Quantum Technologies

IN SLOVAKIA

Djeylan AKTAS (IPSAS)

QUANTAM TECHNOLOGY

Quantum Computing

Quantum Key Distribution

Quantum Software & Quantum Clouds

Post Quantum Encryption

Quantum Sensors & Atomic Clocks

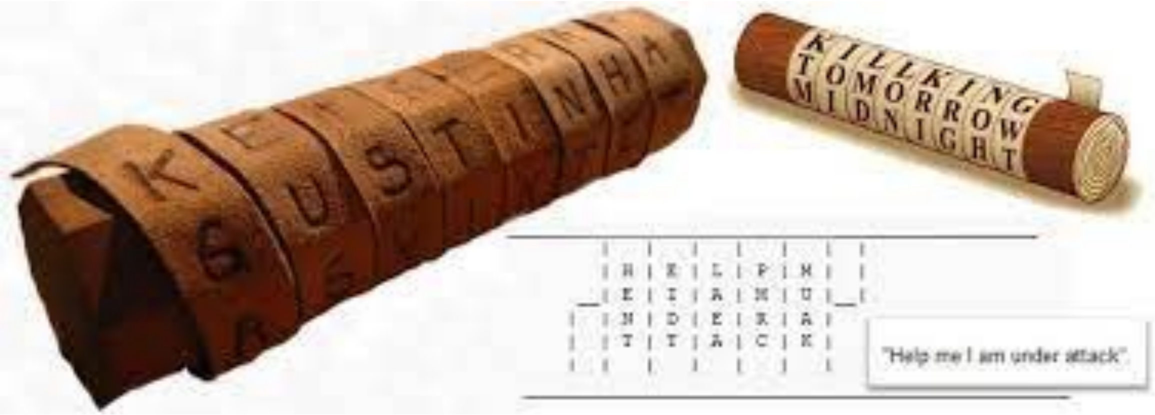
Quantum Materials

Quantum Memories & Other Quantum Components

Introduction to cryptography

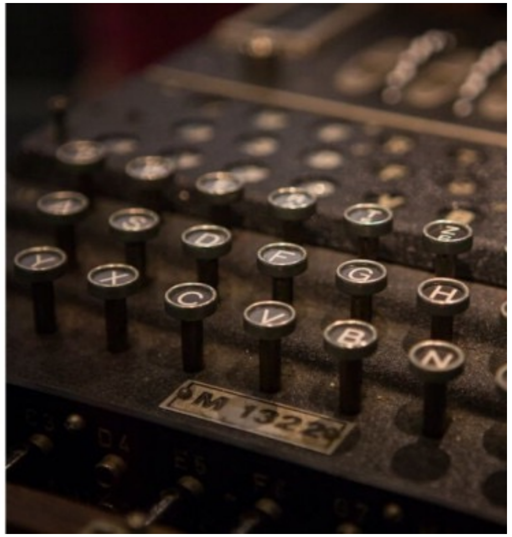
Historically cryptography has always been of paramount interest across the ages and its importance and how much we rely on its performances as a stable society over the years has only been growing with the advent of electronic communication and data storage.

Scytale (2500 yrs ago)



H E L P M
E I A M U
N D E R A
T T A C K

"Help me I am under attack".



Enigma machine (WW2)

Motivation

Today, we use cryptography everywhere to protect anything that demands telecommunication or data storage. Modern cryptography is a fundamental building block for banking application, e-commerce, any kind of secure communication really and it is of course of utmost importance for any National Security agency.

Simply put, modern cryptography uses computational hardness of certain mathematical problems to protect sensitive data. In other words, cryptographic algorithms are difficult or impossible problems to solve using conventional computing means.

Modern Cryptography

Secret Key Cryptography (SYM)

- Single key for both encryption/decryption
- Faster than asymmetric algorithms

Public Key Cryptography (ASYM)

- Need 2 keys (public and private)
- The sender encrypt with receiver public key and the receiver decrypt using the private key

Hash functions

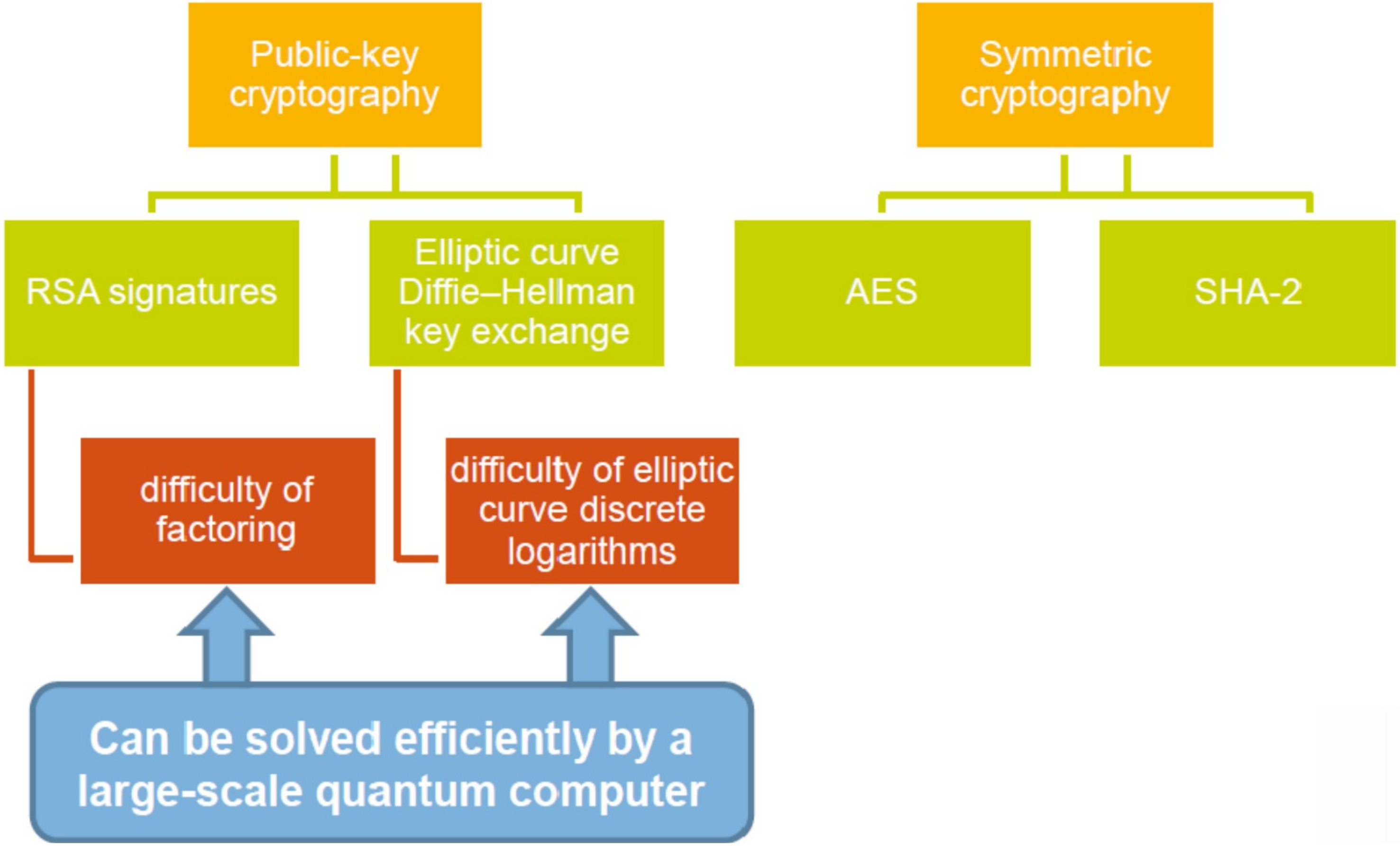
- Without or with a key
- Uses One-Way function (hard to reverse)

Threat to modern cryptography

The advent of **quantum computers** is threatening many widely adopted cryptographic systems. The assumption that some well-known cryptographic problems are difficult to solve in a reasonable amount of time has been proven to not hold against quantum algorithms.

These cryptographic primitives under threat are **mostly ASYM crypto algorithms** (Diffie-Helman, RSA, ECC) which our current communication architecture heavily rely on!

Threat to modern cryptography


Public-key cryptography
Symmetric cryptography
RSA signatures
Elliptic curve Diffie–Hellman key exchange
AES
SHA-2
difficulty of factoring
difficulty of elliptic curve discrete logarithms
Can be solved efficiently by a large-scale quantum computer

Protocols under threat:

- SSH (secure remote access)

- TLS (secure website)

- IPSec (secure tunneling)

- VPN (secure private networks)

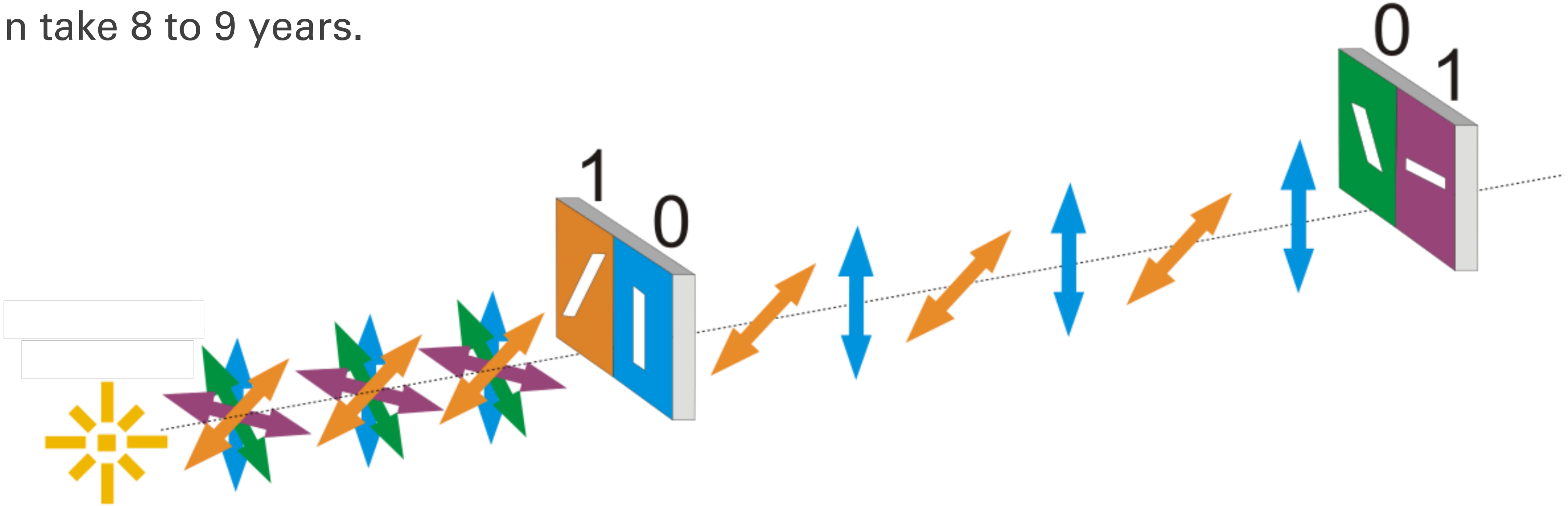
- HTTPS (secure navigation)

- S/MIME (secure emails)

Post-Quantum Crypto & QKD

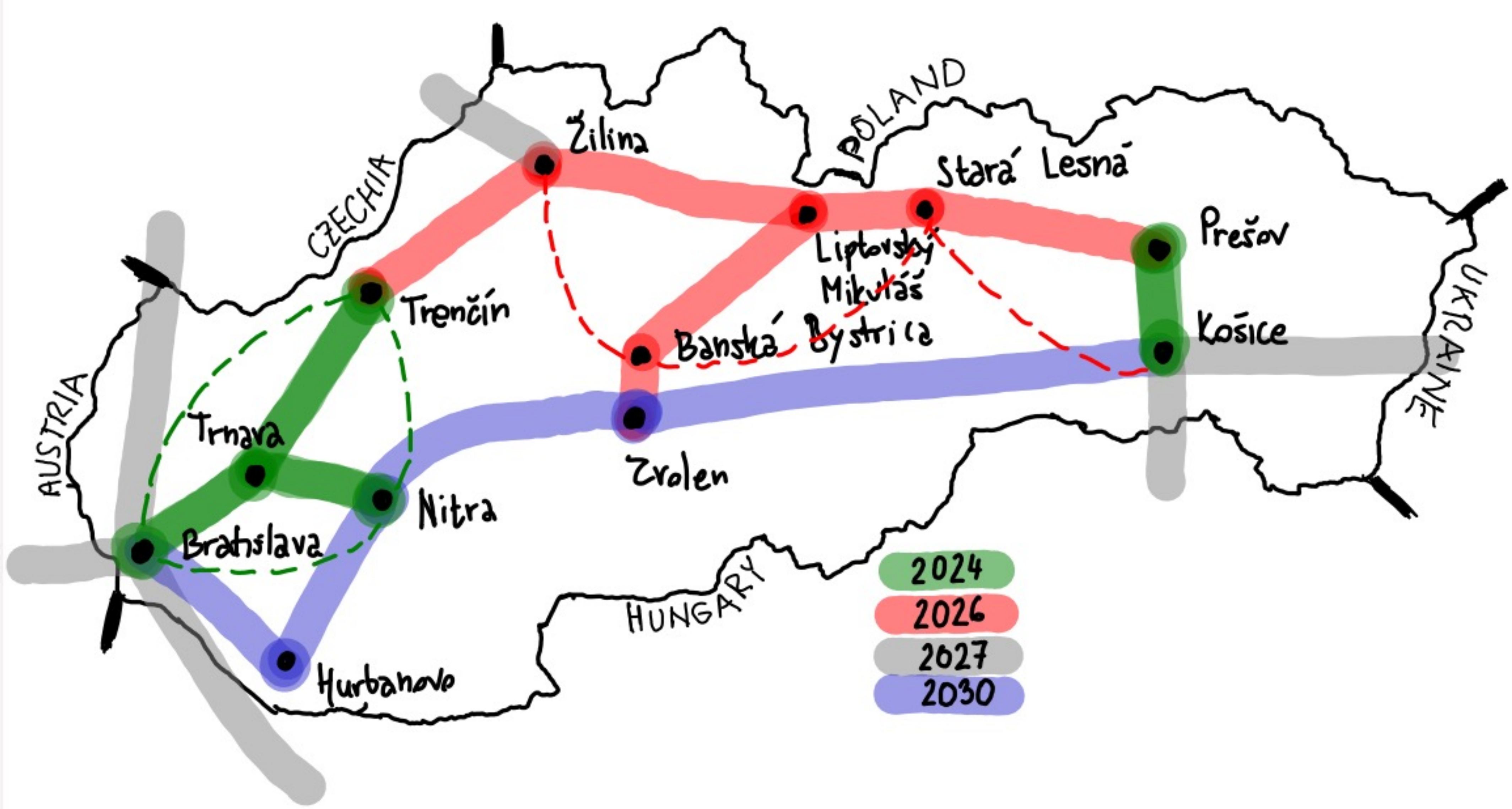
The goal of Quantum-safe cryptography research is to create protocols to replace these current public key cryptosystems with solutions that are safe against quantum algorithms.

Thankfully, quantum technologies not only create the problematic with the quantum computer but also offer us with a solution : **Quantum Key Distribution (QKD).** The field of post-quantum crypto is also working at the international level to bring new standards with classical quantum-resistant algorithms but implementing those changes can take 8 to 9 years.

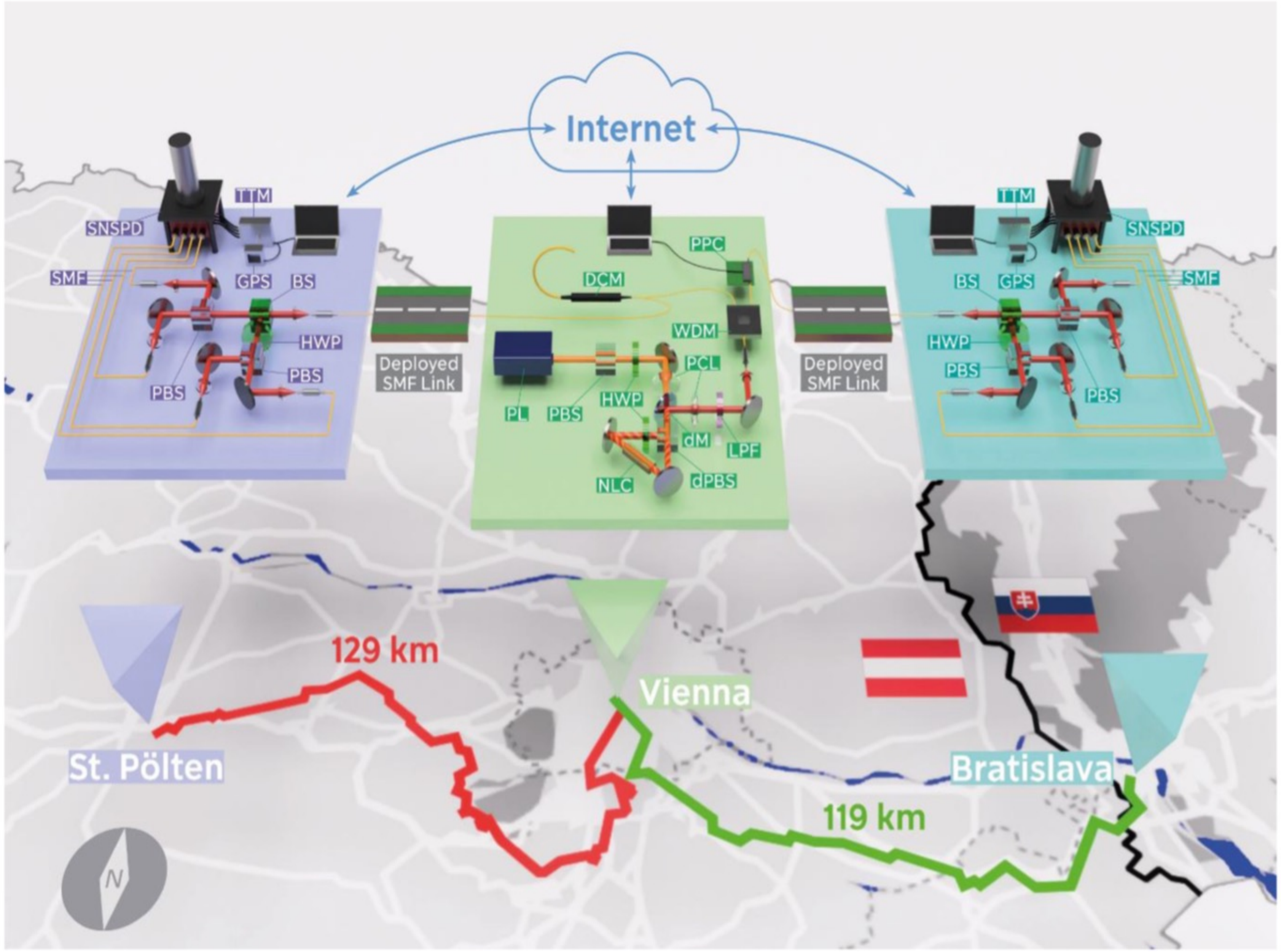


main goals:

1. Benchmarking QKD systems in real-life conditions.
2. Training new quantum engineers & dissemination.

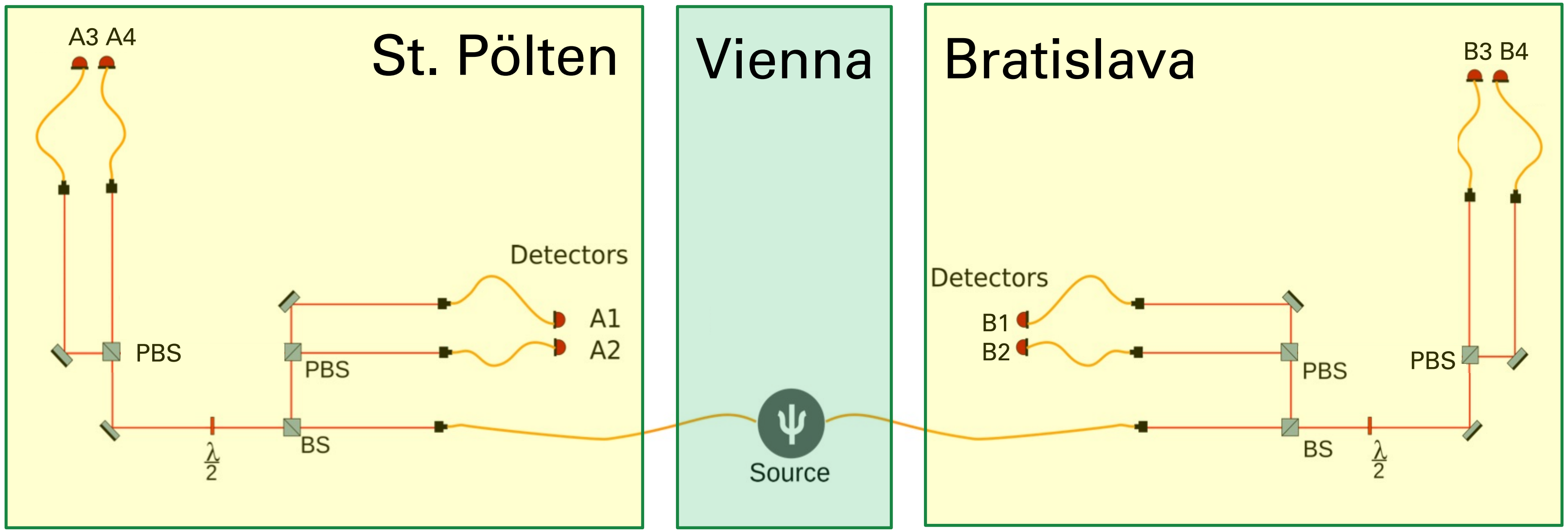


Entanglement-based QKD – The Implementation



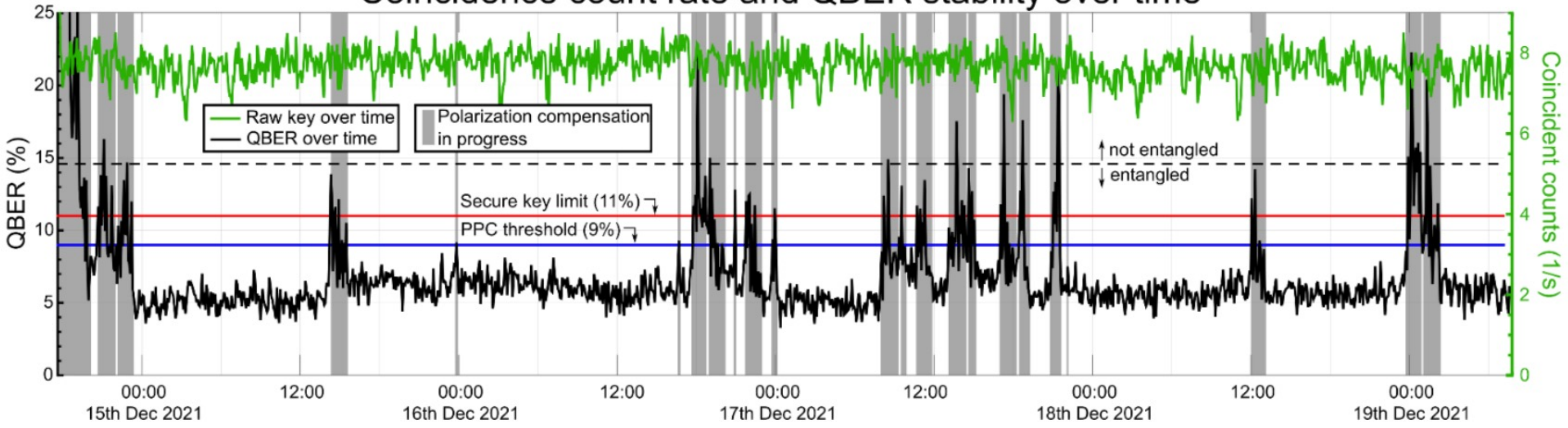
S. Neumann *et al. (2022), preprint arXiv:2203.2417*

Entanglement-based QKD – The Implementation



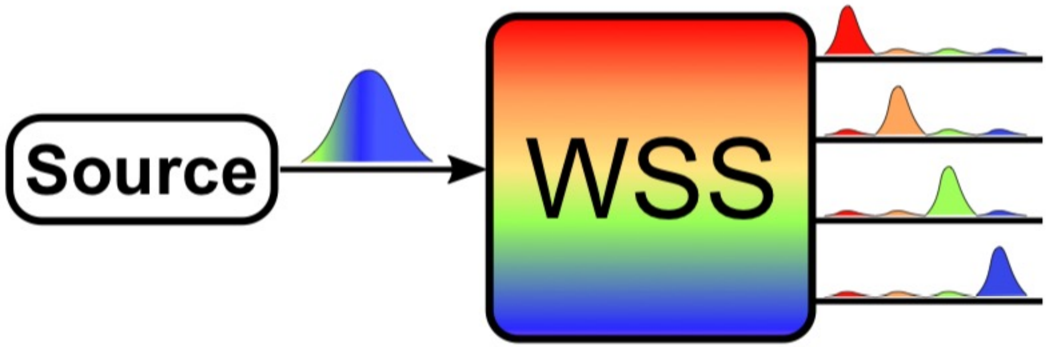
$$|\Phi^{+}\rangle = |H_s H_i\rangle + |V_s V_i\rangle$$

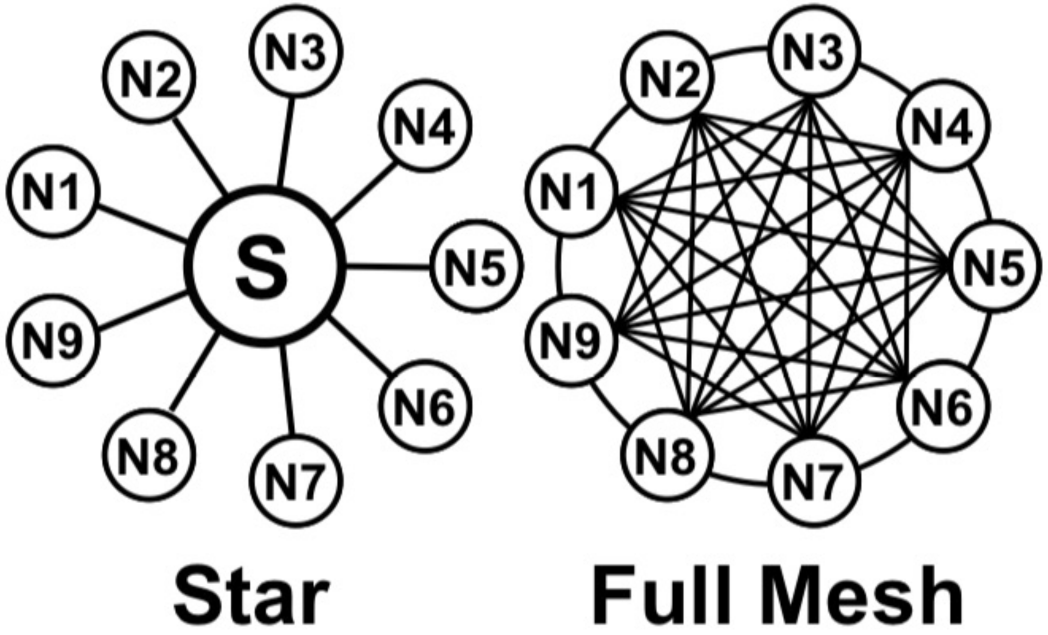
Coincidence count rate and QBER stability over time



Entanglement-based QKD

There are many different quantum protocols for key distribution. The entanglement-based protocols are the only ones offering the unique feature of sharing of sharing a key between all users of a given topology without having to establish a physical link. They all inherit the correlations by being connected to the same source of entanglement.





International & national infrastructure

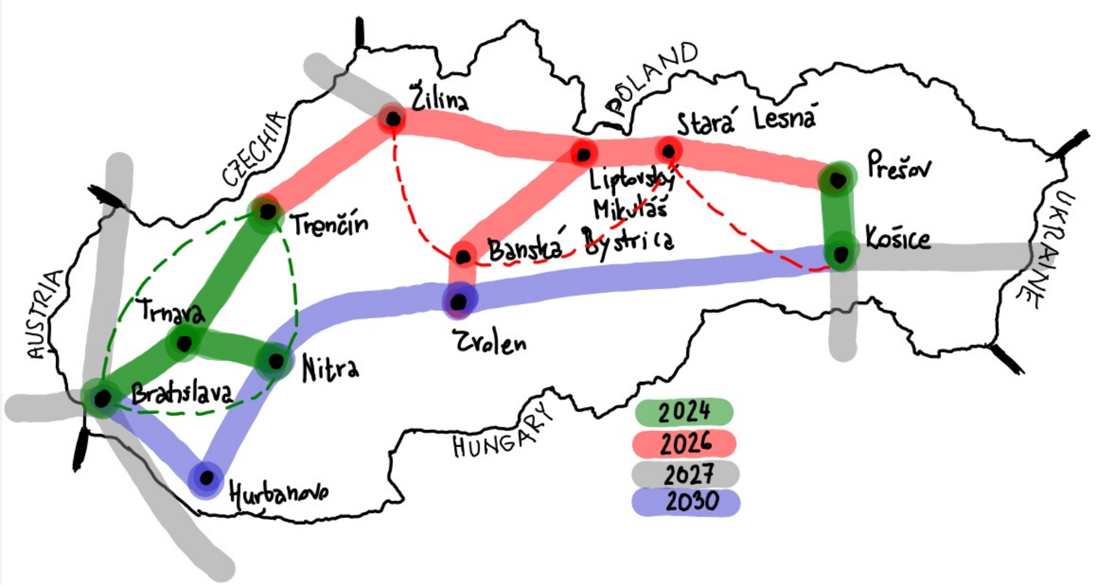
Primary objectives WP1:

1. Demonstrate a 24/7Upgrade IPSAS as a central node (national hub)
2. QKD link between IPSAS and Vienna (international)
3. Establish a local link with the international laser center (national, Bratislava)
4. Evaluate the WR protocol for synchronization instead of GPS solution.

Primary objectives WP2:

1. Benchmarking commercial QKD on the ILC/IPSAS link (IDQ/Toshiba)
2. Feasibility study to determine cost for wide-scale national deployment of QKD.
3. Provide access and consult with experts to integrate QKD with existing security stack
4. Negotiate with governmental agencies to explore possible future full deployment.

The infrastructure will host various solutions of both type: *prepare & measure* and entanglement-based QKD.



Towards domestic human resources in quantum technologies

Primary objectives WP3:

1. Transfer of expertise at IPSAS (new hire, collaboration)
2. Educating future scientific and technical expert and dissemination (Quapital summer school)

Quapital summer school

4-8 Sep 2022, Smolenice castle, Slovakia,
https://kcsmolenice.sav.sk/en/

Training a new cohort of quantum engineers to fulfill the needs of the national effort in developing quantum technologies

Thank you for your attention