## Eavesdropping of two-way coherent-state quantum cryptography via gaussian quantum cloning machines

| | |
|---|---|
| **Citation** | Pirandola, S. et al. "Eavesdropping of Two-Way Coherent-State Quantum Cryptography via Gaussian Quantum Cloning Machines." Quantum, Nano and Micro Technologies, 2009. ICQNM '09. Third International Conference on. 2009. 38-41. © Copyright 2009 IEEE |
| **As Published** | http://dx.doi.org/10.1109/ICQNM.2009.8 |
| **Publisher** | Institute of Electrical and Electronics Engineers |
| **Version** | Final published version |
| **Citable link** | http://hdl.handle.net/1721.1/60056 |
| **Terms of Use** | Article is made available in accordance with the publisher's policy and may be subject to US copyright law. Please refer to the publisher's site for terms of use. |

# Eavesdropping of two-way coherent-state quantum cryptography via Gaussian quantum cloning machines

Stefano Pirandola
Massachusetts Institute of Technology
Research Laboratory of Electronics
Cambridge MA 02139, USA
pirs@mit.edu

Stefano Mancini
Dipartimento di Fisica & CNISM
Università di Camerino
I-62032 Camerino, Italy

Seth Lloyd
Massachusetts Institute of Technology
Research Laboratory of Electronics &
Department of Mechanical Engineering
Cambridge MA 02139, USA

Samuel L. Braunstein
Computer Science
University of York
York YO10 5DD, United Kingdom

## Abstract

*We consider one of the quantum key distribution protocols recently introduced in Ref. [Pirandola et al., Nature Phys. 4, 726 (2008)]. This protocol consists of a two-way quantum communication between Alice and Bob, where Alice encodes secret information via a random phase-space displacement of a coherent state. In particular, we study its security against a specific class of individual attacks which are based on combinations of Gaussian quantum cloning machines.*

## 1 Introduction

Recently [1, 2], we have shown how two-way quantum communication can profitably be exploited to enhance the security of continuous variable quantum key distribution [3, 4, 5, 6]. In particular, we have investigated the security of two-way protocols in the presence of collective Gaussian attacks which are modelled by combinations of entangling cloners [5]. Even though this situation is the most important one from the point view of the practical implementation, the effect of other kinds of Gaussian attacks (i.e., not referable to entangling cloners) must also be analyzed. In this paper, we study the security of the two-way coherent-state protocol of Ref. [1] against individual attacks where an eavesdropper (Eve) combines two different Gaussian quantum cloning machines (also called *Gaussian cloners*). In particular, we are able to show the robustness of the two-way protocol when the first cloner is fixed to be symmetric

in the output clones. This symmetry condition enables us to derive the results quite easily but clearly restricts our security analysis to a preliminary stage. For this reason, the *optimal* performance of Gaussian cloners against two-way quantum cryptography is still unknown at the present stage.

## 2 Additive Gaussian channels and Gaussian cloners

Consider a stochastic variable $X$ with values $x \in \mathbb{R}$ distributed according to a Gaussian probability

$$G_{\Sigma^2}(x) = \frac{1}{\sqrt{2\pi\Sigma^2}} \exp\left[-\frac{x^2}{2\Sigma^2}\right], \qquad (1)$$

with variance $\Sigma^2$. This variable is taken as input of a classical channel that outputs another stochastic variable $Y$ with values $y \in \mathbb{R}$. In particular, the classical channel is called an *additive Gaussian channel* if, for every input $x$, the conditional output $y|x$ is Gaussianly distributed around $x$ with some variance $\sigma^2$. As a consequence, the output variable $Y$ is a Gaussian variable with zero mean and variance $\Sigma^2 + \sigma^2$. According to Shannon's theory, the classical correlations between the input and output variables lead to a mutual information

$$I(X, Y) = \frac{1}{2} \log(1 + \gamma), \qquad (2)$$

where $\gamma \equiv \Sigma^2/\sigma^2$ is the signal to noise ratio (SNR). This formula gives the maximal number of bits per Gaussian value that can be sent through a Gaussian channel with a given SNR (on average and asymptotically).

In quantum information theory, an example of an additive Gaussian channel is provided by the Gaussian quantum cloning machine (GQCM) [7]. Consider a continuous variable (CV) system, like a *bosonic mode*, which is described by a pair of conjugate quadratures $\hat{x}$ and $\hat{p}$, with $[\hat{x}, \hat{p}] = i$, acting on a Hilbert space $\mathcal{H}$. Then, consider a coherent state $|\varphi\rangle$ with amplitude $\varphi = (x + ip)/\sqrt{2}$. A $1 \rightarrow 2$ GQCM is a completely-positive trace-preserving linear map

$$M : |\varphi\rangle\langle\varphi| \rightarrow \rho_{12} \in \mathcal{D}(\mathcal{H}^{\otimes 2}) , \qquad (3)$$

such that the single clone states, $\rho_1 = \mathrm{tr}_2(\rho_{12})$ and $\rho_2 = \mathrm{tr}_1(\rho_{12})$, are given by a Gaussian phase-space modulation of the input state $|\varphi\rangle\langle\varphi|$, i.e.,

$$\rho_k = \int d\mu \, \Omega_{\sigma_k^2}(\mu)\hat{D}(\mu)|\varphi\rangle\langle\varphi|\hat{D}^\dagger(\mu), \quad k = 1, 2, \quad (4)$$

where

$$\Omega_{\sigma_k^2}(\mu) \equiv \frac{1}{\pi\sigma_k^2} \exp\left[-\frac{|\mu|^2}{\sigma_k^2}\right] , \qquad (5)$$

and

$$\hat{D}(\mu) = \exp(\mu\hat{a}^\dagger - \mu^*\hat{a}) . \qquad (6)$$

In Eq. (5), the quantities $\sigma_k^2$ are the error variances induced by the cloning process on both the $x$ and $p$ quadratures of the $k$-th clone. Notice that here we consider a GQCM which clones symmetrically in the quadratures (in general, one can have a Gaussian cloner which is asymmetric both in the clones and the quadratures, with four different noise variances $\sigma_{1,x}^2$, $\sigma_{1,p}^2$, $\sigma_{2,x}^2$ and $\sigma_{2,p}^2$.) The previous variances do not depend on the input state (*universal* GQCM) and satisfy the relation

$$\sigma_1^2 \sigma_2^2 \geq 1/4 , \qquad (7)$$

imposed by the uncertainty principle. In particular, the previous GQCM is said to be *optimal* if $\sigma_1^2\sigma_2^2 = 1/4$. In terms of Shannon's theory, each of the two real variables, $x$ and $p$, is subject to an additive Gaussian channel with noise equal to $\sigma_k^2$ during the cloning process from the input state to the output $k$-th clone.

## 3 Two-way coherent-state protocol

The protocol is sketched in Fig.1 and consists of two configurations, ON and OFF, that can be selected by Alice with probabilities $1 - c$ and $c$ respectively.

Let Bob prepare a *reference* coherent state $|\beta\rangle\langle\beta|$, with amplitude $\beta$ randomly chosen in the complex plane (e.g., according to a Gaussian distribution with a *large* variance). Such a state is sent to Alice on the forward use of the quantum channel. In the ON configuration, Alice encodes a *signal* on this reference state via a phase-space displacement $\hat{D}(\alpha)$ whose amplitude $\alpha \equiv (x_A + ip_A)/\sqrt{2}$ is chosen in the $\mathbb{C}$-plane according to a random Gaussian distribution $\Omega_{\Sigma^2}(\alpha)$ with *large* variance $\Sigma^2$. Notice that
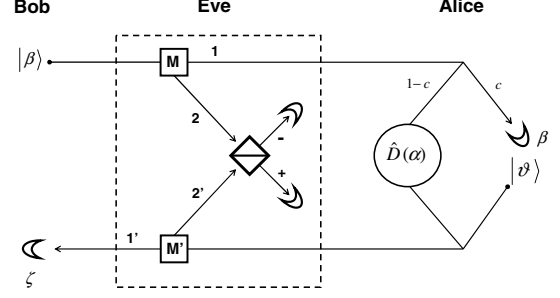


**Figure 1. Two-way coherent-state protocol in both the ON and OFF configurations.**

**(i)** The *signal* amplitude $\alpha$ symmetrically encodes two signal quadratures, $x_A$ and $p_A$, i.e., two independent and real random variables distributed according to Gaussian distributions $G_{\Sigma^2}(x_A)$ and $G_{\Sigma^2}(p_A)$. (8)

**(ii)** The output state

$$\hat{D}(\alpha)|\beta\rangle\langle\beta|\hat{D}^\dagger(\alpha) = |\alpha + \beta\rangle\langle\alpha + \beta| ,$$

encodes the signal amplitude $\alpha$, masked by the reference amplitude $\beta$ chosen by Bob.

The state is finally sent back to Bob, who tries to guess Alice's two numbers $x_A$ and $p_A$ by a joint measurement of conjugate observables. This is accomplished by a heterodyne detection [8] of the state, which will give an outcome $\zeta \approx \alpha + \beta$. After the subtraction of the known value $\beta$, Bob achieves an estimate $\alpha'$ of Alice's complex amplitude $\alpha$, i.e., $x'_A \approx x_A$ and $p'_A \approx p_A$.

In the case of a noiseless channel between Alice and Bob, the only noise in the whole process is introduced by the heterodyne detection. This measurement can be seen as a further Gaussian additive channel at Bob's site, which gives a Gaussian noise equal to 1 for each quadrature. Thus, according to Shannon's formula, we have

$$I_{AB} = I(x_A, x'_A) + I(p_A, p'_A) = \log(1 + \gamma_{AB}) , \qquad (9)$$

with $\gamma_{AB} = \Sigma^2/1$.

Let us now consider a noisy channel adding Gaussian noise with variances $\sigma^2$ (in the forward path) and $\sigma'^2$ (in the backward path) for each quadrature. Then, the total noise of the channel is $\sigma_{\mathrm{ch}}^2 = \sigma^2 + \sigma'^2$ and the total noise which Bob tests, after detection, is equal to $\sigma_B^2 = \sigma_{\mathrm{ch}}^2 + 1$, giving a SNR $\gamma_{AB} = \Sigma^2/\sigma_B^2$. In the OFF configuration, Alice and Bob estimate the noise in the channel by performing two heterodyne detections. After receiving the reference state, Alice simply heterodynes it with outcome $\beta'$ and then reconstructs a coherent state $|\vartheta\rangle$. This state is sent to Bob,

who gets the outcome $\zeta \approx \vartheta$ after detection. In this way, Alice and Bob collect the pairs $\{\beta, \beta'\}$ and $\{\vartheta, \zeta\}$ from which they can estimate the two noise variances $\sigma^2$ and $\sigma'^2$ of the channel via public communication. Notice that here we are using the ON configuration to encode the key and the OFF configuration to check the noise of the channel. This means that we are implicitly assuming that Eve's attack is disjoint between the two paths of the quantum communication (i.e., Eve is using two distinct one-mode GQCMs). More generally, in order to exclude joint attacks between the two paths, the ON and OFF configurations must be used symmetrically for encoding and checking [1].

## 4 Eavesdropping via Gaussian cloners

In the previous two-way quantum communication, the choices of the reference $\beta$ and the signal $\alpha$ are two independent processes. As a consequence, Eve has to extract information on both the reference $\beta$ and the total displacement $\alpha + \beta$ in order to access Alice's encoding $\alpha$ (this is actually true because the attack is disjoint). Let us consider two different attacks, one on the forward use of the channel and the other one in the backward use, by using two optimal GQCMs which we call $M$ and $M'$, respectively (see Fig. 1).

Since the reference $\beta$ and the signal $\alpha$ are chosen with large variances, such cloning machines must be universal, and since the information is symmetrically encoded in the two quadratures, we consider equal cloning noises in $x$ and $p$. For these reasons, Eve's GQCMs are exactly of the kind specified by Eq. (4) with $\sigma_1^2 \sigma_2^2 = 1/4$. After cloning, Eve must extract the information about $\alpha$ from her clones. She can directly heterodyne the clones. Alernatively, she can send the clones to a beam-splitter (BS), with suitable reflection and transmission coefficients $r$ and $t$, and then heterodynes the output ports.

In order to study the eavesdropping depicted in Fig. 1, it is not sufficient to consider the reduced states $\rho_k$ of the two single clones at the output of $M$, but we have to compute explicitly the whole bipartite state $\rho_{12}$ of modes 1 and 2. In fact, mode 1 is sent to Alice (who displaces it) and then cloned by $M'$ into the output modes $1'$ and $2'$. The second mode $2'$ then interferes with the previous mode 2 on the beam-splitter. For this reason, we have to keep all the correlations between the various modes till the interference process. One can prove that the bipartite state $\rho_{12}$ at the output of the optimal GQCM $M$ is a Gaussian state with correlation matrix (CM) equal to

$$V = \frac{1}{2} \begin{pmatrix} (1 + 2\sigma^2)I & I \\ I & (1 + 1/2\sigma^2)I \end{pmatrix} , \qquad (10)$$

where $I$ is the $2 \times 2$ identity matrix. The CM of Eq. (10) has *positive partial transpose* for every $\sigma^2 \geq 0$, and, therefore, $\rho_{12}$ is always a separable state [9]. This means that

Eve cannot exploit strategies based on the entanglement between her clones and the ones of Alice and Bob. In the particular case of symmetric cloning ($\sigma^2 = 1/2$), we can make the useful decomposition

$$\rho_{12} = \int d^2\mu \, \Omega_{1/2}(\mu) \times$$
$$|\beta + \mu\rangle_1 \langle \beta + \mu| \otimes |\beta + \mu\rangle_2 \langle \beta + \mu| . \qquad (11)$$

Then, let us consider the case where the first cloner $M$ is optimal and symmetric ($\sigma_1^2 = \sigma_2^2 = 1/2$), while the second cloner $M'$ is optimal but asymmetric, with $\sigma_{1'}^2 \equiv \omega^2$ and $\sigma_{2'}^2 = 1/4\omega^2$. In this case, at the output modes $+$ and $-$ of the BS, we have the bipartite state

$$\rho_{+-} = \int d^2\mu \, \Omega_{1/2}(\mu) \, \chi(\mu) \qquad (12)$$

where

$$\chi(\mu) \equiv \int d^2\lambda \, \Omega_{1/4\omega^2}(\lambda) \times$$
$$|\theta_+ + \lambda r\rangle_+ \langle \theta_+ + \lambda r| \otimes |\theta_- + \lambda t\rangle_- \langle \theta_- + \lambda t| , \qquad (13)$$

and

$$\theta_+ \equiv (\mu + \beta)(t + r) + \alpha r, \; \theta_- \equiv (\mu + \beta)(t - r) + \alpha t . \quad (14)$$

If we now take a balanced BS (i.e., $t = r = 1/\sqrt{2}$) we have $\theta_- \equiv \alpha/\sqrt{2}$ and, therefore, the output port $-$ no longer contains the reference $\beta$. Here, the action of the BS is very similar to the sum (mod2) performed over a binary key ($k$) and the corresponding encrypted message ($k \oplus m$), operation that reveals the message in the classical case ($k \oplus m \oplus k = m$). On the other hand, the other port $+$ still contains a mixing between $\alpha$ and $\beta$ and, therefore, does not provide further information about the signal. Tracing out this port, we have

$$\rho_- = \int d^2\lambda \, \Omega_{1/4\omega^2}(\lambda) \, |(\alpha + \lambda)/\sqrt{2}\rangle_- \langle(\alpha + \lambda)/\sqrt{2}| . \qquad (15)$$

Heterodyning such a state, Eve can estimate the value of $\alpha$ up to a Gaussian noise with variance

$$\sigma_E^2 = 2 + (4\omega^2)^{-1} , \qquad (16)$$

for each quadrature. For Bob, instead, we have a total noise

$$\sigma_B^2 = 1 + \sigma_{ch}^2 , \qquad (17)$$

equal to the sum of the heterodyne noise (1) and the total channel noise

$$\sigma_{ch}^2 = 1/2 + \omega^2 . \qquad (18)$$

According to Shannon, Bob ($B$) and Eve ($E$) will share with Alice ($A$) a mutual information equal to $I_{AX} = \log(1 + \gamma_{AX})$ with $\gamma_{AX} \equiv \Sigma^2/\sigma_X^2$ for $X = B, E$. Since [10]

$$I_{AB} \geq I_{AE} \Longleftrightarrow \gamma_{AB} \geq \gamma_{AE} \Longleftrightarrow \sigma_B^2 \leq \sigma_E^2 , \quad (19)$$

we can easily compute a security threshold for this kind of attack, which is equal to

$$\tilde{\sigma}_{\text{ch}}^2 = (3 + \sqrt{5})/4 \simeq 1.3 . \quad (20)$$

Such a threshold must be compared with the security threshold (0.5) which characterizes one-way coherent-state protocols [5, 6] against individual GQCM attacks.

## 5 Conclusion and discussion

In this paper we have considered one of the two-way protocols introduced in [1]. Then, we have explicitly studied its security in the presence of a particular kind of individual attack which is based on combinations of one-mode Gaussian cloners. Our analysis indicates that the superadditive behavior of the security threshold should also hold against this kind of Gaussian attack. However, our analysis is far from complete since we have considered only particular combinations of cloners and we have also excluded the possibility of a two-mode cloner (acting coherently on both paths of the quantum communication). Furthermore, the analysis covers the case of direct reconciliation only. Despite these restrictions, the present work represents the first step in the security analysis of two-way protocols against more exotic kinds of Gaussian interactions.

Future investigations may involve the study of completely general two-mode Gaussian cloners, together with the analysis of security in the case of reverse reconciliation. It would be also interesting to analyze the security of the other two-way protocol introduced in [1], where squeezing and entanglement play an important role. Finally, the extension of the two-way coherent-state protocol to a *multi-way* coherent-state protocol is another fascinating possibility to be investigated. In this multi-way protocol, Alice and Bob use $n \geq 2$ rounds of quantum communication for encoding several random displacements before detection. This kind of protocol is currently under our study and will be the subject of a future work.

## 6 Acknowledgements

## References

[1] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, "Quantum cryptography using two-way quantum communication," Nature Phys. **4**, 726 (2008).

[2] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, "Security of two-way quantum cryptography against asymmetric attacks," Proc. SPIE **7092**, 709215 (2008).

[3] T. C. Ralph, "Continuous variable quantum cryptography," Phys. Rev. A **61**, 010303(R) (2000); T. C. Ralph, "Security of continuous-variable quantum cryptography," Phys. Rev. A **62**, 062306 (2000).

[4] D. Gottesman, and J. Preskill, "Secure quantum key distribution using squeezed states," Phys. Rev. A **63**, 022309 (2001); S. Iblisdir, G. Van Assche, and N. J. Cerf, "Security of quantum key distribution with coherent states and homodyne detection," Phys. Rev. Lett. **93**, 170502 (2004).

[5] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states," Nature **421**, 238 (2003); F. Grosshans, and Ph. Grangier, "Continuous variable quantum cryptography using coherent states," Phys. Rev. Lett. **88**, 057902 (2002).

[6] C. Weedbrook *et al.*, "Quantum cryptography without switching," Phys. Rev. Lett. **93**, 170504 (2004); A. M. Lance *et al.*, "No-switching quantum key distribution using broadband modulated coherent light," Phys. Rev. Lett. **95**, 180503 (2005).

[7] N. J. Cerf, A. Ipe, and X. Rottenberg, "Cloning of continuous quantum variables," Phys. Rev. Lett. **85**, 1754 (2000).

[8] H.P. Yuen and J.H. Shapiro, "Optical communication with two-photon coherent states - part III: Quantum measurements realizable with photoemessive detectors," IEEE Trans. Inf. Theory **IT-26**, 78-92 (1980).

[9] R. Simon, "Peres–Horodecki separability criterion for continuous variable systems," Phys. Rev. Lett. **84**, 2726 (2000).

[10] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory **IT-24**, 339 (1978).