

# Quantum Key Distribution over 100 km underwater optical fiber assisted by a Fast-Gated Single-Photon Detector

Domenico Ribezzo,<sup>1,2</sup> Mujtaba Zahidy,<sup>3</sup> Gianmarco Lemmi,<sup>1,2</sup> Antoine Petitjean,<sup>1</sup> Claudia De Lazzari,<sup>4</sup> Ilaria Vagniluca,<sup>4</sup> Enrico Conca,<sup>5</sup> Alberto Tosi,<sup>5</sup> Tommaso Occhipinti,<sup>4</sup> Leif K. Oxenløwe,<sup>6</sup> André Xuereb,<sup>7,8</sup> Davide Bacco,<sup>9,4,\*</sup> and Alessandro Zavatta<sup>1,4,†</sup>

<sup>1</sup>*Istituto Nazionale di Ottica del Consiglio Nazionale delle Ricerche (CNR-INO), 50125 Firenze, Italy*

<sup>2</sup>*Università degli Studi di Napoli Federico II, Napoli, Italy*

<sup>3</sup>*Centre of Excellence for Silicon Photonics for Optical Communications (SPOC),*

*Department of Electrical and Photonics Engineering, Technical University of Denmark, Kgs. Lyngby, Denmark*

<sup>4</sup>*QTI S.r.l., 50125, Firenze, Italy*

<sup>5</sup>*Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, 20133 Milano, Italy*

<sup>6</sup>*Center for Silicon Photonics for Optical Communication (SPOC),*

*Department of Photonics Engineering, Technical University of Denmark, Kgs. Lyngby, Denmark*

<sup>7</sup>*Department of Physics, University of Malta, Msida MSD 2080, Malta*

<sup>8</sup>*Mercury Cybersecurity Limited, Malta*

<sup>9</sup>*Department of Physics and Astronomy, University of Florence, 50019 Sesto Fiorentino, Italy*

Nowadays Quantum Key Distribution represents the most mature quantum technology, and multiple countries as well as private institutions are building their quantum network. However, QKD devices are still far from representing a product within everyone's reach. Indeed, limitations in terms of compatibility with existing telecom infrastructure and limited performances in terms of secret key rate, using non-cryogenic detection systems, are still critical. In this work, we implemented a quantum key distribution link between Sicily (Italy) and Malta utilizing two different Single-Photon Avalanche Diode (SPAD) detectors. The performances of a standard commercial SPAD have been compared with the results achieved with a new prototype of fast-gated System in a Package (SiP) SPAD; the SiP detector has shown to be able to accomplish a fourteen times higher key rate compared with the commercial device over the channel showing 20 dB of losses.

## I. INTRODUCTION

Quantum Key Distribution (QKD), a method for exchanging symmetric cryptographic keys exploiting the laws of physics, is the most mature technology among the ones that appeared within the second quantum revolution [1–4]. Several experiments, both in physics laboratories and in field trial links, have shown QKD potential and readiness. Today, QKD links connecting cities among different continents are already a reality [5, 6] and are employed in commercial applications as well as in governments. Nevertheless, many challenges still need to be faced in order to make QKD an everyday consumer technology. An important and very pragmatic example is the necessity to build QKD devices that are portable, scalable, and can guarantee a high key generation rate in long-distance links. In fact, today the current record in terms of key generation rate over a long-distance link has been achieved using Superconducting Nanowires Single-Photon Detectors (SNSPDs) [5–8], which present ultra-low dark count rates and high quantum efficiencies. The main drawback of this technology is its ultra-low operational temperature (below 4 K) which makes it difficult to integrate into deployable systems.

On the contrary, Single-Photon Avalanche Diodes (SPADs) working at room-temperature or at temperatures achievable with a compact cooling system offer high integrability in current telecommunication networks.

In this work, we realized a QKD link in the middle of the Mediterranean Sea, connecting Italy to Malta through a 100 km fiber-based underwater optical channel. The transmitter was located in a telecom center in the city of Pozzallo (Sicily, Italy), while the receiver was placed in the Melita Limited data center of Madliena (Malta). This link, which can be considered a new step in the frame of a European Quantum Network [9], has been used to test a System in a Package (SiP) Indium Gallium Arsenide (InGaAs) SPAD [10]. This detector features a dedicated fast-gated active quenching circuit that allows it to synchronize with a gate signal locked to the quantum states generation clock [11]. As a result, it is considerably less affected by dark counts and afterpulses. Moreover, we compared the SiP detector with a standard commercial InGaAs SPAD (ID221 by IDQuantique [12]). The new SPAD achieved a fourteen times higher key rate over the 20 dB-attenuation link with respect to the commercial device. We also investigated the behavior of the detector emulating a shorter link budget, showing that the SiP SPAD guarantees a high secret key rate up to 25 kbit/s at 3 dB channel loss.

Finally, we report a comparison of the detectors' performances in controlled laboratory conditions. We added to the comparison a second SiP detector, similar to the first one but with a larger sensor area, intended for free space applications.

## II. QKD PROTOCOL

The implemented protocol is the three-states efficient BB84 with time-bin encoding and one decoy method [13–16]. In this protocol, one basis is used for sharing the key, while the

\* [davide.bacco@unifi.it](mailto:davide.bacco@unifi.it)

† [alessandro.zavatta@ino.cnr.it](mailto:alessandro.zavatta@ino.cnr.it)

second basis is reserved for security checks. This choice allows to simplify the setup and to generate only one of the two eigenstates of the second mutually unbiased basis. The key generation basis is the computational  $\mathbf{Z}$ -basis, whose eigenstates, according to the time-bin encoding, are characterized by the emission time of a pulse into a time slot frame. The eigenstates of the security check basis,  $\mathbf{X}$ -basis, are formed by the superposition of the  $\mathbf{Z}$ -basis with a relative phase (0 or  $\pi$ ). It is worth pointing out that, even if the photon wave function is spread over two pulses, each state is supposed to contain no more than one photon; states with more photons (i.e. multi-photon states) introduce security issues and should be avoided. Unfortunately, multi-photon events cannot be totally suppressed, therefore, the decoy-state method has been introduced to overcome the vulnerabilities deriving from the lack of a real single-photon source [17, 18]. In this method, randomly switching intensity levels helps to detect an eavesdropper that intercepts and re-sends only multi-photon states and blocks the rest and hence, cannot keep the photon number statistics stable. It has been proven that two different intensity levels are enough [14], a technique that is known as the one-decoy method.

For one-decoy 3-state BB84 protocol, in the finite-key regime, the key length  $l$  is bound to [13]:

$$l \leq s_{Z,0}^l + s_{Z,1}^l (1 - H_2(\phi_Z^u)) - \lambda_{EC} - 6 \log_2 \left( \frac{19}{\epsilon_{sec}} \right) - \log_2 \left( \frac{2}{\epsilon_{corr}} \right), \quad (1)$$

with  $s_{Z,0}^l$  and  $s_{Z,1}^l$  being the lower bounds for the vacuum and the single-photon events,  $\phi_Z^u$  the upper bound of the phase error rate,  $\lambda_{EC}$  the number of disclosed bits in the error correction stage,  $H_2(x) = -x \log_2(x) - (1-x) \log_2(1-x)$  the binary entropy and  $\epsilon_{sec} = 10^{-12}$  and  $\epsilon_{corr} = 10^{-12}$  the secrecy and correctness parameters. The  $\epsilon$  parameters are defined as [19]:

$$\begin{aligned} P[S_A \neq S_B] &< \epsilon_{corr}, \\ \mathbb{1}(S_A, S_B; Z, C) &< \epsilon_{sec}, \end{aligned}$$

where  $S_A$  and  $S_B$  are Alice' and Bob's sifted keys,  $P[x]$  the probability of  $x$ ,  $\mathbb{1}(\cdot)$  a generic information measure,  $Z$  is the eavesdropped sequence owned by a potential eavesdropper, and  $C$  is a random variable representing the exchanged information. The second term denotes the probability  $\epsilon_{sec}$  of having a stronger correlation between Alice's and Eve's strings than Alice's and Bob's ones. In the standard BB84, the phase error rate in the  $\mathbf{Z}$ -basis  $\phi_Z$  corresponds to the bit error rate in the  $\mathbf{X}$ -basis  $\delta_X$ , however, since in this protocol Alice sends only one state in the  $\mathbf{X}$ -basis,  $\phi_Z$  cannot be directly measured and it needs to be estimated from the  $\mathbf{X}$ -basis quantum bit error rate  $\text{QBER}_X$  [20]; it is connected to the visibility  $\text{vis}_X$  of the receiver interferometer by  $\text{QBER}_X = (1 - \text{vis}_X)/2$ .

### III. EXPERIMENTAL SETUP

#### A. Network architecture and QKD devices

The link is made by two 96 km long optical fibers deployed under the Mediterranean Sea and connecting Malta to Sicily;

the same channel has already been employed for a demonstration of entanglement distribution in 2018 [21]. The fibers show an attenuation of around 20 and 21 dB, hence, we reserved the former for distributing the quantum states while the latter was used as a service channel (distribution of a synchronization signal, parameters estimation, etc.).

The experimental setup is illustrated in Fig. 1; the pulses encoding the states are generated by carving a continuous wave C-band laser with an intensity modulator controlled by a field programmable gate array (FPGA); after the carving stage, the pulses are attenuated down to single-photon level by a variable optical attenuator (VOA). More details about the transmitter device are reported in [22]. The SiP SPAD can accept a gate trigger signal where the subsequent gating time (the ON and OFF times) of the detector can be set by the user.

The qubit generation rate has been fixed to 119 MHz for both detectors to acquire comparable data. However, the detector can accept up to a 150 MHz gate signal.

Alice and Bob select equal probabilities to generate and measure in the computational basis ( $\mathbf{Z}$ -basis),  $P_{ZA} = P_{ZB} = 0.5$ ; such choices for  $P_{ZA}$  and  $P_{ZB}$  are in accordance with a simulation model that takes into account the channel properties and the detection stage performances.

On the service channel, two classical signals are shared between the two parts: a synchronization signal at 145 kHz and another signal at 119 MHz that is used as the gate signal for the detector. The mean numbers of photons per pulse are chosen such that they maximize the key rate in our simulation model, and are reported in tab. II.

After traveling through the underwater fiber channel, the photons arrive at the receiver setup; there they impinge on a 50:50 beam splitter, which acts as a passive basis choice. The  $\mathbf{Z}$ -basis output brings the photons directly to one Single-Photon Detector (SPD), while the  $\mathbf{X}$ -basis output lets the photons pass through a delay line interferometer (DLI) before reaching the detection part. The DLI is a Mach-Zehnder interferometer with one arm 800 ps longer than the other, so that the two pulses characterizing the wave-function states in the  $\mathbf{X}$ -basis overlap and their relative phase can be measured. The interferometer is stabilized by a phase-lock loop (PLL) which adjusts a phase shifter to compensate for phase fluctuations. The feedback for the loop is provided by sending a weak classical laser, counter-propagating with respect to the quantum signal, and monitoring its phase fluctuation. Finally, the synchronization and the gate signals traveling in the service channel are demultiplexed and sent to the corresponding modules.

#### B. Detecting stage

The employed research-product SiP detector is a state-of-the-art InGaAs/InP SPAD developed at Politecnico di Milano (PoliMi) and designed to operate with low dark count rate, competitive photon detection efficiency, and contained timing jitter. The primary feature of this detector is its time-gating capability. A conventional gated circuits often uses a simple passive quenching circuit, which cannot be gated at high

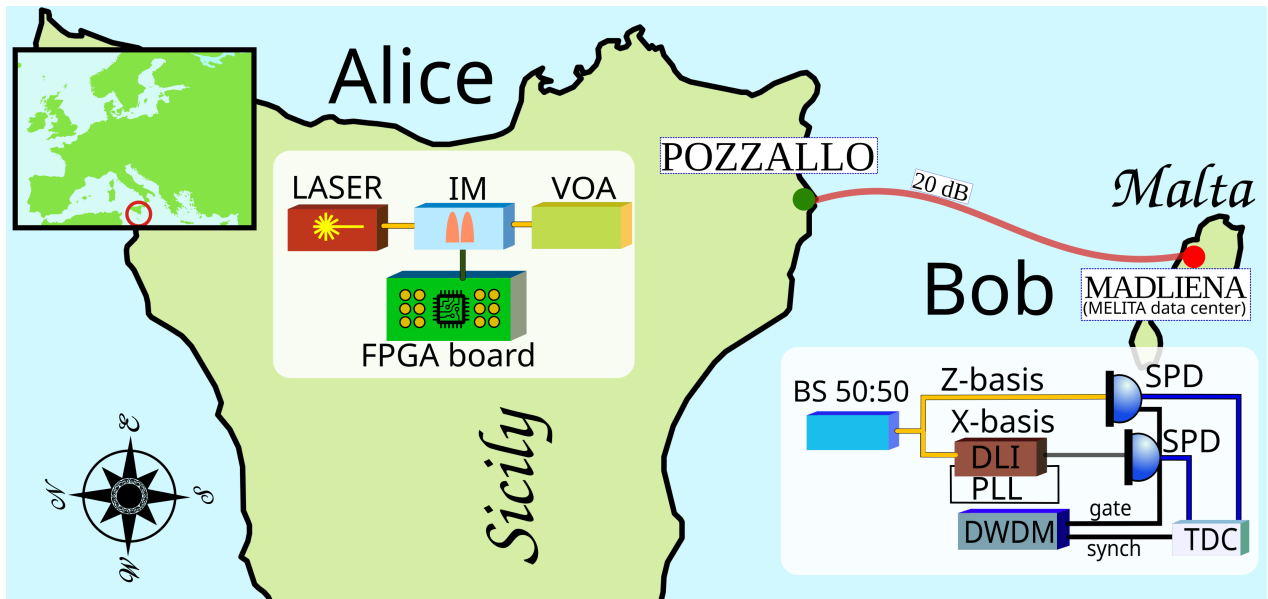


Figure 1. **Sketch of the setup.** Alice produces the states by carving (intensity modulator stage - IM) and attenuating (variable optical attenuation stage - VOA) a continuous wave laser. Bob makes the basis choice with a beam splitter (BS 50:50), then directly reads the arrival time of the photons (Z-basis) or makes an interferometric measurement with a delay line interferometer (DLI) for the X-basis. A second fiber is used to share a synchronization and a gate signal, multiplexed and then divided again by a dense wavelength division multiplexer (DWDM). The single-photon detectors are connected to a time-to-digit converter (TDC) that produces the timestamps to be elaborated by Bob's computer.

	SiP PoliMi	ID221
$\tau_{off}$ ( $\mu$ s)	1	20
$r_{DC}$ (kHz)	10.8	2.5
$n_Z$	$10^9$	
$p_{Z,A}$	50%	
$p_{Z,B}$	50%	
$\nu_{rep}$ (MHz)	119	
$\epsilon_{sec}$	$10^{-12}$	
$\epsilon_{corr}$	$10^{-12}$	
$\tau_Z$ (dB)	1	
$\tau_X$ (dB)	3	

Table I. **Setup parameters.**  $\tau_{off}$  is the hold-off time of the detectors,  $r_{DC}$  the dark count rate,  $n_Z$  is the block size,  $p_{Z,A}$  and  $p_{Z,B}$  the probabilities of choosing the Z basis for Alice and Bob respectively,  $\nu_{rep}$  is the repetition rate,  $\epsilon_{sec}$  and  $\epsilon_{corr}$  are the security and correctness parameters,  $\tau_Z$  and  $\tau_X$  are the losses of Bob for the Z and X basis. SiP PoliMi detector is the SiP detector with  $10 \mu\text{m}$  diameter sensitive area.

frequency and requires a long dead time to limit the afterpulsing effect (APE). APE happens when carriers generated in an avalanche are trapped, and after a certain time (up to a few microseconds for InGaAs/InP SPADs operating at 220 - 240 K), are randomly released, resulting in a secondary avalanche without any real photon impinging on the SPAD. By implementing a fast active quenching circuit in place of a simple passive one, the after-pulses are strongly reduced. The tested detector implements a newly developed circuit able to fast-gate the detector at frequencies up to 150 MHz, with ON-time as short as few hundreds of picoseconds. When a photon is detected, this circuit enforces a hold-off time to the SPAD by

skipping a programmable number of gate periods, resulting in a suppression of the after-pulses impact [11]. The photo-sensitive area of the SPAD has a diameter of around  $10 \mu\text{m}$ , making it the perfect choice for fiber-based applications. A second detector with identical characteristics except for a bigger sensitive area ( $25 \mu\text{m}$ ) has been tested utilizing the same optical setup. The paper [23] reports a detailed description of the detector and an accurate characterization of its specifications in laboratory conditions.

## IV. RESULTS

### A. Field trial

The described setup has been utilized for establishing a QKD protocol from Sicily to Malta. We performed the experiment and data acquisition with both the ID221 detector from IDQuantique and the described SiP PoliMi SPAD. For the ID221, a hold-off time of  $\tau_{off} = 20 \mu\text{s}$  has been set in order to keep the after-pulses within manageable values. The hold-off feature keeps the SPAD turned off for  $\tau_{off}$  after each detection event to empty the active area from possibly trapped carriers. For the fast-gated detector, we have been able to set  $\tau_{off} = 1 \mu\text{s}$  thanks to the limited after-pulse probability.

With the hold-off time set to  $1 \mu\text{s}$ , the SiP PoliMi detector shows a higher dark count rate compared to the commercial SPAD (10.8 kHz vs 2.5 KHz). However, the maximum count rate  $CR_{max} = 1/\tau_{off}$  allows to detect a higher rate of events than the commercial SPAD. It should be noted that a high  $\tau_{off}$  also limits the SPAD performance by reducing its saturation

	3 dB	5 dB	10 dB	15 dB	20 dB
SPAD by Polimi					
$\mu_1$	0.36	0.41	0.46	0.46	0.41
$\mu_2$	0.16	0.16	0.16	0.16	0.16
$\mu_3$	0				
$\varepsilon_Z$ (%)	0.7	0.8	1.1	1.8	4.6
$\varepsilon_X$ (%)	2.8	3.0	3.1	3.4	6.4
SKR (kbps)	24.65	21.75	13.10	5.80	1.50
ID221 SPAD					
$\mu_1$	0.21	0.31	0.31	0.36	0.41
$\mu_2$	0.06	0.11	0.11	0.16	0.16
$\mu_3$	0				
5ttt $\varepsilon_Z$ (%)	4.4	4.4	5.0	6.0	9.3
$\varepsilon_X$ (%)	4	2.9	3.2	4.0	7.2
SKR (kbps)	3.25	3.05	2.10	1.05	0.11

Table II. **Chosen parameters and measured values:**  $\mu_1$ ,  $\mu_2$  and  $\mu_3$  are the numbers of photons per pulse according to the decoy method,  $\varepsilon_Z$  and  $\varepsilon_X$  are the qubit error rate in the two bases and finally, SKR is the secure key rate. The probabilities of choosing each  $\mu$  have been chosen such that it maximizes the key rate.

threshold, resulting in lower detection efficiency. The low  $\tau_{\text{off}}$  setting allows for avoiding such conditions in the SiP PoliMi detector.

In comparison, ID221 shows a dark count rate of around 200 kHz for  $\tau_{\text{off}} = 1\mu\text{s}$ . A specially designed quenching circuit that manages the fast-gate signal allows considerably improved performances for the SiP PoliMi SPAD at low  $\tau_{\text{off}}$ .

Successively, to evaluate the performance of the detector at different channel losses, we repeat the experiment on shorter segments of the channel. To simulate that, we gradually compensated for the losses encountered by photons traveling at different channel lengths by increasing the input power. This is equivalent to placing Alice's transmitter in the corresponding loss-compensated location on the link.

The achieved key rates are reported in Tab. II and are shown in Fig. 2.

## B. Laboratory test

The detector has successively been tested in controlled laboratory conditions. The second SiP detector with a sensitive area diameter of 25  $\mu\text{m}$  has been added to the comparison. Since a bigger sensitive area entails a higher dark count rate, a hold-off time of 10  $\mu\text{s}$  has been preferred for this detector. We performed the test for different channel losses introduced by a tunable attenuator between Alice's and Bob's setups. The results are reported in Tab. III and Fig. 3. The second SiP PoliMi detector does not show a significant improvement over the commercial SPAD. We observed a small-scale increase in SKR up to 15 dB of channel loss, however, due to excess noise and low signal-to-noise ratio (SNR), SKR falls to zero at higher channel losses. Finally, the SiP detector with the smaller active area (10  $\mu\text{m}$  diameter) was tested under different excess bias voltages. While increasing excess bias improves the detector's efficiency, it also increases the afterpulsing effect and the dark count rate. The test results show

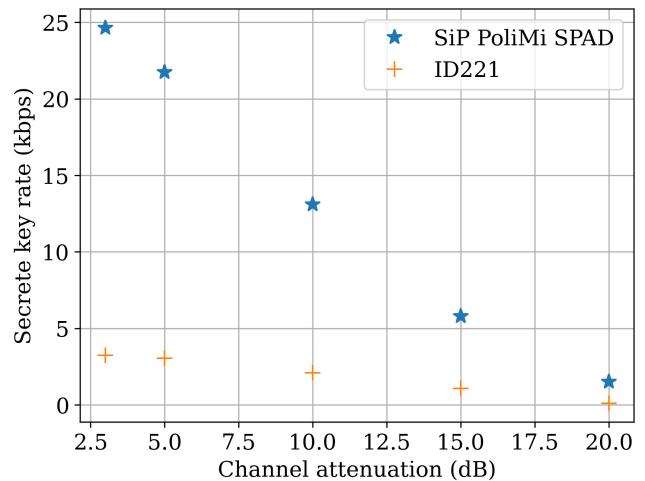


Figure 2. **Key rate results (field trial).** The plot shows the secure key rates achieved by the commercial detector (ID221) and the tested SiP detector fabricated by the research group of Politecnico di Milano (SiP PoliMi SPAD). Thanks to the fast-quenching circuit applying the gate signal, the SiP PoliMi SPAD outperforms the commercial device by a factor of seven in terms of key rate for small attenuation link, and up to fourteen times when the entire channel is considered (20 dB).

an improvement in low channel losses, while the performance dropped with excess bias voltage increase due to the reduction of SNR.

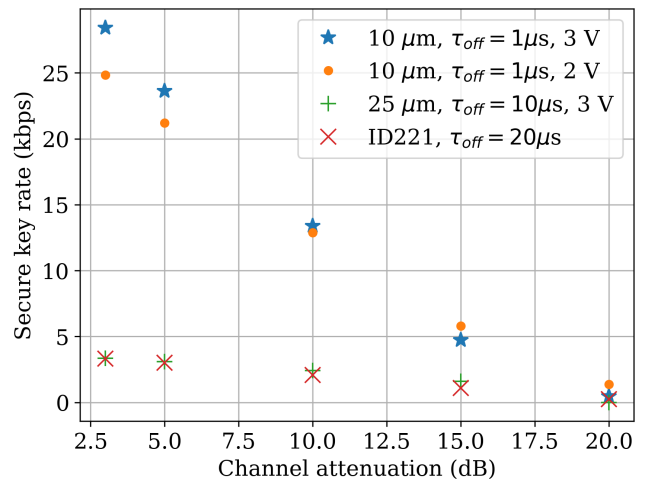


Figure 3. Secure key rate extracted in laboratory conditions with the different detectors for different channel attenuation values. 10  $\mu\text{m}$  and 25  $\mu\text{m}$  are the two SiP PoliMi SPAD and the value is referred to the relative photosensitive active area diameter. The selected detector settings are reported in the legend (hold-off time, excess bias voltage).

3 dB	5 dB	10 dB	15 dB	20 dB
10 $\mu\text{m}$ SPAD, 1 $\mu\text{s}$ , 2V (kbps)				
24.83	21.19	12.89	5.80	1.38
10 $\mu\text{m}$ SPAD, 1 $\mu\text{s}$ , 3V (kbps)				
28.42	23.62	13.39	4.72	0.47
25 $\mu\text{m}$ SPAD, 10 $\mu\text{s}$ , 3V (kbps)				
3.34	3.10	2.42	1.61	0
IDQ, 20 $\mu\text{s}$ , 20% eff. (kbps)				
3.32	3.00	2.07	1.10	0.15

Table III. Secure key rate extracted with the two SiP PoliMi detectors in laboratory conditions. The detector with 10  $\mu\text{m}$  sensitive area has been set with a hold-off time of 1  $\mu\text{s}$  and has been tested for 2V and 3V of excess bias. For the detector with a sensor area of 25  $\mu\text{m}$ , the set parameters are 10  $\mu\text{s}$  of hold-off time and 3V of excess bias. The ID221 has been kept on 20  $\mu\text{s}$  of hold-off time and 20% of detection efficiency.

## V. DISCUSSION

Boosting the key rate on long-distance links is the priority for the widespread deployment of QKD technology. Many new protocols are being experimented and are showing their potentialities: twin field QKD [24] and high dimensional protocols [25–29] are just few examples that go in this direction. Simultaneously, with the appearance of SNSPDs [30, 31] and photon number resolving detectors [32, 33] much attention has been paid to the detection stage. Although InGaAs/InP SPADs established their place as the most common technology for single-photons detection in C-band because of their portability and cost-effectiveness, compared to newer technologies, they present limited performance in terms of quantum efficiency, dead-time, and timing jitter. In addition, they are considerably more affected by dark counts and afterpulsing phenomenon.

In this paper, we enabled quantum communications between two European countries. Although several works already demonstrated a limited European quantum network, a full-scale deployment faces many open challenges regarding range, cost, etc [22]. This work, introducing a more cost-effective approach, represents an additional step toward a European quantum infrastructure.

We demonstrated that in a real QKD scenario, without an important technological replacement and only improving the detection stage, an improvement of up to a factor of 14 in

terms of key rate is achievable thanks to an advanced sensor design and an active quenching circuit implementation.

The advanced innovative built-in quenching circuit together with the adaptive gating technique allows for increasing the detection rate as well as reducing the effect of afterpulsing by minimizing the ON time of the detector to the expected optical pulse width. Thanks to the fast quenching, a gating of up to 150 MHz is achievable, which contributes to the final key rate in significant amounts. In comparison, in the old technology, a long hold-off time was necessary to overcome the effect of afterpulsing, which in turn reduces the detection rate. Besides, the two SiP SPADs have been engineered and designed in order to show state-of-the-art performances in terms of intrinsic dark counts, timing jitter, and detection efficiency.

This work also provides a comparison of performance with the sensitive area dimensions. The second SiP PoliMi detector featuring a 25  $\mu\text{m}$  diameter active area and similar circuitry shows greater susceptibility to dark counts and afterpulsing. In comparison, the new detector produces results slightly better than the commercial detector. It should be noted that the 25  $\mu\text{m}$  detector has been designed and intended for free-space applications where a larger sensitive area is desirable.

Our demonstration proves the effectiveness of the newly introduced detector technology in reducing cost per secure bit and increasing the final key generation rate, and will help to make QKD a more user-accessible technology.

## VI. ACKNOWLEDGEMENTS

This work was partially supported by the Center of Excellence SPOC (ref DNR123), Innovations fonden project Fire-Q (No. 9090-00031B), the NATO Science for Peace and Security program (Grant No. G5485, project SEQUEL), the programme Rita Levi Montalcini QOMUNE (PGR19GKW5T), the EraNET Cofund Initiatives QuantERA within the European Union’s Horizon 2020 research and innovation program grant agreement No.731473 (project SQUARE), the Project EQUO (European QUantum ecOsystems) which is funded by the European Commission in the Digital Europe Programme under the grant agreement No 101091561, the Project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU and the Project QuONTENT under the “Progetti di Ricerca@CNR” program funded by the Consiglio Nazionale delle Ricerche (CNR).

- 
- [1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theoretical Computer Science* **560**, 7 (2014), theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.
  - [2] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, *Nature Photonics* **8**, 595 (2014).
  - [3] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, *Rev. Mod. Phys.* **92**, 025002 (2020).
  - [4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, *Rev. Mod. Phys.* **81**, 1301 (2009).
  - [5] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, Satellite-to-

- ground quantum key distribution, *Nature* **549**, 43 (2017).
- [6] C.-Y. Lu, Y. Cao, C.-Z. Peng, and J.-W. Pan, Micius quantum experiments in space, *Rev. Mod. Phys.* **94**, 035001 (2022).
- [7] B. D. Lio, D. Bacco, D. Cozzolino, F. D. Ros, X. Guo, Y. Ding, Y. Sasaki, K. Aikawa, S. Miki, H. Terai, T. Yamashita, J. S. Neergaard-Nielsen, M. Galili, K. Rottwitt, U. L. Andersen, L. K. Oxenløwe, and T. Morioka, Record-high secret key rate for joint classical and quantum transmission over a 37-core fiber, in *2018 IEEE Photonics Conference (IPC)* (2018) pp. 1–2.
- [8] S. P. Neumann, A. Buchner, L. Bulla, M. Bohmann, and R. Ursin, Continuous entanglement distribution over a transnational 248 km fiber link, *Nature Communications* **13**, 6134 (2022).
- [9] EuroQCI, European quantum communication infrastructure (euroqci) initiative (2017), <https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci>.
- [10] F. Signorelli, F. Telesca, E. Conca, A. D. Frera, A. Ruggeri, A. Giudice, and A. Tosi, Low-noise ingaas/inp single-photon avalanche diodes for fiber-based and free-space applications, *IEEE Journal of Selected Topics in Quantum Electronics* **28**, 1 (2022).
- [11] A. Ruggeri, P. Ciccarella, F. Villa, F. Zappa, and A. Tosi, Integrated circuit for subnanosecond gating of ingaas/inp spad, *IEEE Journal of Quantum Electronics* **51**, 1 (2015).
- [12] IDQuantique, Id221 infrared single-photon detector, <https://www.idquantique.com/resources/id221/>.
- [13] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussi eres, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Secure quantum key distribution over 421 km of optical fiber, *Phys. Rev. Lett.* **121**, 190502 (2018).
- [14] D. Rusca, A. Boaron, F. Gr unenfelder, A. Martin, and H. Zbinden, Finite-key analysis for the 1-decoy state qkd protocol, *Applied Physics Letters* **112**, 171104 (2018), <https://doi.org/10.1063/1.5023340>.
- [15] D. Rusca, A. Boaron, M. Curty, A. Martin, and H. Zbinden, Security proof for a simplified bennett-brassard 1984 quantum-key-distribution protocol, *Phys. Rev. A* **98**, 052336 (2018).
- [16] M. Hayashi and R. Nakayama, Security analysis of the decoy method with the bennett-brassard 1984 protocol for finite key lengths, *New Journal of Physics* **16**, 063009 (2014).
- [17] W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, *Phys. Rev. Lett.* **91**, 057901 (2003).
- [18] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [19] M. Canale, *Classical processing algorithms for Quantum Information Security*, Ph.D. thesis, Department of Information Engineering, University of Padova (2014).
- [20] A. Boaron, B. Korzh, R. Houlmann, G. Boso, C. C. W. Lim, A. Martin, and H. Zbinden, Detector-device-independent quantum key distribution: Security analysis and fast implementation, *Journal of Applied Physics* **120**, 063101 (2016).
- [21] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. H ubel, and R. Ursin, An entanglement-based wavelength-multiplexed quantum communication network, *Nature* **564**, 225 (2018).
- [22] D. Ribezzo, M. Zahidy, I. Vagniluca, N. Biagi, S. Francesconi, T. Occhipinti, L. K. Oxenløwe, M. Lon ari c, I. Cviti c, M. Stip evi c, Z. Pu avec, R. Kaltenbaek, A. Ram sak, F. Cesa, G. Giorgetti, F. Scazza, A. Bassi, P. De Natale, F. S. Cataliotti, M. Inguscio, D. Bacco, and A. Zavatta, Deploying an inter-european quantum network, *Advanced Quantum Technologies* **n/a**, 2200061 (2022).
- [23] A. Tosi, F. Acerbi, M. Anti, and F. Zappa, Ingaas/inp single-photon avalanche diode with reduced afterpulsing and sharp timing response with 30 ps tail, *IEEE Journal of quantum electronics* **48**, 1227 (2012).
- [24] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, *Nature* **557**, 400 (2018).
- [25] H. Bechmann-Pasquinucci and W. Tittel, Quantum cryptography using larger alphabets, *Phys. Rev. A* **61**, 062308 (2000).
- [26] I. Vagniluca, B. Da Lio, D. Rusca, D. Cozzolino, Y. Ding, H. Zbinden, A. Zavatta, L. K. Oxenløwe, and D. Bacco, Efficient time-bin encoding for practical high-dimensional quantum key distribution, *Phys. Rev. Appl.* **14**, 014051 (2020).
- [27] M. Zahidy, D. Ribezzo, C. D. Lazzari, I. Vagniluca, N. Biagi, T. Occhipinti, L. K. Oxenløwe, M. Galili, T. Hayashi, C. Antonelli, A. Mecozzi, A. Zavatta, and D. Bacco, 4-dimensional quantum key distribution protocol over 52-km deployed multicore fibre, in *European Conference on Optical Communication (ECOC) 2022* (Optica Publishing Group, 2022) p. Th3C.6.
- [28] B. Da Lio, D. Cozzolino, N. Biagi, Y. Ding, K. Rottwitt, A. Zavatta, D. Bacco, and L. K. Oxenløwe, Path-encoded high-dimensional quantum communication over a 2-km multicore fiber, *npj Quantum Information* **7**, 63 (2021).
- [29] D. Bacco, N. Biagi, I. Vagniluca, T. Hayashi, A. Mecozzi, C. Antonelli, L. K. Oxenløwe, and A. Zavatta, Characterization and stability measurement of deployed multicore fibers for quantum applications, *Photon. Res.* **9**, 1992 (2021).
- [30] C. M. Natarajan, M. G. Tanner, and R. H. Hadfield, Superconducting nanowire single-photon detectors: physics and applications, *Superconductor Science and Technology* **25**, 063001 (2012).
- [31] E. A. Dauler, M. E. Grein, A. J. Kerman, F. Marsili, S. Miki, S. W. Nam, M. D. Shaw, H. Terai, V. B. Verma, and T. Yamashita, Review of superconducting nanowire single-photon detector system design options and demonstrated performance, *Optical Engineering* **53**, 081907 (2014).
- [32] A. Divochiy, F. Marsili, D. Bitauld, A. Gaggero, R. Leoni, F. Mattioli, A. Korneev, V. Seleznev, N. Kurova, O. Minaeva, G. Gol’tsman, K. G. Lagoudakis, M. Benkhaoul, F. L evy, and A. Fiore, Superconducting nanowire photon-number-resolving detector at telecommunication wavelengths, *Nature Photonics* **2**, 302 (2008).
- [33] J. Provazn k, L. Lachman, R. Filip, and P. Marek, Benchmarking photon number resolving detectors, *Opt. Express* **28**, 14839 (2020).