Role of optical fibre for quantum communication

Latest developments from Stockholm trials

Gemma Vall Llosera, PhD Ericsson GFGO EIT

20241015

Quantum communication definition

Quantum communications is a field of quantum physics that studies the transmission of quantum states or quantum information along two (or more) parties

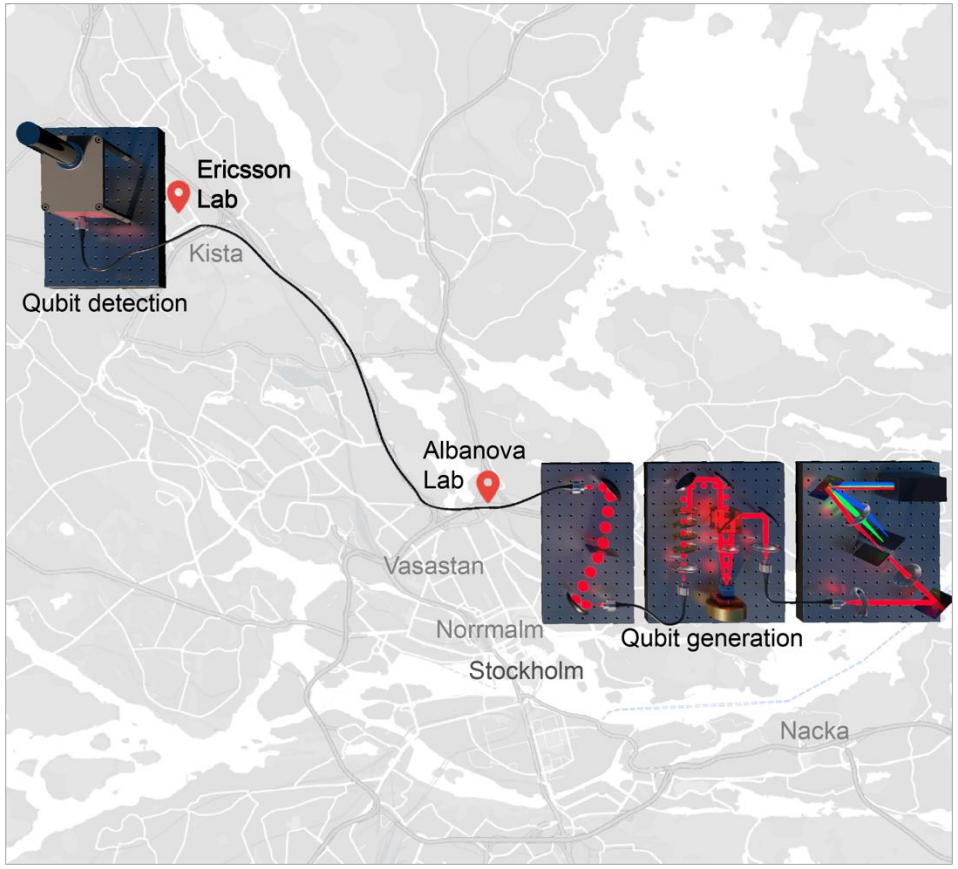
The goal is to distribute random bits, entangle resources or information, or other tasks allowed by quantum mechanics

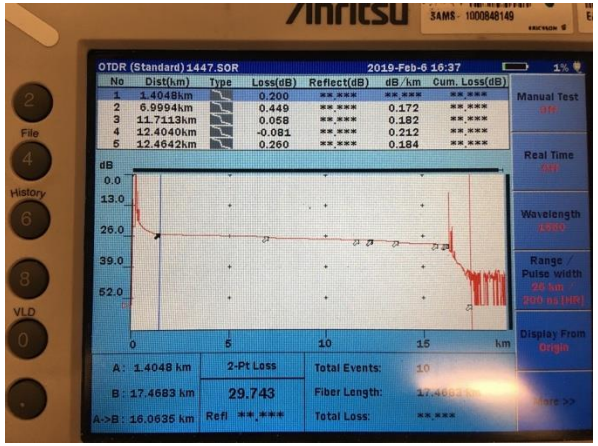
Quantum communication links and nodes build up so-called quantum networks.

At the moment, the most relevant applications of quantum communication, is quantum key distribution (QKD)

Sweden's first quantum link –May 2018

Scientific goal: Show Qubit and entanglement transmission over a deployed fibre network.



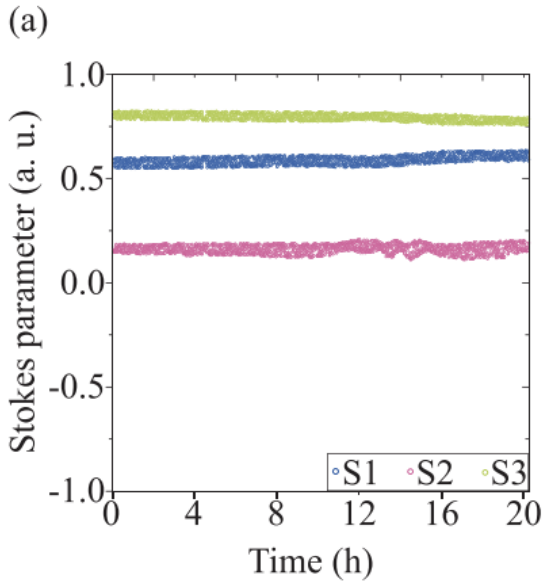


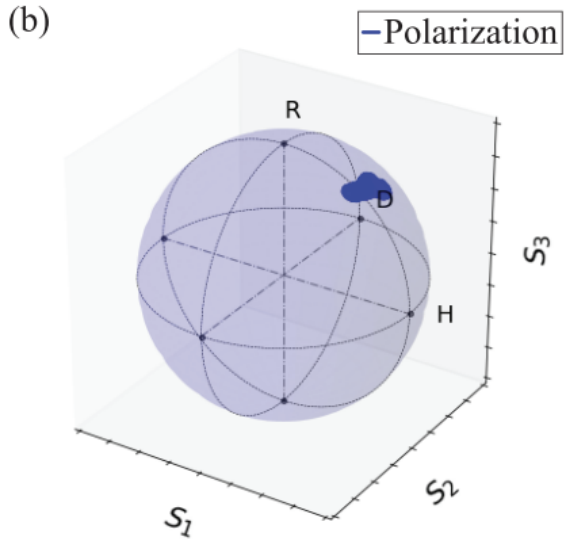
- 18 km fiber connection between KTH Albanova and Ericsson in Kista.
- SMF28 dark fibre link provided by Stokab.

Polarization measurement and stabilization

- Polarization of light is not maintained over fiber (unless we use polarization maintaining fiber) because optical fiber suffers from birefringence and is affected by environmental factors. However, maintaining polarization is crucial for sending information using this degree of freedom.
- One way to maintain the polarization is to stabilize it. This was accomplished by applying a gradient descent algorithm to the feedback loop given to the polarization controller elements in our setup and by using two reference lasers (one for each basis) with a similar wavelength

  - This allows us to control the polarization of single photon qubits in two different bases without measuring them.

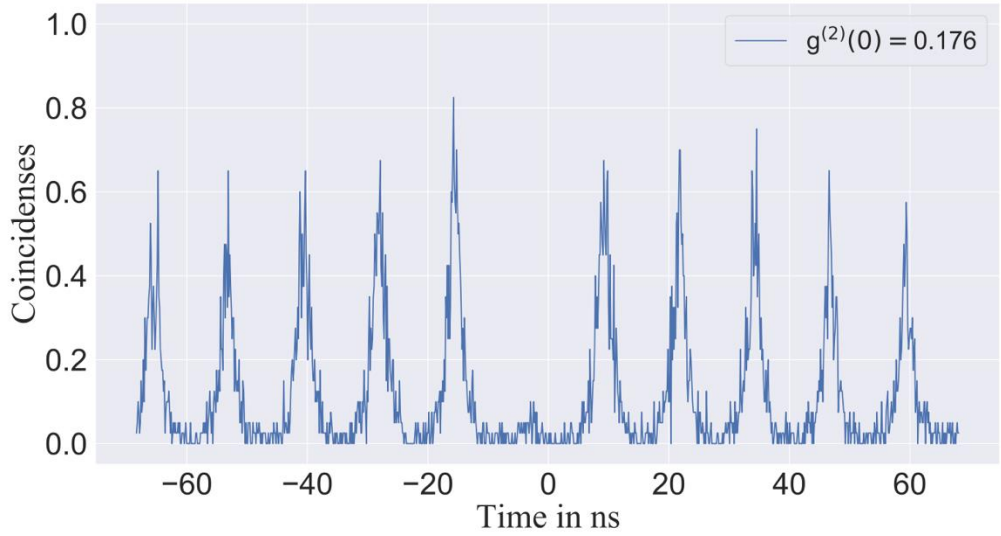




Master student: Liselott Ekemar; PhD student: Katharina Zeuner

Sharing Quantum Resources Across a Metropolitan Network

- We investigated and tested the setup needed to share quantum information across a metropolitan network based on single photon communication.
- First, we characterised the new set of super conducting nanowire single photon detectors (SNSPD)s at KTH.
- Second, we installed the SNSPDs at the Ericsson lab, thus completing the quantum link of about 18 km.
- Third, the single photon light source, based on quantum dots, was characterised and used to send quits over a deployed fiber to generate a $g^2(0)$value of 0.17.
- We measured the X and XX cascade to verify entanglement.
- Finally, we used the cascade from the QD to perform time synchronisation of two time-taggers.

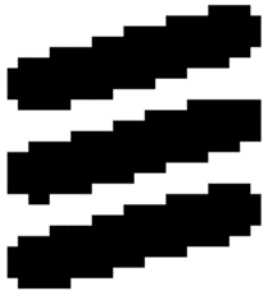


- $g^2(\tau)$: gives a measure of how likely it is to detect a photon within time τ after another when looking at a light beam
- For sub-poissonian light (single photons)
$$g^2(0) < 1$$
- it is less likely to detect two photons simultaneously

Master student: Master Carlnäs

Single-photon communication experiment

Original data:



Red pixel is an error, which can be detected, but not corrected.

The time bins are varied between **0.001 to 0.02**

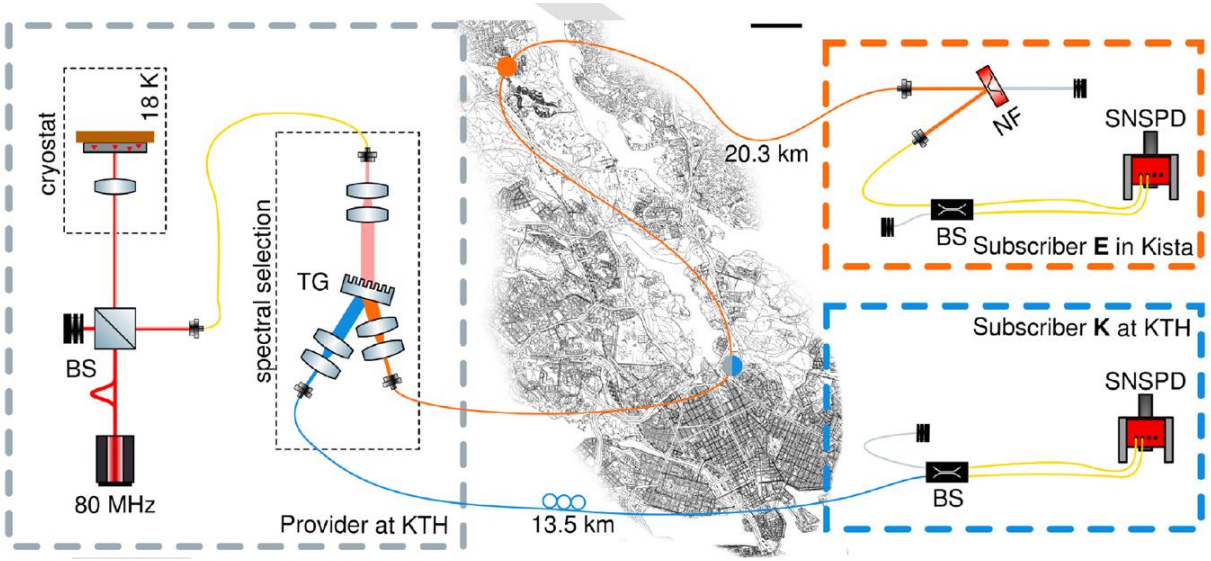
Received data:

- We used time bin encoded blocks of single photons modulated in the linear polarization basis over a dissipative channel to transmit information through the optical fibre link
- in theory, one time-bin = one photon
- we encode the message using $|H\rangle$, $|V\rangle$ and $|0\rangle$ states base, so that when we receive it, we can characterize error correction code performance.
- We performed forward error correction by designing codes to detect, and correct errors.

Master student: Maftuna Gaparova

Quantum link for distributing random numbers

- The same fiber link is also used to implement a provider-subscriber service to distribute single-photon generated random numbers.
- As a first method, we use the randomness extracted by allocating the bit values 0 and 1 to the respective output ports of a beam splitter.
- In a second method, we use the time between subsequent photon emissions as the source of randomness.



- While our source generated, to a very high degree, pure single photons, the slightly different detection rates on the two channels (1:1.12) caused by an imperfect beam splitter ratio combined with the different detection efficiencies, led to biased random numbers in the first method.
- The second method allowed us to distribute 19.1kbit/s and 80 kbit/s of unbiased random numbers to two different subscribers. *

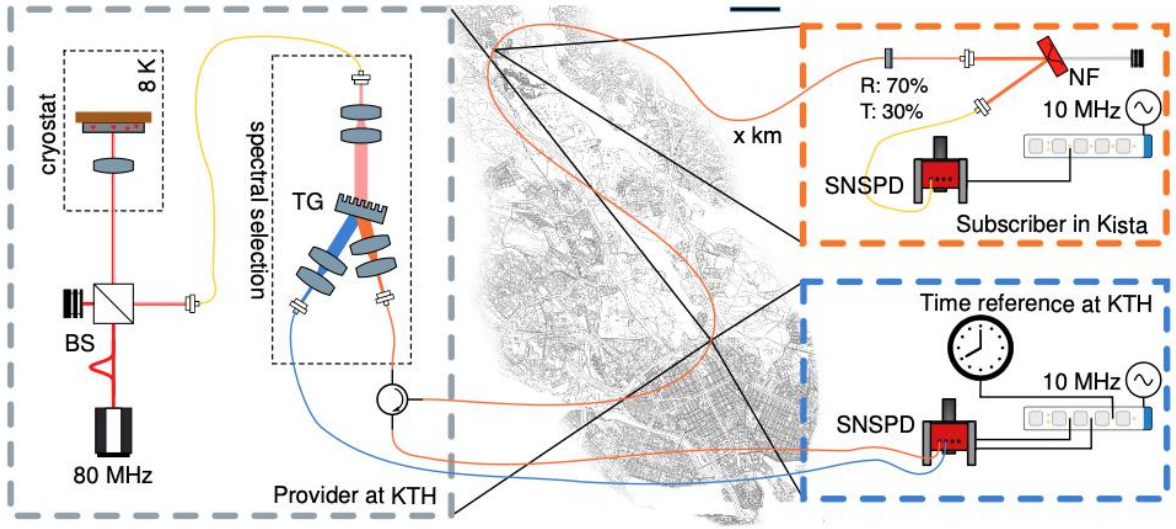
*Gyger, S. et al. ., *Metropolitan single-photon distribution at 1550 nm for rando number generation* , Appl. Phys. Lett. **121**, 194003, 2022, https://doi.org/10.1063/5.0112939

PhD student: Samuel Gyger

Time-sync with Q resources

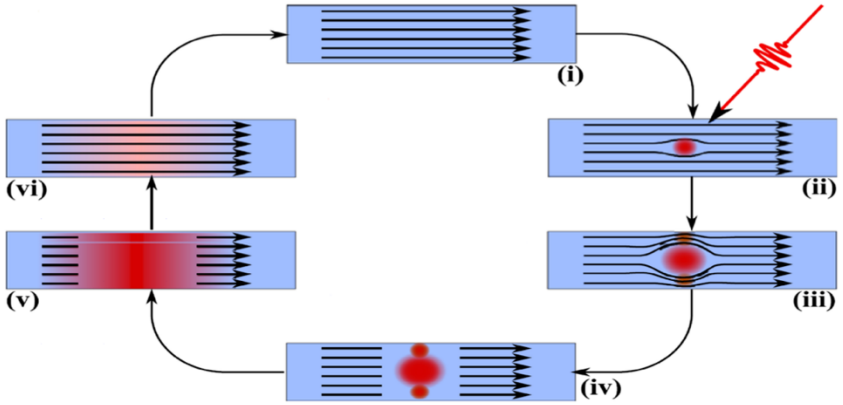
- In another experiment we tested a high accuracy time synchronization method using single photons from a cascaded three-level system e.g. self-assembled quantum dots .
- This method consists of a central provider with a time reference and one or more subscribers that will receive the high accuracy time synchronization.
- Telecommunication networks use highly accurate clocks in order, for example, to time stamp events, and to avoid bit slips during communication.

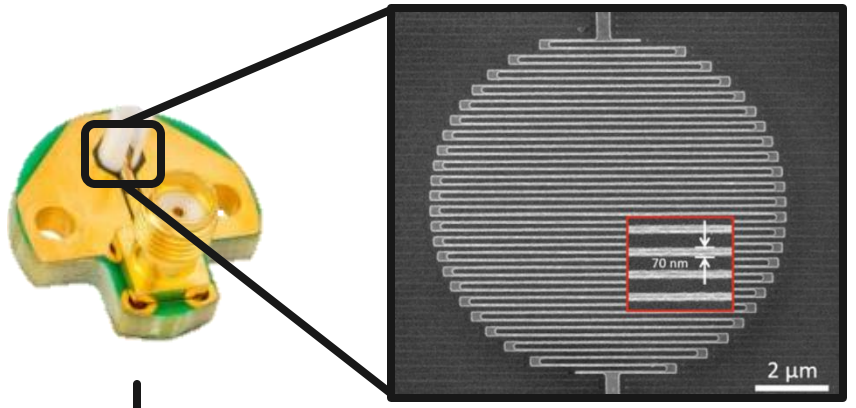
Most of the relevant synchronization requirements for telecom networks are defined by the 3GPP standardization body and delivered by a set of technologies: global navigation satellite system (GNSS), over-the-air-synchronisation (OAS), frequency-over-transport, time/phase over transport, and clocks. The GNSS consists of a set of satellites that host an atomic clock. The signal from the atomic clock is transmitted towards the Earth and received by a GNSS receiver.



PhD student: Samuel Gyger

Single Photon detectors





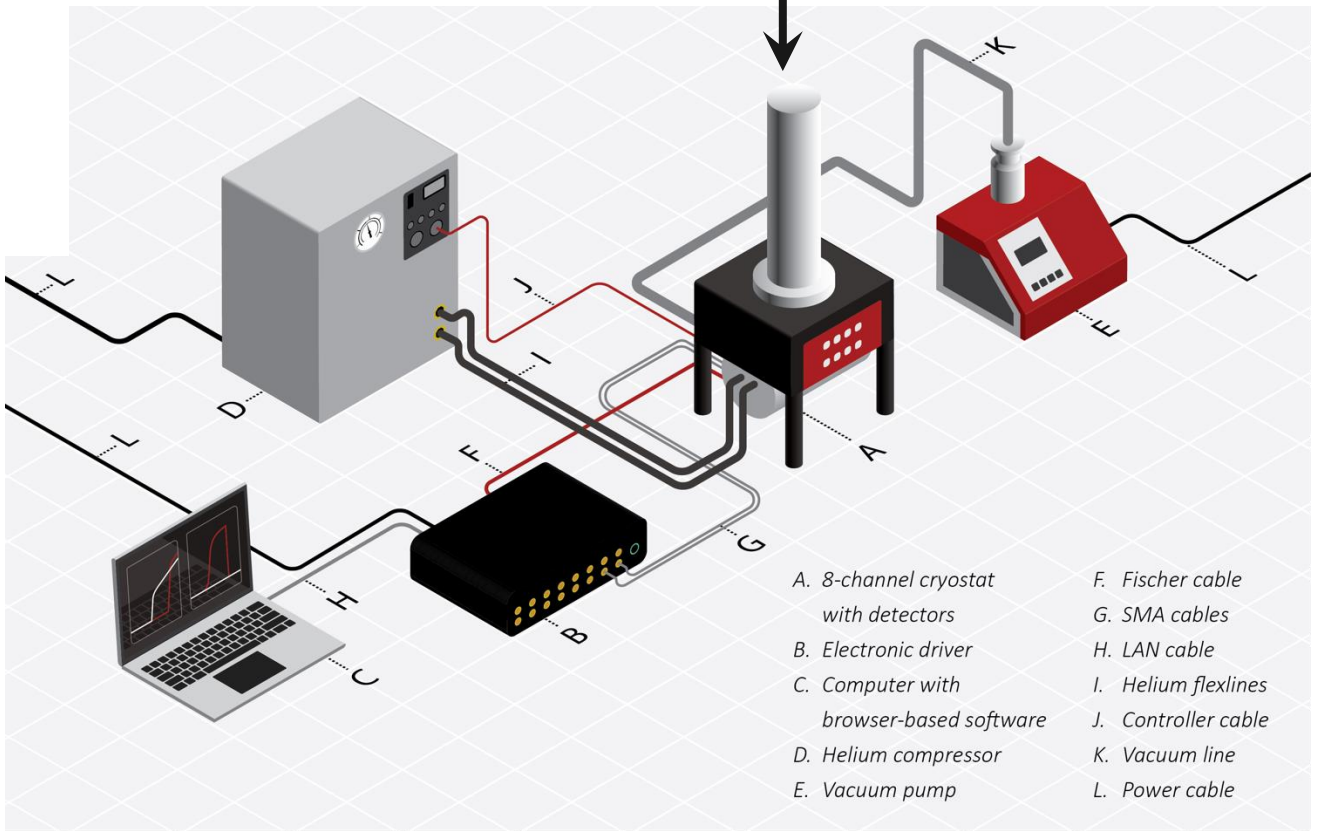


Photo courtesy of Prof. Val Zwiller

EuroQCI and National quantum communication infrastructure in Sweden

- The European Commission recognized Quantum Key Distribution as one of the most important ingredients to secure our future communication. Therefore, the Commission and Member States have agreed to implement a secure communication network based on quantum technology. This is called EuroQCI (European Quantum communication infrastructure).

NQCIS falls under the umbrella of the EuroQCI initiative, where the Swedish consortium formed by industry (Ericsson AB, Quantum Scopes AB, quCertify AB) and academia (KTH, Chalmers, Linköping and Stockholm University) have been granted 100M SEK to test and deploy quantum key distribution systems tailored to the specific needs of Sweden.

With funding from:

Wallenberg Foundations AB

VINNOVA
Sweden's Innovation Agency

Co-funded by the European Union

https://www.ericsson.com/en/blog/2023/8/building-a-quantum-key-distribution-network-in-sweden
https://www.kth.se/om/nyheter/centrala-nyheter/100-miljoner-till-kvantforskning-1.1249349

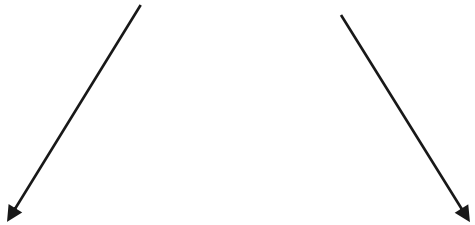
Quantum threat

Security processes at risk: those needed for public-key crypto (PKC).

PKC is the most widely used secure protocol for online browsing, data storage, and server connection. It requires a key and sometimes a signature, which are used to verify users, authenticate access, and provide confidentiality to a server

The authentication process can unfold in two ways: symmetrically and asymmetrically.

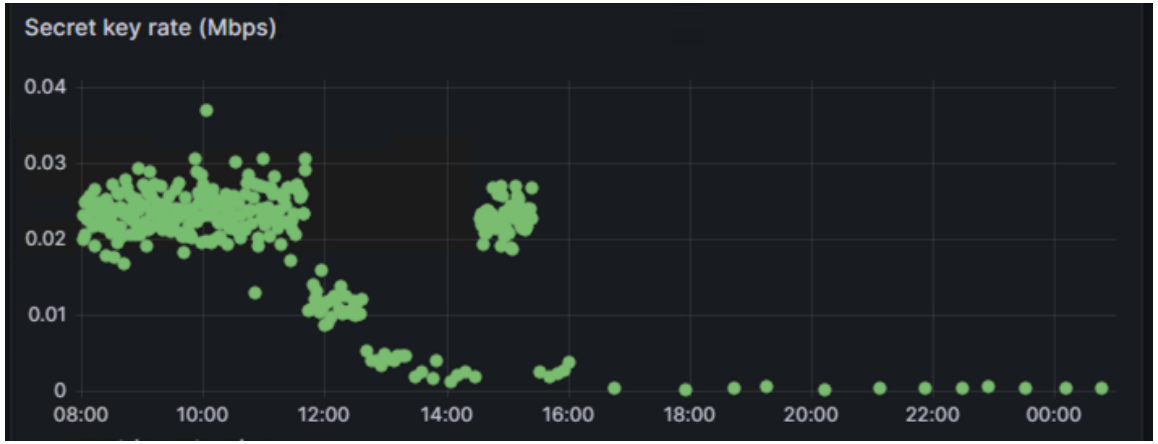
Symmetric encryption occurs when the same key is used for decryption and encryption — this is commonly used for data storage and to protect payment information on secure websites



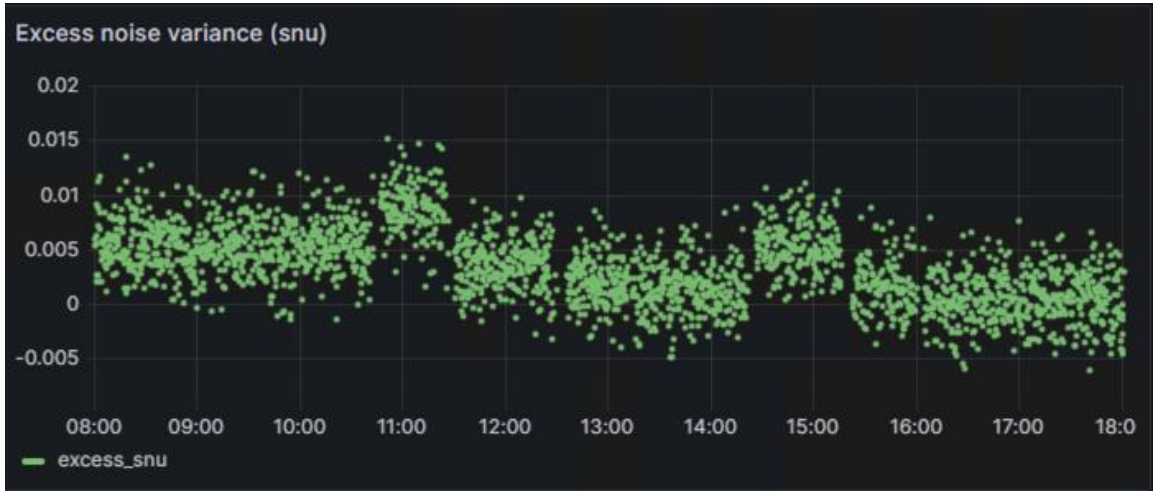
Asymmetric encryption uses a private and a public key pair to decrypt and encrypt sensitive data and/or to sign and verify a signature in authentication. Ex. TLS protected website, in SSH (Secure Shell) and IPsec (IP Security), user authentication in Secure Shell, as well as in all digital certificate-based authentication

Grover's algorithm target Symmetric Key Crypto systems, and **Shor's algorithm,** which can quickly decode the integer factorization process used to generate asymmetric key pairs used in PKC.

National quantum communication infrastructure in Sweden

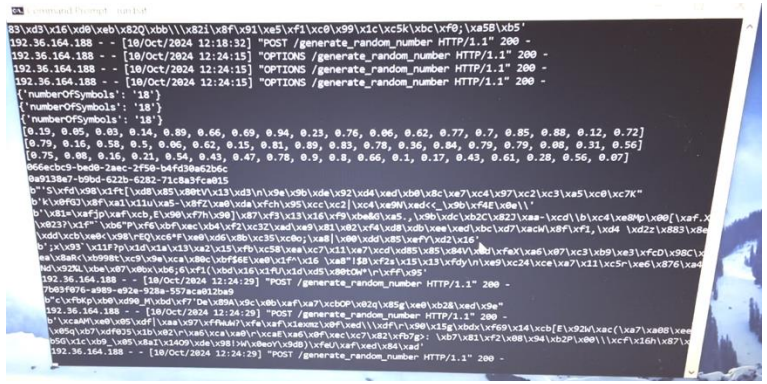


- Luxquanta devices testing
- CV-QKD system with Gaussian modulation
  - $SNR = \frac{\frac{1}{\mu} T V_{mod}}{1+\frac{1}{\mu}\xi}$
  - transmittance
  - excess noise variance
  - secret key rate

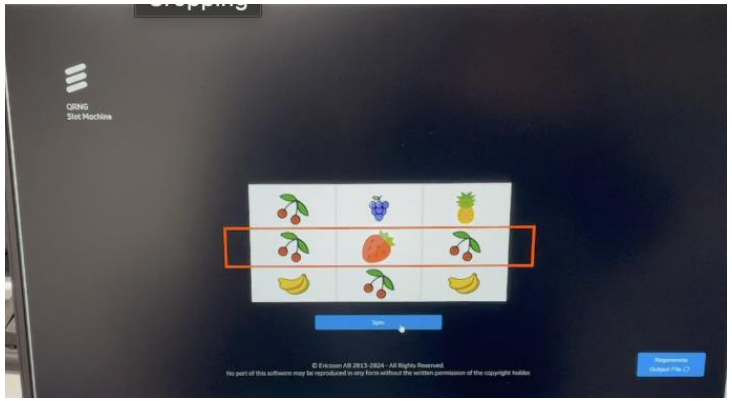


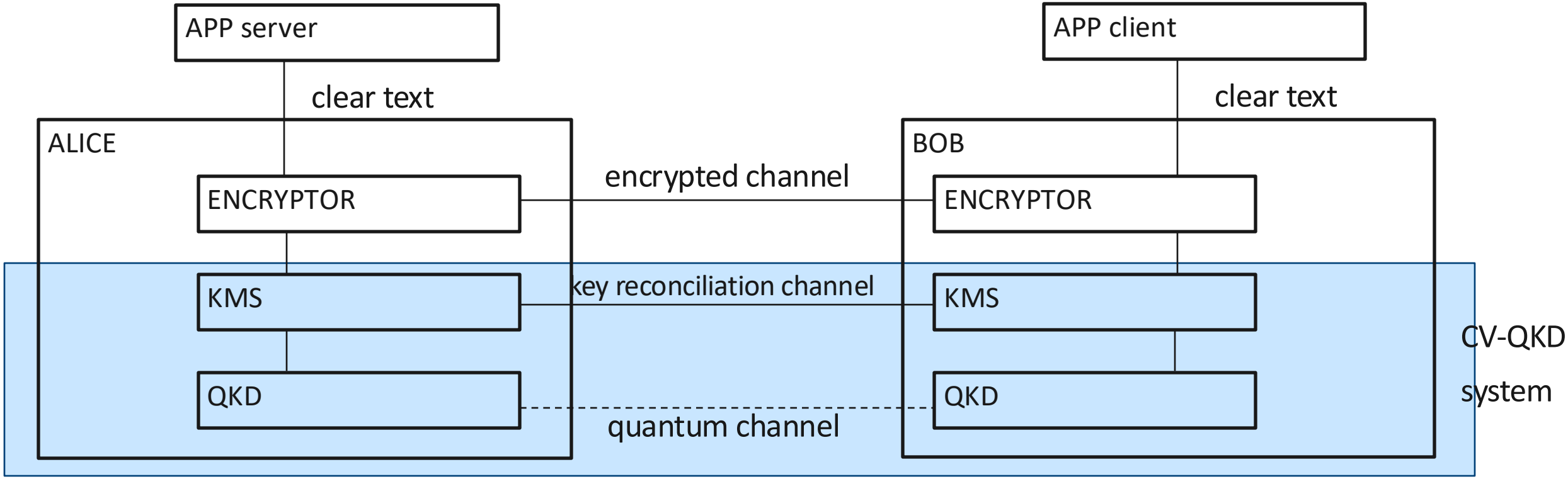
Findings so far

- The higher the loss in the link the more gaussians are needed to accumulate enough data for providing a safe key, which in turns determines the key rate.
- for an attenuation around 13.6 dB the system needed to accumulate 157 gaussians to produce a key length of 1095416
- The system consists of two QKD devices, one Tx and one Rx and two servers that act as a key management layer. Once set up, the system is plug and play and it comes with the key management layer integrated.
- Next steps: keep testing the limits of the system; couple our demo to it and make it work; procurement of a DV-QKD system.



[Quantum lotto app demo]





Summary

- Quantum communication is one of the flavours of quantum technologies w
- Devices developed for QKD are also useful for other applications such entanglement distribution, distributed Q sensing, distributed Q computing, and others yet to come
- The most mature application of quantum communication is quantum key distribution: within this are we tested CV-QKD with secret key rates of 3kbit/s for 9.5dB loss
- QKD can be sold as a service to applications wanting to consume a secure key distribution

Thanks for your attention!