Results of the NATO project: "analysis, design, and implementation of an end-to-end QKD link"

Results of the NATO project: “Analysis, design, and implementation of an end-to-end QKD link”

M. Mondin*[a], F. Daneshgaran[a], S. Arnon[b], M. Genovese[c], I. Bari[d], O. Khan[e], F. Di Stasio[f], J. Kupferman[b], A. Meda[c], I.P. Degiovanni[c], M. Gramegna[c], F.Saccomandi[c], M. M. Khan[e], N. Ullah[g], K. Olia[a], J. May[a], J. Neilson[a]
[a]CSULA, EE Dept., 5151 State Univ. Dr., Los Angeles, CA, USA 90032;
[b]Ben Gurion Univ. of the Negev, P.O Box 653, Beer Sheva, Israel IL-84105,
[c]INRIM, Str. delle Cacce, 91, Torino, Italy 10135,
[d]Military Technological College, Al Matar Street, Muscat 111, Oman,
[e]National University of Computer & Emerging Sciences - FAST Peshawar, Pakistan,
[f]Politecnico di Torino, C.so Duca degli Abruzzi 24, Turin, Italy 10129,
[g]National University of Sciences and Technology, Karachi, Pakistan

ABSTRACT

This manuscript discusses the most relevant aspects of the practical implementation of a long-range Quantum Key Distribution (QKD) link with trusted nodes, achieving the highest possible secret key rate generation within the security and system-level constraints. To this purpose, it describes the implementation of an end-to-end QKD system, including implementation aspects from the physical transmission of photon states through a standard telecommunications grade optical fiber, to consideration of quantum metrology and information reconciliation protocols based on forward error correction codes. In addition, since there are circumstances when a fiber optical link may not be available, it examines the problems involved with the implementation of a Free Space Optics (FSO) QKD link. The manuscript also discusses the problem of information reconciliation in Continuous Variable (CV) QKD scenarios on FSO links, showing that in long-distance links, since the sign of the received Gaussian samples contains the largest fraction of information, Unequal Error Protection (UEP) reverse reconciliation schemes can be designed. The presented results have been achieved within the NATO SPS project “Analysis, design and implementation of an end-to-end 400 km QKD link”.

Keywords: Quantum Key Distribution, Information Reconciliation, CV-QKD, Free Space Optics QKD

1. INTRODUCTION

The described NATO project has been focused on carefully analyzing every aspect of the practical implementation of a long range QKD link with trusted nodes, achieving the highest possible secret key rate generation within the security and system level constraints. To this purpose, a long-range QKD link with trusted nodes has been built and used as test bench. The system includes all implementation aspects, from transmission of photon states through an optical fiber or an optical free-space link, to consideration of device imperfections, low and information reconciliation protocols.

The project has covered theoretical, experimental and metrological analysis. Two links connecting the trusted nodes of Turin and Santhià and Turin and Bardonecchia, for a total distance of roughly 200 Km have been tested. A free-space optical laboratory has also been established, and information reconciliation schemes for both continuous variable and discrete variable QKD applications have been studied. More specifically, the feasibility of a long-distance QKD link with maximum security key rate based on the use of the twin-field QKD technique has been demonstrated, validating the transmission of quantum cryptographic keys between two end points with a trusted node in the middle, using commercial QKD devices and commercial optical networks. The metrological characterization of ultra-weak laser pulses generated by free running 1550 nm single-photon detectors has also been performed, and the use of short and medium BCH and Polar codes for Information Reconciliation has been studied. Finally, the setup of a free-space-optics laboratory has been completed, and the effects of the optical link parameters on the performance of an information reconciliation schemes for free space optics CV-QKD has been studied.

*marina.mondin@calstatela.edu; phone 1 322 343-4548; fax 1 323 j343-4547; www.calstatela.edu

These aspects will be discussed in further detail in the next sections. In particular, section 2 describes the feasibility of a long-distance QKD link, while section 3 discusses the metrological aspects. Section 4 is dedicated to the coding aspects related to information reconciliation and finally section 5 deals with the problems involved in the implementation if a Free Space Optics (FSO) QKD link.

2. IMPLEMENTATION OF A LONG DISTANCE QKD LINK

The main goal of the project was the realization of a long-distance QKD link with trusted nodes. More specifically, the project demonstrated the feasibility of a long-distance QKD link with maximum security key rate based on the use of the twin-field QKD technique.

In QKD, the maximum secure key rate for an unrepeated transmission scales as T, where T is the transmittance of the channel between the parties. With a weak dependence on the channel transmissivity, proportional to the square root of T, the recently proposed Twin-Field QKD (TF-QKD) surpasses this limit, establishing a new framework towards implementation on long-distance, high loss telecom networks.

In TF-QKD, the information is encoded as a discrete phase state on dim laser pulses generated at distant Alice and Bob terminals and sent through optical fiber to a central node, Charlie, where they interfere. The underlying assumption is that the optical pulses are phase-coherent in Alice and Bob, and preserve coherence throughout the path to Charlie.

To demonstrated its feasibility, TF-QKD was implemented over long-haul fiber backbones connecting INRIM, in the city of Torino (Italy), where the Charlie terminal was located, to network nodes located 114km and 92km apart (Alice and Bob terminals respectively). The distance between the two remote parties was 206 km with an overall attenuation of 65 dB.

By exploiting frequency metrology stabilization techniques, it was demonstrated [1] the feasibility of the TF-QKD scheme on such a distance: when stabilization was activated [1].

In parallel, a trusted node QKD system was deployed; the trusted node allows to extend QKD end-points distance limitation due to losses in realistic fiber infrastructures. A QKD transmission between two end-points was implemented and tested, exploiting two commercial QKD systems (Id Quantique Clavis3 and Cerberis3). Regenerating the key, the trusted node allowed the two nodes to successfully share the same cryptographic key.

Finally, portable single photon Optical Time-Domain Reflectometer (OTDR), able to identify reflections of optical components in QKD systems that can be exploited by an eavesdropper, was also been assembled and tested in order to investigate possible weak points of QKD systems.

3. METROLOGICAL CHARACTERIZATION OF DEVICES

As part of the metrological characterization of QKD devices, a study on the detection of ultra-weak laser pulses by free running 1550 nm single-photon detectors was performed, modeling dead time and dark counts effects [2].

For the count rate measurements we exploited a free-running Single-Photon Avalanche Diode (SPAD) under pulsed laser radiation with variable repetition frequency and optical power. A monitor detector connected to a beam splitter (BS) tracks any changes of the optical laser power. Two calibrated variable attenuators reduce the optical power by several orders of magnitude so that it lies below the saturation value of the SPAD. The electrical signals from the pulse generator and from the SPAD are connected to channels 1 and 2 of a time-to-digital converter for filtering of the clicks correlated with laser pulses. A laser (IDQ, id300) with an emission wavelength of 1550.5 nm is triggered by a pulse generator (Keysight, 33600A) with a variable repetition frequency. The laser light, which is monitored in intensity, passes through two identical variable attenuators (Agilent, 81571A) and reaches the active area of an InGaAs/InP SPAD (IDQ, id220-FR-SMF). The arrival times of the electrical pulses from the pulse generator on channel 1 and from the SPAD detector on channel 2 are recorded by a time-to-digital converter (Swabian Instruments, Time Tagger 20). It should be noted that both signals have been synchronized by choosing an appropriate delay compensation on channel 1 to account for the difference in cable lengths. All measurements are performed in free-running mode.

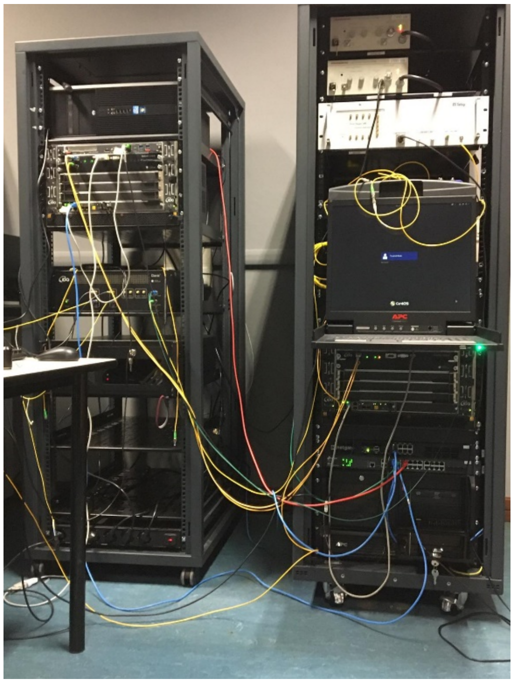

Figure 1. The trusted node QKD setup in INRIM.

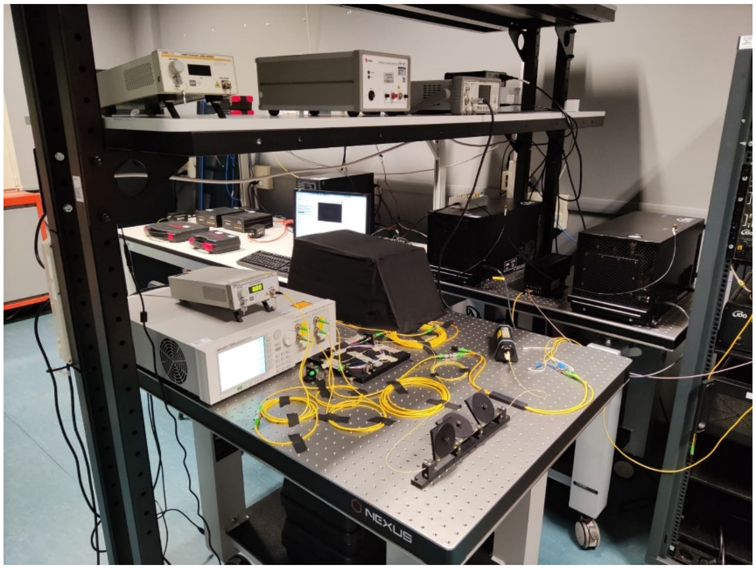

Figure 2. The laboratory setup in INRIM.

We demonstrated an experimental method for separating photon detections from dark counts via a software-induced gating mechanism, which has been proven valuable for gaining a better understanding of the influence of dead time. Our model gives a much better description of the effective dark counts compared to previous models [2].

The presented model in principle should give a good estimation of the count rate for an arbitrary laser repetition frequency, so that it could be implemented in QKD-based applications aiming for high data rates [2]. The model will be useful for testing the expected response of a free-running detector illuminated by a pulsed source in QKD devices to detect any deviation from the ideal behavior that can be exploited by an eavesdropper to gain information about the system.

4. INFORMATION RECONCILIATION

The goal of the Information Reconciliation activity (IR) is that of correcting as many errors as possible in the sifted key obtained after the initial exchange of quantum states between Alice and Bob. To achieve this, often extremely long Forward Error Correction (FEC) codes [3, 4] have been typically used are used in conjunction with very powerful iterative decoding techniques. The result is that the IR process introduces a significant delay and becomes a bottleneck in terms of this metric for the whole system. In many real-time applications, this delay is undesirable and low latency key generation is necessary. For this reason we have investigated FEC codes with short or medium length (in order to minimize the processing delay) and low complexity decoding. More specifically, Bose-Chaudhuri-Hocquenghem (BCH) codes and Polar codes have been considered, together with different decoding techniques (Berlekamp-Massey decoding, ordered statistics, belief propagation, successive cancellation and list decoding) and different channel models for the systematic q-bits and the redundancy bits. Table 1 summarizes all the considered cases.

Table 1. Summary of the considered FEC codes, channel models and decoding algorithms (Q-BSC: Quantum Binary Symmetric Channel, AWGN: Additive White Gaussian Noise, BEC: Binary Erasure Channel, BIMO: Binary Input Multiple Output).

Codes	Code Type	Channel Model	Decoding Technique
BCH	Systematic Cyclic	Q-BSC, AWGN	Berlekamp-Massey Decoder (BMD)
BCH	Systematic Cyclic	Q-BSC, AWGN	Ordered Statistics (OS)
BCH	Systematic Cyclic	Q-BSC, AWGN	Belief Propagation (BP)
Polar	Non-Systematic Block	Q-BSC, BEC	Successive Cancellations (SC)
Polar	Non-Systematic Block	Q-BSC, BEC	Successive Cancellations (SC)
Polar	Systematic Block	Q-BSC, AWGN Q-BIMO, AWGN	CRC Enabled Successive Cancellations List Decoding

When analyzing short and medium length BCH codes, we could observe that short length algebraic BCH codes perform very well as compared to Low Density Parity Check (LDPC) codes, and represent therefore a valid and simpler alternative to longer codes, and that Ordered Statistics Decoding (OSD) offers better performance than Berlekamp-Massey (BM) decoding, offering a valid decoding alternative.

As far as Polar codes are concerned, they have recently received widespread attention due to their capacity of achieving Shannon capacity on binary symmetric memoryless channels [5]. They are known to outperform BCH and LDPC codes, and represent therefore an interesting solution for IR in QKD applications. We considered them in conjunction with a successive cancellation decoding algorithm, obtaining the encouraging performances shown in Figure 3.

5. FREE SPACE OPTICS QKD

5.1 Pointing Jitter Effect on the Performance of CV-QKD

The goal of QKD is to agree on a common stream of bits that we denote as “reconciled key”. Key exchange can be implemented using sampling of Gaussian signals. The received Gaussian samples, due to the characteristics of the of communication system, are function of the magnitude of the jitter.

Continuous Variable (CV) QKD is a method to implement key exchange using sampling of Gaussian signals [6]. Reconciliation in CV-QKD is fundamentally realized via coding of the Alice or Bob binary labels of the Gaussian samples using either one-way or interactive communications between the parties.

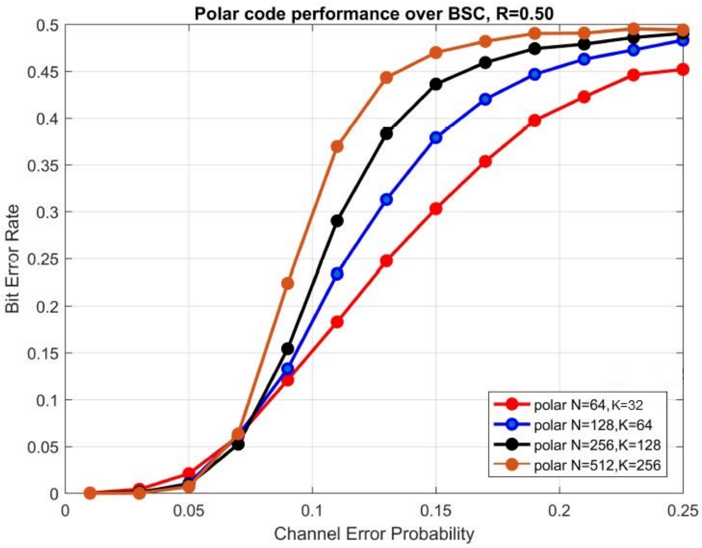

Figure 3. Performance of Polar codes.

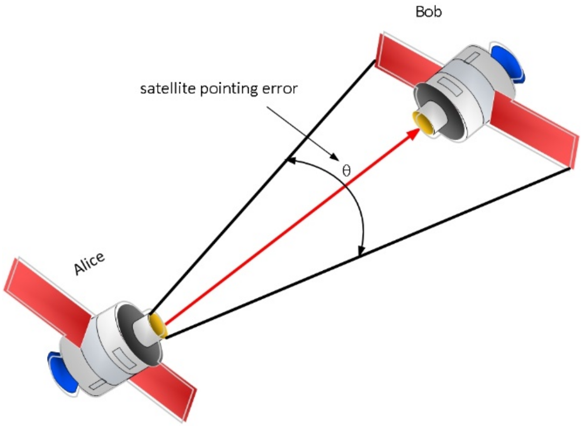

Figure 4. The considered FSO scenario and the pointing error θ.

Continuous Variable (CV) Quantum Key Distribution (QKD) [6] can be a viable alternative to its Discrete Variable (DV) counterpart. The key rate in DV-QKD is really limited by technology and physical constraints associated with construction of reliable high rate single photon (or at least low photon count) sources, and more importantly, fast and reliable single photon detectors with very low dark count rates.

Free Space Optics (FSO) QKD is emerging technology that could be found in many platform such as drone, satellite, airplane, ship, train, and unman aerial vehicle [7]. We assume that Alice is located on one of this vibrating platform and Bob on the other one. Alice and Bob are equipped with two telescopes with gain G, in line of sight. The telescopes have pointing direction error angles equal to θ, (see Figure a), which is a random variable with variance σ_θ^2.

The received sample Y at Bob can be written as

$$Y=AX+N$$

where the signal X and the noise N have a Gaussian distribution, and the random amplitude A is a function of the random phase jitter , the telescope gains, their optical efficiency and their wavelength.

5.2 Reconciliation protocol

Reconciliation is performed by using permutation modulation [8, 9, 10] for labelling of the magnitudes of the Gaussian samples at Alice and Bob over as large a dimension as desired. The goal is to achieve a very efficient vector quantization technique providing fractional bit per sample accuracy to whatever extent desired. At very low SNR, very little information is carried by the magnitude of the Gaussian samples. Quantization of magnitudes of the Gaussian samples at Bob in reverse reconciliation (RR) is simply used to provide side information to Alice about the quantized sample magnitudes.

There is an intimate relationship between the error probability of sign of the samples and the sample magnitudes [11, 12]. The probability that the sign of the sample observed at Bob is different from that at Alice can be expressed as a function of the parameters that defined the random variables A, X and N. Unequal Error Protection (UEP) coding can then be used by Bob in Reverse Reconciliation (RR) to ensure the error rate on the sign of the samples is below a desired threshold [11, 12].

If we assume that the amplitude of the received Gaussian samples are quantized in L=10 bins with size equal to $3\sigma_Y/L$, (where σ_Y^2 is the variance of the received variable Y), the sign error probability for the various bins as a function of the signal to noise ratio SNR0 and for a telescope gain G = 5dB is shown in Figure 5 (where the jitter variance σ_θ^2 is equal to 0.1).

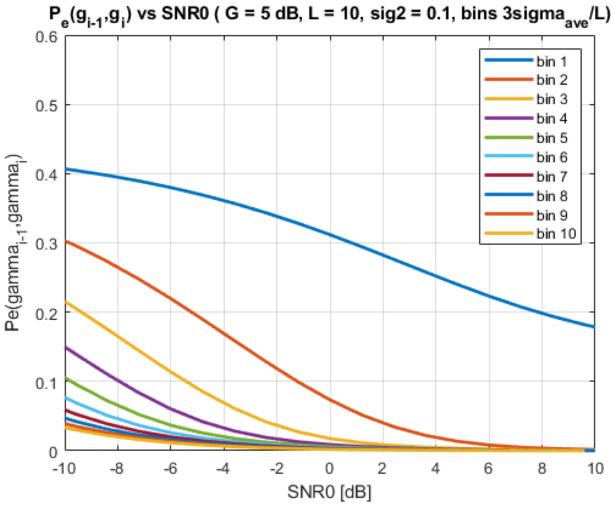

Figure 5. Example of sign error probability as a function of the interval in which the amplitude of the sample at Bob falls into and of the signal to noise ration *SNR0* ($\sigma_\theta^2 = 0.1$, *G*=5 dB).

It can be observed from Figure 5 how bins associated to larger received amplitudes are associated to lower sign error probability [13, 14]. Furthermore, the telescope gain can affect the sign error probability, and therefore the overall performance of the reconciliation scheme, and its value can be appropriately optimized.

In Reverse Reconciliation (RR), Bob uses FEC to correct the errors that exist between the sign of his samples and those of Alice. For Bob, the magnitude dependent sign error probability represents a Binary Symmetric Channel (BSC) that exists between himself and Alice for the collection of samples with magnitudes falling in prescribed windows. Hence, from Bob's perspective, the communication channel with Alice is composed of a collection of BSC with different error probabilities, on which an unequal error protection coding scheme could be applied, using the encoding schemes described in the section 4.

6. CONCLUSIONS

This paper summarizes the results obtained in the NATO SPS project "Analysis, design and implementation of an end-to-end 400 km QKD link", starting from the implementation of a long distance QKD link, the discussion on the use of Gaussian samples obtained from a free space optics CV-QKD link to implement a UEP-based IR scheme, to the discussion on the possible use of BCH and Polar FEC codes for information reconciliation.

7. ACKNOWLEGMENTS

We acknowledge funding from the following projects: NATO project SPS G5263, the project 19NRM06 METISQ (a project that received funding from the EMPIR program co-financed by the Participating States and from the European Union Horizon 2020 research and innovation program) and the ENYGMA project, financed by the Italian Ministry of Foreign Affairs and International Cooperation.

REFERENCES

[1] Clivati, C. et al., “Coherent phase transfer for real-world twin-field quantum key distribution”, arXiv:2012.15199.

[2] Georgieva, H. et al., “Detection of ultra-weak laser pulses by free- running single-photon detectors: modeling dead time and dark counts effects”, Appl. Phys. Lett. 118, p. 174002 (2021)

[3] Mondin, M., Delgado, M., Mesiti, F., Daneshgaran, F., “Soft-processing for Information Reconciliation in QKD Applications”, International Journal of Quantum Information, 9, 155-164, ISSN 0219-7499 (2011).

[4] Mondin, M., Daneshgaran, F., Bari, I., Delgado, M.T., Olivares, S., Paris, M.G.A., “Soft-Metric-Based Channel Decoding for Photon Counting Receivers”, IEEE Journal of Selected Topics in Quantum Electronics, 21(3), 6400407 (May/June 2015).

[5] Arikan, E., “Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels”, IEEE Transactions on Information Theory, 55(7), 3051-3073 (2009).

[6] Grosshans, F. , Van Assche, G., Wenger, J., Brouri, R., Cerf, N.J. and Grangier, P., "Quantum key distribution using gaussian-modulated coherent states," *Nature,* 421(6920), 238 (2003).

[7] Kupferman, J. and Arnon, S., “Zero-error attacks on a quantum key distribution FSO system,” OSA Continuum 1, no. 3, 1079-1086 (2018).

[8] Slepian. D., "Permutation modulation," Proceedings of the IEEE, 53(3), 228-236 (1965).

[9] Daneshgaran, F., Mondin M. and Olia, O., “Quantization of high dimensional Gaussian vector using permutation modulation with application to information reconciliation in continuous variable QKD,” International Journal of Quantum Information, 15(8), 1740028 (2017).

[10] Daneshgaran, F., Mondin M. and Olia, O., “Permutation modulation for quantization and information reconciliation in CV-QKD systems,” Quantum Communications and Quantum Imaging XV (2017).

[11] Daneshgaran, F., Mondin M., Arnon, S., Di Stasio, F. and Kupferman, J., “Information reconciliation (IR) for continuous variable quantum key distribution (QKD) over free space optics (FSO) channel,” Free-Space Laser Communications XXXI, 10910, p. 1091017, International Society for Optics and Photonics (2019).

[12] Daneshgaran, F., Di Stasio, F., Mondin, M., Arnon, S. and Kupferman, J., “System parameter optimization for minimization of sign error probability in free space optical CV-QKD,” Quantum Communications and Quantum Imaging XVII, 11134, p. 111340O (2019).

[13] Daneshgaran, F,, Mondin, M., Kupferman, J., Arnon, S., Genovese, M., Degiovanni, I.P., Meda, A., Di Stasio, F. and Bari, I., “Realistic QKD system hacking and security,” Quantum Communications and Quantum Imaging XVI, 10771, p. 107710T (2018).