CV-MDI-QKD with coherent state: beyond one-mode Gaussian attacks

IOP SciNotes

ARTICLE

CV-MDI-QKD with coherent state: beyond one-mode Gaussian attacks

Carlo Ottaviani , Gaetana Spedalieri, Samuel L Braunstein and Stefano Pirandola

Department of Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, United Kingdom

E-mail: carlo.ottaviani@york.ac.uk

Keywords: quantum information, quantum cyrptography, quantum continuous variables, measurement-device independent quantum cryptography

OPEN ACCESS

RECEIVED
30 March 2020

REVISED
5 May 2020

ACCEPTED FOR PUBLICATION
13 May 2020

PUBLISHED
21 July 2020

Abstract

A general security proof of continuous variable (CV) measurement device independent (MDI) quantum key distribution (QKD) should not be automatically reduced to the analysis of one-mode Gaussian attacks (in particular, independent entangling-cloner attacks). To stress this point, the present work provides a very simple (almost trivial) argument, showing that there are an infinite number of two-mode Gaussian attacks that cannot be reduced to or simulated by one-mode Gaussian attacks. This result further confirms that the security analysis of CV-MDI-QKD must generally involve a careful minimization over two-mode attacks as originally performed in (Pirandola *et al*, 2015 *Nature Photon.* **9**, 397–402; arXiv:1312.4104 (2013)).

1. Introduction

Measurement-device-independent quantum key distribution MDI-QKD [1, 2] promises to be a remarkably effective solution for the practical implementation of the next generation of QKD infrastructures, in which privacy should be granted over a quantum network. In MDI-QKD the authorized users of the network, Alice and Bob, exploit a swapping-like protocol where secret correlations are established by the measurement of a third untrusted party, the relay [1, 3–6]. This performs a Bell measurement but, in order to achieve security, it is not required to pass a Bell test. By contrast, in full device independent QKD [7, 8], the privacy of the shared key depends on passing a Bell test, which is still an operation performed with very poor success rates [9–11]. The power of the MDI approach relies indeed on its practicality: One can achieve high-rate side-channel-free unconditionally secure network communication.

In recent years the study of QKD protocols [12] based on quantum continuous variables (CVs) [13] has attracted increasingly attention because of several appealing properties of CV systems: Protocols use bright coherent states, and exploit standard telecommunication technologies; in particular coherent detection techniques, already developed for classical optical communication [14]. In addition, CV-QKD is interesting for the relatively simple implementation of protocols at different frequencies [15, 16]. Finally, exploiting CV point-to-point protocol with state-of-the-art classical reconciliation and error correction schemes [17–19] allowed the implementation CV-QKD in laboratory over a distance of 80 Km [20]. After this work, several other experimental realizations have shown progress for integrated miniaturization [21] and implementation of long-distance communication [22, 23]. The high rate performance of CV-QKD is not so far from the secret key capacity of the lossy channel, also known as PLOB bound [24, 25], which is achievable by a CV-QKD protocol based on the reverse coherent information [26].

In 2013 we proposed a CV-MDI-QKD protocol, which we have also successfully tested in a proof-of-principle experiment [3]. In particular, we proved that our scheme is capable of remarkably high key-rates per use of the communication channel, over the length of metropolitan range distances. This performance is sensibly higher than implementations based on discrete variables [27]. We therefore believe that CV-QKD will play a crucial role in future implementation of metropolitan quantum cryptography. At this scale, in fact, both

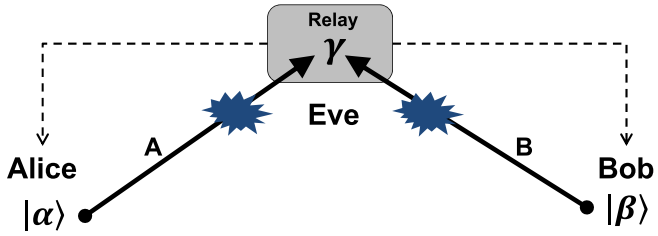

Figure 1. Basic protocol of CV-MDI-QKD. Alice and Bob encode information by modulating the amplitude of coherent states, which are sent to an untrusted intermediate station. The relay detects the incoming signals by performing a Bell measurement whose outcome γ is broadcast to the parties. The knowledge of γ allows Alice and Bob to determine the amplitude of the other honest party, by post-processing γ and the amplitudes (α and β) in their hands.

high density of untrusted nodes and high rates should be considered nonnegotiable properties, if we want a quantum network able of competing with present classical infrastructure.

In this work we provide a further discussion on the security analysis of CV-MDI-QKD given in [3, 4]. We show, by simple arguments, that the security analysis restricted to one-mode Gaussian (entangling-cloner) attacks can only account for a subclass of all possible eavesdropping strategies. In particular we provide a counterexample in order to explicitly prove that, if we model Eve's attack assuming a restricted strategy, based on independent entangling cloners, one cannot generate all the possible covariance matrices shared between Alice and Bob. Our analysis confirms that a complete security analysis of CV-MDI-QKD cannot indeed avoid to consider two-mode Gaussian attacks, as originally done in [3, 4].

The structure of the paper is the following. In section 2 we present the protocol. Section 3 gives general consideration about the security analysis, marking the difference between theoretical and experimental analyses. Section 4 provides a simple counter example to the (wrong) assumption that an attack by independent entangling cloners would be complete. Finally, section 5 is for our conclusions.

2. Description of the protocol

We start with a brief description of the protocol [3]. At one side, Alice prepares a mode A in a coherent state $|\alpha\rangle$ whose amplitude α is modulated by a Gaussian distribution with zero mean and large variance. At the other side, Bob prepares his mode B in another coherent state $|\beta\rangle$ whose amplitude β is modulated by the same Gaussian distribution as Alice. Modes A and B are then sent to an intermediate relay where a CV Bell detection is performed. The classical outcomes are combined in a complex variable γ, which is communicated to Alice and Bob via a public channel. As a result, knowledge of γ enables each party to infer the variable of the other party by simple post-processing (see figure 1).

In general, the relay is assumed to be untrusted [1], i.e., operated by Eve, and also the links with the relay are subject to eavesdropping. The protocol is assumed to be performed many times, so that the honest parties collect a large amount of classical data (we consider asymptotic security here). Using several tools, including de Finetti arguments and the extremality of Gaussian states (see [3] for more details), one can reduce the security analysis to considering a two-mode Gaussian attack against the two links with the relay (performing a proper CV Bell detection). This type of attack can be constructed by suitably combining two canonical forms [28] into a correlated-noise Gaussian environment. The most relevant canonical forms are clearly the lossy channels.

In this scenario, the two modes A and B are mixed with two ancillary modes, E_1 and E_2, by two beam splitters with transmissivities τ_A and τ_B, respectively. These ancillary modes belong to a reservoir of ancillas (E_1, E_2 plus an extra set $\mathbf{e}$) in a pure Gaussian state. The reduced state $\sigma_{E_1E_2}$ is a correlated thermal state with zero mean and covariance matrix (CM) in the normal form

$$\boldsymbol{\sigma}_{E_1E_2} = \begin{pmatrix} \omega_A \mathbf{I} & \mathbf{G} \\ \mathbf{G} & \omega_B \mathbf{I} \end{pmatrix}, \quad \mathbf{G} := \begin{pmatrix} g & 0 \\ 0 & g' \end{pmatrix}, \tag{1}$$

where ω_A, $\omega_B \geqslant 1$ are the variances of the thermal noise affecting each link, while g and g' are correlation parameters, satisfying suitable physical constraints [29, 30]. After interaction, Eve's ancillas are stored in a quantum memory, measured at the end of the protocol (see figure 2).

In order to deal with the joint attack, Alice and Bob must retrieve the joint statistics of the variables α, β, and γ. For this purpose, they publicly compare a small part of their data and reconstruct the probability distribution $p(\alpha, \beta, \gamma)$. The empirical values of the transmissivities τ_A and τ_B are accessible to the parties from the first-order

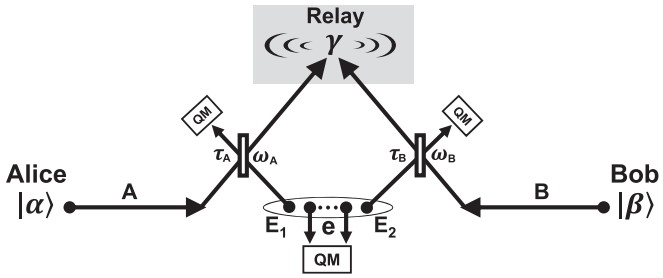

Figure 2. Two-mode Gaussian attack against CV-MDI-QKD. Figure adapted from [3]. The traveling modes A and B interact with ancillary modes E_1 and E_2. The links to the relay are described by beam splitters with transmissivities $\tau_{A,B}$ and thermal noise $\omega_{A,B}$. Modes E_1 and E_2, together with the general set of additional modes $\mathbf{e}$, describe the reservoir of ancillas $\{E_1, E_2, \mathbf{e}\}$ controlled by the eavesdropper. Modes E_1 and E_2 are quantum-correlated, while the global ancillary quantum state $\rho_{E1,E2,\mathbf{e}}$ is pure and Gaussian. Eve's output ancillary modes are stored in a quantum memory (QM), measured at the end of the protocol.

moments of $p(\alpha, \beta, \gamma)$. Knowing these values is essential in order to apply the correct post-processing and re-scaling of the output data. Then, from the second-order moments of $p(\alpha, \beta, \gamma)$, Alice and Bob can extract the CM $\mathbf{V}_{ab|\gamma}$ that they would share in an equivalent entanglement-based representation of the protocol [31] and conditioned to the outcome γ of the Bell detection at the relay (see [3] for more details). From this shared post-relay CM, they can derive the secret-key rate of the protocol.

3. General considerations on the security analysis

It is important to note that, once the shared CM $\mathbf{V}_{ab|\gamma}$ is reconstructed by Alice and Bob, the secret-key rate can be (numerically) computed no matter what the actual eavesdropping strategy was. In fact, it is sufficient to consider the purification of the state $\rho_{ab|\gamma}$ into an environment which is assumed to be fully controlled by Eve. This is a pretty standard method in CV-QKD.

However, while this approach is valid for experimental demonstrations, it is generally not sufficient for deriving analytic expressions of the key rate R, just because there are too many free parameters in the CM. Having simple analytic expressions is crucial in order to theoretically compare the performances of different QKD protocols. The next theoretical step is therefore the reduction of the free parameters to a minimum set which is accessible to the parties and that allows us to write a closed formula for R (or a lower-bound to R).

It is typical to derive a single quantifier of the noise, the so-called 'excess noise' ε, to be associated to the observed values of the transmissivities τ_A and τ_B. Such a reduction is the non-trivial part of the theoretical analysis since it requires a minimization of the rate with respect to all degrees of freedom of Eve, once that the triplet τ_A, τ_B, and ε has been fixed. One important pre-requisite for such a reduction is the correct modelling of the most general attack that Eve can perform against the protocol. The entire 'space of the attacks' must be covered in this analysis. As pointed out in [3], CV-MDI-QKD requires the explicit consideration of all two-mode Gaussian attacks, not just one-mode Gaussian attacks, where $g = g' = 0$. The latter class is in fact restricted and can only lead to partial security proofs.

4. Simple counter-example to one-mode attacks

Here we easily show that one-mode Gaussian attacks represent a restricted class and, therefore, a security proof of CV-MDI-QKD based on these attacks can only be partial. Furthermore, since they form a restricted class, it does not make sense to claim their optimality.

For the sake of simplicity, consider the symmetric configuration [4], where Alice's and Bob's channels are identical lossy channels, with the same transmissivity τ. Extension to asymmetric configurations is just a matter of technicalities. After the action of the relay, the shared CM of Alice and Bob is simply given by [3]

$$\mathbf{V}_{ab|\gamma} = \begin{pmatrix} \mu\mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mu\mathbf{I} \end{pmatrix} - (\mu^2 - 1)\tau \begin{pmatrix} \frac{1}{\theta} & 0 & -\frac{1}{\theta} & 0 \\ 0 & \frac{1}{\theta'} & 0 & \frac{1}{\theta'} \\ -\frac{1}{\theta} & 0 & \frac{1}{\theta} & 0 \\ 0 & \frac{1}{\theta'} & 0 & \frac{1}{\theta'} \end{pmatrix}, \tag{2}$$

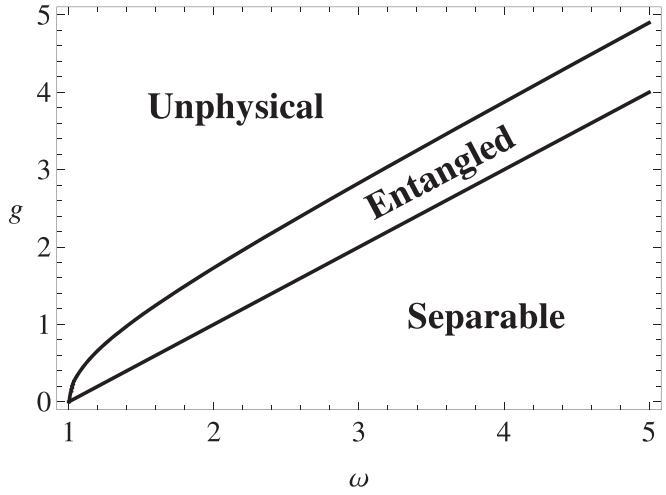

Figure 3. Correlation parameter g versus thermal noise ω. For any value of ω, two-mode attacks with $0 \leqslant g \leqslant \omega - 1$ are performed with separable ancillas, while two-mode attacks satisfying the stronger condition of equation (6) have entangled ancillas and cannot be simulated by one-mode attacks. Values of g above $\sqrt{\omega^2 - 1}$ are prohibited by quantum mechanics.

where

$$\theta \coloneqq 2[\tau\mu + (1 - \tau)x], \quad \theta' \coloneqq 2[\tau\mu + (1 - \tau)x']. \tag{3}$$

with

$$x = \frac{\omega_A + \omega_B}{2} - g, \quad x' = \frac{\omega_A + \omega_B}{2} + g'. \tag{4}$$

In the previous CM, the modulation parameter μ is known to Alice and Bob, and also the transmissivity τ which is derived by comparing the shared data and computing the first-order moments. By contrast, Alice and Bob do not directly access the values of the thermal noise and the correlation parameters, since they are combined in the x-parameters of equation (4)). The fact that the parameters ω_A, ω_B, g and g' get scrambled in x and x' has led some authors [32] to claim that one-mode attacks ($g = g' = 0$) with suitable values of the thermal noise (ω_A and ω_B) could simulate any two-mode attack with arbitrary ω_A, ω_B, g, and g'. However, this is not the case.

To understand this point, it is important to note that the components of the CM $\mathbf{V}_{ab|\gamma}$ are monotonic in x and x'. As an example, the top-left component

$$\mathbf{V}_{11} = \mu - \frac{(\mu^2 - 1)\tau}{2[\tau\mu + (1 - \tau)x]} \tag{5}$$

is increasing in x, so that $\mathbf{V}_{11}$ is minimum when x is minimum. In the case of one-mode attacks ($g = g' = 0$), we have $x \geqslant 1$. It is therefore clear that any two-mode attack such that $x < 1$ cannot be simulated by one-mode attacks. Indeed there is an infinite number of such two-mode attacks. In fact, let us assume that Eve performs a two-mode attack with $\omega_A = \omega_B = \omega$ and $g' = -g$. In this case, we have $x = x' = \omega - g$, and the condition $x < 1$ corresponds to imposing

$$\omega - 1 < g \leqslant \sqrt{\omega^2 - 1}\,, \tag{6}$$

in which case Eve's ancillas are entangled [30].

Thus, for any value of ω, we can pick an entangled two-mode attack which cannot be simulated by one-mode attacks. In other words, this entangled attack generates a shared CM $\mathbf{V}_{ab|\gamma}$ which does not belong to the set of possible CMs associated with one-mode attacks. As depicted in figure 3, there is an infinite number of entangled attacks which cannot be reduced to one-mode attacks.

One may attempt to enlarge the set of one-mode attacks by allowing for squeezed thermal noise, i.e., the use of thermal states with asymmetric variances, ω_A^q for the q-quadrature and ω_A^p for the p-quadrature (and similarly, ω_B^q and ω_B^p, for the other ancilla). In this case, equation (4) for one-mode attacks would become

$$x = \frac{\omega_A^q + \omega_B^q}{2}, \quad x' = \frac{\omega_A^p + \omega_B^p}{2}. \tag{7}$$

However, since $\omega_A^q \omega_A^p \geqslant 1$ and $\omega_B^q \omega_B^p \geqslant 1$, it is easy to check that realizing $x < 1$ would imply $x' > 1$, and vice versa. As a result, there will always be components in the shared CM $\mathbf{V}_{ab|\gamma}$ whose values, for entangled attacks, cannot be realized by assuming one-mode attacks.

5. Conclusion

We have considered the security analysis of CV-MDI-QKD. We have explicitly shown that one-mode Gaussian (entangling-cloner) attacks represent a restricted class, which cannot generate all the possible shared CMs for Alice and Bob. This is true for any fixed value of the transmissivity τ for the two lossy channels (extension to different transmissivities τ_A and τ_B is trivial). This very simple result confirms the necessity of explicitly studying two-mode Gaussian attacks in a general security analysis of CV-MDI-QKD, as originally considered in [3].

Note that the advantage of using attacks based on correlated ancillas has been also discussed for two-way protocols [33, 34]. In that case the honest parties have to resort to additional strategies to re-establish security, as described in [35].

Acknowledgments

This work has been supported by the EPSRC 'UK Quantum Communications HUB' (EP/M013472/1, EP/T001011/1).

Data availability statements.

Any data that support the findings of this study are included within the article.

ORCID iDs

Carlo Ottaviani https://orcid.org/0000-0002-0032-3999
Stefano Pirandola https://orcid.org/0000-0001-6165-5615

References

[1] Braunstein S L and Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502
[2] Lo H-K *et al* 2012 *Phys. Rev. Lett.* **108** 130503
[3] Pirandola S *et al* 2015 *Nature Photon* **9** 397–402 See also arXiv:1312.4104 (2013).
[4] Ottaviani C, Spedalieri G, Braunstein S L and Pirandola S 2015 *Phys. Rev.* A **91** 022320
[5] Li Z, Zhang Y-C, Xu F, Peng X and Guo H 2014 *Phys. Rev.* A **89** 052301
[6] Zhang Y-C, Li Z, Yu S, Gu W, Peng X and Guo H 2014 *Phys. Rev.* A **90** 052325
[7] Ekert A 1991 *Phys. Rev. Lett.* **67** 661
[8] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
[9] Vazirani U and Vidick T 2014 *Phys. Rev. Lett.* **113** 140501
[10] Colbeck R 2014 *Physics* **7** 99
[11] Hensen B *et al* 2015 *Nature* **526** 682 See also preprint arXiv:1508.05949, (2015).
[12] Pirandola S *et al* 2019 arXiv:1906.01645
[13] Diamanti E and Leverrier E 2015 *Entropy* **17** 6072
[14] Ralph T C and Lam P K 2009 *Nature Phot* **3** 671–3
[15] Weedbrook C, Ottaviani C and Pirandola S 2014 *Phys. Rev.* A **89** 012309
[16] Usenko V C and Filip R 2016 *Entropy* **18** 20
[17] Leverrier A *et al* 2008 *Phys. Rev.* A **77** 042325
[18] Jouguet P, Kunz-Jacques S and Leverrier A 2011 *Phys. Rev.* A **84** 062317
[19] Zhou C, Wang X, Zhang Y, Zhang G, Yu S and Guo H 2019 *Phys. Rev. Applied* **12** 054013
[20] Jouguet P *et al* 2013 *Nat. Photonics* **7** 378–81
[21] Zhang G *et al* 2019 *Nat. Photon.* **13** 839
[22] Zhang Y *et al* 2019 *Quantum Sci. and Tech.* **4** 035006
[23] Zhang Y-C, Chen Z, Pirandola S, Wang X, Zhou C, Chu B, Zhao Y, Xu B, Yu S and Guo H 2020 *Phys. Rev. Lett.* **125** 010502 arXiv:2001.02555
[24] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2015 *Nat. Commun.* **8** 15043 See also arXiv:1510.08863 (2015).
[25] Pirandola S, Braunstein S L, Laurenza R, Ottaviani C, Cope T P W, Spedalieri G and Banchi L 2018 *Quantum Science and Technology* **3** 035009
[26] Pirandola S, García-Patrón R, Braunstein S L and Lloyd S 2009 *Phys. Rev. Lett.* **102** 050503
[27] Pirandola S *et al* 2015 *Nat. Photonics* **9** 773–5
[28] Weedbrook C *et al* 2012 *Rev. Mod. Phys.* **84** 621
[29] Pirandola S, Serafini A and Lloyd S 2009 *Phys. Rev.* A **79** 052327
[30] Pirandola S 2013 *New J. Phys.* **15** 113046

[31] In an entanglement-based representation, Alice has an EPR state [28] ρ_{aA} of modes a and A. By heterodyning mode a, she probabilistically prepares coherent states on mode A. Similarly, Bob has another EPR state ρ_{bB}.
[32] Ma X-C private communication
[33] Ottaviani C, Mancini S and Pirandola S 2017 *Phys. Rev.* A **95** 052310
[34] Ottaviani C, Mancini S and Pirandola S 2015 *Phys. Rev.* A **92** 062323
[35] Ottaviani C and Pirandola S 2016 *Sci. Rep.* **6** 22225