteza Ahmadian, Marc Ruiz, Jaume Comellas, and Luis Velasco

Recent research

JOURNAL OF LIGHTWAVE TECHNOLOGY, VOL. 40, NO. 13, JULY 1, 2022 4119

Cost-Effective ML-Powered Polarization-Encoded Quantum Key Distribution

Morteza Ahmadian, Marc Ruiz, Jaume Comellas, and Luis Velasco

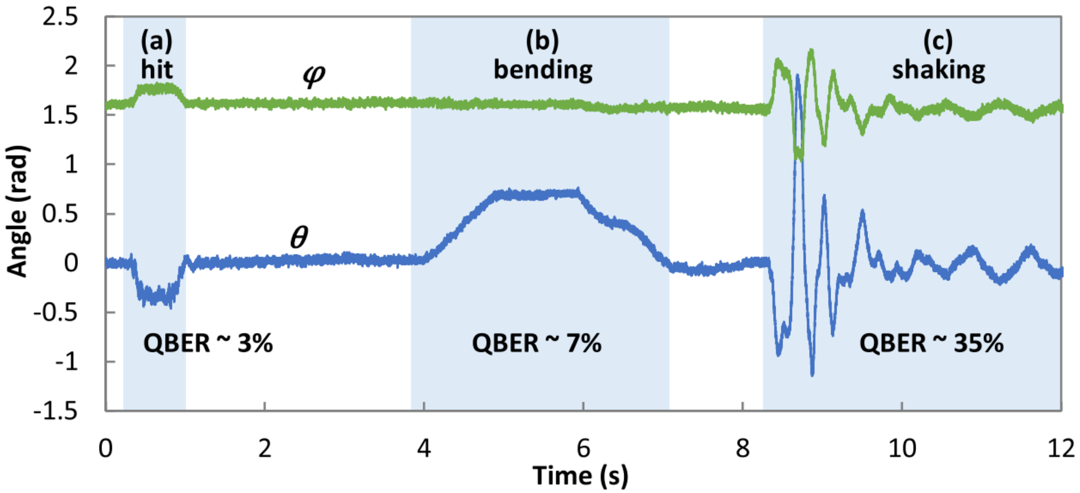


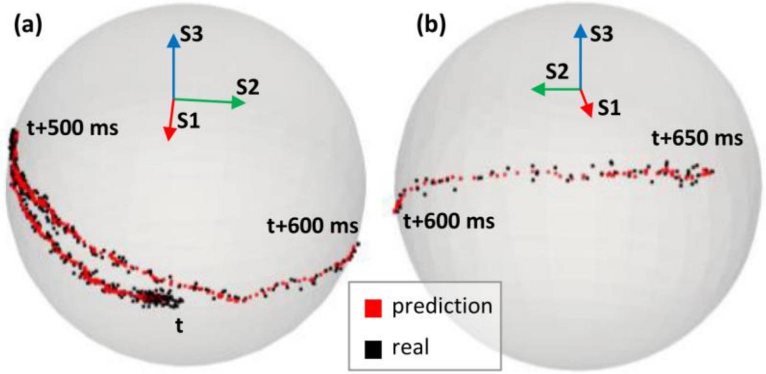
Recent research

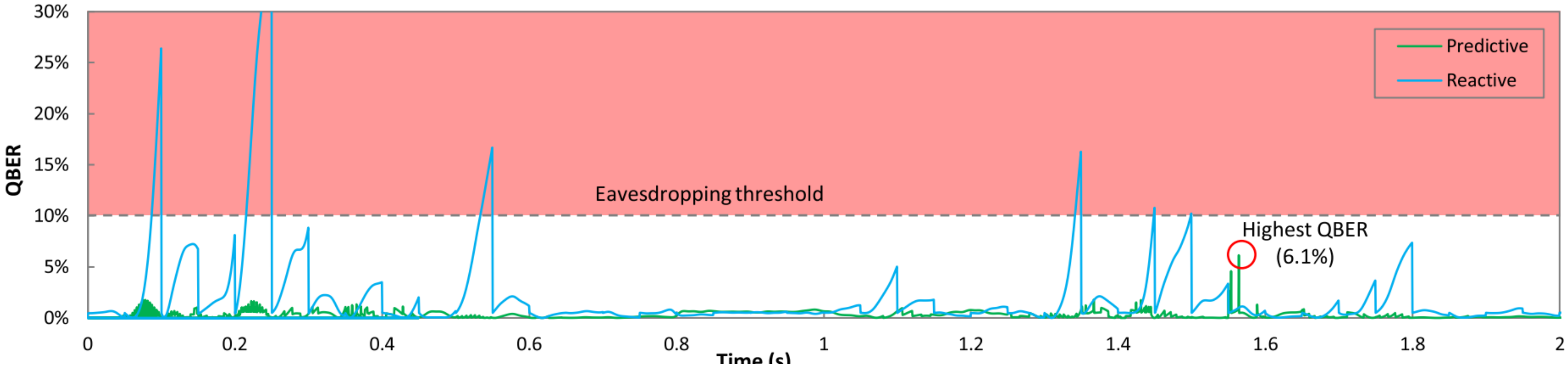
JOURNAL OF LIGHTWAVE TECHNOLOGY, VOL. 40, NO. 13, JULY 1, 2022 4119

Cost-Effective ML-Powered Polarization-Encoded Quantum Key Distribution

Morteza Ahmadian, Marc Ruiz, Jaume Comellas, and Luis Velasco







Post-Quantum Cryptography

Classical Cryptography

- Uses difficult mathematical problems to protect data from non-quantum threats.
- Encompasses the standard encryption algorithms that pretty much every business or government entity uses today to protect its data.
  - AES (Advanced Encryption Standard)
  - RSA (Rivest-Shamir-Adleman).
- Built on math problems like large number factorization and discrete logarithms.
- Vulnerable to quantum threats
  - Shor's algorithm is a quantum algorithm for finding the prime factors of an integer.

Post-Quantum Cryptography

- Evolution of classical cryptography.
- Based on math problems, that are not tractable by quantum computers..

Lattice-based cryptography	Code-based cryptography	Multivariate-based cryptography
Based on abstract structures of mathematics. It currently looks like the most promising method.	Uses error-correcting-codes that allows read or data being transmitted to be checked for errors and corrected in real time.	Based on solving multi variable equations. These equations are hard to solve using brute force.

References QKD

- Wehner, Stephanie & Elkouss, David & Hanson, Ronald. (2018). Quantum internet: A vision for the road ahead. Science. 362. eaam9288. 10.1126/science.aam9288.
- Introduction to QKD
    - https://medium.com/quantum-untangled/quantum-key-distribution-and-bb84-protocol-6f03cc6263c5
- BB84 short video
    - https://www.youtube.com/watch?v=2kdRuqvIaww
- Online QKD simulator
    - https://www.qkdsimulator.com/
- Open-Source Quantum Development
    - https://qiskit.org/
- https://en.wikipedia.org/wiki/Post-quantum_cryptography

Cybersecurity Management
T10 – Quantum Security

2025-2026

Prof. Marc Ruiz

marc.ruiz-ramirez@upc.edu