

# Quantum key distribution over 100 km of 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> Iliaria 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), Firenze 50125, 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., Firenze 50125, Italy*


<sup>5</sup>*Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, Milano 20133, 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, Sesto Fiorentino 50019, Italy*

 (Received 3 March 2023; revised 27 June 2023; accepted 20 September 2023; published 19 October 2023)

Nowadays quantum key distribution (QKD) 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 noncryogenic 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 an alternative prototype of fast-gated system in a package (SIP) SPAD; the SIP detector has shown to be able to accomplish a 14 times higher key rate compared with the commercial device over the channel showing 20 dB of losses.

DOI: [10.1103/PhysRevApplied.20.044052](https://doi.org/10.1103/PhysRevApplied.20.044052)

## 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 [1–5]. 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 [6,7] and are employed in commercial applications as well as in governments. Many alternative protocols have been developed as well, allowing optical fiber-based QKD to achieve rates exceeding hundreds of MHz [8] and a record-breaking distance of up to 830 km [9]. Nevertheless, many challenges still need to be faced in order to make QKD an

everyday consumer technology. A useful 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. Indeed, today the current record in terms of key generation rate over a long-distance link has been achieved using superconducting nanowire single-photon detectors (SNSPDs) [6,7,10,11], which present ultralow dark-count rates and high quantum efficiencies. The main drawback of this technology is its ultralow operational temperature (below 4 K), which makes it difficult to integrate into deployable systems.

In contrast, 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 and have been proved to show impressive performances while remaining safe against coherent attacks [12].

However, SPADs are affected by the after-pulsing effect (APE), which leads to false extra detections within a

\*davide.bacco@unifi.it

†alessandro.zavatta@ino.cnr.it

certain time interval following a real photon detection. When the SPAD is employed in free-running mode, APE makes it necessary to keep the device inactive after each detection event (hold-off time). A long hold-off time reduces the maximum count rate of the detector. Therefore, InGaAs/InP SPADs, which are employed in fiber communications, are often operated in gated mode. Shortening the gate duration ensures lower dark count rates, whereas extending the time intervals between consecutive gates decreases the after-pulse events. Two recently introduced techniques act on suppressing APE by strongly decreasing the gate duration (to few hundreds of picoseconds), which subsequently reduces the avalanche charges. However, distinguishing tiny avalanche pulses from background noise is challenging, so the primary objective of these techniques is to enhance the signal-to-noise ratio. The sine gating (SG) method employs sine waves as gate signals and band-stop filters (BSFs), or other cancellation techniques, to eliminate the background noise due to gate feed through [13–15]. The self-differencing (SD) technique utilizes square-wave gate signals and a differencing circuit to subtract the output signals during two consecutive periods, enabling the detection of the weak avalanche signal [16]. Furthermore, several variations of these approaches have also been proposed [17,18], each with its own advantages and disadvantages. Unfortunately, the filters required for sinusoidal-wave gating distort the waveform of the avalanche [19]. On the other hand, the self-differencing technique, which allows the use of arbitrary waveforms, has the not-trivial constraint that the attenuation and dispersion of two delay lines remain constant across the entire detection bandwidth [20].

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 another step in the frame of a European Quantum Network [21], has been used to test a system in a package (SIP), including an InGaAs/InP SPAD [22]. This detector (hereafter called SIP SPAD) features an integrated fast-gated active quenching circuit that allows it to synchronize with a gate signal locked to the quantum state generation clock [23]. Thanks to the capability to generate short gates (even few hundreds of picoseconds), it is considerably less affected by dark counts and afterpulsing compared to many commercially available InGaAs/InP SPAD modules, whose minimum gate duration is longer. Simultaneously, by not relying on SG or SD techniques, it is not affected by the issues connected to those systems. In detail, the SIP SPAD detector is a much simpler system, since the SPAD gating and avalanche detection are performed by a small ASIC. Therefore, we believe that, even if it operates at lower repetition rate and shows

performances that are lower than GHz-gated systems, it is still an interesting approach to evaluate for large-scale QKD systems, since the disadvantages are counter-weighted by the simplicity and lower per-unit cost. We also compared the SIP SPAD with a standard commercial InGaAs/InP SPAD module (ID221 by ID Quantique [24]). The alternative SPAD system achieved a 14 times higher key rate with respect to the commercial device over the entire link, whose attenuation is 20 dB. We also investigated the behavior of the detector emulating a shorter link, 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 SPAD, 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-state efficient BB84 with time-bin encoding and one decoy method [25–28]. In this protocol, one basis is used for sharing the key, while the 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  $Z$  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,  $X$  basis, are formed by the superposition of the  $Z$  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., multiphoton states) introduce security issues and should be avoided. Unfortunately, multiphoton 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 [29,30]. In this method, randomly switching intensity levels helps to detect an eavesdropper that intercepts and resends only multiphoton 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 [26], a technique that is known as the one-decoy method.

For one-decoy three-state BB84 protocol, in the finite-key regime, the key length  $l$  is bound to [25]

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

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 [31]

$$P[S_A \neq S_B] < \epsilon_{corr},$$

$$\mathbb{1}(S_A, S_B; Z, C) < \epsilon_{sec},$$

where  $S_A$  and  $S_B$  are Alice’s 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  $Z$  basis  $\phi_Z$  corresponds to the bit error rate in the  $X$  basis  $\delta_X$ , however, since in this protocol Alice sends only one state in the  $X$  basis,  $\phi_Z$  cannot be directly measured and it needs to be estimated from the  $X$  basis quantum bit error rate  $QBER_X$  [32]; it is connected to the visibility  $vis_X$  of the receiver interferometer by  $QBER_X = (1 - vis_X)/2$ .

### 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 [33]. 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, while Table I reports some important setup parameters. 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 Ref. [34]. 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 SIP SPAD detector can accept up to a 150-MHz gate signal.

Alice and Bob select equal probabilities to generate and measure in the computational basis ( $Z$  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

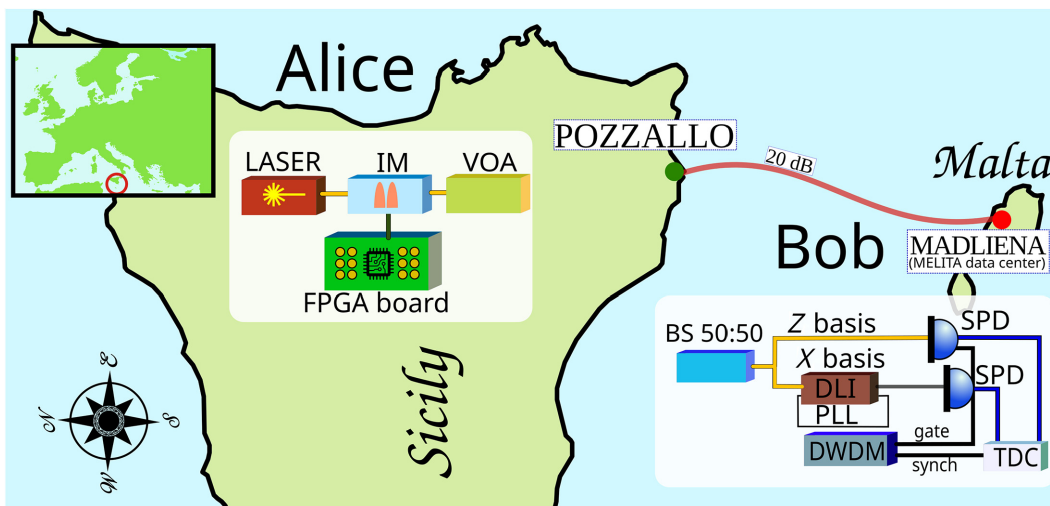


FIG. 1. Sketch of the setup. Alice produces the states by carving (intensity modulator stage, IM) and attenuating (variable optical attenuation stage, VOA) a continuous-wave laser. Bob makes the basis choice with a beam splitter (BS 50:50), then directly reads the arrival time of the photons ( $Z$  basis) 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.

TABLE I. Setup parameters.  $\tau_{\text{off}}$  is the hold-off time of the detectors,  $R_{\text{DC}}$  the dark-count rate, PDE the photon detection efficiency,  $n_Z$  is the block size,  $p_{Z,A}$  and  $p_{Z,B}$  the probabilities of choosing the  $Z$  basis for Alice and Bob, respectively,  $\nu_{\text{rep}}$  is the repetition rate,  $\epsilon_{\text{sec}}$  and  $\epsilon_{\text{corr}}$  are the security and correctness parameters,  $\tau_Z$  and  $\tau_X$  are the losses of Bob for the  $Z$  and  $X$  basis. SIP SPAD detector has an active area diameter of 10  $\mu\text{m}$ .

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

pulse are chosen such that they maximize the key rate in our simulation model, and are reported in Table 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  $Z$ -basis output brings the photons directly to one single-photon detector (SPD), while the  $X$ -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  $X$  basis overlap and their

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,  $\epsilon_Z$  and  $\epsilon_X$  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.

	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		
$\epsilon_Z$ (%)	0.7	0.8	1.1	1.8	4.6
$\epsilon_X$ (%)	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		
$\epsilon_Z$ (%)	4.4	4.4	5.0	6.0	9.3
$\epsilon_X$ (%)	4	2.9	3.2	4.0	7.2
SKR (kbps)	3.25	3.05	2.10	1.05	0.11

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, counterpropagating 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 SPAD is based on 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 circuit often uses a simple passive quenching circuit, which cannot be gated at high 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 recently 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 [23]. The photosensitive 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 [35] 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. The operating conditions of a field test are radically different from those in a laboratory scenario. When installing the devices in telecom data centers, the primary concern is to fit the entire setup into rack boxes that comply with safety standards. Additionally, a data center area lacks stable temperature control and is subject to mechanical disturbances from device cooling fans, which generate both vibrations and airflow. These factors pose a significant challenge, particularly

for the receiver setup, which includes an interferometer. Precise and accurate fine tuning of the phase lock loop PID has been necessary to counteract these issues. Furthermore, the fibers have been previously characterized to ensure they are not susceptible to crosstalk or other processes resulting in dark counts in quantum communication. We have 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  $\tau_{OFF} = 20 \mu s$  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  $\tau_{OFF} = 1 \mu s$  thanks to the limited after-pulse probability.

With the hold-off time set to  $1 \mu s$ , 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 detection of 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 threshold, resulting in lower detection efficiency. The low  $\tau_{OFF}$  setting allows for avoiding such conditions in the SIP PoliMi detector. Since the temporal duration of a quantum state is 1.68 ns, an ON time  $\tau_{ON} = 1.68 \text{ ns}$  is selected. Figure 2 reports the histogram of photon detections during a gate ON time.  $\tau_{ON} = 1.68 \text{ ns}$  proves to be a good choice considering the shape of the pulses.

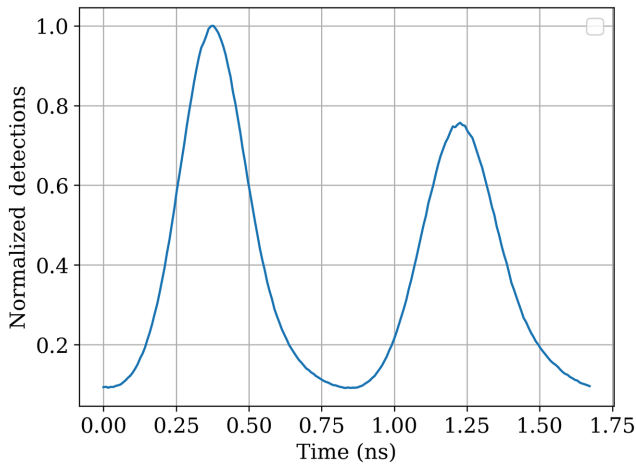


FIG. 2. Histogram of photon detections. The figure shows the histogram of photon detections during a gate ON time, which corresponds to the temporal duration of a quantum state. The histogram, referring to a 5-min-long acquisition in the case of a 5-dB attenuation channel, has been normalized in order to showcase only the shape of the pulses. The first peak is higher than the second one due to the fact that in the preloaded sequence of states in the FPGA, there is an imbalance in generating the Z basis  $|0\rangle$  and  $|1\rangle$  states for characterization purposes.

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

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 measured quantum bit error rates (QBERs) and the achieved key rates are reported in Table II and are shown in Fig. 3. We said that the ID221 detector, due to its hold-off time settings, has a saturation threshold 20 times lower than the SIP PoliMi detector. This implies that the ID221 detector is more susceptible to a series of effects that occur in the saturation regime, such as an increase in timing jitter, while the SIP SPAD detector has been specifically designed to minimize the increase in timing jitter even at saturated count rates. These effects are more pronounced in the Z basis than in the X basis, due to the higher losses introduced by the interferometric apparatus that reduce the impinging photons. When comparing the two detectors based on QBERs, it is evident that the SIP SPAD exhibits a more significant improvement in the Z basis than in the X one. The value of  $QBER_X$  represents the

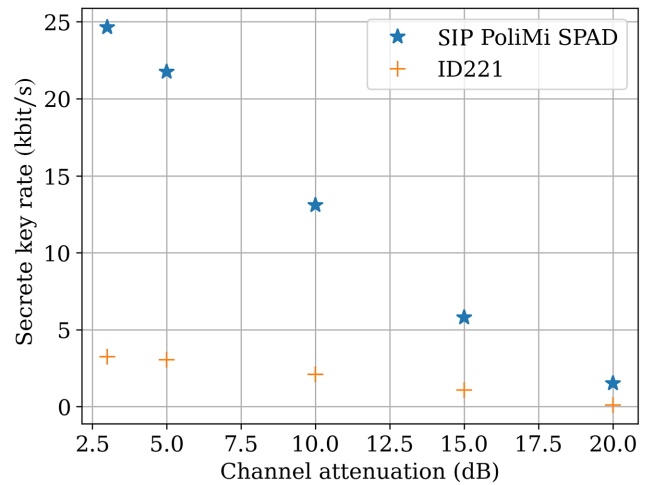


FIG. 3. Key rate results (field trial). The plot shows the secure key rates achieved by the commercial detector (ID221) and the tested SIP detector fabricated by the research group of Politecnico di Milano (SIP Polimi SPAD). Thanks to the fast-quenching circuit applying the gate signal, the SIP PoliMi SPAD outperforms the commercial device by a factor of 7 in terms of key rate for a small attenuation link, and up to 14 times when the entire channel is considered (20 dB).

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 2 and 3 V 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 3 V of excess bias. The ID221 has been kept on 20  $\mu\text{s}$  of hold-off time and 20% of detection efficiency.

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

visibility of an interferometer operating in an environment that deviates from optimal laboratory conditions. In a non-saturation regime, the measurement obtained with ID221 closely approximates the actual value.

### 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

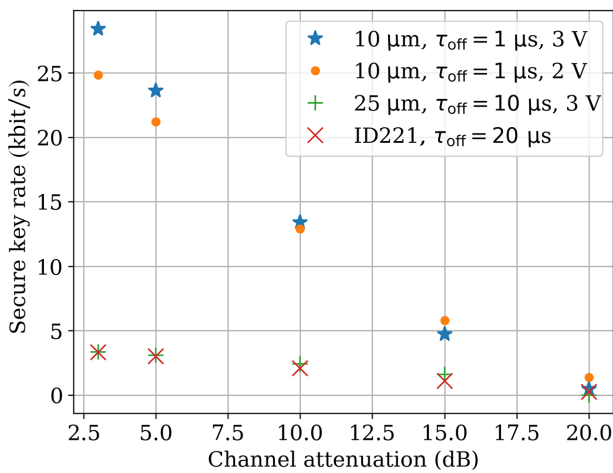


FIG. 4. Secret key rate extracted in laboratory conditions with the different detectors for different channel attenuation values. 10 and 25  $\mu\text{m}$  are the two SIP PoliMi SPAD and the value is referred to the relative photosensitive active area diameter. The selected detector settings are reported in the legend (hold-off time, excess bias voltage), the photon-detection efficiency is 20% for ID221 and around 20% and 15% for the SIP SPADs with 3 and 2 V of excess bias, respectively [35].

channel losses introduced by a tunable attenuator between Alice's and Bob's setups. The results are reported in Table III and Fig. 4. 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 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 an improvement in low channel losses, while the performance dropped with excess bias voltage increase due to the reduction of SNR.

### V. DISCUSSION

Boosting the key rate on long-distance links is the priority for the widespread deployment of QKD technology. Many alternative protocols are being experimented and are showing their potentialities: twin-field QKD [36,37] and high-dimensional protocols [38–42] are just a few examples that go in this direction. Simultaneously, with the appearance of SNSPDs [43,44] and photon-number-resolving detectors [45,46] much attention has been paid to the detection stage. Although InGaAs/InP SPADs established their place as the most common technology for single-photon detection in C band because of their portability and cost effectiveness, compared to other 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. [34]. 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 a key 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 after pulsing. In comparison, the alternative 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 recently 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.

### ACKNOWLEDGMENTS

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 Grant Agreement No. 101091561, the Project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU, the Project QuONTENT under the "Progetti di Ricerca@CNR" program funded by the Consiglio Nazionale delle Ricerche (CNR) and by the European Union - PON Ricerca e Innovazione 2014-2020 FESR - Project ARS01\_00734 QUANCOM, the Project QUID (Quantum Italy Deployment) funded by the European Commission in the Digital Europe Programme under the grant agreement No. 101091408.

- 
- [1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.* **560**, 7 (2014).
  - [2] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, *Nat. 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. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, *Adv. Opt. Photonics* **12**, 1012 (2020).
- [6] S.-K. Liao *et al.*, Satellite-to-ground quantum key distribution, *Nature* **549**, 43 (2017).
- [7] C.-Y. Lu, Y. Cao, C.-Z. Peng, and J.-W. Pan, Micius quantum experiments in space, *Rev. Mod. Phys.* **94**, 035001 (2022).
- [8] W. Li, L. Zhang, H. Tan, Y. Lu, S.-K. Liao, J. Huang, H. Li, Z. Wang, H.-K. Mao, B. Yan, Qiong Li, Yang Liu, Qiang Zhang, Cheng-Zhi Peng, Lixing You, Feihu Xu, and Jian-Wei Pan, High-rate quantum key distribution exceeding 110 mb s<sup>-1</sup>, *Nat. Photonics* **1**, 416 (2023).
- [9] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Yong-Gang Zhu, Pavel V. Morozov, Alexander V. Divochiy, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han, Twin-field quantum key distribution over 830-km fibre, *Nat. Photonics* **16**, 154 (2022).
- [10] 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, in *2018 IEEE Photonics Conference (IPC)* (IEEE, Munich, Germany, 2018), p. 1.
- [11] S. P. Neumann, A. Buchner, L. Bulla, M. Bohmann, and R. Ursin, Continuous entanglement distribution over a transnational 248 km fiber link, *Nat. Commun.* **13**, 6134 (2022).
- [12] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, Long-distance quantum key distribution secure against coherent attacks, *Optica* **4**, 163 (2017).
- [13] N. Namekata, S. Sasamori, and S. Inoue, 800 MHz single-photon detection at 1550-nm using an InGaAs/InP avalanche photodiode operated with a sine wave gating, *Opt. Express* **14**, 10043 (2006).
- [14] N. Namekata, S. Adachi, and S. Inoue, 1.5 GHz single-photon detection at telecommunication wavelengths using sinusoidally gated InGaAs/InP avalanche photodiode, *Opt. Express* **17**, 6275 (2009).
- [15] Y. Fan, T. Shi, W. Ji, L. Zhou, Y. Ji, and Z. Yuan, Ultra-narrowband interference circuits enable low-noise and high-rate photon counting for InGaAs/InP avalanche photodiodes, *Opt. Express* **31**, 7515 (2023).
- [16] Z. Yuan, B. Kardynal, A. Sharpe, and A. Shields, High speed single photon detection in the near infrared, *Appl. Phys. Lett.* **91**, 041114 (2007).
- [17] A. Restelli, J. C. Bienfang, and A. L. Migdall, Single-photon detection efficiency up to 50% at 1310 nm with an InGaAs/InP avalanche diode gated at 1.25 GHz, *Appl. Phys. Lett.* **102**, 141104 (2013).
- [18] Y.-Q. Fang, W. Chen, T.-H. Ao, C. Liu, L. Wang, X.-J. Gao, J. Zhang, and J.-W. Pan, InGaAs/InP single-photon detectors with 60% detection efficiency at 1550 nm, *Rev. Sci. Instrum.* **91**, 083102 (2020).

- [19] Y. Liang, E. Wu, X. Chen, M. Ren, Y. Jian, G. Wu, and H. Zeng, Low-timing-jitter single-photon detection using 1-GHz sinusoidally gated InGaAs/InP avalanche photodiode, *IEEE Photonics Technol. Lett.* **23**, 887 (2011).
- [20] A. Restelli and J. C. Bienfang, in *Advanced Photon Counting Techniques VI*, Vol. 8375 (SPIE, Baltimore, Maryland, United States, 2012), p. 224.
- [21] EuroQCI, European quantum communication infrastructure (euroqci) initiative (2017), <https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci>.
- [22] 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 J. Sel. Top. Quantum Electron.* **28**, 1 (2022).
- [23] A. Ruggeri, P. Ciccarella, F. Villa, F. Zappa, and A. Tosi, Integrated circuit for subnanosecond gating of InGaAs/InP SPAD, *IEEE J. Quantum Electron.* **51**, 1 (2015).
- [24] IDQuantique, Id221 infrared single-photon detector, <https://www.idquantique.com/resources/id221/>.
- [25] 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).
- [26] D. Rusca, A. Boaron, F. Gr unenfelder, A. Martin, and H. Zbinden, Finite-key analysis for the 1-decoy state QKD protocol, *Appl. Phys. Lett.* **112**, 171104 (2018).
- [27] 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).
- [28] M. Hayashi and R. Nakayama, Security analysis of the decoy method with the Bennett-Brassard 1984 protocol for finite key lengths, *New J. Phys.* **16**, 063009 (2014).
- [29] W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, *Phys. Rev. Lett.* **91**, 057901 (2003).
- [30] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [31] M. Canale, Ph.D. thesis, Department of Information Engineering, University of Padova, 2014.
- [32] 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, *J. Appl. Phys.* **120**, 063101 (2016).
- [33] 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).
- [34] D. Ribezzo *et al.*, Deploying an inter-European quantum network, *Adv. Quantum Technol.* **n/a**, 2200061 (2022).
- [35] 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 J. Quantum Electron.* **48**, 1227 (2012).
- [36] 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).
- [37] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, *Nat. Commun.* **8**, 15043 (2017).
- [38] H. Bechmann-Pasquinucci and W. Tittel, Quantum cryptography using larger alphabets, *Phys. Rev. A* **61**, 062308 (2000).
- [39] I. Vagniluca, B. Da Lio, D. Rusca, D. Cozzolino, Y. Ding, H. Zbinden, A. Zavatta, L. K. Oxenl owe, and D. Bacco, Efficient time-bin encoding for practical high-dimensional quantum key distribution, *Phys. Rev. Appl.* **14**, 014051 (2020).
- [40] M. Zahidy, D. Ribezzo, C. D. Lazzari, I. Vagniluca, N. Biagi, T. Occhipinti, L. K. Oxenl owe, M. Galili, T. Hayashi, C. Antonelli, A. Mecozzi, A. Zavatta, and D. Bacco, in *European Conference on Optical Communication (ECOC) 2022* (Optica Publishing Group, Basel, Switzerland, 2022), p. Th3C.6.
- [41] B. Da Lio, D. Cozzolino, N. Biagi, Y. Ding, K. Rottwitz, A. Zavatta, D. Bacco, and L. K. Oxenl owe, Path-encoded high-dimensional quantum communication over a 2-km multicore fiber, *Npj Quantum Inf.* **7**, 63 (2021).
- [42] D. Bacco, N. Biagi, I. Vagniluca, T. Hayashi, A. Mecozzi, C. Antonelli, L. K. Oxenl owe, and A. Zavatta, Characterization and stability measurement of deployed multicore fibers for quantum applications, *Photon. Res.* **9**, 1992 (2021).
- [43] C. M. Natarajan, M. G. Tanner, and R. H. Hadfield, Superconducting nanowire single-photon detectors: physics and applications, *Supercond. Sci. Technol.* **25**, 063001 (2012).
- [44] 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, *Opt. Eng.* **53**, 081907 (2014).
- [45] A. Divochiy, F. Marsili, D. Bitauld, A. Gaggero, R. Leoni, F. Mattioli, A. Korneev, V. Seleznev, N. Kaurova, 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, *Nat. Photonics* **2**, 302 (2008).
- [46] J. Provazn ik, L. Lachman, R. Filip, and P. Marek, Benchmarking photon number resolving detectors, *Opt. Express* **28**, 14839 (2020).