IL NUOVO CIMENTO **45 C** (2022) 176
DOI 10.1393/ncc/i2022-22176-6

COMMUNICATIONS: SIF Congress 2021

Implementation and security analysis of continuous variable quantum secure direct communication protocols

I. PAPARELLE([1]), M. G. A. PARIS([2]) and A. ZAVATTA([3])

([1]) *Istituto Nazionale di Ottica (CNR-INO), Sezione di Trieste - Trieste, Italy*
([2]) *Dipartimento di Fisica Aldo Pontremoli, Università degli Studi di Milano - Milano, Italy*
([3]) *Istituto Nazionale di Ottica (CNR-INO) - Firenze, Italy*

received 31 January 2022

Summary. — The development of supercomputers and quantum computers will threaten current secure communication protocols. However, quantum mechanics offers a solution guaranteeing physical layer and provable security of communications. In particular, quantum secure direct communication (QSDC) allows secret messages to be directly and securely communicated over a quantum channel. We investigate implementations of continuous variable QSDC using single-mode squeezed coherent states, and state-of-the-art quantum optical technology. Indeed, the continuous variable regime can be well compatible with fully developed optical telecommunication technologies. The security of the protocols against different forms of attacks (*e.g.*, intercept-resend attack and collective attack) and against losses and noise is investigated, both analytically and numerically.

1. – Introduction

Secure communications are unsusceptible to eavesdropping or interception and can protect individual privacy as well as safety-critical public infrastructures. Mathematically proved security is too expensive, while the most common computational one is threatened by the development of supercomputers and quantum computers. Quantum mechanics offers instead physical layer security, regardless of the eavesdropper's computational capabilities, and it is of strategic importance today, such that it is encouraged by the European Commission [1].

One of the most mature quantum technologies for secure communication is quantum key distribution (QKD) [2-4]. On the other hand, quantum secure direct communication (QSDC) avoids the security loopholes of key storage and cyphertext attacks, by directly transmitting the message. QKD and QSDC can be implemented using discrete or continuous variables (DV or CV). CV do not need single photon source and/or detector and promise better performances for metropolitan networks, with current optical communication technology.

The goal of this work is to describe, improve and test security for two promising CV QSDC protocols.

2. – Quantum Secure Direct Communication with Continuous Variables

Coherent states are important states of light: their dynamics is resembling classical harmonic oscillators and they can easily be obtained with lasers, as in our protocols. They are described by complex numbers ($\alpha = |\alpha|e^{i\theta}$) that can be modified through displacement operations. Squeezing, instead, allows one to engineer the field uncertainty below the vacuum state noise on one canonical quadrature. These states and operations altogether with beam-splitter transformations can be described by the Gaussian formalism [5]. Homodyne detection allows us to measure quadratures providing the full characterization of the quantum state under investigation [6].

The protocols. The first protocol studied is inspired by [7]. In this scheme, Alice sends a message to Bob, while Eve tries to eavesdrop. First, Bob randomly chooses $2n$ complex numbers $\{z\}$ and $\{\alpha\}$, and creates n randomly squeezed coherent states, he then sends them to Alice through a quantum channel. Alice uses an optical switch to randomly divide these n states into two sets: one will be used as information support, the other to control the channel. She tells the position $\{t_i\}$ of the control mode states to Bob, classically, via a public channel. Bob reveals squeezing $\{z_i\}$ and displacement $\{\alpha_i\}$ of the control states to Alice, so that she can perform a homodyne measurement in the corresponding position/momentum quadrature on the control-mode states, and compare the result with what Bob told her, to obtain an estimate of the losses of the channel and to check for eavesdropping. If Alice obtains satisfying results, she encodes the message by applying displacements to part of the remaining states. The other remaining states are again used as control mode states, to check for Eve in the communication from Alice to Bob. Alice tells Bob which states contain the message. Bob checks the control mode states and then performs a homodyne measurement on the information support states, to get the message. This protocol is termed "symmetric" because both initial displacement and squeezing are applied by Bob and these features travel in both directions of the channel.

In the second protocol, referred to as "asymmetric", Alice applies random squeezing to the quantum states instead of Bob. This simplifies the protocol and makes the squeezing subject to the channel losses only once.

Attacks. We realistically focus on individual attacks, as joint attacks require long-lived quantum memories and the ability to perform coherent quantum operations with high fidelity. The no-cloning theorem allows us to exclude intercept-resend attacks [8]. However, Eve can use two beam-splitters to intercept the exchange of quantum states from Bob to Alice, and vice versa. With this approach, Eve does not directly modify the states and can be confused with losses. In fact, optical beam-splitters are used to model linear optical losses of any kind.

Analytical approach. The Wyner wire-tap channel model defines a quantity, secrecy capacity C_s, such that when $C_s > 0$, reliable transmission at a rate up to C_s is possible in approximately perfect secrecy ([9]). We calculate C_s using the Shannon-Hartley theorem and the tools from [10].

In both protocols, the secrecy capacity depends on the transmissivity of Eve's beam splitter η_E, the losses, the variance of the message and the squeezing parameter. Our results show that C_s is positive for $\eta_E > 0.5$ and, in this case, is greater for the asymmetric protocol, which should be preferred in applications. Moreover, the larger the squeezing, the larger the secrecy capacity and difference between the two protocols. Our results also show that C_s is larger for smaller losses and larger variance of the message.

Numerical simulations. The analytical is meaningful for a large set of samples, when

the concept of typical sequences is viable. Numerical simulations allow us to assess whether the analytical relations are still valid for a finite number of states. Moreover, we investigate in a concrete way how Eve and Bob can try to get the message from their measures. We use Python libraries and add the following parameters: the number of control states and the number of letters M (in case of a discrete alphabet). In fact, Alice can either discretize the possible displacements or use them as a continuum. In each case, we calculate the mean error both for Bob and Eve and, to mimic the secrecy capacity, we compute the difference. We consider the worst case scenario in which Eve knows the losses of the channel, and, for the asymmetric protocol, Bob's initial squeezing.

Bob's error is smaller for the asymmetric protocol and he makes less errors than Eve for $\eta_E \gtrapprox 0.5$, despite our unfavorable assumptions. For a discrete alphabet, the error increases when narrowing the bins corresponding to the discretization of the available displacement interval, instead with fixed bin length, there is slight improvement for large M. Concerning squeezing and losses, the analytical trends are confirmed.

3. – The experimental setup

In order to test the feasibility of the protocols, we reduce them to one by executing them without squeezing, which is indeed an expensive resource. For simplicity, instead of displacement, we use coherent states of different amplitudes $|\alpha|$.

Bob uses a continuous wave laser at 1550 nm and the whole protocol is implemented using the scheme depicted in fig. 1 with single mode optical fibers. The coherent states are laser pulses of 50 ns, sent with a repetition rate of 10 MHz.

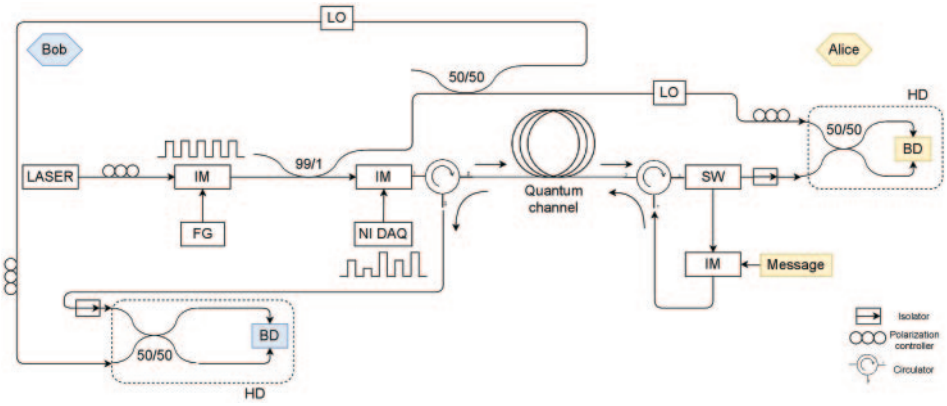

Fig. 1. – Bob creates pulses with an intensity modulator guided by a function generator. The necessary local oscillators for the two homodyne detectors are created with fiber couplers. A second intensity modulator implements the random initial displacements through the NIDAQ board (here squeezing is not considered); circulators allow propagating pulses along the quantum channel, then Alice divides the states with an optical switch to perform a homodyne measurement on the control states and implement the attenuation corresponding to the message on some of the others. The unmeasured pulses travel backwards, thanks to circulators. Bob performs a homodyne measurement to control the channel and read the message. IM (intensity modulator); GF (function generator); LO (local oscillator); SW (optical switch); NIDAQ (I/O board); HD (homodyne detection); BD (balanced detector).

We first tested the efficiency and the response of the balanced detectors by varying the local oscillator and α. Then, we read different messages from Bob's point of view, with different initial attenuations: the uncertainty of the measures is compatible with what Alice sent, and the uncertainty on the losses estimation. The next steps are implementing the squeezing resource and the phase stabilization control loop.

4. – Conclusions

We have studied a CV QSDC protocol assisted by quantum squeezing. The protocol has been analyzed from an analytical point of view, considering possible individual attacks and linear losses. The secrecy capacity of the Wyner's wiretap model shows the influence of different parameters on the security of the protocol. A new "asymmetric" scheme has been proposed, which improves the secrecy capacity of the overall protocol. Secondly, the two protocols have been simulated numerically, to test the analytical results on a limited number of states and understand how sender, receiver and wiretapper would concretely act. Numerical results confirm analytical findings. Then, we have implemented the experimental setup for the protocols, with wavelengths compatible with current optical telecommunications networks. The results are definitely encouraging, however there is still room for improvement concerning stability. Moreover, squeezing will be introduced as well as Eve's presence.

REFERENCES

[1] De Touzalin A., Marcus C., Heijman F., Cirac I., Murray R. and Calarco T., *Quantum Manifesto: A New Era of Technology* (European Commission) 2016, pp. 1–20.
[2] Cavaliere F., Prati E., Poti L., Muhammad I. and Catuogno T., *Quantum Rep.*, **2** (2020) 80.
[3] Pirandola S., Andersen U. L., Banchi L. *et al.*, *Adv. Opt. Photon.*, **12** (2020) 1012.
[4] Bacco D., Vagniluca I., Lio D. *et al.*, *EPJ Quantum Technol.*, **6** (2019) 5.
[5] Serafini A., *Quantum Continuous Variables: A Primer of Theoretical Methods* (CRC Press) 2017.
[6] Paris M. and Rehacek J., *Quantum State Estimation*, Vol. **649** (Springer Science & Business Media) 2004.
[7] Srikara S., Thapliyal K. and Pathak A., *Quantum Inf. Process.*, **19** (2020) 1.
[8] Chai G., Cao Z., Liu W., Zhang M., Liang K. and Peng J., *Laser Phys. Lett.*, **16** (2019) 095207.
[9] Wyner A. D., *Bell Syst. Tech. J.*, **54** (1975) 1355.
[10] Gallager R. G., *Information Theory and Reliable Communication*, Vol. **2** (Springer) 1968.