AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

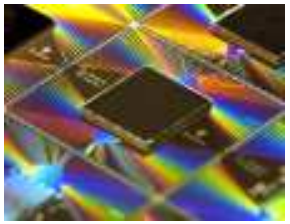
DIVING INTO QUANTUM COMMUNICATIONS: AN EXPERIMENTAL OVERVIEW

Dr. Mariana Ramos– AIT Austrian Institute of Technology

QUANTUM TECHNOLOGY RESEARCH @ AIT

AUSTRIAN INSTITUTE OF TECHNOLOGY

Secure Communication in the Age of Quantum Computers



Quantum Key Distribution Networks

Quantum Internet

Quantum Random Numbers

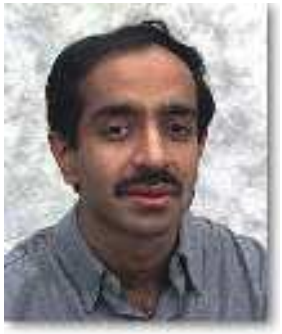
25+ researchers and engineers – 1 lab

A BIT OF HISTORY

RSA → Based on computational complexity.

Public key

Private key



1994 Peter Shor - Integer factorization which runs in polynomial time in a quantum computer.

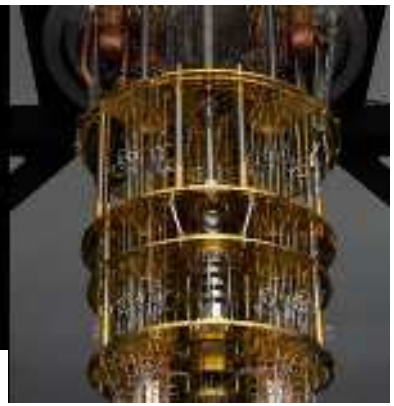
1996 Lov Grover - searching problem can be solved by a quantum computer performing brute-force inversions of one-way functions

2019 - The superior computational power of a quantum computer with 54 qubits goes already beyond the largest classical supercomputer.

Article

Quantum supremacy using a programmable superconducting processor

SOME RECENT NEWS



https://phys.org/news/2023-08-quantum.html

https://www.forbes.com/sites/bernardmarr/2023/08/16/how-quantum-safe-is-your-business/

Top ten data breaches in 2023

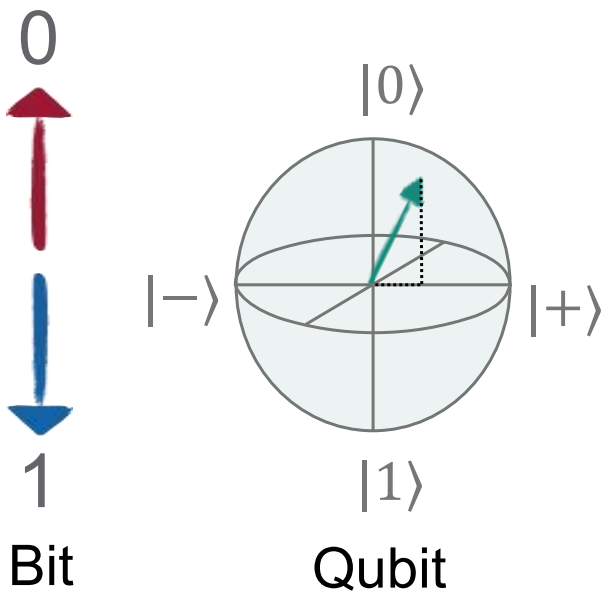
	Organisation name	Sector	Location	Known records breached	Month of public disclosure
1	DarkBeam	Cyber security	UK	>3,800,000,000	September
2	Real Estate Wealth Network	Construction/ real estate	USA	1,523,776,691	December
3	Indian Council of Medical Research (ICMR)	Healthcare	India	815,000,000	October
4	Kid Security	IT services/ software	Kazakhstan	>300,000,000	November
5	Twitter (X)	IT services/ software	USA	>220,000,000	January
6	TunnelBear	IT services/ software	Hong Kong	>151,000,000	December
7	Dori Media Group	Media	Israel	>100 TB*	December
8	Tigo	Telecoms	Hong Kong	>100,000,000	July
9	SAP SE Bulgaria	IT services/ software	Bulgaria	95,592,696	November
10	Luxottica Group	Manufacturing	Italy	70,000,000	May

source: https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023

QUANTUM MECHANICS: THE BASICS

AUSTRIAN INSTITUTE OF TECHNOLOGY

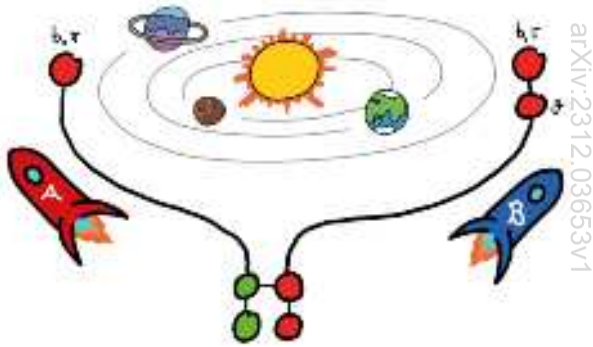
Superposition



Bit Qubit

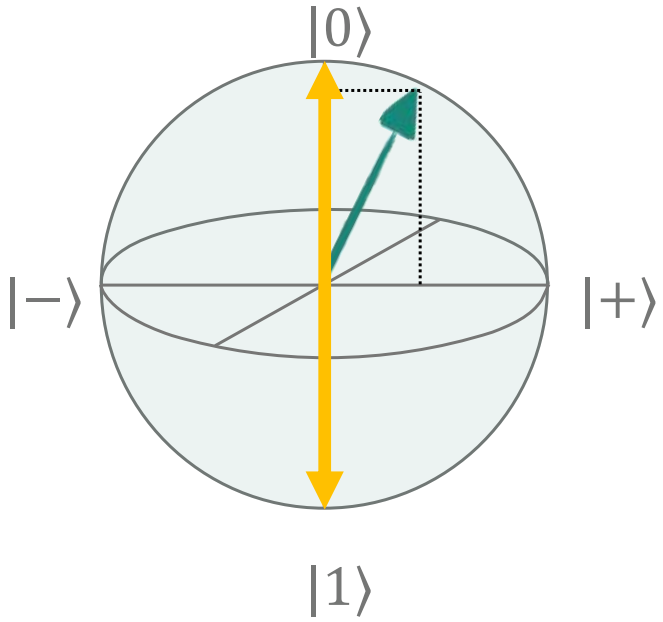
No-cloning

Entanglement



- *Spooky* action at a distance
- Non-local
- Super correlation

MEASURING A QUBIT GIVES A BIT



When we measure a qubit we **project** the **state** (arrow on sphere)

onto one line or **basis**.

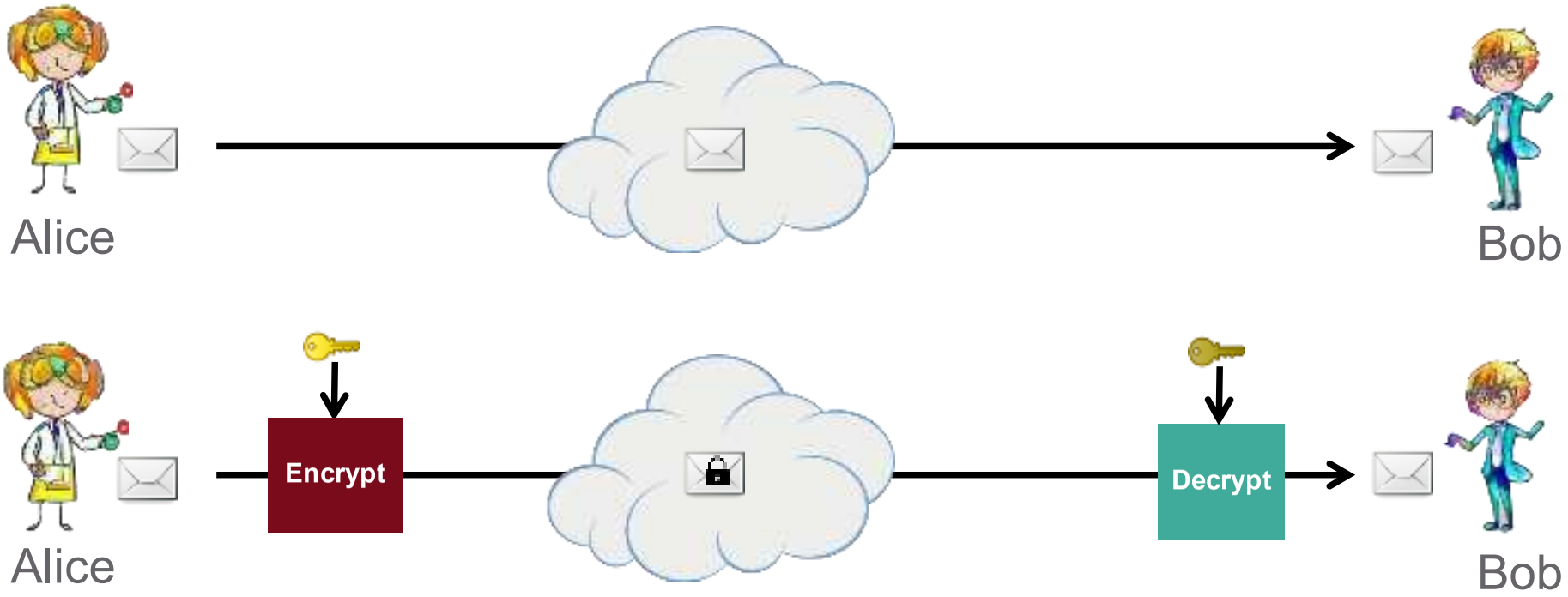
This will return a **bit** (0,1) as answer.

The **probability** of getting a particular answer depends on the **state** and the **basis**.

AUSTRIAN INSTITUTE OF TECHNOLOGY

Quantum Key Distribution

Using quantum physics to distribute a cryptographic key between two parties



Symmetric Crypto → Alice & Bob use same key

Asymmetric /Public Key Crypto → Alice and Bob use different Key

Alice & Bob by: craiyon.com

ONE-TIME PAD ENCRYPTION

AUSTRIAN INSTITUTE OF TECHNOLOGY

- Using a **random** key of the **same length as the message** to be encrypted
- If key is random and only used once, a OTP encryption **cannot be broken**
- **Information theoretically secure**
- How does it work?
  - Perform Exclusive OR (XOR) on message & key

Message	1	0	0	1	1	0
Key	0	0	1	0	1	1
Cipher	1	0	1	1	0	1

]XOR

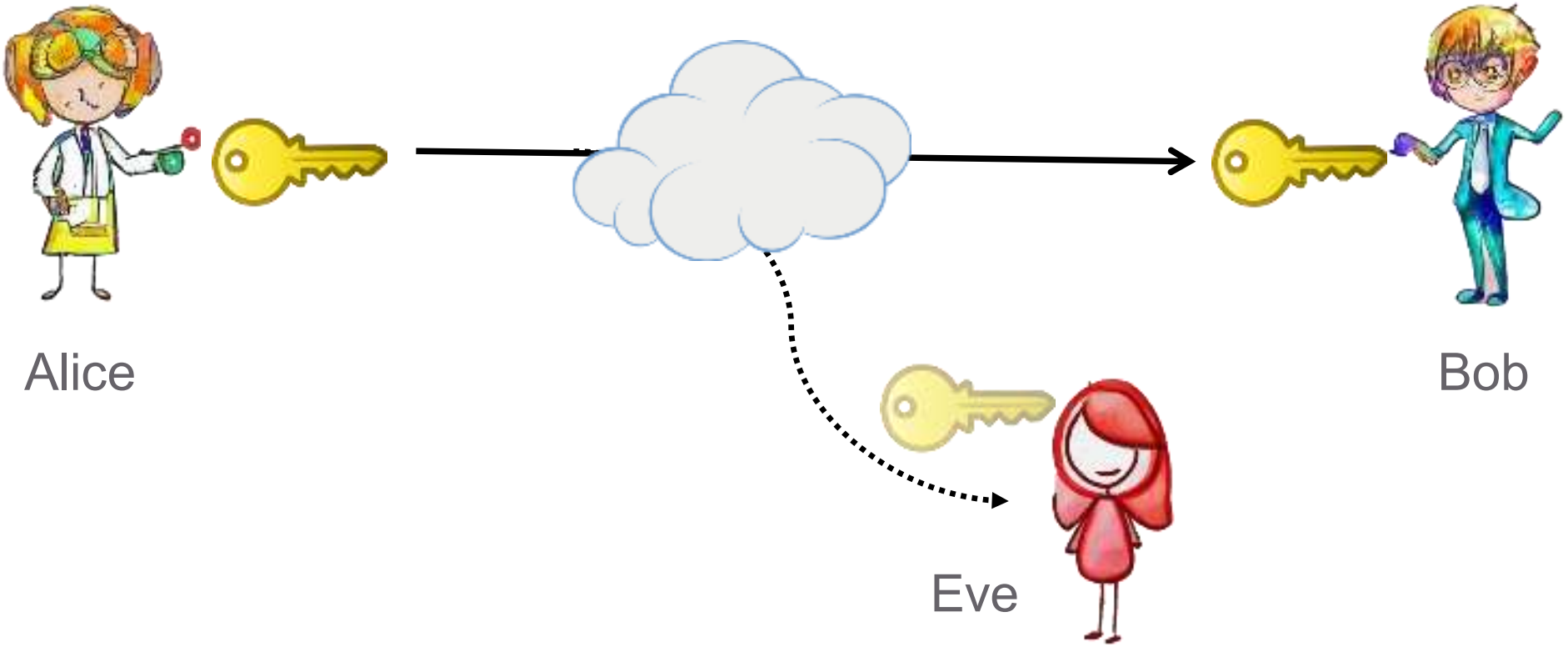
Cipher	**1**	**0**	**1**	**1**	**0**	**1**
Key	0	0	1	0	1	1
Message	1	0	0	1	1	0

]XOR

XOR

In	Out
0 0	0
0 1	1
1 0	1
1 1	0

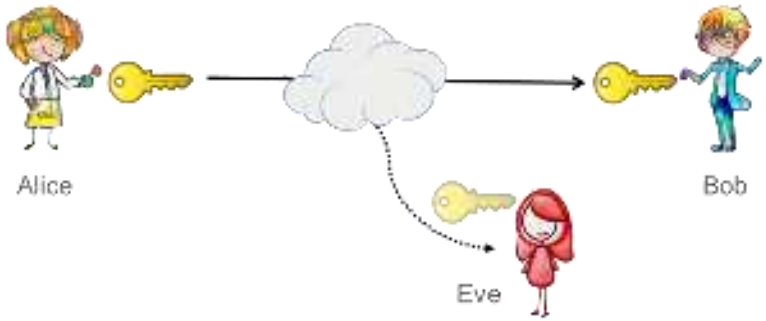
HOW DO WE DISTRIBUTE A KEY – SECURELY?



Alice, Bob & Eve by craiyon.com

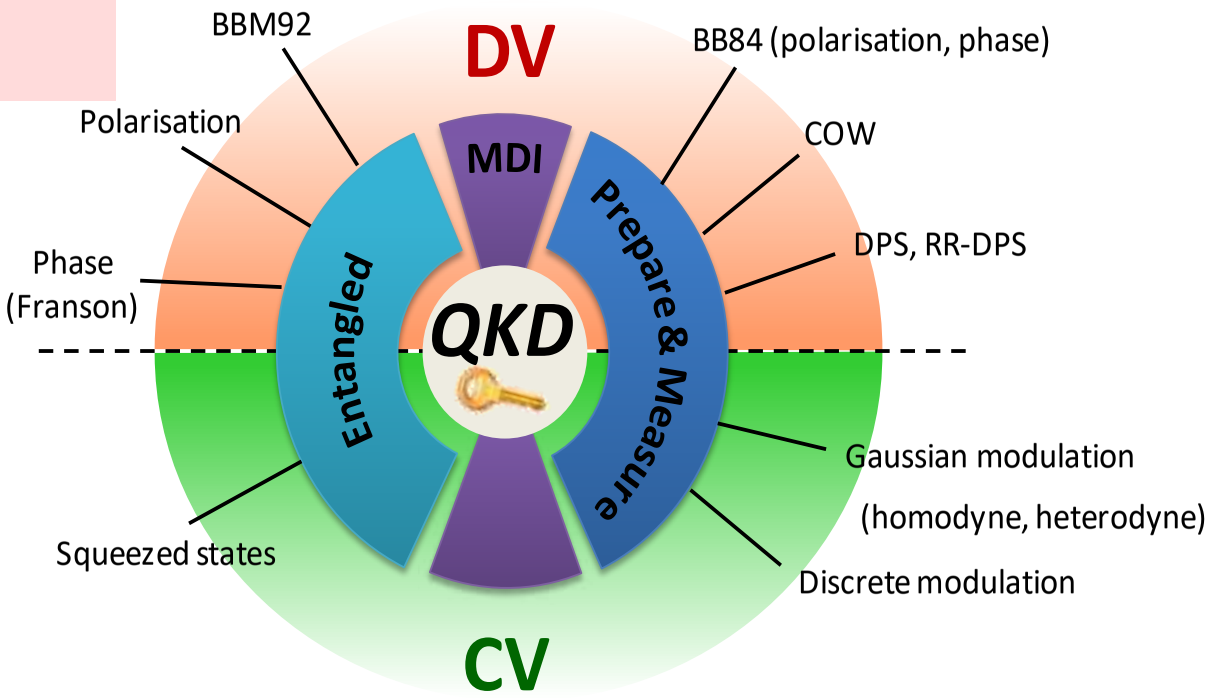
WE CAN USE THIS TO EXCHANGE A KEY

- Alice encodes her key into quantum states 
- Eve cannot copy the states 
- If Eve measures the states she changes them 
- Alice and Bob can detect if Eve was listening in



PHYSICAL IMPLEMENTATIONS

- Conceptually simpler
- More mature technology
- Expensive detectors required



Quantum Information carrier

Quantum information mostly encoded in

- Polarisation
- Time of arrival
- Optical phase

Quantum states:

- Entangled photons
- Weak coherent pulses (faint laser pulses)
- Coherent states (CV) avoiding single photon detectors

- Can be implemented based on standard telecom equipment
- Security proofs less mature
- Shorter range than DV

QKD AT AIT

AUSTRIAN INSTITUTE OF TECHNOLOGY

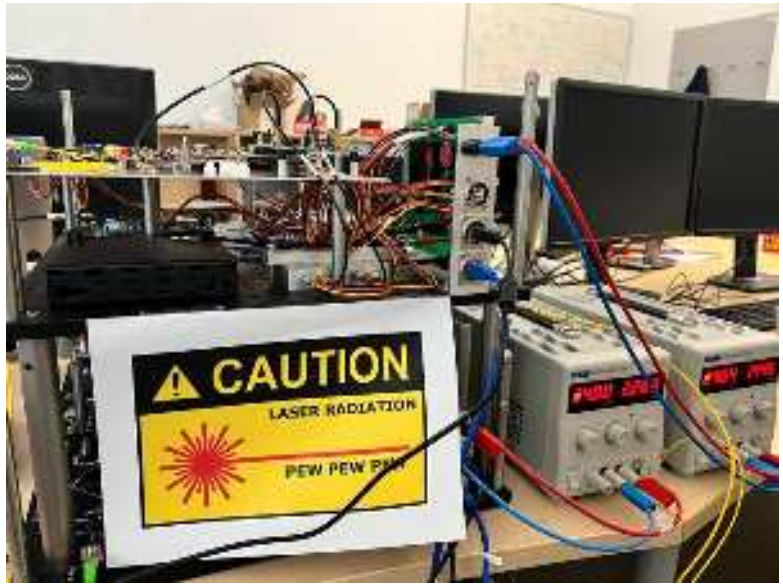
QKD system integration

Ingredients for a QKD system: Theory, Quantum Optics, Photonics, Electronics and Software

AIT designs, manufactures and test QKD systems for various protocols up to prototype stage

DV-QKD Polarization

CV-QKD



QKD AT AIT

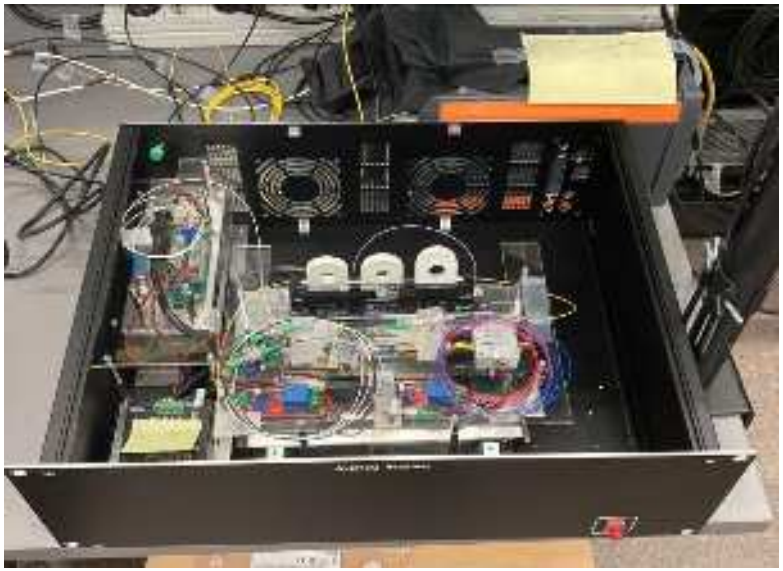
AUSTRIAN INSTITUTE OF TECHNOLOGY

QKD system integration

Ingredients for a QKD system: Theory, Quantum Optics, Photonics, Electronics and Software

AIT designs, manufactures and test QKD systems for various protocols up to prototype stage

DV-QKD suits for rack-scale integration

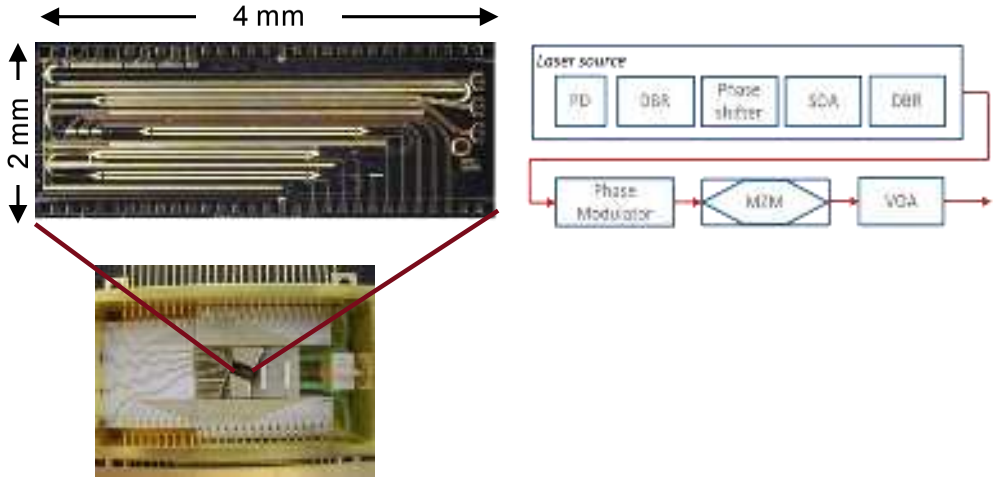


QKD BASED ON PHOTONIC INTEGRATED CIRCUITS

InP quantum-PIC

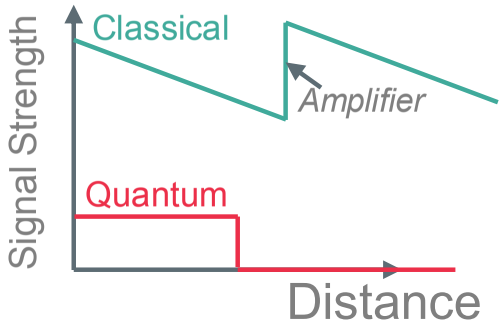
QKD transmitter chip (DV and CV)

- Laser
- Modulators (Phase, amplitude, I/Q)
- Passive elements (couplers, variable optical attenuators)
- Packaging with TEC and optical and RF outputs



LONG DISTANCE – A PRACTICAL CHALLENGE

- Quantum States cannot be copied
  - → we cannot use classical repeaters or amplifiers when photons are lost
- Trusted node networks allow for point-to-point security
- Quantum Repeaters would allow for end-to-end security but do not exist yet (ongoing research)



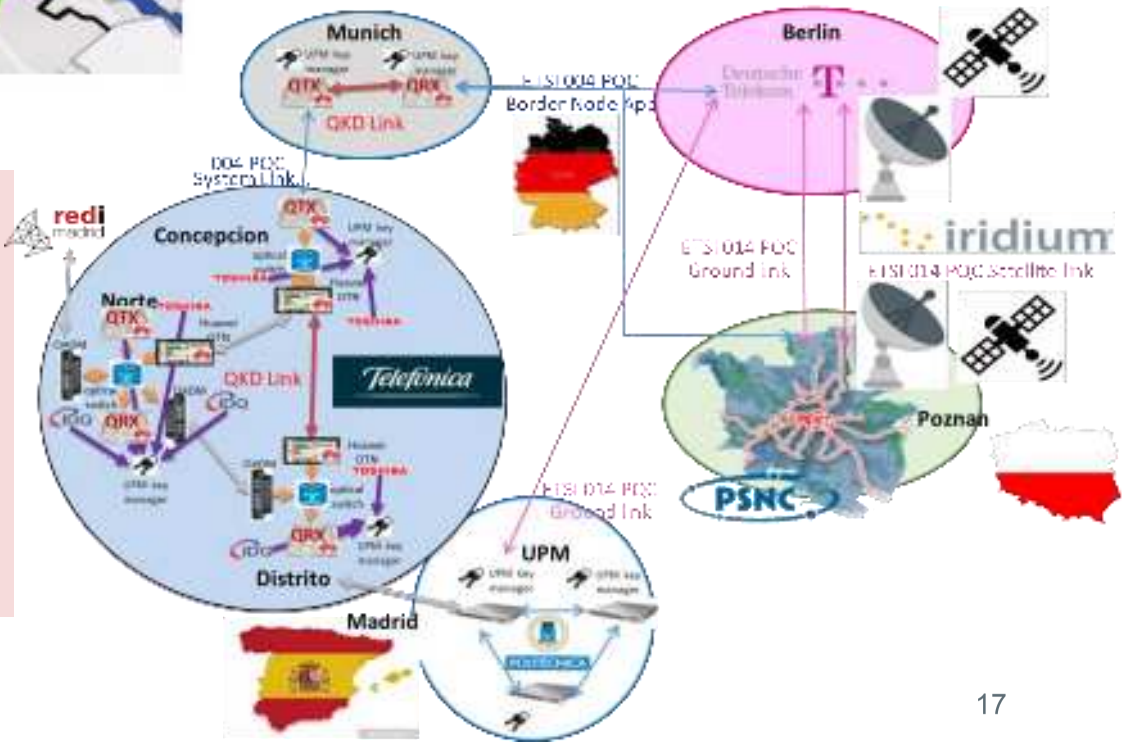
GOING THE DISTANCE

Bratislava – St. Pölten

- **250 km**; single QKD link based on entanglement

5 sites in 3 Countries: Spain, Germany, Poland

- Border Node App transport QKD keys protected with PQC Hybrid PQC+QKD
  - Multipath keys distribution
  - Long-range connections using QKD interfaces



EuroQCI

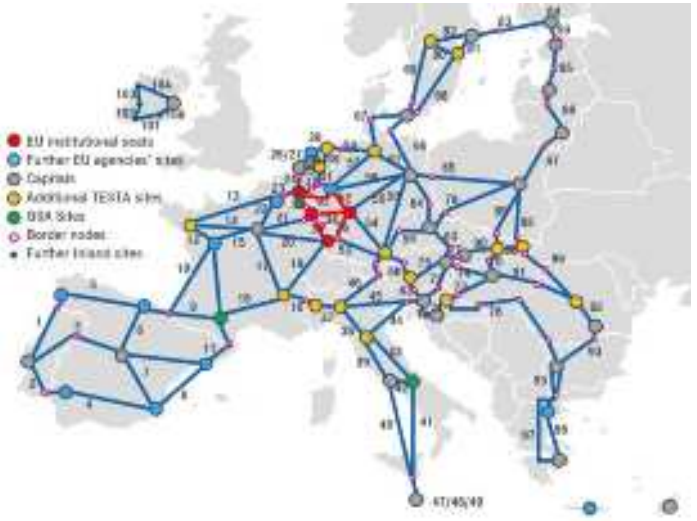
European Quantum Communication Infrastructure:

- Quantum secured network
- Quantum internet

Phase 1 (2022-2025)
Building of a European QKD network

- Terrestrial QKD
- Satellite based QKD

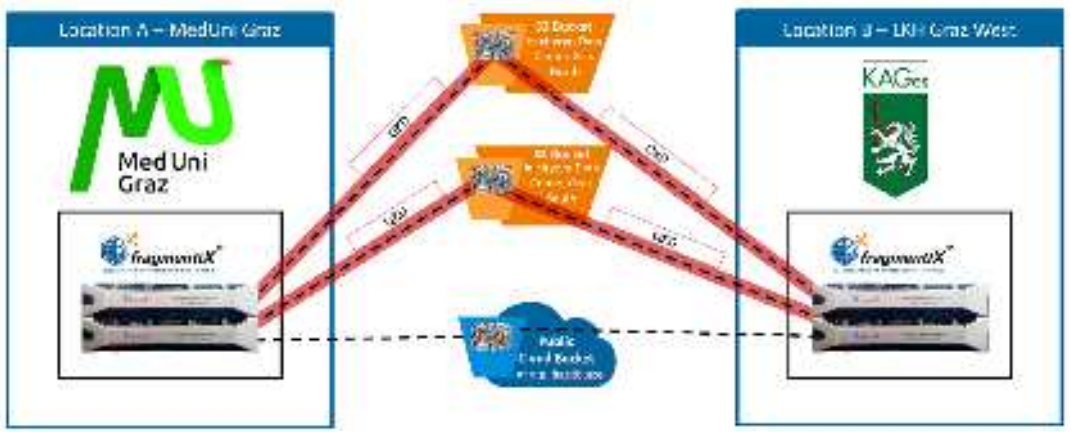
24 EU member states will launch **national QKD TEST networks** from 2023 onwards.



QCI-CAT: Austrian Quantum Communication Infrastructure

- Metropolitan area network in Vienna between different ministries
- Long-distance network Vienna – Graz
- Demonstrators:
  - Secure storage and key backup
  - Sharing of genome data
  - Secure video chat

GRAZ QKD DEMONSTRATOR

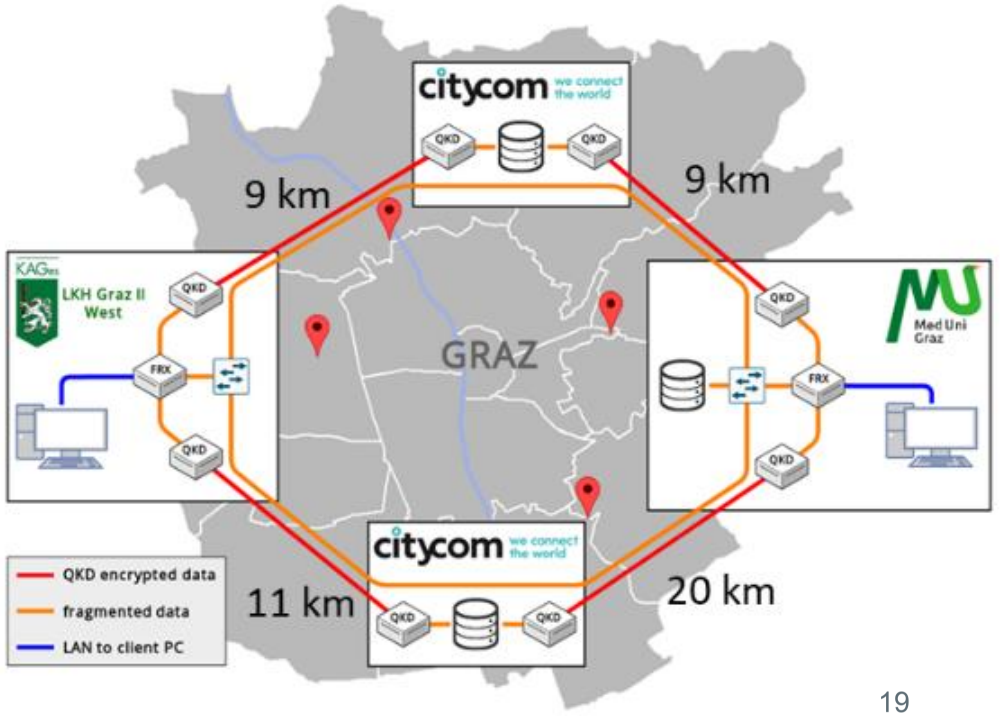


QKD devices
- ❑ 4 IDQ Cerberis systems
- ❑ 2 Toshiba QKD systems

Encryption devices
- ❑ 4 pairs of ADVA encryptors
- ❑ Layer-2, 20 min AES key refresh
- ❑ ETSI 014 interface

Secret sharing devices
- ❑ 2 fragmentiX CLUSTER
- ❑ Dell & Minio S3 servers

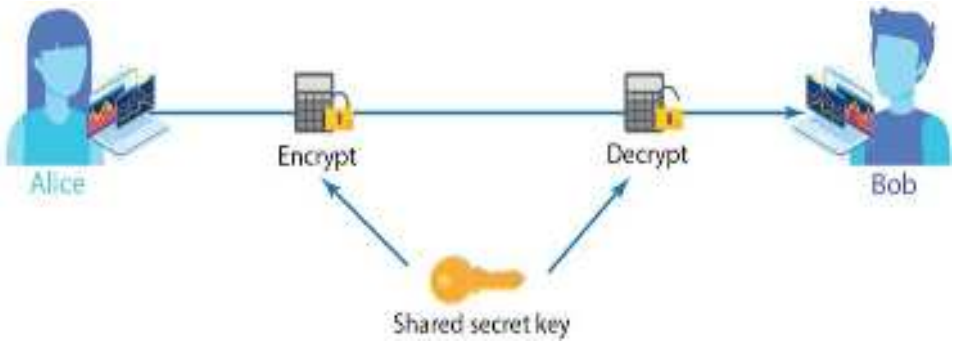
- **4 Nodes** (2 data centers, 2 hospitals)
  - 1 rack
- **4 Fiber links**



AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

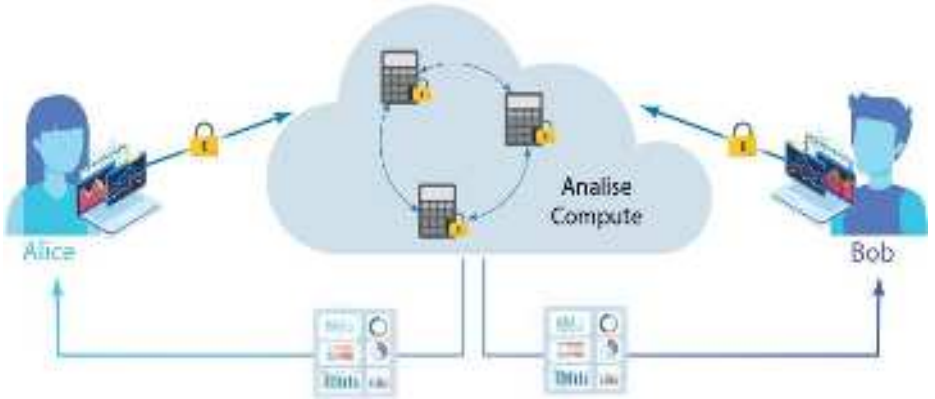
Security

Symmetric cryptography – BB84



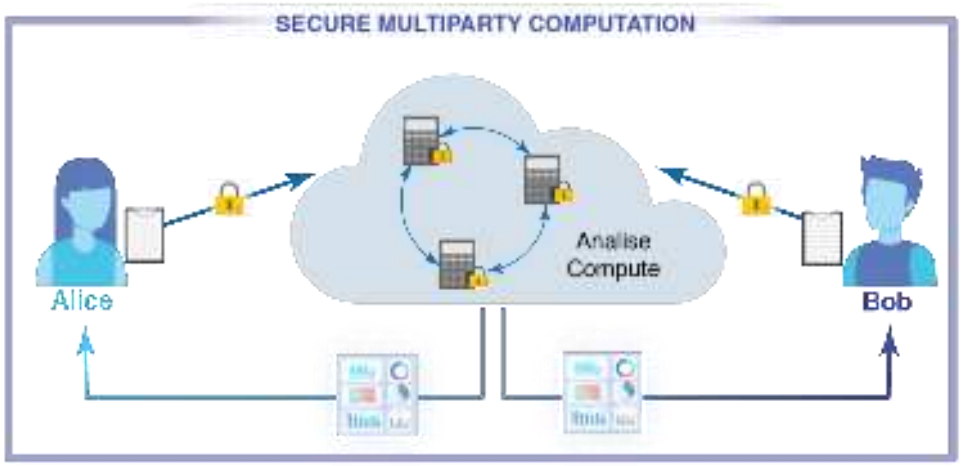
Privacy

Asymmetric cryptography – QOT

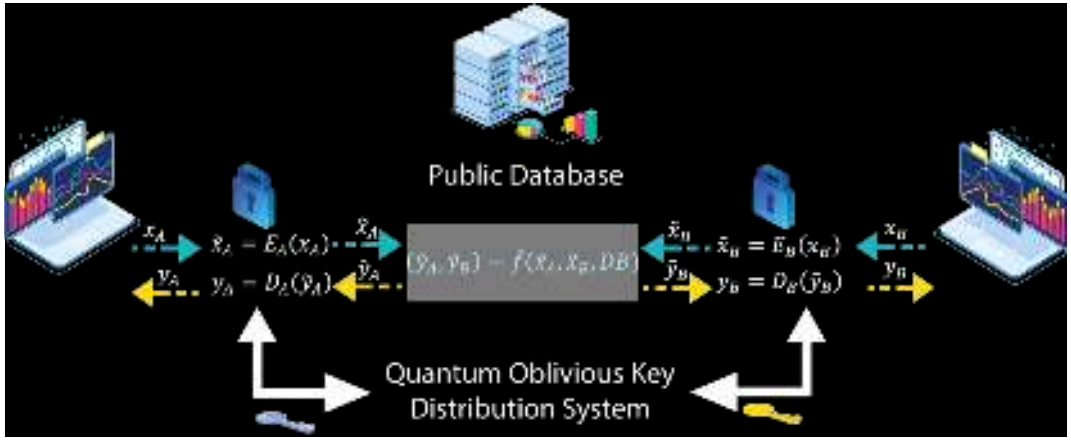


PROTOCOLS BEYOND QKD

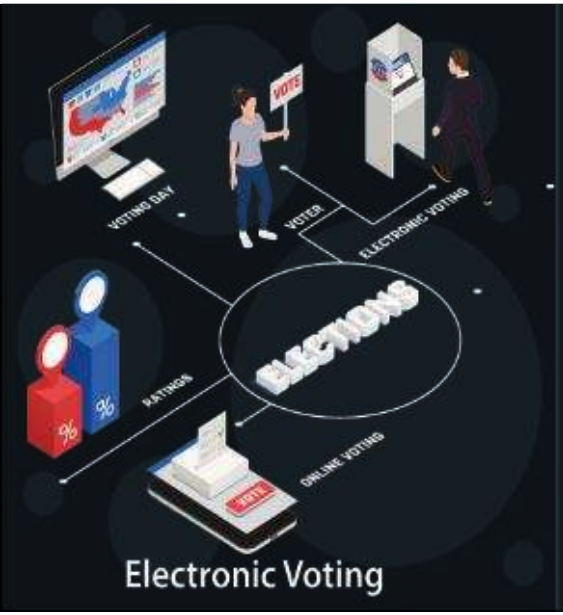
OBLIVIOUS TRANSFER



- The security and privacy in telecommunications networks must be guaranteed to allow secure large-scale interaction between parties that do not trust in each other.
- Secure multiparty computation occurs as a generic tool for computing on private data.
- Oblivious transfer arises as the cryptographic primitive to enable secure multiparty computation implementation.

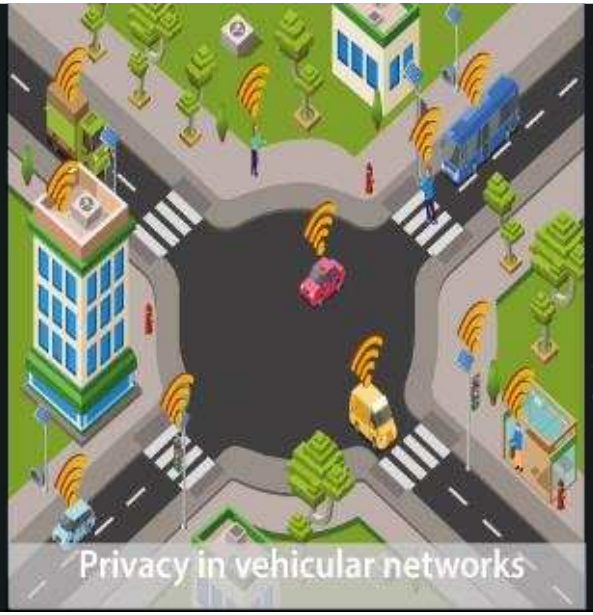


OBLIVIOUS TRANSFER - USE CASES

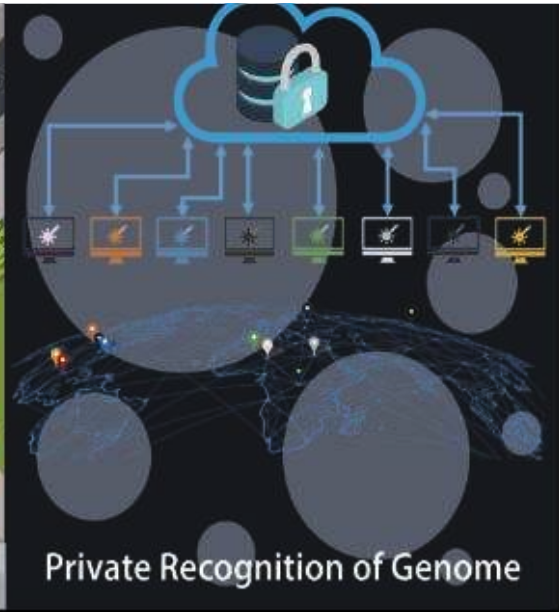


Enables the computation on citizens votes keeping private their identity and the input.

Each holder performs a transaction without revealing identity and input data.



In case of accident investigation: more than 1 witnesses can give testimony keeping identity and information about time and space location private.



Companies can work together even if they are competitors. Allows for the computing on common databases keeping private sensitive information.

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Any Questions?

Dr. Mariana Ramos
AIT Austrian Institute of Technology
mariana.ferreira-ramos@ait.ac.at

FFG
FTE NATIONALSTIFTUNG FORSCHUNG | TECHNOLOGIE | ENTWICKLUNG
EuroQCI
QSN

Figures by craiyon.com