Kvantne komunikacije in distribucija ključev: aktivno in pasivno generiranje naključnosti

Peter Jeglič
Laboratorij za kvantno prepletenost
Laboratorij za hladne atome
Institut Jožef Stefan

Funded by
the European Union
NextGenerationEU

THE RECOVERY
AND RESILIENCE
PLAN

Delavnica o generatorjih naključnih števil, 11. september 2024

Why now?

- A quantum computer can break currently encrypted messages (RSA public-key cryptosystem).
- Shor's algorithm (1994) is a quantum algorithm for factoring large integers.
- “Store now, decrypt later” puts today’s data in danger.
- U.S. national security memo from January 2022, directs federal agencies to migrate to quantum resistant cryptography protocols.
- Solution: **one-time pad** (random secret key).

$$\begin{aligned} \mathcal{P} &\quad \cdots 001011010 \cdots, \\ \mathcal{K} &\quad \cdots 101110100 \cdots, \\ \mathcal{C} = \mathcal{P} \oplus \mathcal{K} &\quad \cdots 100101110 \cdots. \end{aligned}$$

$$\begin{aligned} \mathcal{C} &\quad \cdots 100101110 \cdots, \\ \mathcal{K} &\quad \cdots 101110100 \cdots, \\ \mathcal{P} = \mathcal{C} \oplus \mathcal{K} &\quad \cdots 001011010 \cdots. \end{aligned}$$

How to exchange random secret key?

- **Quantum key distribution (QKD)**
- No-cloning theorem of quantum information, wave function collapse.
- Different protocols for QKD: Bennett-Brassard (1984), Ekert (1991), Bennett (1992), Bennett-Brassard-Mermin (1992)
- Quantum internet (distribution of entanglement)

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|H_A H_B\rangle + |V_A V_B\rangle\right)$$

S

…101110100…

…101110100…

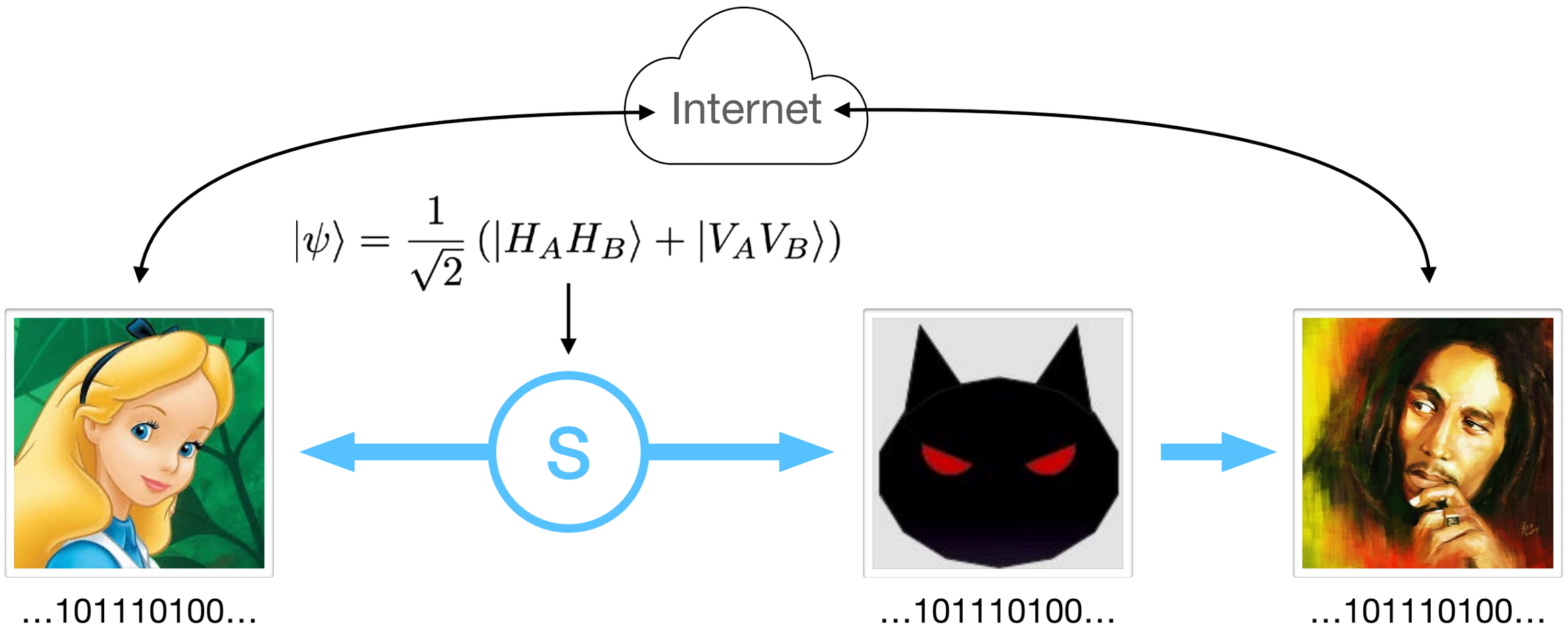
Quantum key distribution

QKD in the real world:

- Transmission (fiber) loss
- Coupling loss
- Detector inefficiency
- Imperfect source
- **Eavesdropper Eve!**

Additional steps:

- Random choice of measurement basis
- Basis reconciliation via the classical channel
- Determination of error rate
- Removal of the errors
- Privacy amplification

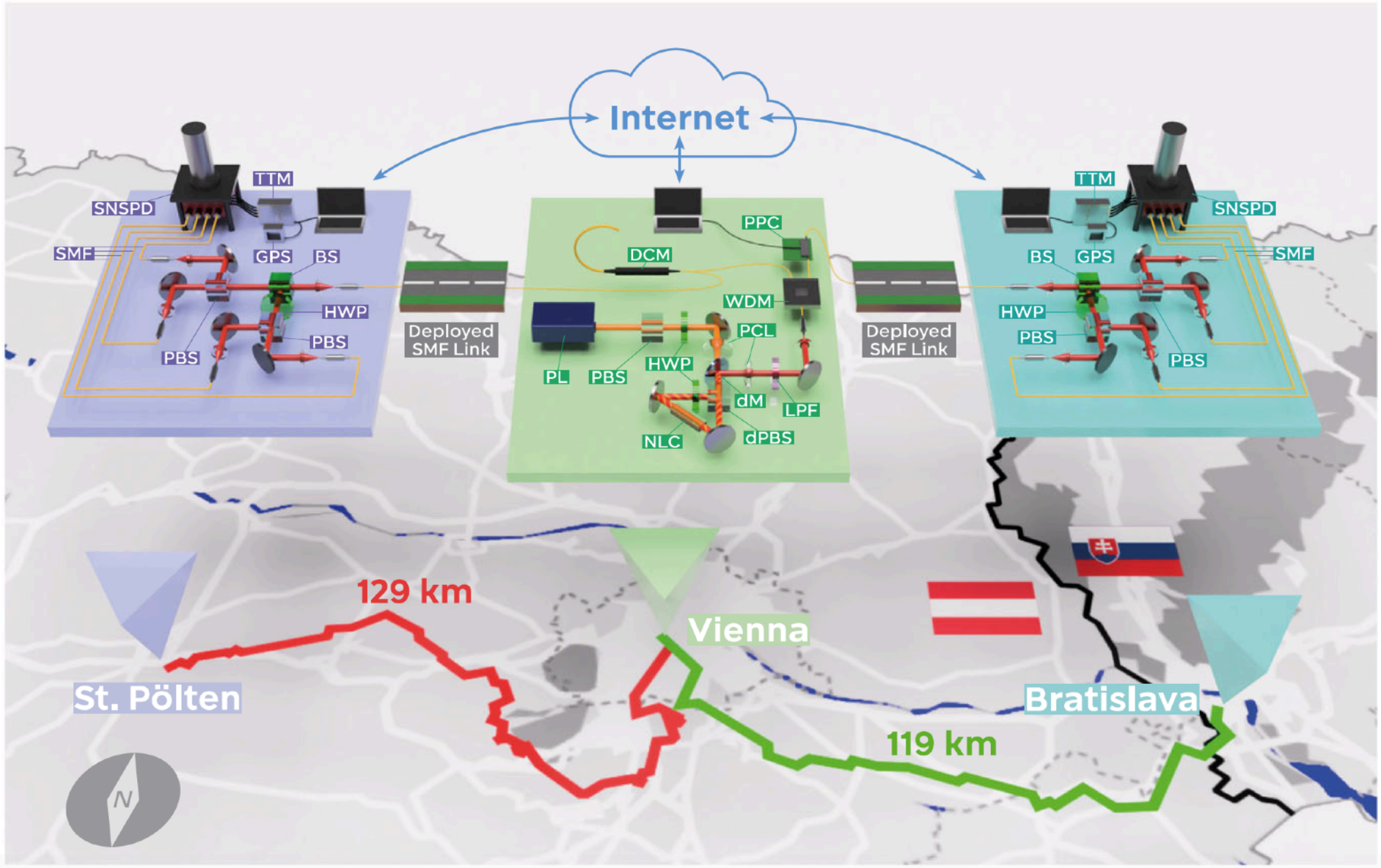


Quantum key distribution

State-of-the-art

- Entanglement distribution over 248 km fiber link
- Fiber losses: 0.2 dB/km @ 1550 nm
- Stable detected pair rate: 9/s
- Secure key rate: 1.4 bits/s

$$|\phi^+\rangle = 1/\sqrt{2}(|H\rangle_{SP}|H\rangle_B + |V\rangle_{SP}|V\rangle_B)$$
$$= 1/\sqrt{2}(|D\rangle_{SP}|D\rangle_B + |A\rangle_{SP}|A\rangle_B)$$

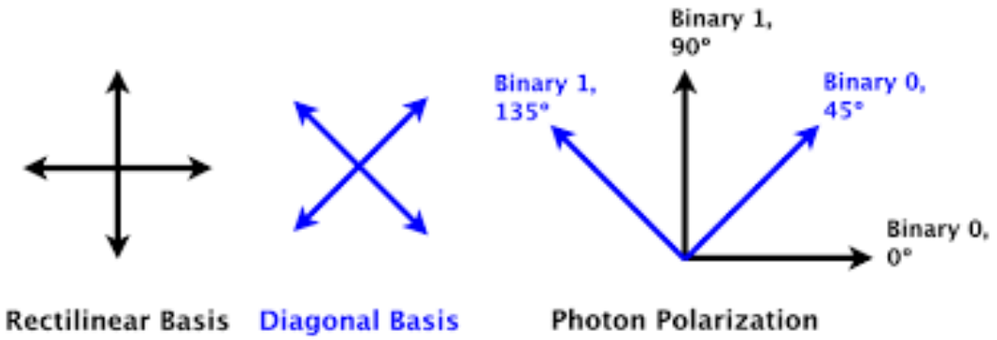


Neumann *et al*., *Nature Communications* **13**, 6134 (2022).

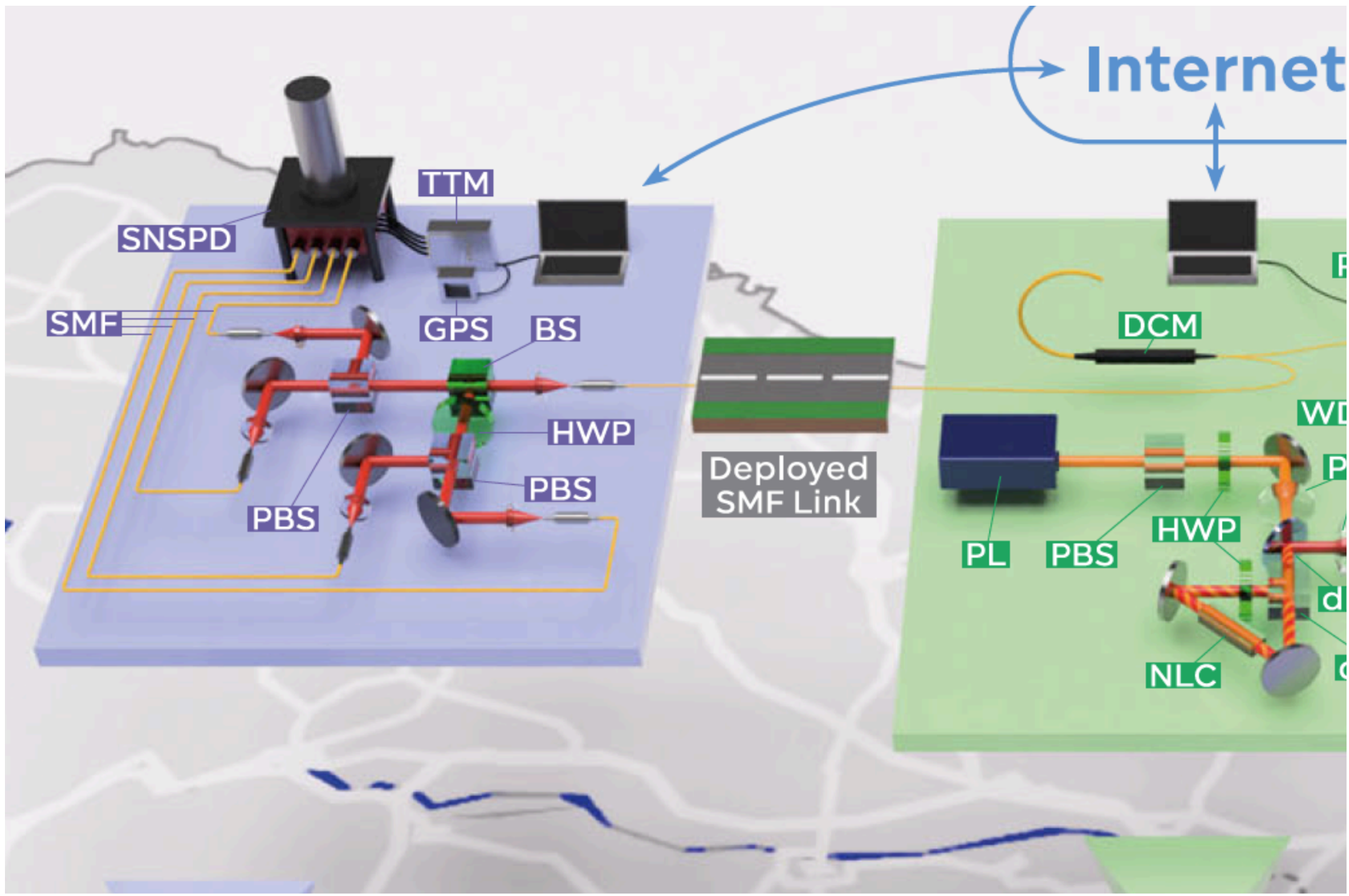
Kje potrebujemo naključna števila?

Izbira baze:

- Aktivna
- Pasivna



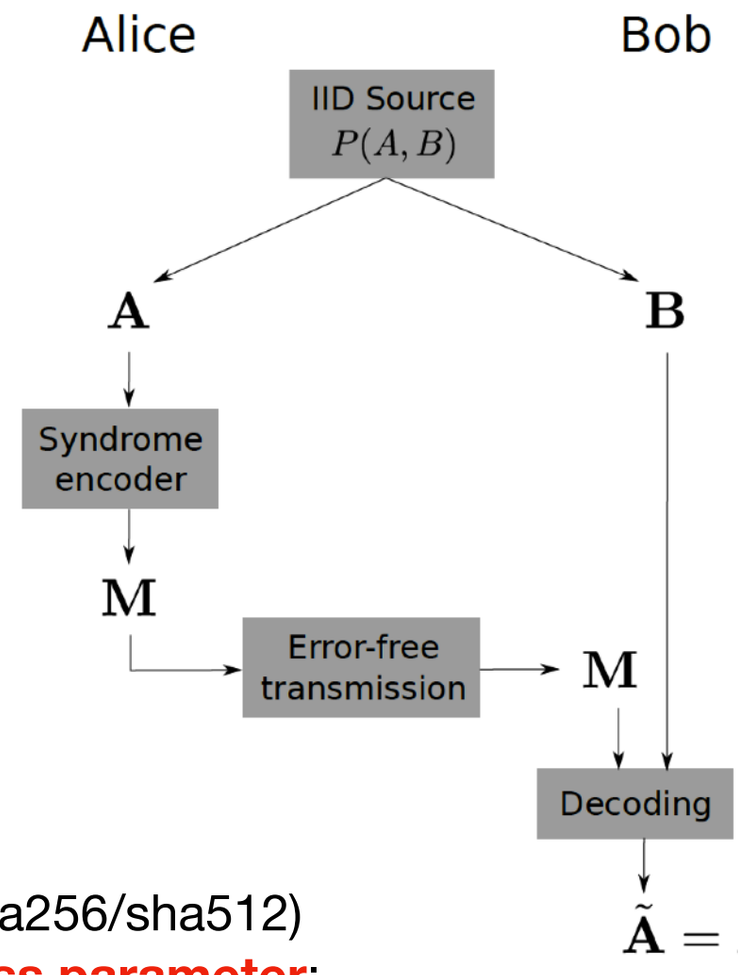
$$|\phi^+\rangle = 1/\sqrt{2}(|H\rangle_{SP}|H\rangle_B + |V\rangle_{SP}|V\rangle_B)$$
$$= 1/\sqrt{2}(|D\rangle_{SP}|D\rangle_B + |A\rangle_{SP}|A\rangle_B)$$



Kje potrebujemo naključna števila?

Postprocesiranje:

- **Key sifting** (Alice in Bob primerjata baze in zavržeta neujemajoče)
- **Parameter estimation** (Alice in Bob izbereta naključne indekse ključa in primerjata rezultate, določita QBER = quantum bit error rate)
- **Error correction** (LDPC = low density parity check)



Asymmetric Slepian-Wolf coding

- Kontrola z uporabo hash funkcije (sha256/sha512)
- Velikost hash niza določa **correctness parameter**:

$$\varepsilon_1 = 2^{-t}$$

Kje potrebujemo naključna števila?

Postprocesiranje:

- **Privacy amplification** (Toeplitzova matrika, v prvi vrstici in stolpcu so naključna števila, aritmetika je modulo 2)

$$h = T \cdot k = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

- Cilj je doseči **security parameter** $\epsilon = 10^{-10}$. To je ekvivalentno temu, da ne bo prišlo do uhajanja niti enega bita ključa v obdobju več mesecev pri hitrostih generiranja kbit/s.

$$\varepsilon_2(\nu) = \frac{1}{2}\sqrt{2^{-(m-k)\left(\log\frac{1}{\bar{c}} - h(\delta+\nu)\right)+r+t+l}} + 2e^{-\frac{(m-k)k^2\nu^2}{m(k+1)}}$$

$$h(x) = -x\log x - (1-x)\log(1-x)$$

- Običajno se “security parameter” izbere vnaprej. Sproti pa se na primer določa razmerje kompresije, kar v praksi pomeni spreminjanje hitrosti generiranja končnih varnih ključev.
- **Varnostni dokaz predpostavlja popolno naključnost (i.i.d). Vsako odstopanje zmanjšuje “security parameter”. Zato je treba uporabiti “full-entropy" generatorje naključnih števil.**

QKD security assumptions

- **Quantum theory:** The operations performed by the users and by the adversary admit a description in terms of quantum states, operations and measurements. In particular, the statistics observed by the legitimate parties admit a quantum description.
- **Isolation:** The parties can prevent information leaking to the adversary. The users' systems can be shielded so that classical and quantum information only leave Alice's (Bob's) lab under her (his) control.
- **Input randomness:** Alice and Bob's input choices are truly random, i.e. they are not correlated with their other devices nor the adversary.
- **Trusted information processing:** The computers processing Alice and Bob's classical information perform the expected computations.
- **Trusted quantum operations:** Alice and Bob's quantum devices perform the expected quantum operations. In particular, quantum devices are accurately characterized and they maintain perfect calibration: sources of quantum states produce the expected quantum states and quantum measurements are performed according to their specifications.

- QKD is often presented with the additional assumption that the classical channel between Alice and Bob is **authenticated**, i.e. so that the adversary cannot alter the content of messages transiting on it.

SiQUID

Slovenian Quantum Communication Infrastructure Demonstration
Vzpostavitev slovenske infrastrukture za kvantne komunikacije

Si quid?
What if?
Kaj če?

Ribezzo *et al*., *Adv. Quantum Technol.* **6**, 2200061 (2023).

SiQUID

Basic information:

- Project name: Slovenian Quantum Communication Infrastructure Demonstration
- Project acronym: SiQUID
- Call: DIGITAL-2021-QCI-01
- Topic: DIGITAL-2021-QCI-01-DEPLOY-NATIONAL
- Type of action: DIGITAL Simple Grants
- Granting authority: European Commission-EU

- Project starting date: 1 January 2023
- Project end date: 31 December 2025
- Project duration: 36 months

Budget:

- Total: EUR 4.48 million
- EU: EUR 2.24 million
- NOO: EUR 2 million
- Beyond Semiconductor d.o.o.: EUR 0.24 million

Website:

- http://siquid.fmf.uni-lj.si

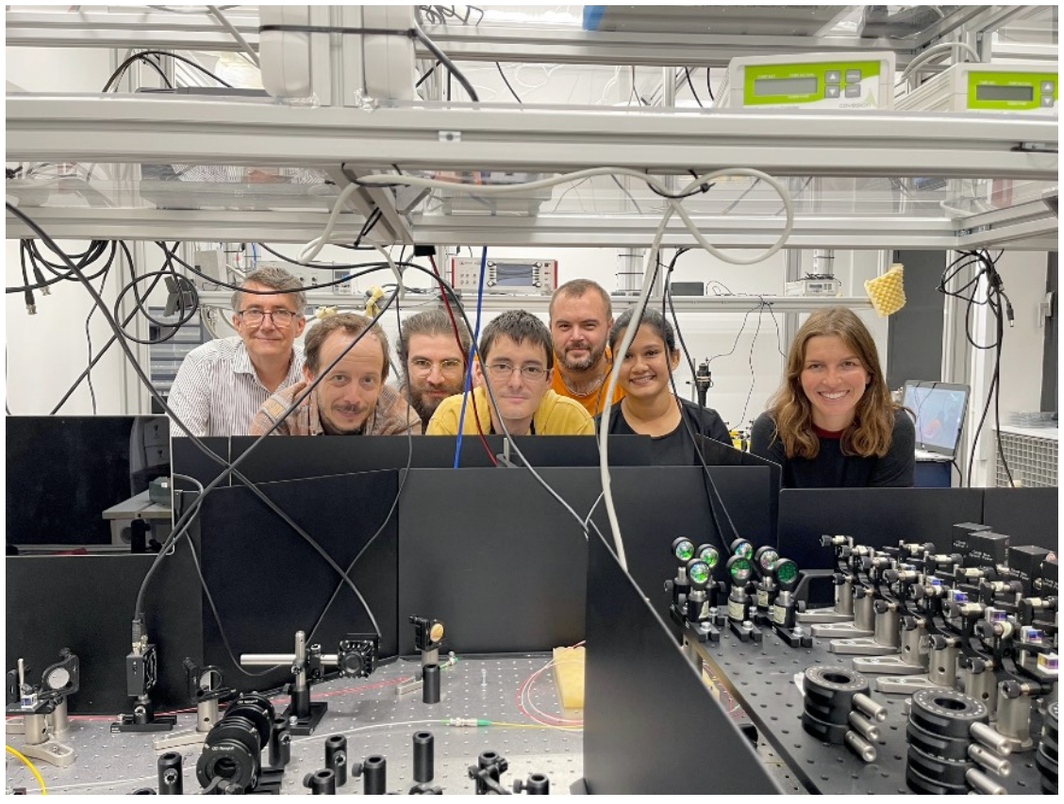
Kick-off event (FMF, 16 June 2023)

SiQUID

Key Contacts:

- Anton Ramšak – Project Coordinator
- Rainer Kaltenbaek – Scientific & Technical Coordinator
- Barbara Dorić – Project Manager

FMF



Laboratory for Quantum Optics & Quantum Foundations

IJS

Laboratory for quantum entanglement F1, F5, E5, E6 & CMI

SiQUID

BEYOND SEMICONDUCTOR

Xiphra enkriptorji

URSIV

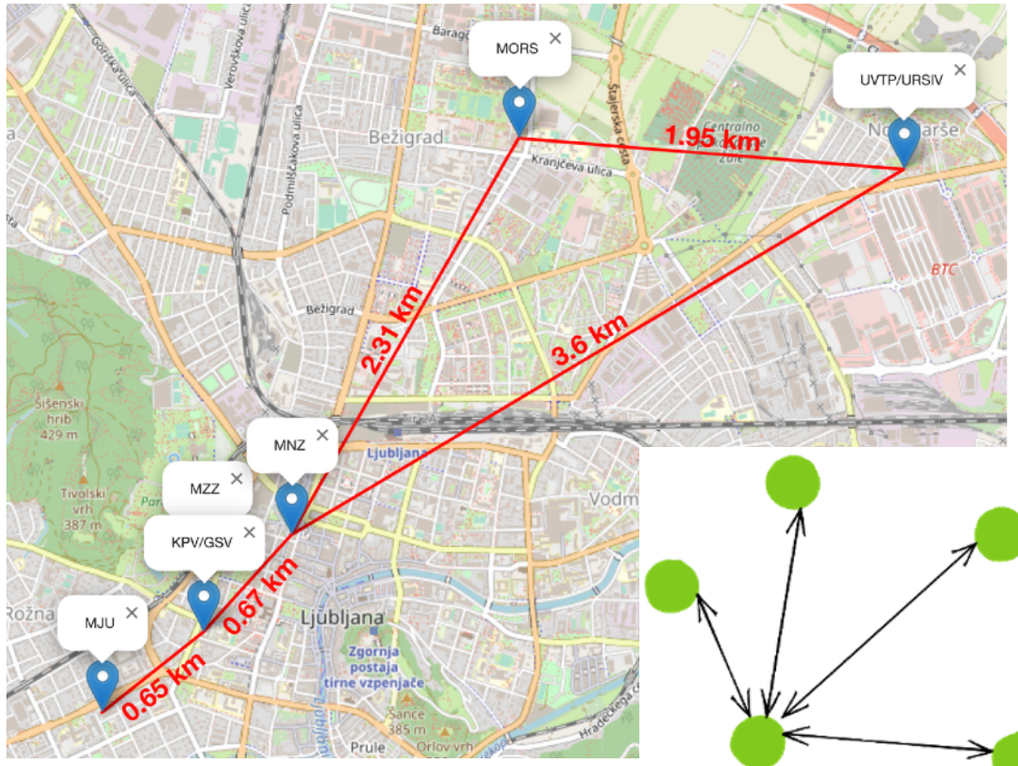
Urad Vlade Republike Slovenije
za informacijsko varnost

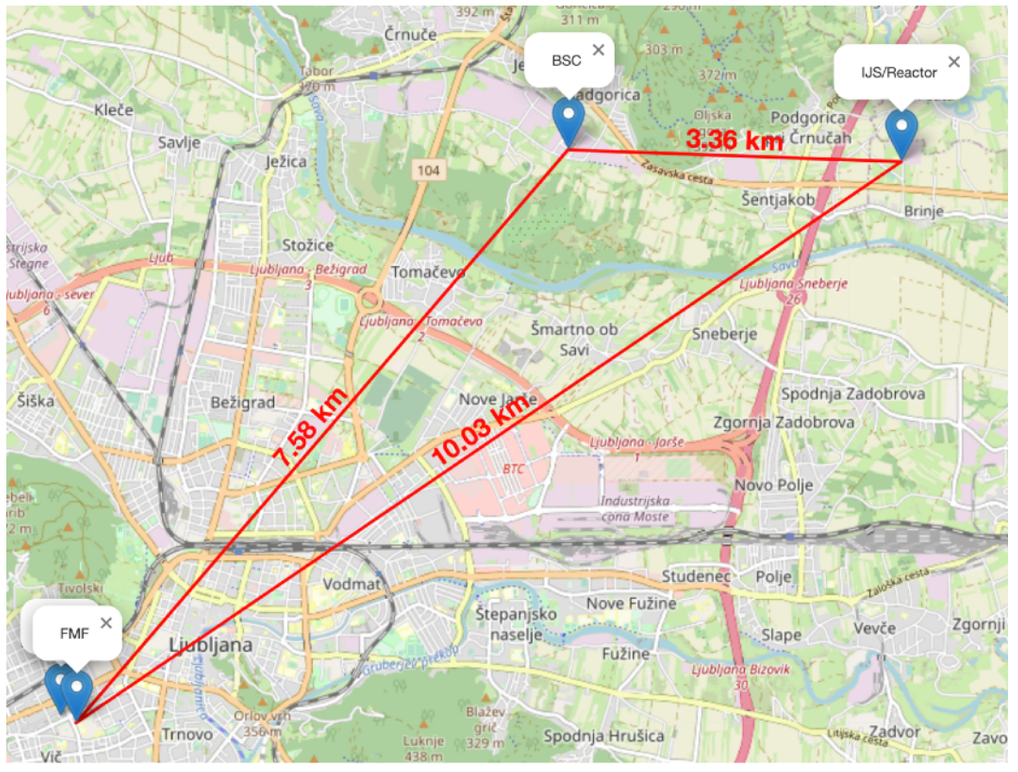
Republika Slovenija
Urad Vlade RS za varovanje tajnih podatkov
UVTP

Urad Vlade Republike Slovenije
za varovanje tajnih podatkov

The main project goals:

- To establish QKD between several government nodes
- To establish a test quantum network between research institutions
- Training young researchers and engineers in the field of quantum communications





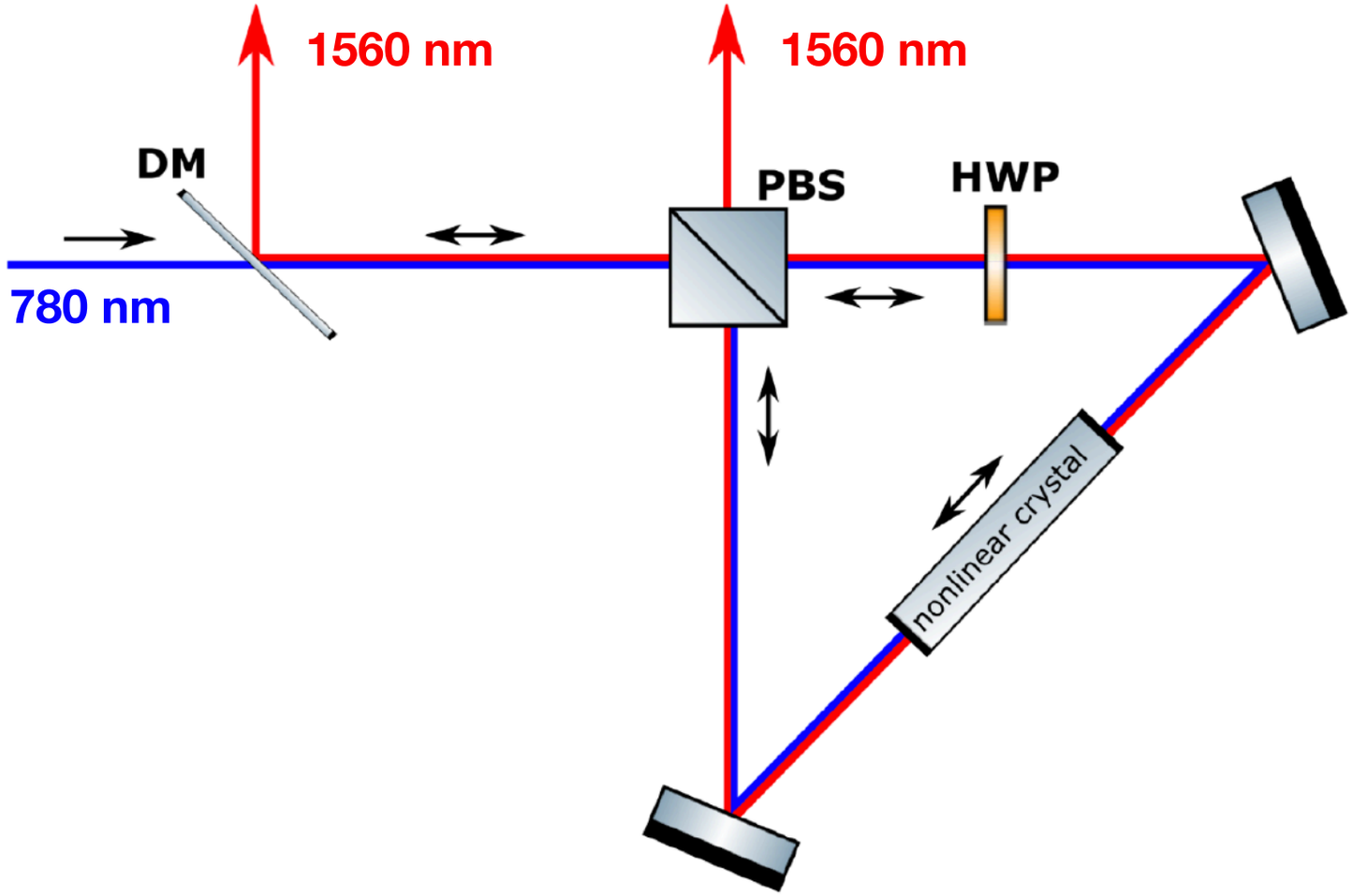
The planned locations for government and experimental nodes and the air distance between them.

SiQUID

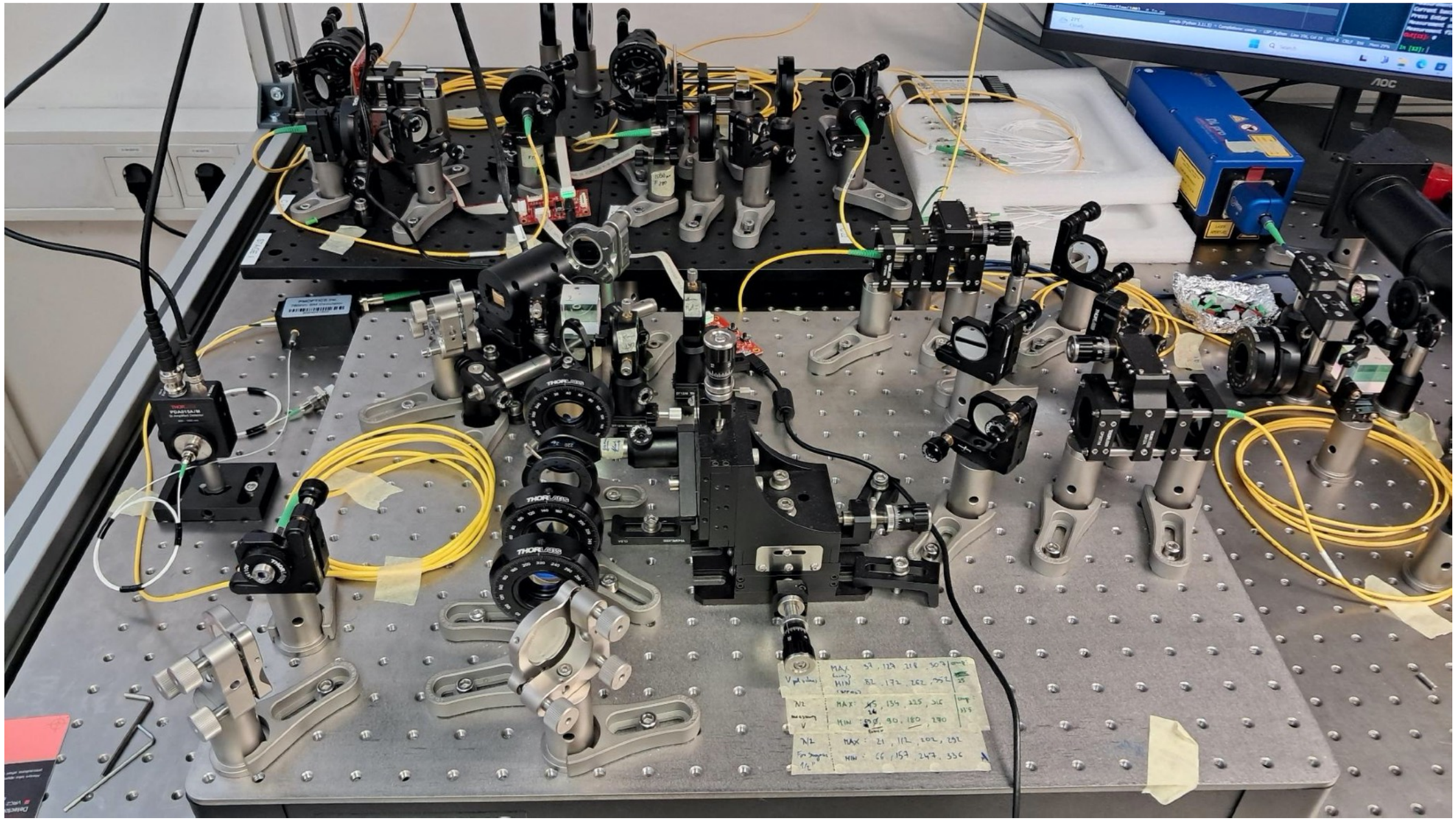
A source of entangled photons at 1560 nm:

- Spontaneous Parametric Down-Conversion (SPDC)
- Nonlinear crystal (periodically poled lithium niobate)
- Sagnac interferometer

$$|\psi\rangle_1|\psi\rangle_2 = \frac{1}{\sqrt{2}}\Big(|HV\rangle + e^{i\varphi}|VH\rangle\Big)$$

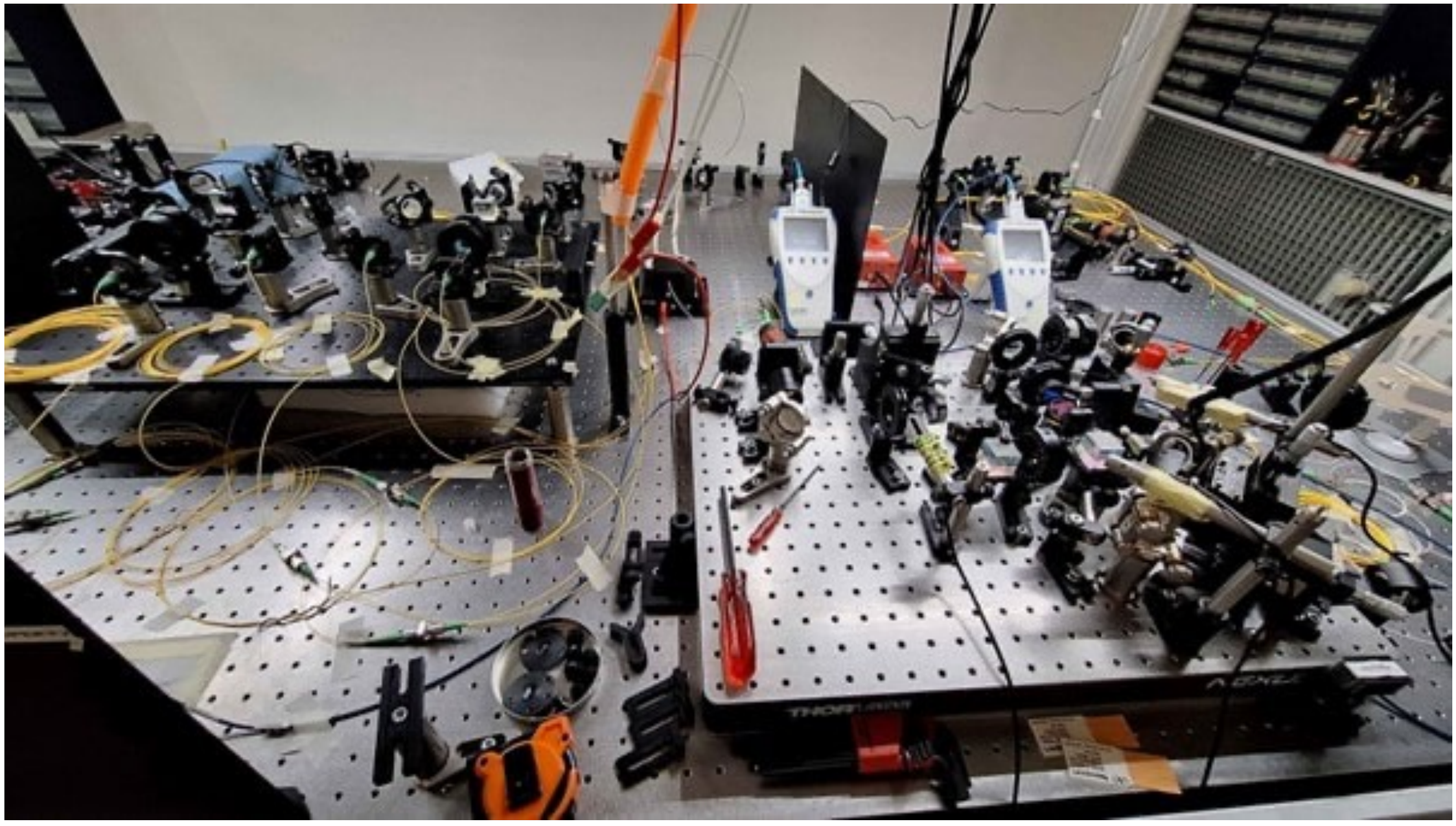


SiQUID



Izvor prepletenih fotonov na IJS (tip 2)

SiQUID

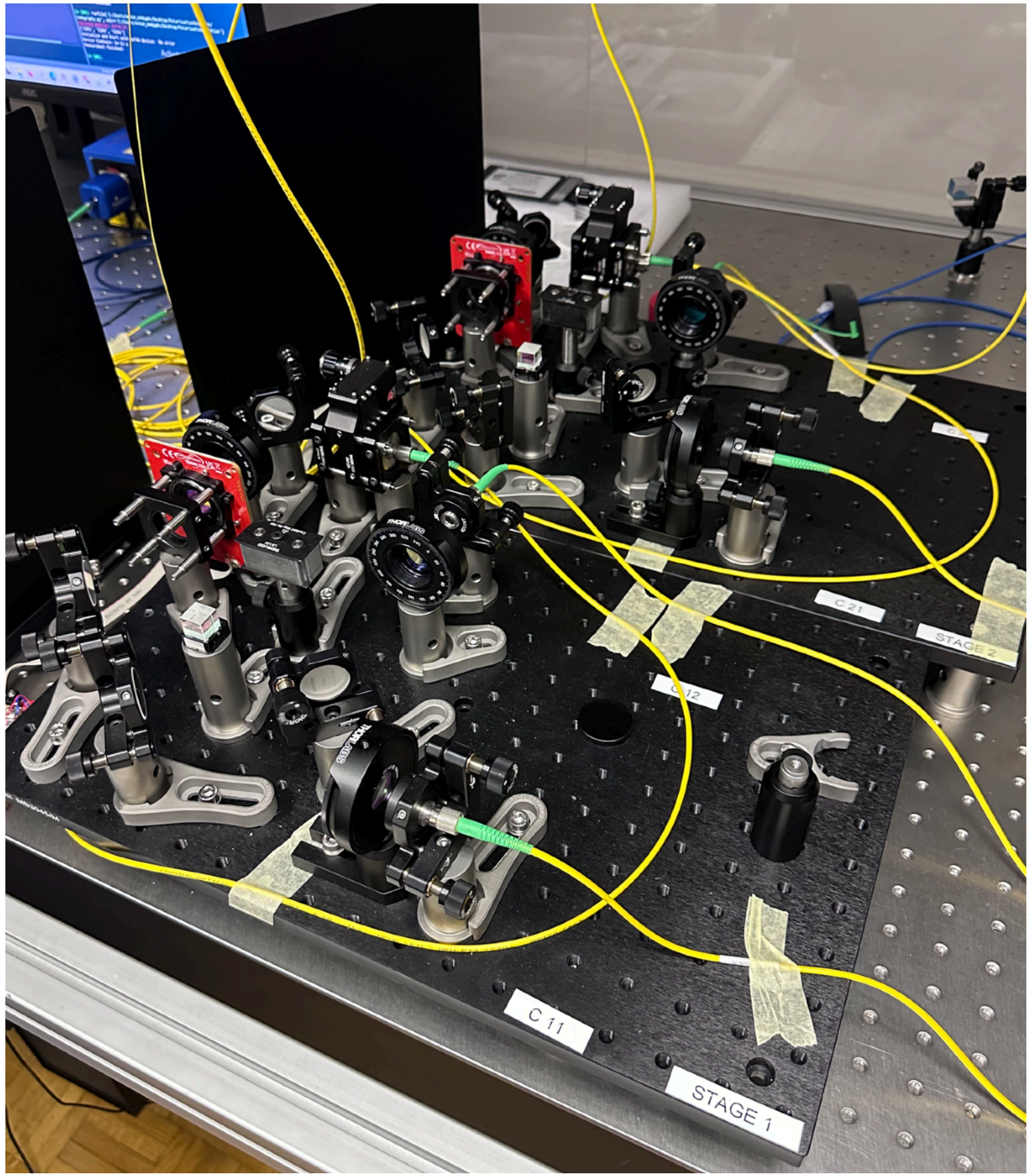


Izvor prepletenih fotonov na FMF (tip 0)

SiQUID

Receivers at 1560 nm:

- Analysis stages
- Superconducting nanowire single-photon detectors
- Time-taggers

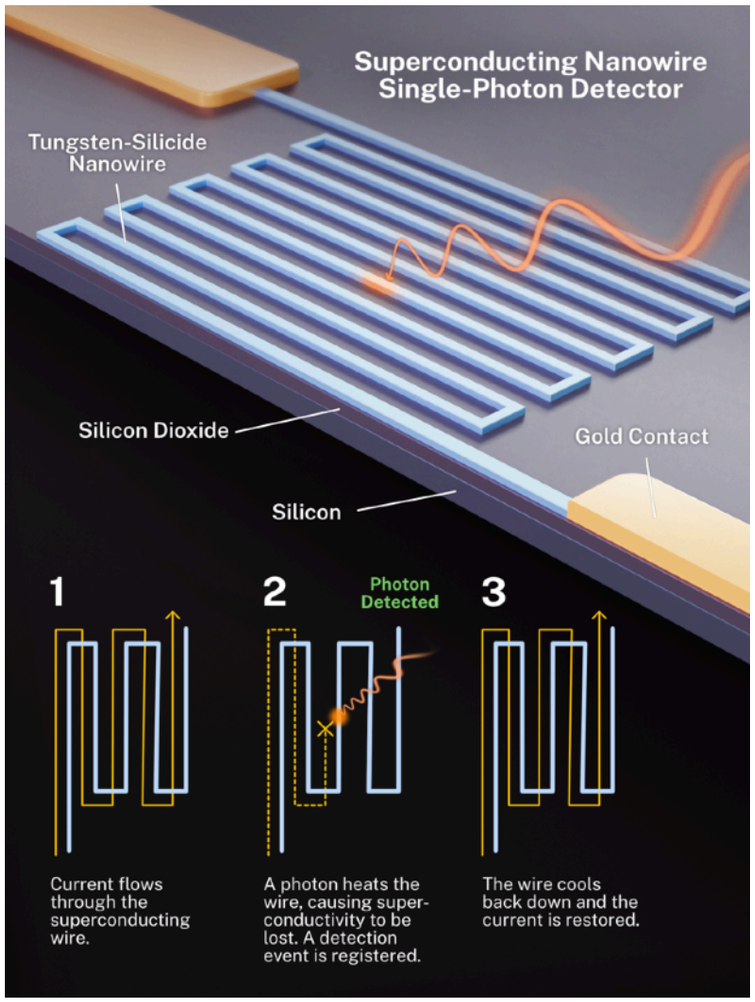


SiQUID

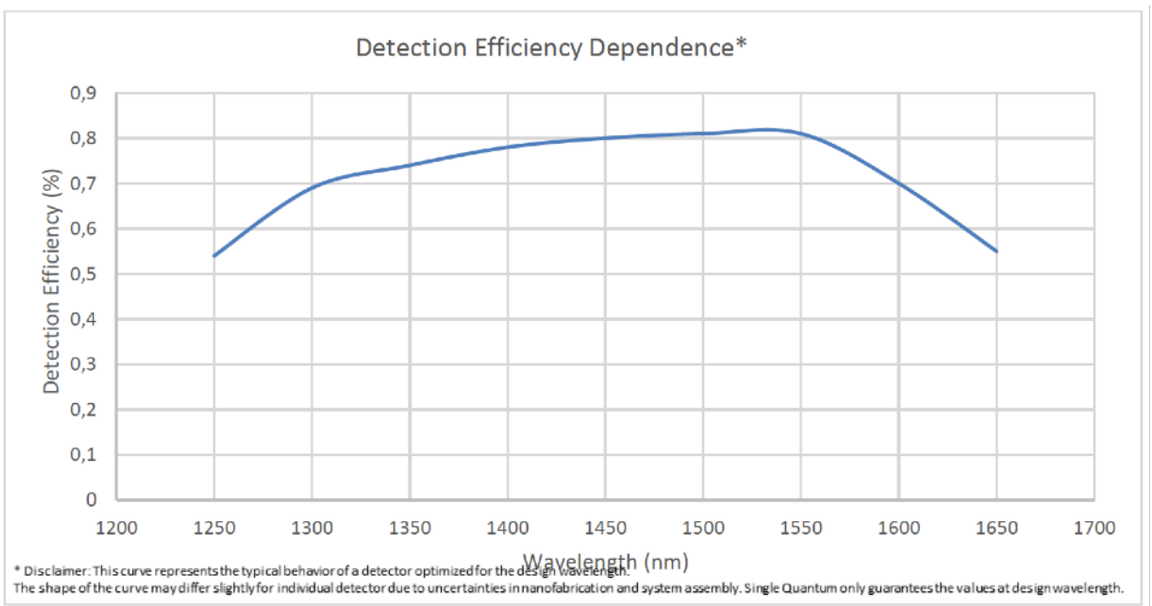
SINGLE QUANTUM
Excellence in photon detection

Superconducting nanowire single-photon detectors:

- High quantum efficiency
- Ultra-high timing resolution
- High count rate
- Very low dark count rate
- Broad spectral range



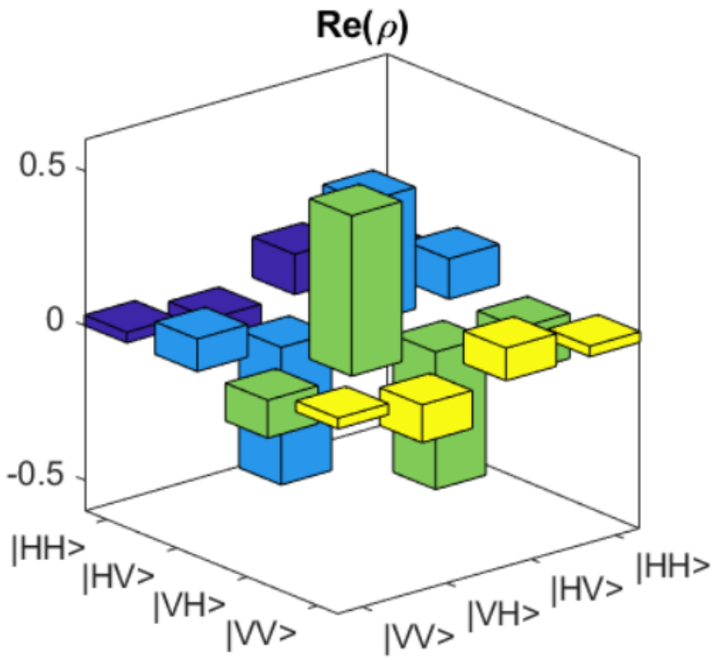
Superconducting material shaped into a meandering nanowire.
© NIST

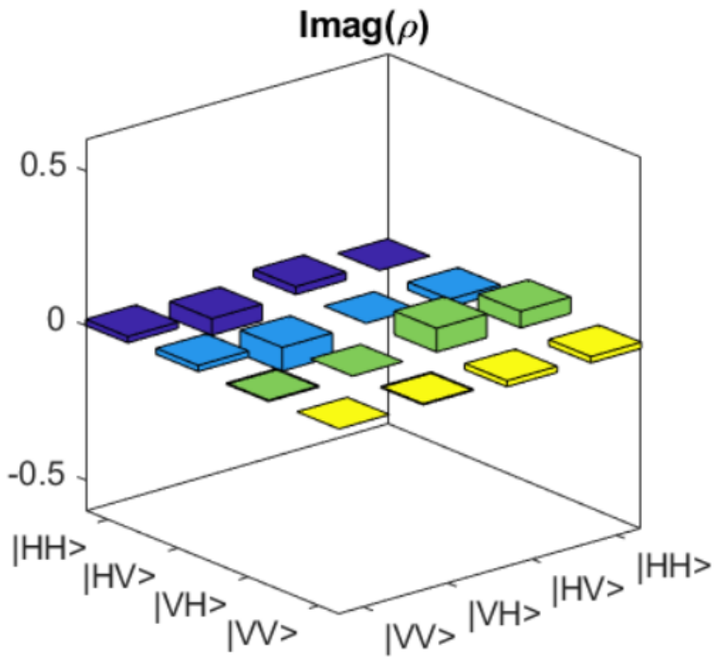


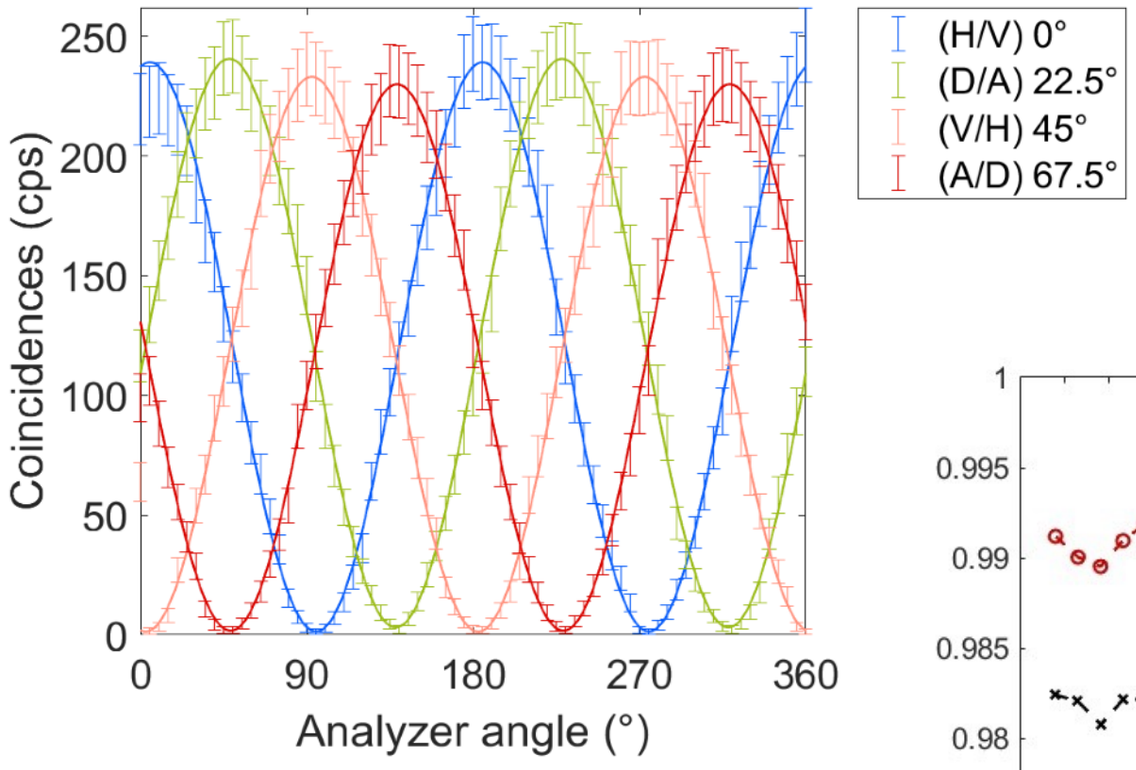
SiQUID

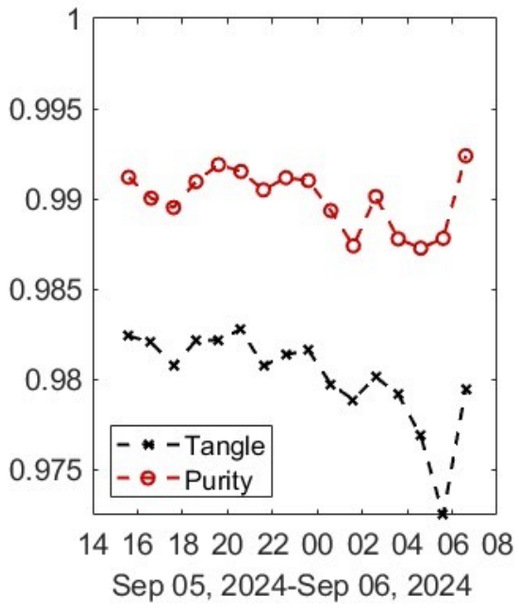
Karakterizacija izvora:

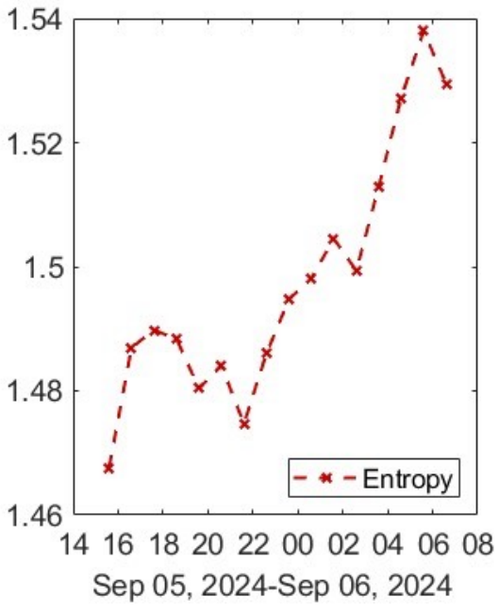
- Kotna odvisnost korelacij
- Kvantna tomografija
- Merjenje stabilnosti

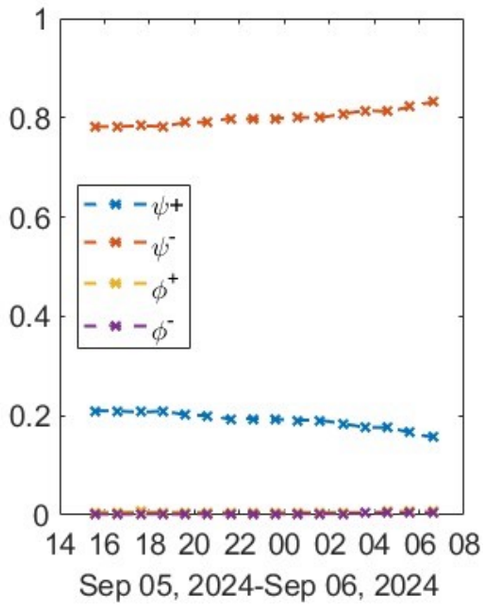












SiQUID

Karakterizacija izvora prepletenih fotonov:

Quantity	Measurement
Pump power	2.7 mW
Detector efficiency	77 - 83 %
Detector type	SNSPD
Number of detectors	4
Dead time	200 ns
Coincidence window	10 ns
Measured coincidences	240/s
Measured singles	3000 - 8000 /s
Heralding ratio	0.05
Brightness	110 cps/mW nm
Tangle	0.927 ± 0.004
Fidelity of the Bell state	0.901 ± 0.001 (with $\|\psi_-\rangle$)
CHSH inequality	2.75 ± 0.015
Bandwidth	0.8 nm
Contrast visibility	H/V basis: (89 ± 8) : 1 D/A basis: (74 ± 6) : 1 R/L basis (42 ± 2) : 1

SiQUID

Trenutno stanje projekta:

- Beyond Seminconductor razvija QEE za vladno kvantno mrežo
- Na eksperimentalni mreži na relaciji FMF-IJS implementiramo QKD na osnovi protokola BBM92
- UVTP in URSIV urejata povezave med vladnimi vozlišči. IJS ureja povezavo z reaktorskim centrom v Podgorici.

Obstoječe povezave s temnimi vlakni