Digital Europe Programme Project **QCI-CAT**
QCI: Proof of Concept – Secure Connectivity Austria
Digital Europe Work Programme 2021-2022
EU Secure Quantum Communication Infrastructure (DIGITAL-2021-QCI-01)
Project number: 101091642

Project starting date: fixed date: 1 January 2023
Project end date: 31 March 2026
Project duration: 39 months

Document:	**Deliverable**
Type:	Demonstration
Dissemination Level:	Public
Title:	**Testing and developing experimental national EuroQCI components**
Work-Package	WP8
Document number:	**D8.2**
Document Owner:	AIT / T. Strobl
Contributors:	T. Strobl, G. Humer, J. Piso
Abstract:	A dual channel SPD module was developed, assembled and tested at AIT. Meanwhile, AIT's DV-QKD system was tested over a terrestrial link and its long-term stability improved.
Key words:	QKD, Time-Bin Encoding, Single Photon Detection
Pages	21
Delivery Date Planned	2025-09-30 (M33)

Revision History

Version	Revision Points	Author(s) & Organization	Date
V 1.0	Initial version	M. Kos (AIT)	2023-02-20
V 1.1	First draft	T. Strobl	2025-09-14
V 1.2	Refined version	T. Strobl	2025-09-29
V 1.3	Revision integration	T. Strobl	2025-09-30

Author List

Organization	Name	E-Mail address
AIT	T. Strobl	Theodor.Strobl@ait.ac.at
AIT	G. Humer	gerhard.humer@ait.ac.at
AIT	J. Piso	Julius.Piso@ait.ac.at

Reviewer List

Organization	Name	E-Mail address
ALL	QCI-CAT Consortium	-
X-NET	K. Kloiber	kk@x-net.at
X-NET	W. Eibner	we@x-net.at

Copyright Statement

Funding Acknowledgement:

This project has received funding from the European Union's Digital Europe Work Programme 2021-2022 under Project number 101091642 and the National Foundation for Research, Technology and Development.

Table of content

List of Figures

Executive Summary

This deliverable reports on the development, testing, and demonstration of key experimental components for Austria's national contribution to the EuroQCI initiative. The work focuses on three main areas:

1. **Automation and stabilisation of the BB84 1550 nm DV-QKD reference system** – A series of control loops and software integrations were implemented to enable long-term, hands-off operation. These measures stabilised optical power output, automated delay correction, and enabled continuous laser current tuning. As a result, a stable positive secret key rate (SKR) can now be maintained for up to 10 hours without manual intervention.
2. **Development of a dual-channel single-photon detector (SPD) module** – A fully modelled and re-engineered detector module was designed with improved thermal isolation, upgraded moisture-resistant enclosure, and enhanced high-frequency electronics. The new module demonstrated robust cooling stability, improved mechanical reliability, and optimised detection performance, including reduced afterpulsing probability.
3. **Deployment of AIT's DV-QKD system over a terrestrial fibre link** – A field trial was conducted between Vienna and St. Pölten over a 119 km fibre link with more than 30 dB channel loss. Secure key exchange was demonstrated with a measured SKR of 4 kbps under laboratory conditions and positive SKR under adjusted field settings. The trial highlighted both the system's robustness and current limitations under real-world conditions, especially when operating at higher photon numbers.

These results provide important insights for scaling quantum key distribution technologies towards integration into the European Quantum Communication Infrastructure (EuroQCI). They represent significant progress in the automation, hardware development, and deployment readiness of national QKD components in Austria.

1. Introduction

The QCI-CAT project contributes to the European Union's vision of a secure pan-European quantum communication infrastructure (EuroQCI). Within this context, Deliverable D8.2 presents work carried out on testing, developing, and demonstrating experimental Austrian EuroQCI components.

1.1. Purpose and scope of the document

The document provides specifications, design insights, and experimental results related to automation of DV-QKD systems, development of novel single-photon detector modules, and deployment of QKD technologies in field conditions. Its purpose is to document both technical progress and practical challenges encountered in preparing Austrian infrastructure components for EuroQCI integration.

1.2. Target Audience

The deliverable is intended for project partners, the European Commission, and the wider quantum communication research and development community. It provides both technical results for experts and higher-level insights relevant to stakeholders involved in national and European-level QCI planning.

1.3. Relation to other project work

The work builds upon earlier efforts from AIT (e.g., [1]) to establish a BB84 reference system and design modular hardware components. It provides input for subsequent integration and deployment activities, particularly in relation to WP8, which focuses on experimental validation.

1.4. Structure of the document

The report is organized as follows:

- Section 2 describes automation and stabilization measures implemented in the DV-QKD reference setup.
- Section 3 presents the design, construction, and testing of a new dual-channel SPD module.
- Section 4 details the deployment and field demonstration of the DV-QKD system over a long-haul fiber link.

2. BB84 1550nm System Automation and Hands-Off Operation

To facilitate long-term hands-off operation of the 1550 nm BB84 reference setup, automation and stabilisation steps were implemented.

2.1. Receiver Script Preparation

Modifications were implemented to prepare the receiver script for integration in a hands-off measurement framework and to enhance its robustness for potential future adaptations:

- Changing the analysis script architecture from object-based to functional
- Enforcing a single-source-of-truth principle throughout the receiver framework. All protocol, measurement and analysis parameters were stored to, and referenced from, a metadata file accompanying each individual measured dataset.

2.2. Optical Power Stabilization

In prior tests using a manually controlled variable optical attenuator (VOA), the optical output power at the quantum channel usually exhibited a drift over time. This prevents the transmitter to achieve the optimal mean photon number (MPN) for secret key rate (SKR) maximisation. Additionally, if Alice's optical output power is not tracked, the output MPN drift leads to a systematic error during the privacy amplification, causing either an excessively reduction of the secret key or a part of the key left vulnerable to attackers.

To stabilise the optical output power for a more long-term hands-off operation, a control loop was established and integrated into the transmitter script.

- As a sensor, the optical power meter (OPM) POM-600 by OZ Optics was connected to the monitoring output (99% arm of the transmitter-side beam splitter). A C++ class was written to integrate serial communication with the OPM into the transmitter script.
- The output power was regulated using the voltage-controlled MEMS-based VOA VOAD-T57115313 by Agiltron, replacing the manually controlled VOA used earlier. The voltage input of the VOA was connected to an FPGA Mezzanine Card (FMC) DAC output.
  The voltage-attenuation response of the VOA was measured and saved as a lookup table for reference.

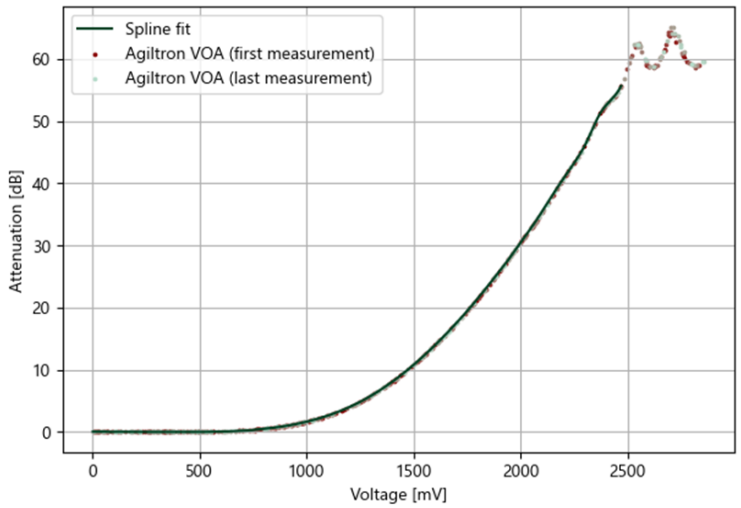


Figure 1: Voltage-attenuation curve of the Agiltron VOAD-T57115313 variable output attenuator.The data was recorded over a random sequence of voltages to avoid the systematic error caused by a potential attenuation drift. No significant drift was detected. This data was then fitted to a cubic spline model to create a reference lookup table.

As the optimization routine to reach the desired optical output power, a secant method was chosen, with the value taken from the lookup table serving as a starting voltage.

- At longer hands-off measurements, the optical power was reset between acquisition periods.

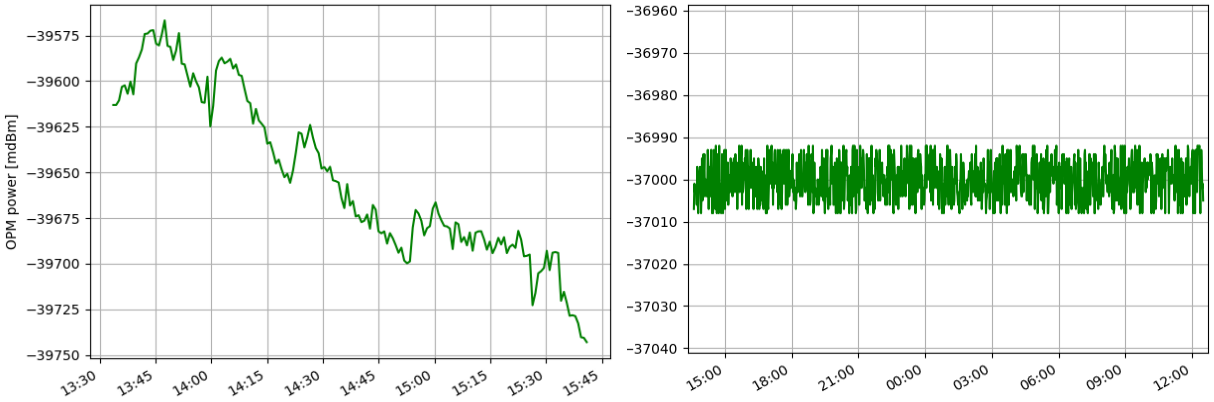


Figure 2: Optical power meter reading during an extended measurement before (left, 20241111) and after (right, 20250919) implementation of a stabilisation control loop. Note the different X and Y axis scaling.

2.3. Sync-Pattern Delay Measurement

As the sync and quantum signals are transmitted over separate fibre connections, the delay between the sync pulse and the start of the pattern is inconsistent due to the varying lengths of the fibres used for transmission, and to thermal expansion. Even when multiplexing both signals over the same fibre, chromatic dispersion influences the delay, as both channels use different wavelengths (sync at 1310 nm and quantum channel at 1550 nm). Knowing the delay with a higher precision than the time bin length (1 ns) is vital to correct qubit attribution during signal processing.

Up to this point, the delay had been determined semi-automatically by analyzing a histogram of detections using first the framewise sum, then the symbol-wise sum. Filtering the signal by qubit according to Alice's pattern indicated correct symbol attribution. However, this is not possible in a realistic scenario in which Bob does not know Alice's pattern during signal processing.

New routine:

1. Calculate the photon count distribution for each detector within the frame period.
2. Compute the convolution of a step function (1 for the duration of the pattern payload and 0 for the rest of the frame) with the photon count distribution. The maximum of this convolution provides an initial estimate of the delay. Its resolution corresponds to that of the distribution.
3. Subtract the delay estimate obtained in step 2 from the timestamps in the dataset.
4. Calculate the photon count distribution within the symbol period for each detector.
5. Convolve a step function like in step 2, but with the distribution within the symbol period. The maximum of this convolution is the correction to the delay value. Its resolution corresponds to that of the distribution.
6. Subtract the delay correction determined in step 5 from the data.
7. Test the analysis on a subsample of the dataset. Symbol errors approaching 50% indicate that the delay of that specific channel is off by a multiple of the symbol length (10 ns). If the error of the X channels approach 100%, it indicates that the X channels are swapped.
8. Correct accordingly. Repeat steps 7 and 8 until optimal delay values are obtained.

This routine requires no manual steps.

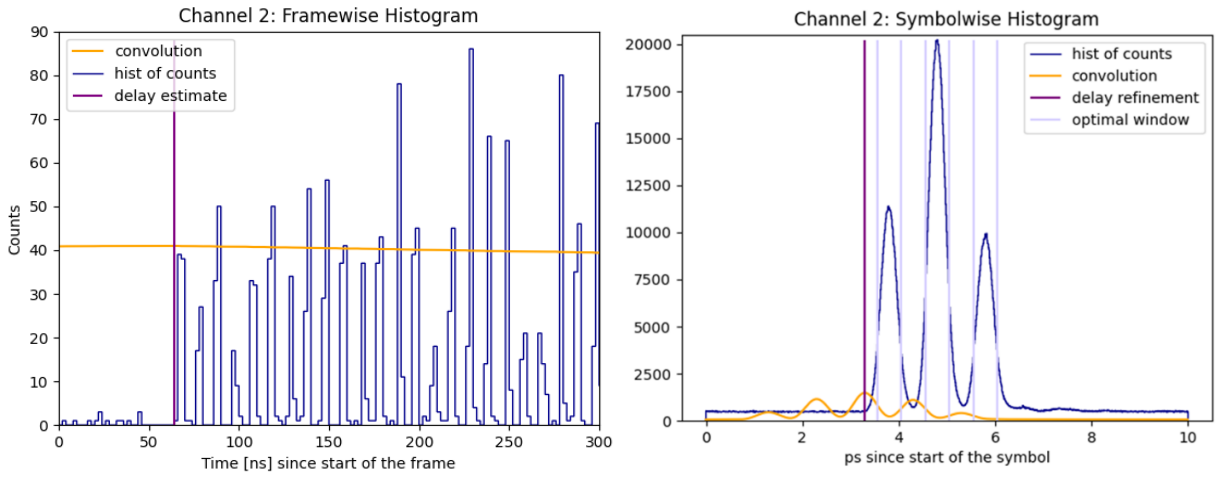


Figure 3:Distribution of photon counts within the frame (left) or symbol (right).Left: The start of the pattern is found by maximising the convolution of a step function s(t)={0 for t<τ;1 for τ<t<τ+T_Pattern;0 else} with the distribution. Right: The start of the pattern is refined by maximising the convolution of a step function modelling the time bins with the distribution.

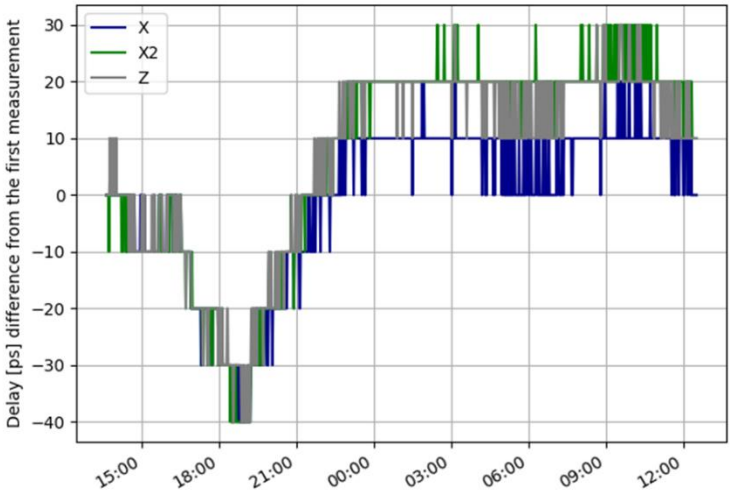


Figure 4: Automatic delay corrections during an extended hands-off measurement (2025-09-19 APD measurement).

Laser Current Tuning

In the BB84 receiver, the phase information of X-basis qubits is decoded via interference in a Mach–Zehnder interferometer (MZI). Careful control of the phase difference at the MZI arms' outputs is necessary to maximize the sensitivity and specificity of the receiver. This phase difference is mainly influenced by two parameters: the optical path length difference of the MZI arms and the laser frequency.

Both the laser diode and MZI are temperature-controlled, however, small phase drifts cannot be ruled out. In fact, prior experiments have demonstrated an ongoing increase in X-basis errors and divergence in X-basis count rates.

Phase tuning is achieved by adjusting the laser frequency via the diode laser current. Prior to automation, this step had been performed manually before each QKD transmission. Experience has shown that, when the setup is reset, the optimal laser current value is not usually the same.

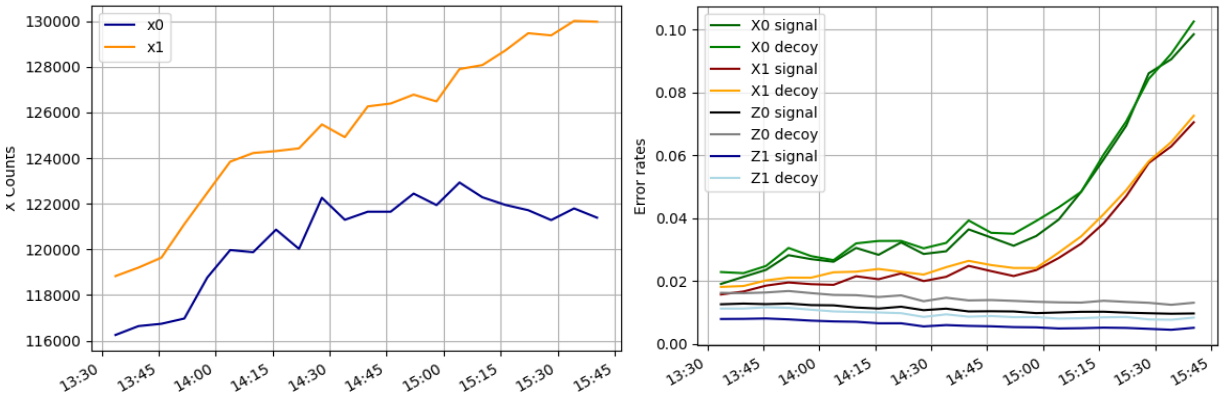


Figure 5: X basis count rates (left, counts per 180s) and error rates (right) over an extended period (2024-11-11 SNSPD measurement). Left: In addition to a constant offset caused by unequal detector efficiency and MZI imbalance, the X0 and X1 count rates diverge over time. Right: Whereas Z error rates (QBER) remain relatively stable and are even slightly decreasing, X error rates rapidly rise synchronous to the X0-X1 count rate divergence. Possible causes for both drifts, X count and error rate, are temperature changes or a laser frequency drift. Both effects can be compensated by continuous adjustment of the laser current.

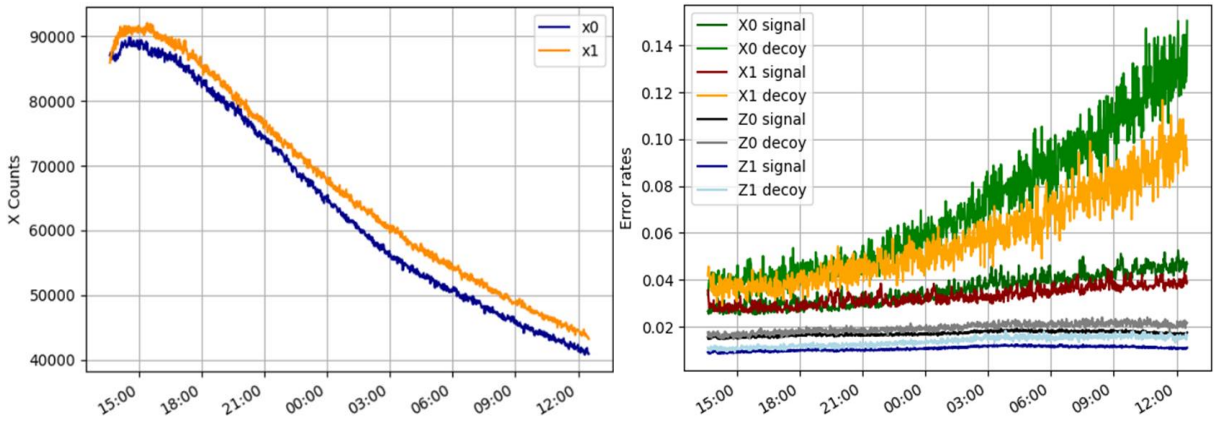


Figure 6: X basis count rates (left, counts per 60s) and error rates (right) over an extended period (2025-09-19 APD measurement), after the implementation of automated laser current tuning. Left: The X0 and X1 count rates no longer diverge. Right: The rise in the X channel error rate now happens more slowly (note the different time scale to the previous figure) and can probably be attributed to other causes (see discussion).

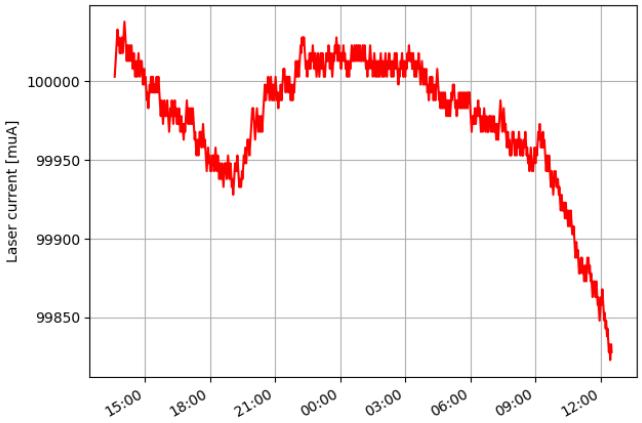


Figure 7: Automatic laser current adjustment over the course of an extended period (2025-09-19 APD measurement). The laser current was adjusted by 5 µA at a 60s interval between data acquisition periods. X basis QBER change steered the direction of adjustments.

Automation and stabilization steps:

- Integration of Thorlabs laser driver APT functions into the transmitter script.

- Control loop: the parameter chosen as the process variable was the X basis QBER, which needed to be minimized. The control action consisted of small adjustments to the laser current (with a fixed step size of 5 µA and a step direction according to the change in QBER) between data acquisition periods.

With laser current automation active, X-basis count rates no longer diverged over time. However, the X basis QBER still increased over time, albeit over a much longer timescale.

2.5. Result and Discussion

Using APDs for single photon detection (SNSPDs would require additional polarization stabilization), a positive secret key rate can now be maintained for 10 hours without manual intervention.

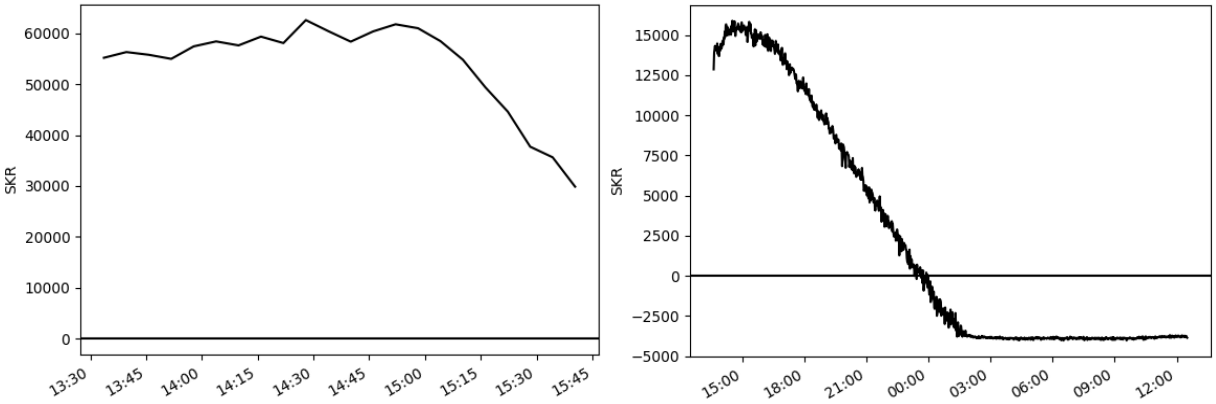


Figure 8: Secret key rate of extended-time QKD transmissionbefore (left, 2024-11-11 SNSPD measurement) and after (right, 2025-09-19 APD measurement) automation and stabilization efforts. Note the different X axis scaling.

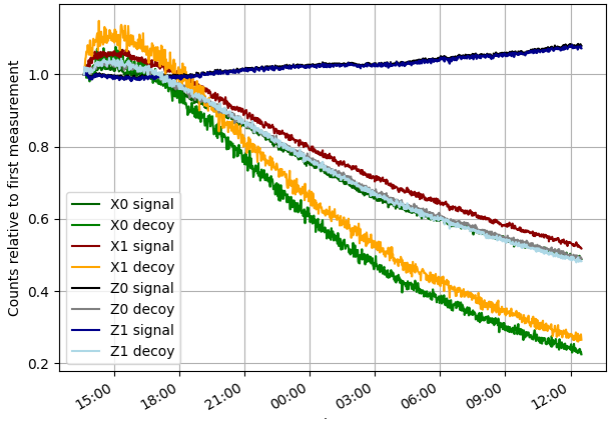


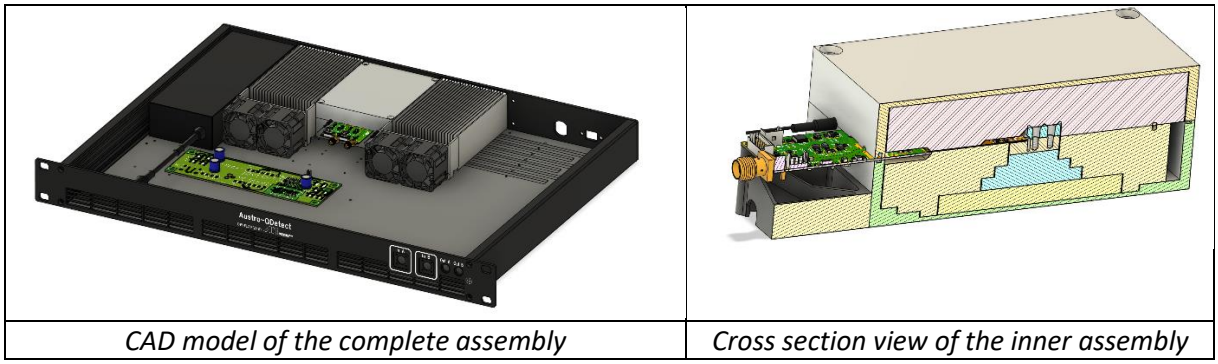
Figure 9: Count rates by qubit and amplitude (2025-09-19 APD measurement) relative to the respective initial count rates. The change correlates with the amplitude, suggesting an AM bias point drift.

Even though the average count rate is now stabilized using the OPM-VOA control loop, symbol-specific count rates still diverge over time. This progression appears to correlate with the decrease in the secret key rate. The dependence of the count rate change on the symbol-specific amplitude (Z, X, signal, decoy) suggests a drift of the amplitude modulator bias point. At the time of writing, the bias point can only be determined through manual steps, as the procedure requires increased optical power (by setting the carver to pass) that necessitates the disconnection of the single photon detectors. There are options for indirectly tracking the AM bias point, and these will be addressed in the near future.

3. Dual Channel Single-Photon Detector Module Development

3.1. CAD Modelling of Entire Assembly

To simplify the coordination between the mechanical and electronics design, the complete detector assembly was modelled in CAD. With this model we could quickly test new component arrangements as well as simply extract components for 3D printing or classical fabrication.

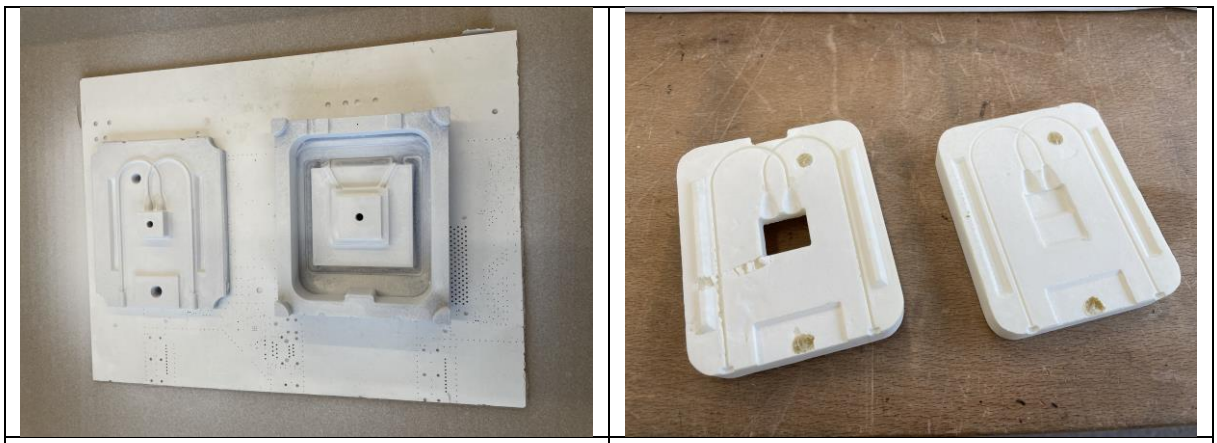


CAD model of the complete assembly	*Cross section view of the inner assembly*

Figure 10: CAD model of detector.

3.2. New Thermal Isolation

The CAD model enabled us to use the negative volume within the inner enclosure as a template for an PU-foam isolation body. We designed a three-part mold into which the foam can be injected. This mold was 3D printed to enable quick iteration for fine tuning the geometry for the molding process.



3D printed mold	*Final foam isolation created by the molding process*

Figure 11: Foam mold

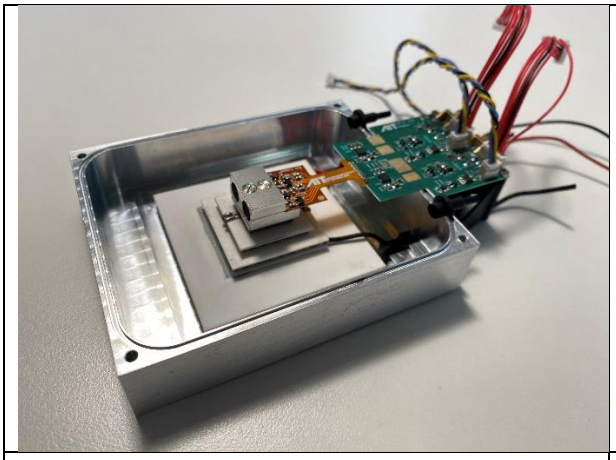
The PU foam we used hardens in a closed cell configuration which should reduce the likelihood of moist air being introduced to the system.

3.3. Upgraded Enclosure

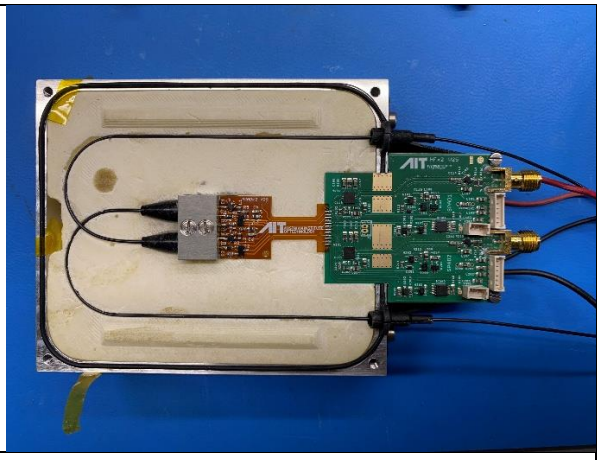
One of the main obstacles in the long-term operation of the device is the build-up of moisture around the electronics due to parts of the device being cooled well below the dew point of the surrounding air. Multiple steps have been undertaken to minimize this issue:

- **Enclosure Redesign:** Now the enclosure consists of two aluminium shells, each CNC fabricated from a single block of aluminium. Thus, no gluing of individual parts is required, which reduces the number of possible ingress points.

- **Rubber Gasket:** The shells' designs were updated to incorporate a rubber gasket at the contact areas, as well as around the PCB.
- **Desiccant:** The new thermal isolation includes cutouts to accommodate silica gel, to minimize the remaining humidity within the sealed enclosure.



Inner enclosure without isolation foam and optical components.



Inner Enclosure complete with electronics, gaskets and isolation foam installed.

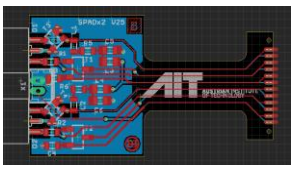
Figure 12: inner enclosure of detector.

Previously the inner enclosure was constructed from multiple interlocking aluminum parts that had to be glued together for the final assembly. In addition to being more difficult to assemble, this also led to potential air gaps which could let moist air pass into the enclosure leading to condensation on colder components. With the redesigned enclosure, there is only a single gap where a grove for the rubber gasket could be milled into.

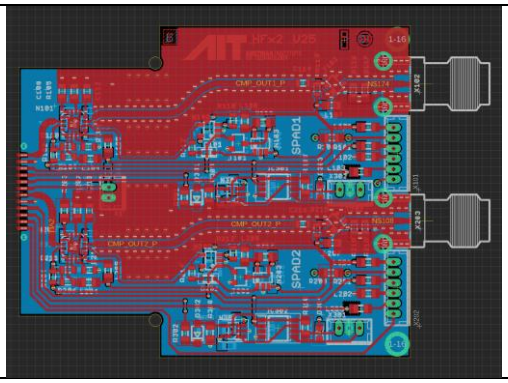
During the design phase of the isolation foam geometry, a cutout was added to one of the two foam halves, to accommodate for silica gel desiccant.

3.4. Improved Electronics

A major design revision of the internally developed high-frequency electronics was done to incorporate the findings of the previous iteration. Now a better RF substrate is used, and the fast signals are routed with an improved coplanar waveguide structure. Also, the interface between the rigid and flexible PCB was improved to enhance mechanical reliability as well as simplify the assembly. The 3D CAD model enabled us to fine tune the enclosure geometry towards the requirements of the PCB layout (e.g. have special cutouts above the high frequency traces).



Flexible PCB – dual SPAD frontend



Rigid RF optimized PCB

Figure 13: Picture of PCB print.

3.5. Measurement Results

Cooling

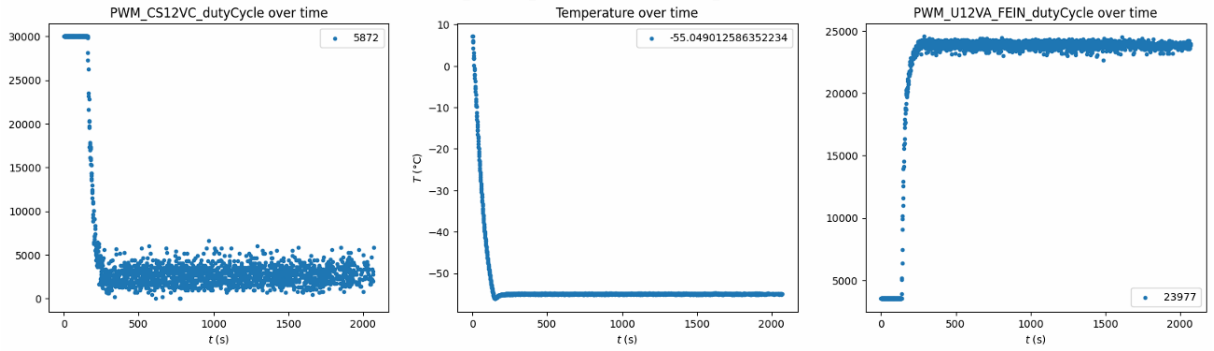


Figure 14: Measurement of temperature over time (central plot).

The figure above shows the cooldown process and related system parameters over time. The plot in the centre shows the temperature curve. The control parameters are tuned to reach the target value quickly with minimal initial oscillations. The measured temperature stays within +/- 0.1°C of the target value (-55°C in this case). The plot on the left shows the duty cycle of the cooling fan, while the plot on the right shows the how much the power sent to the Peltier cooling stack needs to be downregulated (both quantities are given in the values provided by the controller, which are 16-bit unsigned integers).

Detector Characterization

The figure on the right shows the result of a characterization measurement of the detector module with our in-house developed detector testbench. The plot on the bottom shows the relationship between detection efficiency and the applied reverse bias voltage at different threshold values. This threshold is used to adjust the minimum avalanche intensity that is needed for an event to register as a detection. The plot on the top shows the estimated afterpulsing probability in percent at the different detection efficiencies and threshold levels.

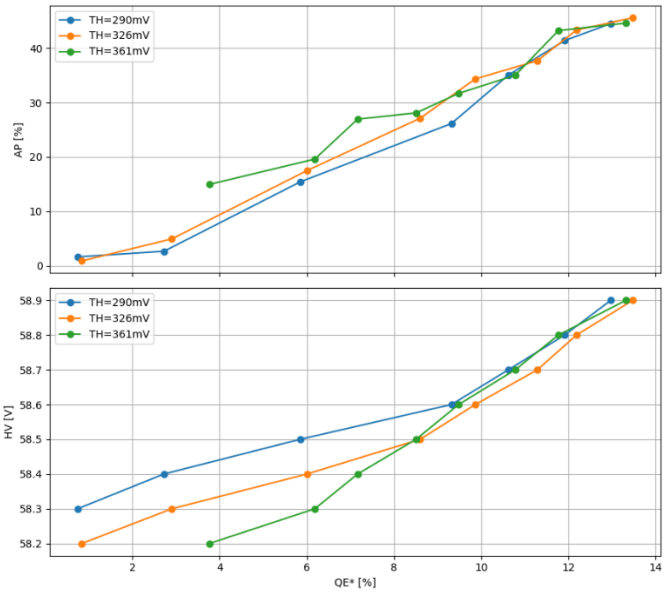


Figure 15: Measurement results of the detector with afterpulsing probability (top) and detector efficiency (bottom).

4. Deployment of AIT's DV-QKD System over a Terrestrial Fibre Link

We present a demonstration of AIT's DV-QKD system over a network fibre segment with 21 dB signal attenuation, utilizing a link between St. Pölten and Vienna.

A secret key rate of 4 kbps was measured, matching prior test measurements under laboratory conditions.

4.1. Setup and Operating Parameters

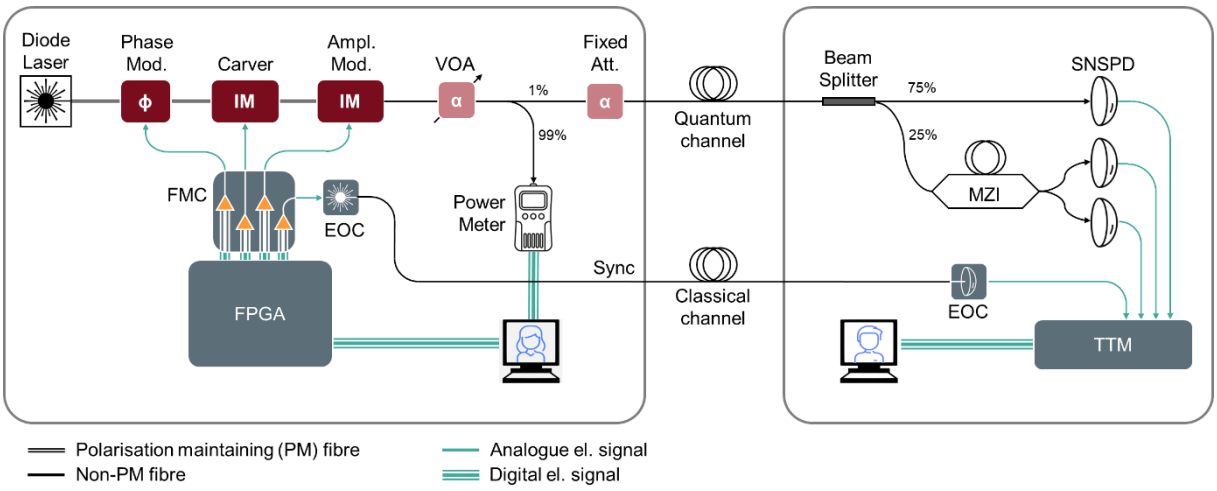


Figure 16: Schematic diagram of the BB84 DV-QKD setup.The transmitter consists of a 1550 nm diode laser followed by a chain of modulators and passive components. The receiver comprises passive components and a single-photon detection system; in this case, nanowire detectors were used. Transmitter and receiver are linked by two fibre connections: one carrying the quantum signal, one a synchronization pulse train that is used to synchronize both components' clocks.

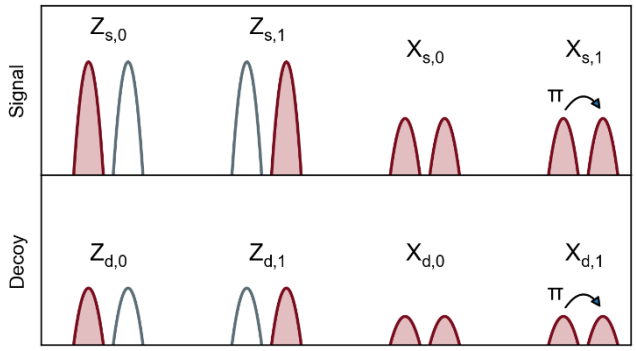


*Figure 17: States and amplitudes produced by AIT's BB84 DV-QKD system.This system implements one-decoy, four-state time-bin encoding at 1550 nm.*The deployed QKD system uses 4-state time-bin encoding with one signal and one decoy amplitude, leveraging the security proof presented by Rusca et al [2]. The transmitter - Alice - prepares qubits from a 1550.12 nm continuous-wave (CW) beam using a string of modulators and passive elements.

All modulators on Alice's side are controlled by a custom-programmed Field Programmable Gate Array (FPGA) via a custom-built FMC that acts as a signal digital-to-analogue converter and amplifier.

On Bob's side, the random basis choice for detection is implemented using a passive component, an asymmetric beam splitter with a 75-25 splitting ratio chosen appropriately to the transmission conditions. For single-photon detection and time tagging, AIT's in-house SNSPD system was used.

Optical pulses were used to synchronise Alice's and Bob's clocks. These classical pulses were implemented using an in-house developed electro-optical transmitter-receiver pair and transmitted over a separate fibre.

Operating parameters were optimised to the field conditions using a routine based on [5]. For simplicity of post-processing, a framewise repetitive random pattern was chosen with a 61-39 signal-decoy distribution and a 71-29 Z-X distribution. Qubits were emitted at a 10 ns interval; the time bin length was set to 1 ns. Sync pulses were sent every 1.1 ms, heralding the start of a new pattern frame.

4.2. Characterization under Laboratory Conditions

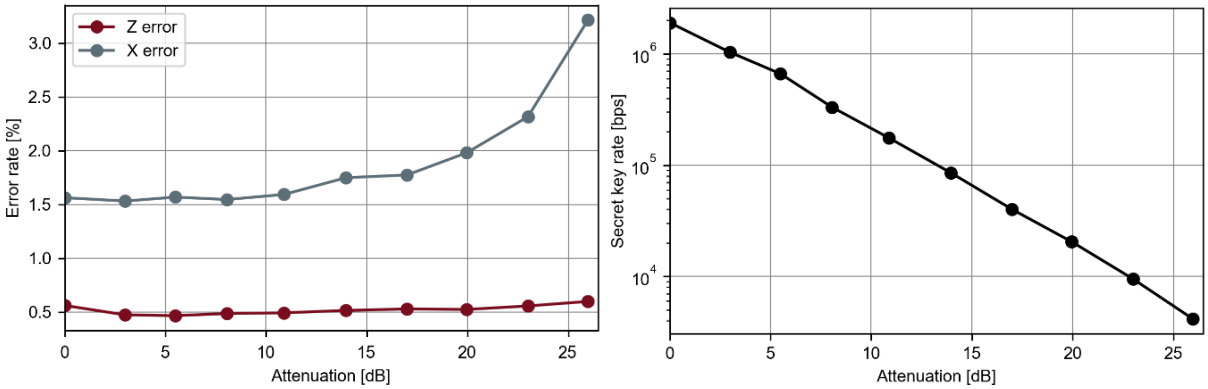


Figure 18: Error rates and SKR of the DV-QKD system during a laboratory characterization prior to the field test.

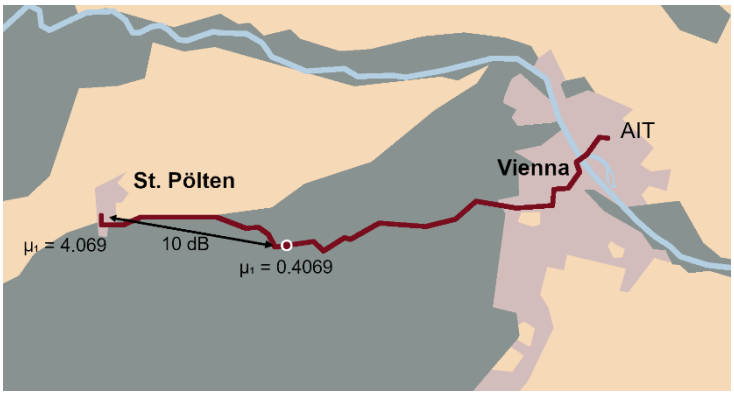


Figure 19: Fibre link between AIT and St. Pölten. Since the optical loss caused by the fibre exceeded the system's tolerance, the quantum signal was emitted at a higher MPN. Consequently, the signal was vulnerable to PNS attacks in the first segment of the link until it was attenuated by 10 dB.

Prior to the field test, the system's performance was characterized under laboratory conditions, where the transmission loss of the fibre connection was imitated using the VOA in the transmitter. Secure QKD, indicated by a positive SKR, was achieved at up to a signal attenuation of 25.9 dB.

4.3. Field Measurement using Network Fibre Link

For the field test, a fibre pair linking AIT to a telecom fibre network hub in St. Pölten was established. Both fibres measured 119.07 km in length, transmission losses were recorded at 31.3 dB and 30.87 dB by Optical Time Domain Reflectometry (OTDR) measurements. The sync channel was assigned to the fibre with the lower loss. From the prior system characterization, it was anticipated that the attenuation of this fibre link would exceed the BB84 system's tolerance by 5 dB.

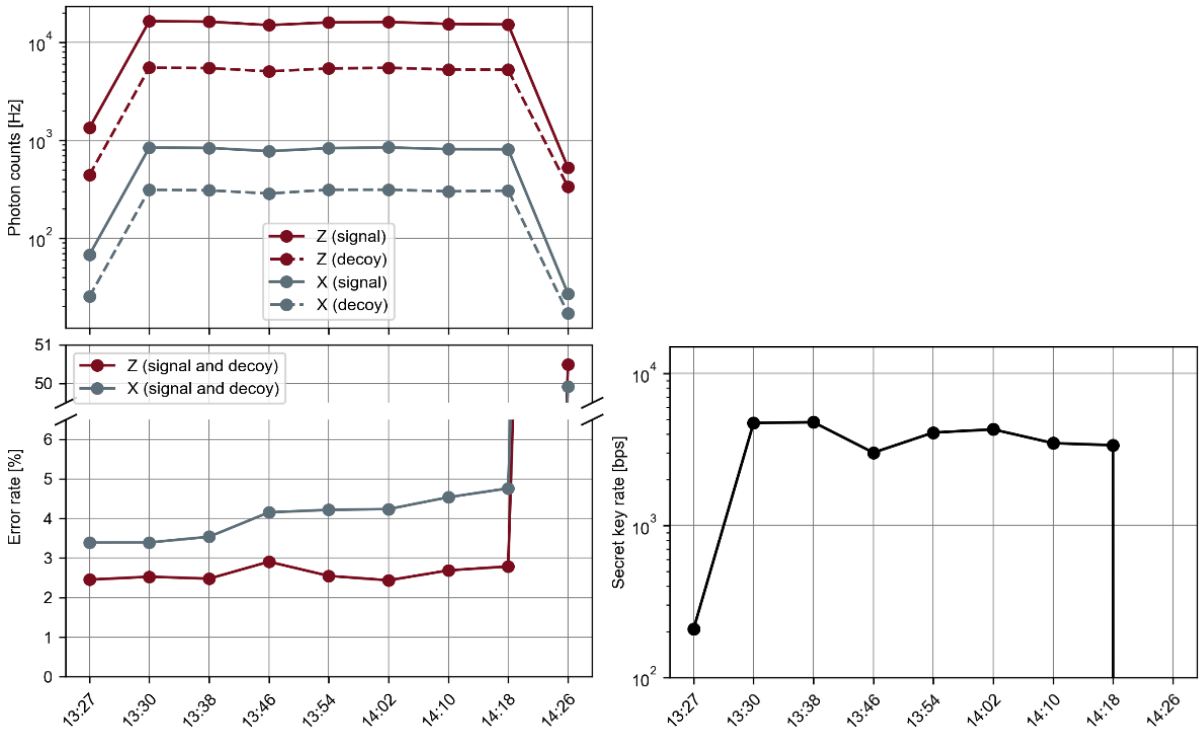


Figure 20: Result of the field measurement.

Consequently, the transmitter MPN was increased tenfold to 4.1 photons per qubit to overcome the loss in the quantum channel. In the real-world context, this signal would be vulnerable to photon number splitting attacks near the transmitter, before it has been attenuated to the single-photon regime by fibre-related losses. Therefore, the distance of secure QKD has been shortened by approximately 30% because of the MPN increase.

A 45-minute measurement sequence was run at this configuration at the increased MPN, followed by 120 s of data acquisition at 0.41 photons per pulse to assess the real-world performance on the entire link.

From the recorded data, the SKR was lower-bounded using a secrecy parameter of 1.0 ×10−9 and correctness parameter of 1.0 ×10−15. This approach also considered finite-size effects; the block size was given by the number of Z basis qubits after sifting (as the key was encoded in the Z basis, X served as the control basis). The mean photon number per pulse of the signal was assumed as 0.41 photons per qubit for all measurements (the amplitudes of all other states scaled accordingly). As stated before, when a higher MPN was transmitted, this interpretation only holds for part of the fibre link.

During the transmission at the increased photon rate, a positive SKR could always be achieved. X error rates were rising during the measurement, which was likely caused by a temperature shift in the Mach-Zehnder-Interferometer. This issue was later addressed by means of continuous laser current tuning.

As anticipated, no positive SKR was observed when a pattern was transmitted at 0.41 photon per pulse.

Summary

This deliverable presented the implementation and validation of experimental Austrian EuroQCI components within QCI-CAT.

Automation of the BB84 DV-QKD reference setup enabled long-term hands-off operation. Optical power stabilization, automated delay correction, and laser current tuning ensured consistent system performance and supported secure key generation for up to 10 hours without manual intervention.

A dual-channel single-photon detector module was developed, featuring enhanced thermal isolation, a redesigned sealed enclosure, and improved high-frequency electronics. The module demonstrated stable cooling behavior, reduced afterpulsing, and reliable detection efficiency.

Finally, AIT's DV-QKD system was deployed over a 119 km fiber link between Vienna and St. Pölten. Despite high channel losses, secure key rates were achieved under adjusted conditions, confirming the system's field readiness while highlighting operational limits in real-world environments.

Overall, these results demonstrate substantial progress towards national EuroQCI readiness, with key advancements in automation, detector hardware, and field deployment of quantum key distribution technologies.

Appendix A - List of Acronyms

Acronym	Meaning
QKD	Quantum Key Distribution
SPD	Single Photon Detector
CW	Continuous Wave
FPGA	Field Programmable Gate Array
FMC	FPGA Mezzanine Card
SNSPD	Superconducting Nanowire Single Photon Detector
SKR	Secret Key Rate
OTDR	Optical Time Domain Reflectometer
MPN	Mean Photon Number
VOA	Variable Optical Attenuator
OPM	Optical Power Meter
MZI	Mach-Zehnder Interferometer
MBC	Modulator Bias Controller

Appendix B – Bibliography

[1] A. Poppe, M. Peev, and M. Stierle, “New free-running, low noise 1550nm single photon detector for commercial applications: QCMC - 11th International Conference on Quantum Communication, Measurement and Computing,” in *QCMC - 11th International Conference on Quantum Communication, Measurement and Computing*, G. Humer, Ed., 2012, p. 305.

[2] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, “Finite-key analysis for the 1-decoy state QKD protocol,” *Appl. Phys. Lett.*, vol. 112, no. 17, p. 171104, Apr. 2018, doi: 10.1063/1.5023340.