QKD protocol over 100 km long submarine optical fiber assisted by a system-in-package fast-gated InGaAs single photon detector

Domenico Ribezzo[1], Mujtaba Zahidy[2], Antoine Petitjean[1], Gianmarco Lemmi[1], Claudia De Lazzari[3], Ilaria Vagniluca[3], Enrico Conca[4], Alberto Tosi[4], Tommaso Occhipinti[3], Francesco Saverio Cataliotti[6], Leif K. Oxenløwe[2], André Xuereb[5], Davide Bacco[6,*], Alessandro Zavatta[1]

[1] Istituto Nazionale di Ottica del Consiglio Nazionale delle Ricerche (CNR-INO), 50125 Firenze, Italy [2] Centre for Silicon Photonics for Optical Communications (SPOC), Department of Electrical and Photonics Engineering, Technical University of Denmark, Kgs. Lyngby, Denmark. [3] QTI S.r.l., 50125, Firenze, Italy [4] Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, 20133 Milano, Italy [5] Department of Physics, University of Malta, Msida MSD 2080, Malta [6] Dipartimento di Fisica, Università degli Studi di Firenze, Firenze, Italy

[*] davide.bacco@unifi.it

Abstract: A QKD link established between Sicily (Italy) and Malta has been utilized to test the performances of a fast-gated InGaAs single photon detector, achieving a fourteen times higher key rate than using a commercial detector. © 2022 The Author(s)

1. Introduction

Quantum Key Distribution (QKD) is the most mature technology coming out from the second quantum revolution. Many experiments have shown its potentialities [1, 2], to the point that today establishing a quantum communication link between two parties that are hundreds of kilometers far away is within our grasp [3]. However, for the technology to be employed in our daily basis infrastructure, it requires to become even more cost-effective. Hence, great research activities are focused on high-performance single photon detectors (SPD) and in particular single-photon avalanche diodes (SPAD).

In this work, we established a QKD link connecting two different countries in the middle of the Mediterranean sea through a 100 km long submarine optical fiber connecting the Sicilian city of Pozzallo (Italy) to Madliena, in Malta. The link has been utilized to test the performances of a fast-gated InGaAs detector, a system-in-package single photon avalanche diode (SPAD) from Politecnico di Milano (Polimi), and to compare it with the results obtained by using a commercial InGaAs SPAD. On the entire channel, which exhibits an attenuation of 21 dB, it has been found that with the fast-gated detector it is possible to achieve a key rate fourteen times bigger with respect to the setup with the receiver implementing the commercial SPD.

2. QKD Protocol

The adopted protocol is the 3-state efficient BB84 with time-bin encoding and 2-decoy method [4, 5]. In this protocol, only one basis is used for sharing the key, while the second one is reserved for security checks. This makes the implementation simpler since only one of the two eigenstates of the second basis needs to be prepared. The data basis is the computation **Z**-basis, whose eigenstates, according to the time-bin encoding, are made by one pulse located in the first or in the second half of the time-bin. Being the checks basis eigenstates their superposition, the diagonal **X**-basis is made by two pulses, and their relative phase (0 or π) makes the state. The π state is not generated. Finally, the 2-decoy method is utilized for limiting the issues deriving from the lack of a real single-photon source [6]. In a weak coherent pulses source, multi-photon emission probability can compromise the security of the communication. However, randomly varying mean photon number per pulse helps to detect an on-going photon number splitting attack. More information about the protocol, such as the key length expression, can be found in [5].

3. Experimental Setup

As shown in fig. 1, the pulses encoding the **X** and **Z** 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, a variable optical attenuator (VOA) brings the intensity down to single-photon level. More details can be found

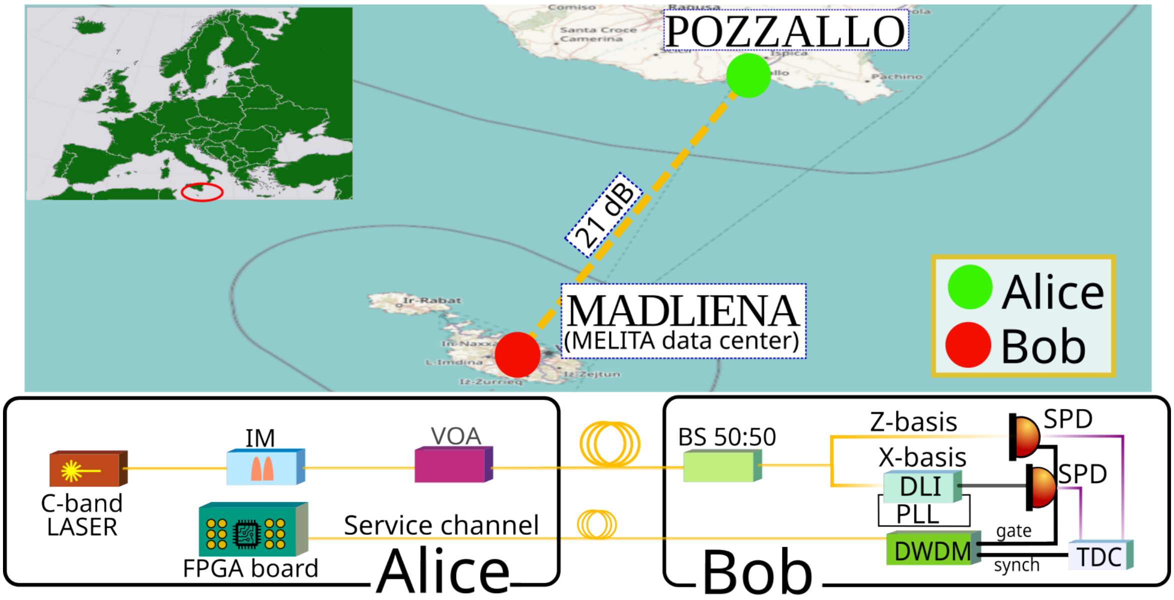

Fig. 1. **Top:** QKD link shown on a map. **Bottom:** scheme of the setup. IM: intensity modulator, VOA: variable optical attenuator, FPGA board: field programmable gate array, BS: beam splitter, DWDM: dense wavelength division multiplexer, DLI: delay line interferometer, PLL: phase lock loop, SPD: single photon detector, TDC: time to digit converter. Other details and explanations can be found in the text.

in [7].The qubit generation rate is 119 MHz and the probability for Alice to choose the computational basis (**Z**) is $P_{ZA} = 0.5$. On a second fiber, two classical signals are shared between the two parties; a synchronization signal at 145.358 kHz and a second signal at 119 MHz that is used as a gate signal for the detector. The numbers of photons per pulse have been chosen as the ones that maximize the key rate in a simulation model, and are reported in [4]. Travelling through the submarine fiber channel, the photons arrive at the receiver setup; there they meet a 50:50 beam splitter that acts as basis choice. The **Z**-basis output brings the photons directly to one SPD, while the **X**-basis output lets the photons pass through a Mach-Zehnder delay line interferometer (DLI) before they are detected. A phase-lock-loop (PLL) helps to stabilize the interferometer. Phase fluctuation of a weak continuous laser counter-propagating with respect to the quantum signal is monitored to provide the feedback for the PLL which drives a phase shifter to compensate for any phase drift. Finally, the synchronization and gate signals travelling in the service channel are demultiplexed and utilized.

4. Results

The system-in-package fast-gated detector has been compared with a commercial InGaAs single photon detector produced by ID Quantique (model ID221). Since the state generation rate of the source for the first detector is limited by the gate signal, Alice's repetition rate has been set to 119 MHz in order to have comparable results. To test the performances of the gated detector for different channel attenuations, shorter channels have been simulated by compensating for the attenuation introduced by the fiber link: this is equivalent to positioning the Alice unit in different locations through the fiber. The data have been taken in the same conditions, only with different detectors. All the preparation, detections and post-processing parameters are reported in table 4.

5. Comments and conclusions

The biggest advantage introduced by a fast-gated detector is that, since it stays off when no events are expected, the measurement is less affected by the detector's dark counts, being so possible to use shorter hold-off times. It brings higher detection rates since the saturation threshold is pushed forward and it is possible to collect more photons. Considering that the quantum bit error rate (QBER) is the ratio of the wrong detection events (affected by the dark counts) over the total events, it has been possible to use a hold-off time for the system-in-package SPAD that is twenty times smaller than the one that optimizes the results for the ID221 ($1\ \mu s$ vs $20\mu s$). In this condition, the gated detector shows a dark count rate four times bigger than the other detector, but a QBER sensibly smaller (see table 4). From fig. 2 appears also that the ID221 at 3 dB is already in saturation regime. As a consequence,

	Polimi	ID221
τ_{off} (μs)	1	20
$\mathbf{r}_{\mathrm{DC}}$ (kHZ)	10.8	2.5
n_Z	10^6	
$p_{Z,A}$	50%	
$p_{Z,B}$	50%	
ν_{rep} (MHz)	119	
ε_{sec}	10^{-12}	
ε_{corr}	10^{-12}	
τ_Z (dB)	1	
τ_X (dB)	3	

	3 dB	5 dB	10 dB	15 dB	21 dB
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				
$\varepsilon_Z(\%)$	4.4	4.4	5.0	6.0	9.3
$\varepsilon_X(\%)$	4	2.9	3.2	4.0	7.2
SKR	12300	11500	3700	800	80
System-in-package 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	19100	16800	8700	3500	1100

Table 1. **Setup parameters. Left:** τ_{off} is the hold-off time of the detectors, $\mathbf{r}_{DC}$ 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, ν_{rep} is the repetition rate, ε_{sec} and ε_{corr} are the security and correctness parameters, τ_Z and τ_X are the losses of Bob for the Z and X basis. **Right:** mu_1, mu_2 and mu_3 are the numbers of photons per pulse according to the decoy method, ε_Z and ε_X are the qubit error rate in the two bases and finally, SKR is the secure key rate.

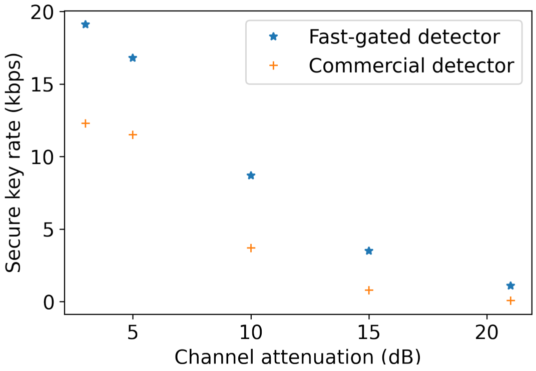

Fig. 2. **Secure key rate achieved by the two detectors.**

the secret key rate for the fast-gated SPD is 55% higher for the 3 dB fiber channel (19100 vs 12300 bps), and increases up to fourteen times for the full 21 dB channel (1100 vs 80 bps).

References

1. S.-K. Liao et al., “Satellite-to-ground quantum key distribution,” Nature **549**, 43–47 (2017).
2. D. Bacco et al., “Field trial of a three-state quantum key distribution scheme in the florence metropolitan area,” EPJ Quantum Technol. **6**, 5 (2019).
3. Y.-A. Chen et al., “An integrated space-to-ground quantum communication network over 4,600 kilometres,” Nature **589**, 214–219 (2021).
4. A. Boaron et al., “Simple 2.5 GHz time-bin quantum key distribution,” Appl. Phys. Lett. **112**, 171108 (2018).
5. D. Rusca et al., “Security proof for a simplified Bennett-Brassard 1984 quantum-key-distribution protocol,” Phys. Rev. A **98**, 052336 (2018).
6. H.-K. Lo et al., “Decoy state quantum key distribution,” Phys. review letters **94**, 230504 (2005).
7. D. Ribezzo et al., “Deploying an inter-european quantum network,” arXiv preprint arXiv:2203.11359 (2022).