On the contribution of detector's noise and efficiency to the security of Gaussian modulated continuous-variable quantum key distribution

Maron Freitas Anka[1*], Alexandre Baron Tacla[1]
[1] *QuIIN - Quantum Industrial Innovation, EMBRAPII CIMATEC Competence Center in Quantum Technologies, SENAI CIMATEC, Av. Orlando Gomes 1845, Salvador, BA, Brazil, CEP 41650-010.*
**maron.anka@fbest.org.br*

Abstract: Quantum key distribution (QKD) protocols rely on the exchange of information encoded in quantum states of light to generate a secure symmetric cryptographic key between two honest parties, the sender, Alice, and the receiver, Bob. In order for communication to be secure, one needs to consider that a third untrusted entity, Eve, may try to eavesdrop the communication. The usual pessimistic approach in QKD protocols assumes that all noise sources and losses of information are due to the presence of an eavesdropper. However, in a trusted device scenario, one can loosen this assumption by considering that Bob has full control of his lab, which, in principle, is isolated from Eve. In the so-called trusted-noise model, one assumes that Bob's detector noise and efficiency are not influenced by Eve's attempts to gain information. Compared to the case of untrusted noise sources, Eve's knowledge about Alice and Bob's communication is reduced, which in turn allows for higher secret key rates and improves the overall performance of the protocol. In this work, we explore the role of Bob's detector noise and efficiency in the performance of Gaussian modulated continuous-variable quantum key distribution for both homodyne and heterodyne detections. We analyze the numerical results of this model in comparison to the pessimistic case, searching for regimes where considerable gain is achieved. We also investigate the influence of such trusted parameters in the information reconciliation process efficiency and maximum value of tolerable excess noise.

Keywords: continuous-variable, quantum key distribution, trusted noise, Gaussian modulation.

1. Introduction

One of today's most important applications of quantum information and communication science is quantum key distribution (QKD), a protocol that enables two remote parties, Alice and Bob, to establish secure secret cryptographic keys by transmitting information via quantum states [1,2]. The security of such protocols relies on the fundamental principles of quantum mechanics [1-3]. Any attempt by an eavesdropper, usually called Eve, to intercept information inevitably leads to information leakage, which disturbs the system and typically introduces noise. However, this additional noise makes Eve's presence detectable, thereby exposing potential security breaches in the protocol. The security proof in QKD allows one to quantify the maximum amount of information that Eve can potentially acquire through her attack during the protocol. This quantity allows Alice and Bob to determine how much information must be removed from their correlated data to generate a provably secure secret key. In general, higher noise levels indicate an increased potential information leakage to Eve, thus reducing the final secret key length [4]. The usual pessimistic approach assumes that all noise sources are due to Eve's attack, therefore all noise is considered to be untrusted. While Eve's power is fundamentally limited by quantum mechanics, her effective power also depends on one's assumptions about her technological abilities. This complete untrusted noise assumption may overestimate her potential information and reduce the protocol performance.

In experimental implementations, no device is free from imperfections. In a trusted device scenario, one may find reasonable to assume that Eve has no access to all noise sources.

In this so-called *trusted noise model* of QKD, one may assume, for instance, that Bob's lab is isolated from Eve [5]. Within this assumption, the detector's noise and efficiency may be excluded from the total excess noise attributed to Eve, which, in turn, leads to higher secret key rates.

In this work, we explore the influence of such trusted noise parameters in Gaussian-modulated (GM) continuous-variables (CV) QKD protocols. This family of QKD protocols emerged as promising alternatives to avoid technological difficulties of working with discrete-variables systems, such as single photon detection. CV-QKD offers practical advantages, such as compatibility with standard optical telecommunication components (e.g. commercial lasers and coherent receivers) and photonic integrated circuits. This compatibility allows for miniaturization, cost reduction, and potentially higher secret key rates. However, these benefits come at the expense of more complex security proofs and greater sensitivity to noise [1,2].

Here, we study such protocols under the assumption of trusted noise model, with the goal of quantifying the consequent increase in performance. We explore the regimes where the two main GM-CV-QKD protocols, the GG02 [6] and No-switching [7], can achieve considerable gains over the untrusted model case.

2. CV-QKD protocol

There are two equivalent scenarios in a CV-QKD, the prepare-and-measure (PM) and entanglement-based (EB) protocols. While the first approach guides experimental implementation, the second is more convenient for security analysis [4].

2.1. Step-by-step description

A generic PM GM CV-QKD protocol can be divided into the following steps:

1. **State preparation**: Alice encodes classical variables in the quadrature components q and p, sampled from two independent and identically distributed (i.i.d) Gaussian distributions, each with zero mean and modulation variance $\boldsymbol{V_{Mod}}$, i.e., $\boldsymbol{\mathcal{N}(0, V_{Mod})}$. Alice then prepares the coherent states $|\boldsymbol{\alpha_k}\rangle = |\boldsymbol{q_k + ip_k}\rangle$, where $\boldsymbol{\alpha_k = q_k + ip_k}$ is the complex amplitude in phase space, with total symmetric variance of each state given by $\boldsymbol{V_q = V_p =: V =: V_{Mod} + 1 = 2 < n > +1}$, where the vacuum fluctuations is normalized to 1 in shot-noise units (SNU).
2. **Transmission**: The states are sent from Alice to Bob through an untrusted Gaussian quantum channel, which is assumed to be fully controlled by Eve. This channel is completely characterized by two parameters: the transmittance $\boldsymbol{T}$ and the excess noise $\boldsymbol{\xi}$.
3. **Detection**: After receiving the channel output signals, Bob can either perform a homodyne detection to randomly measure

one of the quadratures (GG02 protocol), or a heterodyne detection (No-switching protocol) to measure both quadratures simultaneously.

4. **Post-processing**: At this stage, the trusted parties possess a correlated database of prepared and detected random variables (corresponding to asymmetric and insecure raw keys). To ensure a shared secure symmetric key, Alice and Bob must perform a series of classical post-processing procedures, which involves using an authenticated public classical channel. The first step is parameter estimation, where Alice and Bob use part of their data to estimate $\boldsymbol{T}$ and $\boldsymbol{\xi}$. These parameters can be used to define an upper limit of information that may have leaked to Eve. The following step consists of the information reconciliation process. In this stage, sophisticated error correction algorithms are applied to make the remaining of the raw key symmetric. If Alice is chosen to send information to Bob through the classical channel, this process is called direct reconciliation (DR). Otherwise, Bob serves as the reference and the process is referred to as reverse reconciliation (RR). While DR is limited to a maximum transmission corresponding to 3 dB of loss [8], the reverse process does not present a similar limitation and offers better performance. Finally, they perform privacy amplification (using hash functions) to reduce the key length in order to eliminate the amount of information that Eve may have learned about the generated key [2]. The result is a secure symmetric key.

2.2. Covariance matrix

Quantum systems with continuous-variable are described by an infinity dimension Hilbert space [1]. In particular, Gaussian states can be fully characterized by the two first statistic moments of the field quadratures, i.e., the mean value and the covariance matrix.

In the case of PM GM protocols, Alice prepares her coherent states according to a Gaussian probability distribution with zero mean and variance $\boldsymbol{V_A = V_{Mod}}$. Bob will receive coherent states with variance $\boldsymbol{V_B = V_{Mod} + 1}$ due to the minimal uncertainty of 1 (in shot-noise units). One can show that the covariance matrix describing this system is given by

$$\boldsymbol{\Sigma_{PM}} = \begin{bmatrix} \boldsymbol{V_{Mod}I} & \boldsymbol{V_{Mod}I} \\ \boldsymbol{V_{Mod}I} & \boldsymbol{(V_{Mod}+1)I} \end{bmatrix},$$

where I = diag(1,1).

In the entanglement-based (EB) scenario, one can define an equivalent protocol to simplify the security analysis. This is done by first purifying Alice's overall state, which is a Gaussian mixture of coherent states. One can achieve this by assuming that Alice prepares an entangled two-mode squeezed vacuum state (TMSVS). Alice then keeps one of the two modes and sends the other to Bob through the quantum channel. The TMSVS is represented by the covariance matrix

$$\boldsymbol{\Sigma_{EB}} = \begin{bmatrix} \boldsymbol{V\,I} & \sqrt{\boldsymbol{(V^2-1)}}\boldsymbol{\sigma_z} \\ \sqrt{\boldsymbol{(V^2-1)}}\boldsymbol{\sigma_z} & \boldsymbol{V\,I} \end{bmatrix},$$

where $\boldsymbol{\sigma_z} = \boldsymbol{diag(1,-1)}$. To collapse Bob's mode into a coherent state, Alice performs a heterodyne detection on her mode (a homodyne detection would lead Bob's mode to a squeezed state) [4]. The covariance matrix of the shared TMSVS after the heterodyne detection is modified to [4]

$$\boldsymbol{\Sigma'_{EB}} = \begin{bmatrix} \frac{\boldsymbol{V+1}}{\boldsymbol{2}}\,\boldsymbol{I} & \sqrt{\frac{\boldsymbol{1}}{\boldsymbol{2}}\boldsymbol{(V^2-1)}}\boldsymbol{\sigma_z} \\ \sqrt{\frac{\boldsymbol{1}}{\boldsymbol{2}}\boldsymbol{(V^2-1)}}\boldsymbol{\sigma_z} & \boldsymbol{V\,I} \end{bmatrix}.$$

In a practical realistic scenario, where Alice modulates coherent states instead of measuring one mode of a TMSVS, she can rescale the values of the prepared quadratures to simulate an entanglement-based case:

$$\boldsymbol{q_A^{EB}} = \sqrt{\frac{\boldsymbol{V+1}}{\boldsymbol{2(V-1)}}}\boldsymbol{q_A^{PM}},$$

$$\boldsymbol{p_A^{EB}} = -\sqrt{\frac{\boldsymbol{V+1}}{\boldsymbol{2(V-1)}}}\boldsymbol{p_A^{PM}}.$$

The result of such rescale leads to an equivalence between the P&M and EB scenarios: $\boldsymbol{\Sigma_{PM}} = \boldsymbol{\Sigma'_{EB}}$. Thus, Alice can simulate the EB protocol without Bob or Eve noticing.

3. Security analysis

The performance of CV-QKD protocols is measured by the secret key rate (SKR), which quantifies the amount of secure bits generated in a given protocol, after many rounds of the steps described in section 2.1. In the asymptotic regime, where no finite-size statistical effects are considered, the SKR can be written as [9]:

$$K = \beta I(A:B) - \chi_{E:B},$$

where β is the reconciliation efficiency, $I(A:B)$ is the classical mutual information between the classical variables of Alice and Bob, and $\chi_{E:B}$is the Holevo information, which quantifies Eve's information. Here we assume RR.

The mutual information is computed from the maximum channel capacity value of an Additive White Gaussian Noise (AWGN) channel. In this limit, the mutual information is given by

$$I(A:B) = \frac{\mu}{2}\log_2(1-SNR),$$

where $\mu = 1(2)$ represents the homodyne (heterodyne) detection. SNR stands for signal-to-noise ratio, and it is defined here as

$$SNR = \frac{T\boldsymbol{V_{Mod}}}{\mu + T\,\xi}.$$

The Holevo information can be obtained from the symplectic eigenvalues of the covariance matrix after the transmission. In this case, considering the transmission effects and excess noise, the covariance matrix takes the following form

$$\boldsymbol{\Sigma_{AB}} = \begin{bmatrix} \Sigma_A & \sigma_{AB} \\ \sigma_{AB} & \boldsymbol{\Sigma_B} \end{bmatrix},$$

where $\Sigma_A = V\mathrm{I}$ and $\Sigma_B = T(V+\chi)\mathrm{I}$, with $\chi = 1/T - 1 + \xi$, stand for the states quadratures variance of Alice and Bob, while $\sigma_{AB} = \sqrt{T(V^2-1)}\sigma_z$ represents the correlation between them. The transmittance is defined as $T = \eta T_{ch}$, where η is the detector's efficiency and $T_{ch} = 10^{-\gamma d/10}$ is the transmittance of the quantum channel, with $\gamma = 0.2dB/km$ for a standard fiber and d is the transmission distance. Assuming that the global state is pure, we can write the Holevo information as

$\chi_{E:B} = S(\rho_E) - S(\rho_{E|B}) = S(\rho_{AB}) - S(\rho_{A|B})$,

where $S(\rho_{AB})$ is the von Neumann entropy of Alice and Bob state and $S(\rho_{A|B})$ is the entropy of the same state after the homodyne (or heterodyne) detection. For Gaussian systems, the von Neumann entropy can be written as $S(\rho) = \sum_i^N g(\nu_i)$, with

$g(\nu_i) = \left(\frac{\nu_i + 1}{2}\right) log_2\left(\frac{\nu_i + 1}{2}\right) - \left(\frac{\nu_i - 1}{2}\right) log_2\left(\frac{\nu_i - 1}{2}\right)$,

where ν_i are the symplectic eigenvalues of the covariance matrix.

In the untrusted noise model, where all noise source is attributed to Eve, the Holevo information is simply given by $\chi_{E:B} = g(\nu_1) + g(\nu_2) - g(\nu_3)$, where $\nu_{1,2} = \sqrt{\frac{1}{2}(A \pm \sqrt{A^2 - 4B})}$, with $A = det(\Sigma_A) + det(\Sigma_B) + 2\,det(\sigma_{AB})$ and $B = det(\Sigma_{AB})$. The third eigenvalue is $\nu_3 = \sqrt{V\left(V - \frac{{Z_G}^2}{T(V+\chi)}\right)}$ for homodyne detection and $\nu_3 = V - \frac{{Z_G}^2}{T(V+\chi)+1}$ for heterodyne detection. Here, we defined $Z_G := \sqrt{T(V^2 - 1)}$ as the correlation function between Alice and Bob variables.

In the trusted noise model, we split the detector's noise contribution apart from the total excess noise ξ. Therefore, we rewrite the noise from the channel as $\chi_{ch} = 1/T - 1 + \xi$, where ξ represents the total noise from all sources except Bob's detector, and, as usual, it is associated with Eve. The total noise originating from Bob's lab is defined as

$\chi_{det} = \begin{cases} \chi_{hom} = (1 - \eta + \xi_{el})/\eta \\ \chi_{het} = (2 - \eta + 2\xi_{el})/\eta \end{cases}$, where ξ_{el} is the electronic noise from Bob's detector and η is the detector's efficiency as usual. The total noise is then defined as $\chi = \chi_{ch} + \frac{\chi_{det}}{T_{ch}}$. The mathematical derivation of such results is beyond the scope of this work. We refer the reader to Ref.[10] for more details. However, in Fig.1, we reproduce the schematic model of such protocol in the EB scenario for the GG02 protocol.

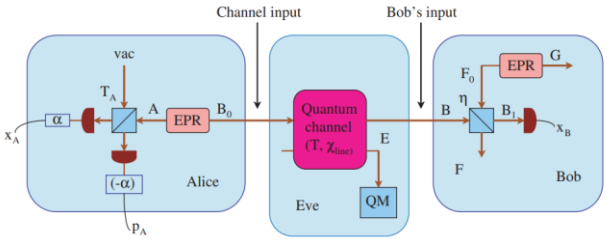

Fig.1: EB GG02 protocol in the trusted-noise model. Figure removed from [10].

In this case, Alice keeps one of the two modes of the TMSVS (EPR state in Fig. 1) to herself (A) and performs a heterodyne detection, collapsing Bob's mode (B_0) to a coherent state. After interacting with the quantum channel, the mode is modified to B. At Bob's lab, an extra setup is implemented. It consists of another TMSVS, with modes F_0 and G, which simulates the detector's noise, and a beam splitter that simulates the detector's efficiency. Bob performs a homodyne detection on the output mode B_1.

The final result is the Holevo information with the following form: $\chi_{E:B} = \sum_1^2 g(\nu_i) - \sum_3^5 g(\nu_i)$, where ν_1 and ν_2 have the same form as before, but are now computed from the modified covariance matrix such that $\Sigma_B = T(V + \chi_{ch})\mathrm{I}$, without the detector's noise contribution. The other eigenvalues are given by $\nu_{3,4} = \sqrt{\frac{1}{2}(C \pm \sqrt{C^2 - 4D})}$ and $\nu_5 = 1$, where

$$C_{hom} = \frac{A\,\chi_{hom} + T_{ch}(V + \chi_{ch}) + V\sqrt{B})}{(T_{ch}(V + \chi))^2},$$

$$D_{hom} = \sqrt{B}\,\frac{V + \chi_{hom}\sqrt{B}}{T_{ch}(V + \chi)},$$

$$C_{het} = \frac{A\,{\chi_{het}}^2 + B + 1 + 2\chi_{het}(V\sqrt{B} + T(V + \chi_{ch}) + 2{Z_G}^2)}{(T_{ch}(V + \chi))^2},$$

$$D_{het} = \left(\frac{V + \chi_{het}\sqrt{B}}{T_{ch}(V + \chi)}\right)^2.$$

3. Numerical results

In this section, we discuss our numerical results for the GG02 and No-switching protocols in both untrusted and trusted models. Fig.2 shows the curves for GM-CV-QKD protocols for homodyne (solid) and heterodyne (dashed) detections. We optimized the amplitude for each distance, maximizing the SKR, and fixed the reconciliation efficiency at a typical value of 95%. First, we note that the type of detection does not make a substantial difference on the SKR value with this efficiency value. The SKR curves for different detections only show significant deviation for unrealistically low reconciliation efficiency values (below 60%) and for excess noise above 1% of the shot noise.

We explore different sets of parameters of detector's noise and efficiency and the total excess noise. The first figure (top left) of the panel confirms that both models are equivalent when the detector's noise is zero and the excess noise from all other sources amounts to the same value, in this case 1% of SNU, with perfect detector's efficiency. Even though no detector presents zero intrinsic noise, this scenario helps us to notice the importance of the measurement efficiency. In the second figure (top right), just by lowering efficiency, the trusted-noise model already shows a small gain over the untrusted one over short distances up to 25 km.

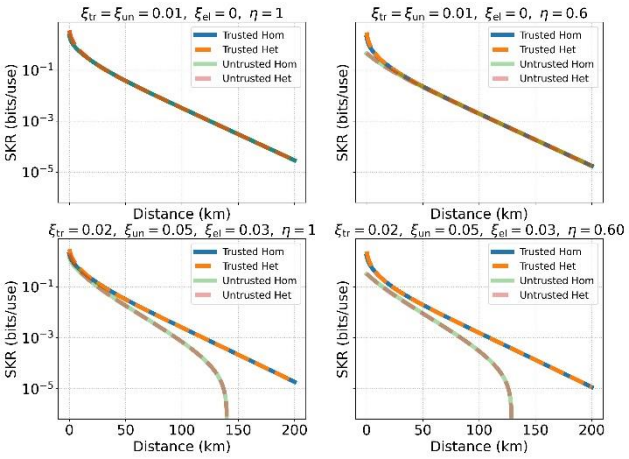

Fig.2: Secret key rate for trusted and untrusted models with homodyne and heterodyne detection for $\beta = 95\%$.

In the bottom figures, we present a more realistic case, where the detector's noise contribution is of the order of 60% of the total excess noise, leading to a lower excess noise attributed to Eve. With this approach, significative gain is obtained for long distances and perfect detector's efficiency (bottom left), while non-perfect efficiency increases the difference on the SKR between both models, even for short distances (bottom right). It is worth noticing that, while the untrusted-noise model reaches a maximum transmission distance of 125 km for this example, the trusted-noise case goes beyond 200 km for this example.In addition, it is also possible to use such trusted parameters to analyze the limits of operation of the information reconciliation process. While $\beta = 95\%$ is a viable value, we can seek for its minimum possible value which allows for secure communication. In Fig.3, we show the minimal reconciliation efficiency to generate a secret key for the untrusted and trusted models. We used the same parameters than Fig.2 (bottom right plot). In

this case, it is clear that the trusted-noise model tolerates information reconciliation efficiencies significantly lower than the untrusted case, ranging from ~20% for short distances to ~80% for long distances (up to 200 km).

The last analysis consists of finding the maximum tolerable excess noise that such protocols can support, while enabling a non-negative SKR. In this sense, we keep the detector's noise at 60% of the total excess noise for each distance. The untrusted-noise model supports approximately a maximum of 30% of

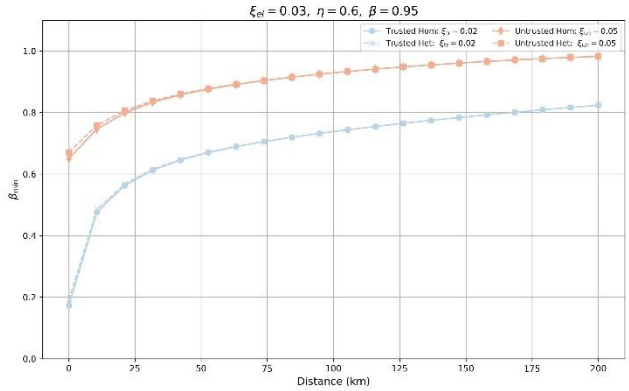

Fig.3: Minimum value of $\boldsymbol{\beta}$ which allows the extraction of a secret key. We use the same parameters as in the bottom right plot from Fig.2.

shot noise, while the trusted-noise handles nearly 15% of shot noise, since, in this case, the major noise comes from Bob's detector (inset), for very short distances. However, for mid-to-long distances, neither trusted- and untrusted-noise models support higher excess noise values beyond 5% and 10% of SNU, respectively.

4. Conclusion

In this work, we analyzed a comparison between the standard pessimistic (untrusted-noise) and the more realistic (trusted-noise) approaches to CV-QKD protocols. It is clear that splitting the noise contribution between what can be controlled by Eve and what is isolated from her can significantly enhance the performance of the protocol. The trusted-noise model tolerates a significantly lower efficiency of the information reconciliation process. The maximum tolerable excess noise allowed by each model can support up to nearly 15% and 30% of shot noise, respectively for the trusted and untrusted cases, with the detector's noise representing 60% of the total excess noise for each distance.

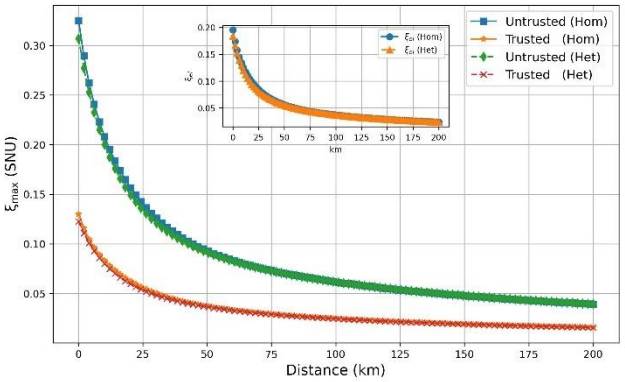

Fig.3: Maximum excess noise for the untrusted and trusted noise models.

In the future, we seek to investigate this same scenario for discrete modulation CV-QKD protocols.

Acknowledgement

This work has been fully funded by the project "Comparative Analysis of Prepare-and-Measure Protocols for Quantum Cryptography" supported by QuIIN - Quantum Industrial Innovation, EMBRAPII CIMATEC Competence Center in Quantum Technologies, with financial resources from the PPI IoT/Manufatura 4.0 of the MCTI grant number 053/2023, signed with EMBRAPII.

References

[1] Pirandola, Stefano, et al. **Advances in quantum cryptography**. *Advances in optics and photonics* 12.4 (2020): 1012-1236.

[2] Usenko, Vladyslav C., et al. **Continuous-variable quantum communication**. *arXiv preprint arXiv:2501.12801* (2025).

[3] Bennett, Charles H., and Gilles Brassard. **An update on quantum cryptography**. *Workshop on the theory and application of cryptographic techniques*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1984.

[4] Laudenbach, Fabian, et al. **Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations**. *Advanced Quantum Technologies* 1.1 (2018): 1800011.

[5] Usenko, Vladyslav C., and Radim Filip. **Trusted noise in continuous-variable quantum key distribution: a threat and a defense.** *Entropy* 18.1 (2016): 20.

[6] Grosshans, Frédéric, and Philippe Grangier. **Continuous variable quantum cryptography using coherent states**. *Physical review letters* 88.5 (2002): 057902.

[7] Weedbrook, Christian, et al. **Quantum cryptography without switching**. *Physical review letters* 93.17 (2004): 170504.

[8] Grosshans, Frédéric, et al. **Quantum key distribution using Gaussian-modulated coherent states.** Nature 421.6920 (2003): 238-241

[9] Devetak, Igor, and Andreas Winter. **Distillation of secret key and entanglement from quantum states**. *Proceedings of the Royal Society A: Mathematical, Physical and engineering sciences* 461.2053 (2005): 207-235.

[10] Lodewyck, Jérôme, et al. **Quantum key distribution over 25 km with an all-fiber continuous-variable system**. *Physical Review A—Atomic, Molecular, and Optical Physics* 76.4 (2007): 042305.