Continuous-variable quantum cryptography using two-way quantum communication

STEFANO PIRANDOLA[1]*, STEFANO MANCINI[2], SETH LLOYD[1,3] AND SAMUEL L. BRAUNSTEIN[4]

[1]Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA
[2]Dipartimento di Fisica & CNISM, Università di Camerino, Camerino 62032, Italy
[3]Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA
[4]Department of Computer Science, University of York, York YO10 5DD, UK
*e-mail: pirs@mit.edu

Published online: 11 July 2008; doi:10.1038/nphys1018

Quantum cryptography has recently been extended to continuous-variable systems, such as the bosonic modes of the electromagnetic field possessing continuous degrees of freedom. In particular, several cryptographic protocols have been proposed and experimentally implemented using bosonic modes with Gaussian statistics. These protocols have shown the possibility of reaching very high secret key rates, even in the presence of strong losses in the quantum communication channel. Despite this robustness to loss, their security can be affected by more general attacks where extra Gaussian noise is introduced by the eavesdropper. Here, we show a 'hardware solution' for enhancing the security thresholds of these protocols. This is possible by extending them to two-way quantum communication where subsequent uses of the quantum channel are suitably combined. In the resulting two-way schemes, one of the honest parties assists the secret encoding of the other, with the chance of a non-trivial superadditive enhancement of the security thresholds. These results should enable the extension of quantum cryptography to more complex quantum communications.

In recent years, quantum information has entered the domain of continuous-variable systems, that is, quantum systems described by an infinite-dimensional Hilbert space[1,2]. So far, the most studied continuous-variable systems are the bosonic modes, such as the optical modes of the electromagnetic field. In particular, the most important bosonic states are the ones with Gaussian statistics, owing to their experimental accessibility and the relative simplicity of their mathematical description[3,4]. Accordingly, quantum key distribution (QKD) has been extended to this new framework[5–21] and Gaussian cryptographic protocols using coherent states have been shown to fully exploit the potentialities of quantum optics[12,16]. These coherent-state protocols are robust with respect to the noise of the quantum channel, as long as such noise can be ascribed to pure losses[12,16]. In contrast, their security is strongly affected when channel losses are used to introduce a thermal environment, which is assumed to be controlled by a malicious eavesdropper[12,22]. In this Gaussian eavesdropping scenario, we present a method to enhance the security thresholds of the basic coherent-state protocols. This is achieved by extending them to two-way quantum communication protocols, where one of the honest parties (Bob) uses its quantum resources to assist the secret encoding of the other party (Alice). In particular, the enhancement of security is proved to be effective because the security thresholds are superadditive with respect to the double use of the quantum channel. Such a result is achieved when the Gaussian attack corresponds to a memoryless Gaussian channel. More generally, we also consider Gaussian channels with memory, therefore creating classical and/or quantum correlations between the paths of the two-way quantum communication. To overcome this kind of eavesdropping strategy, the two-way protocols must be modified into suitable hybrid protocols, which represent their safe formulation against every kind of collective Gaussian attack.

ONE-WAY PROTOCOLS

In basic coherent-state protocols[11,15], Alice prepares a coherent state $|\alpha\rangle$, the amplitude $\alpha = (Q_A + iP_A)/2$ of which is stochastically modulated by a pair of independent Gaussian variables $\{Q_A, P_A\}$, with zero mean and variance $V - 1$. This variance determines the portion of phase space that is available to Alice's classical encoding $\{Q_A, P_A\}$ and, therefore, quantifies the amount of energy that Alice can use in the process. This energy is usually assumed to be very large $V \gg 1$ (large modulation limit) to reach the optimal and asymptotic performances provided by the infinite-dimensional Hilbert space. The modulated coherent state is then sent to Bob through a quantum channel, the noise of which is assumed ascribable to the malicious action of a potential eavesdropper (Eve). In a homodyne (Hom) protocol[11], Bob detects the state through a single quadrature measurement (by a homodyne detection). More exactly, Bob randomly measures the quadrature $\hat{Q}$ or $\hat{P}$, getting a real outcome $X_B = Q_B$ (or P_B) that is correlated to the encoded signal $X_A = Q_A$ (or P_A). In a heterodyne (Het) protocol[15], Bob carries out a joint measurement of $\hat{Q}$ and $\hat{P}$ (a heterodyne detection). In such a case, Bob decodes the $\mathbb{R}^2$-variable $X_B = \{Q_B, P_B\}$ correlated to the total signal $X_A = \{Q_A, P_A\}$ encoded in the amplitude α. In both cases, Alice and Bob finally possess two correlated variables X_A and X_B, characterized by some mutual information $I(X_A{:}X_B)$. To access this mutual information, either Bob estimates Alice's encoding X_A through a direct reconciliation or Alice estimates Bob's outcomes X_B through a reverse reconciliation[22]. However, to extract some shared secret information from $I(X_A{:}X_B)$, the honest parties must estimate the noise of the channel by broadcasting and comparing part of their data. In this way, they are able to bound the information $I(X_A{:}E)$ or $I(X_B{:}E)$ that has been potentially stolen

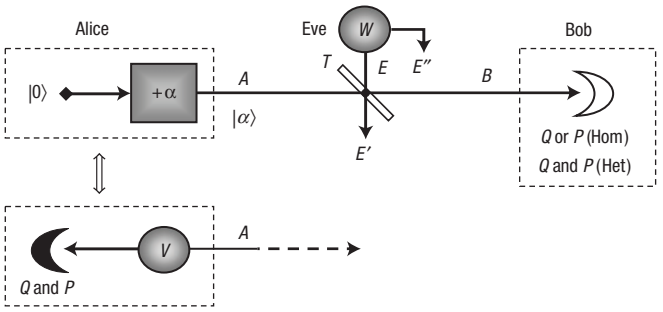

Figure 1 Coherent-state protocols. Alice prepares a coherent state $|\alpha\rangle$ that Bob detects using a homodyne or heterodyne detector. A Gaussian (entangling cloner) attack by Eve is also shown. Note that preparing a coherent state (by modulating the vacuum) can be equivalently achieved by heterodyning one of the two modes of an EPR pair.

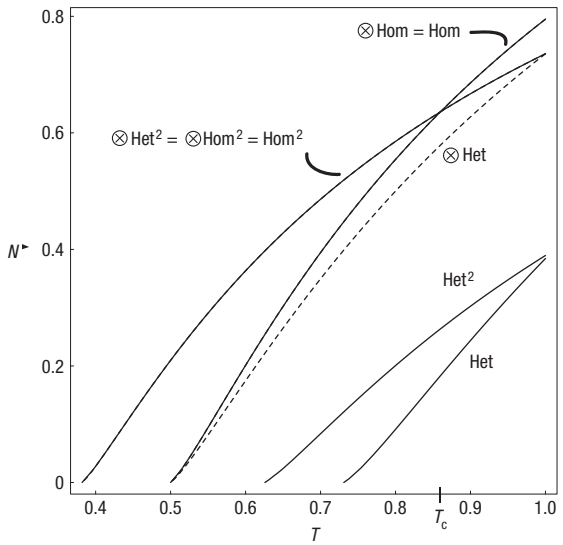

Figure 2 Security thresholds in direct reconciliation. Tolerable excess noise $N^{\blacktriangleright}$ (in quantum shot-noise units) versus transmission T. Curves compare the various one-way and two-way protocols against one-mode Gaussian attacks $\{N, T\}$ in the limit of large modulation ($V \to +\infty$).

by Eve during the process. Then, the accessible secret information is simply given by $R^{\blacktriangleright} := I(X_A{:}X_B) - I(X_A{:}E)$ for direct reconciliation and by $R^{\blacktriangleleft} := I(X_A{:}X_B) - I(X_B{:}E)$ for reverse reconciliation. Such secret information can be put in the form of a binary key by slicing the phase space and adopting the standard techniques of error correction and privacy amplification[23]. In particular, Alice and Bob can extract a secret key whenever the channel noise is less than certain security thresholds, which correspond to the boundary conditions $R^{\blacktriangleright} = 0$ and $R^{\blacktriangleleft} = 0$.

In the continuous-variable framework, collective Gaussian attacks represent the most powerful tool that today can be handled in the cryptoanalysis of Gaussian-state protocols[24–27]. In the most general definition of a collective attack, all of the quantum systems used by Alice and Bob in a single run of the protocol are made to interact with a fresh ancillary system prepared by Eve. Then, all of the output ancillas, coming from a large number of such single-run interactions, are subject to a final coherent measurement that is furthermore optimized on all of Alice and Bob's classical communications. In particular, the collective attack is Gaussian if the single-run interactions are Gaussian, that is, corresponding to unitaries that preserve the Gaussian statistics of the states. Notice that for standard one-way QKD, a single run of the protocol corresponds to a single use of the channel. As a consequence, every collective Gaussian attack against one-way protocols results in a memoryless channel and, therefore, can be called a one-mode Gaussian attack. As the quadratures encode independent variables $\{Q_A, P_A\}$, the single-run Gaussian interactions do not need to mix the quadratures[24,25,28,29]. As a consequence, the Gaussian interaction can be modelled by an entangling cloner[12] (Fig. 1) where a beam splitter (of transmission T) mixes each signal mode A with an ancillary mode E belonging to an Einstein–Podolsky–Rosen (EPR) pair (see the Supplementary Information). Such an EPR pair is characterized by a variance W and correlates the two output ancillary modes E', E'' to be detected in the final coherent measurement. Notice that, from the point of view of Alice and Bob, this EPR pair simply reduces to an environmental thermal state ρ_E with thermal number $\bar{n}_E = (W-1)/2$. A one-mode Gaussian attack can therefore be described by two parameters: transmission T and variance W or, equivalently, by T and $N := (W-1)(1-T)T^{-1}$, the latter being the excess noise of the channel. This parameter quantifies the amount of extra noise that is not referable to losses, that is, the effect of the thermal noise scaled by the transmission[12]. The security thresholds against these powerful attacks can be expressed in terms of tolerable excess noise $\{N^{\blacktriangleright}, N^{\blacktriangleleft}\}$ versus the transmission T of the channel. For protocols Hom and Het, these thresholds are shown in Fig. 2 for direct reconciliation and Fig. 3 for reverse reconciliation, and they confirm the results previously found in refs 30,31 (see the Supplementary Information).

FROM ONE-WAY TO TWO-WAY PROTOCOLS

The above coherent-state protocols have been simply formulated in terms of prepare-and-measure schemes. Equivalently, they can be formulated as entanglement-based schemes, where Alice and Bob extract a key from the correlated outcomes of the measurements made on two entangled modes (Fig. 1). In fact, heterodyning one of the two entangled modes of an EPR pair (with variance V) is equivalent to remotely preparing a coherent state $|\alpha\rangle$ with an amplitude that is randomly modulated by a Gaussian (with variance $V-1$)[22]. In this dual representation of the protocol, Alice owns a physical resource that can be equivalently seen as an amount of energy $\sim V$ for modulation (in the prepare-and-measure representation) or as an amount of entanglement $\sim \log 2V$ to be distributed (in the entanglement-based representation). Because of this equivalence, the previous entanglement is also called virtual[22]. In the above one-way protocols, all of these physical resources are the monopoly of Alice and their sole purpose is the encoding of secret information. However, we can also consider a scenario where these resources are symmetrically distributed between Alice and Bob, and part of them is used to assist the encoding. This is achieved by combining Alice and Bob in a two-way quantum communication where Bob's physical resources, to be generally intended as entanglement resources, assist the secret encoding of Alice, which is realized by unitary random modulations (Fig. 4).

Let us explicitly construct such a two-way quantum communication. In simple two-way generalizations, Hom^2 and Het^2, of the previous one-way protocols, Hom and Het, Bob exploits an assisting EPR pair (with variance V) of which he keeps one mode B_1 while sending the other to Alice (Fig. 5). Then, Alice encodes her information through Gaussian modulation (with variance $V-1$) by adding a stochastic amplitude $\alpha = (Q_A + iP_A)/2$

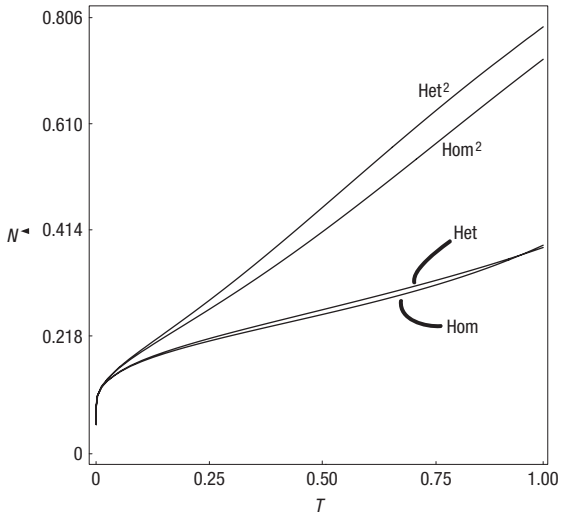

Figure 3 Security thresholds in reverse reconciliation. Tolerable excess noise $N^{\blacktriangleleft}$ (in quantum shot-noise units) versus transmission T. Curves compare the individual one-way and two-way protocols against one-mode Gaussian attacks $\{N, T\}$ in the limit of large modulation ($V \to +\infty$).

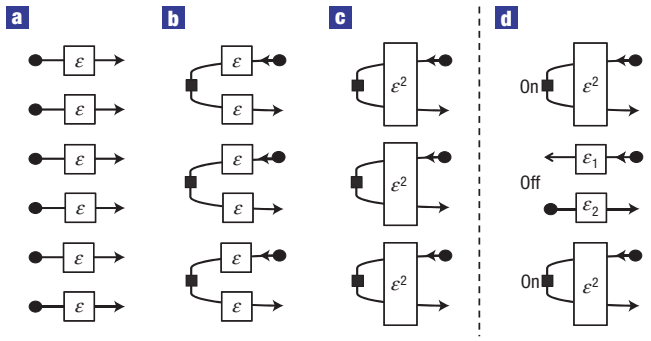

Figure 4 General structure of the one-way, two-way and hybrid protocols, together with their possible collective attacks. Circles and squares represent the physical resources available in the process. In particular, circles represent entanglement (possibly virtual), whereas squares are unitary modulations. **a**, The basic one-way scheme, where all of the resources are owned by Alice. **b**,**c**, Scheme where the physical resources are instead distributed between Alice and Bob, where Bob uses them for assisting and Alice uses them for encoding (two-way scheme). **d**, The hybrid protocol where one-way (off) and two-way (on) quantum communications are randomly switched. All of the parts also show Eve's collective attacks. **a** shows the collective attacks against one-way protocols (one-mode attacks). **b**,**c** show instead the collective attacks against the two-way protocols. These are one-mode (or reducible two-mode) in **b** and two-mode in **c**. **d** shows the effects of a two-mode attack on the hybrid protocol.

to the received mode. Such a mode is then sent back to Bob, where it is detected together with the unsent mode B_1. Depending on the protocol, Bob will carry out different detections on modes B_1 and B_2. In particular, for the Hom^2 protocol, Bob will detect the $\hat{Q}$ (or $\hat{P}$) quadrature of such modes (homodyne detections), whereas, for the Het^2 protocol, he will detect both $\hat{Q}$ and $\hat{P}$ (heterodyne detections). From the outcomes, Bob will finally construct an optimal estimator X_B of Alice's corresponding variable X_A, equal to Q_A (or P_A) for Hom^2 and to the $\mathbb{R}^2$-vector $\{Q_A, P_A\}$ for Het^2.

As Bob's decoding strategy consists of individual incoherent detections, these entanglement-assisted QKD schemes are actually equivalent to two-way schemes without entanglement, where Bob stochastically prepares a quantum state to be sequentially transmitted forward and backward in the channel. In fact, it can be assumed that Bob detects B_1 at the beginning of the quantum communication, so that the travelling mode C_1 is randomly prepared in a reference quantum state (which is squeezed for Hom^2 and coherent for Het^2). This reference state reaches Alice, who stores the encoding transformation and, then, is finally detected by the second decoding measurement of Bob. Therefore, if we restrict Bob to incoherent detections (classical Bob), then the two-way schemes also possess a dual representation, where the assisting entanglement resource is actually virtual, that is, it can be replaced by an equivalent random modulation. In this dual (entanglement-free) representation, the advantage brought by the two-way quantum communication can be understood in terms of an iterated use of the uncertainty principle, where Eve is forced to produce a double perturbation of the same quantum channel. For instance, let us consider the Het^2 protocol in the absence of eavesdropping. By heterodyning mode B_1, Bob randomly prepares mode C_1 in a reference coherent state $|\beta\rangle$ containing a random modulation γ known only to him. Then, Alice transforms this state into another coherent state $|\alpha+\beta\rangle$ that is sent back to Bob. By the subsequent heterodyne detection, Bob is able to estimate the total amplitude $\alpha+\beta$ and, therefore, to infer the signal α from his knowledge of β. If we now insert Eve in this scenario, we see that she must estimate both the reference β and the masked signal $\alpha+\beta$ to access the signal α. This implies attacking both the forward and the backward channel (Fig. 5) and, because the noise of the first attack will perturb the second attack, we expect a non-trivial security improvement in the process. Such an effect intuitively holds under the assumption of one-mode attacks (where the two paths are attacked incoherently) and it is indeed confirmed by our analysis. Quantitatively, we have tested the security performances of the two-way protocols against the one-mode Gaussian attacks $\{N, T\}$ and the corresponding security thresholds $N^{\blacktriangleright,\blacktriangleleft} = N^{\blacktriangleright,\blacktriangleleft}(T)$ are shown in Figs 2 and 3 (see the Supplementary Information). For the two-way protocols, such thresholds relate the tolerable excess noise to the transmission in each use of the channel and, therefore, they are directly comparable to the thresholds of the corresponding one-way protocols. By comparing Hom^2 with Hom and Het^2 with Het, we see that the security thresholds are improved almost everywhere (the only exception being Hom^2 for $T > T_c \simeq 0.86$ in direct reconciliation). Such a superadditive behaviour is the central result of this work. Roughly speaking, even if two communication lines (for example, two optical fibres) are too noisy for one-way QKD, they can be combined to enable a two-way QKD, as long as the quantum channel is memoryless.

To deepen our analysis on superadditivity, we also tested the previous one-way and two-way protocols when a classical Bob is replaced by a quantum Bob. This means that Bob is no longer limited to incoherent detections but can access a quantum memory storing all of the modes involved in the quantum communication. Then, Bob carries out a final optimal coherent measurement on all of these modes to retrieve Alice's information. Such a coherent measurement can be disjoint, that is, designed to estimate a single quadrature for each encoding, or joint, that is, designed to estimate both quadratures. Correspondingly, the modified one-way and two-way protocols will be denoted by $\otimes$Hom, $\otimes$Het, $\otimes$Hom^2 and $\otimes$Het^2. Notice that these collective protocols may not admit an equivalent entanglement-free representation (where Bob's entanglement is replaced by a random modulation) if Bob's coherent measurement cannot be reduced to incoherent detection. The corresponding security thresholds are shown in Fig. 2

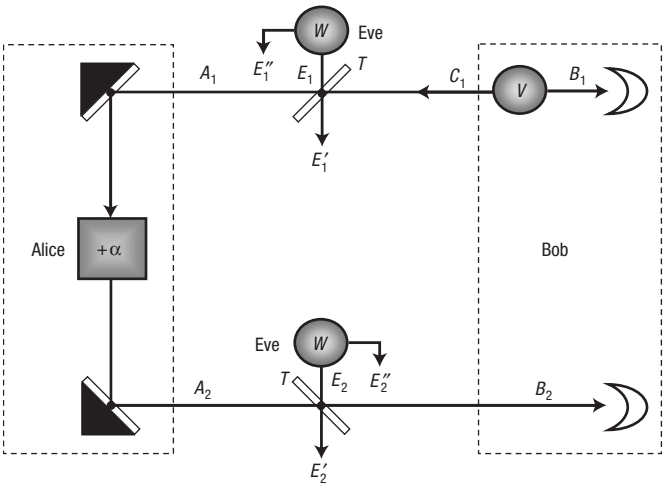

Figure 5 Two-way quantum communication scheme. Bob exploits an EPR pair to assist Alice's encoding. He keeps one mode B_1 while sending the other one C_1 to Alice who, in turn, carries out a stochastic phase-space displacement $+\alpha$. The resulting mode A_2 is then sent back to Bob. The final modes B_1 and B_2 are incoherently detected by means of two homodyne detectors (Hom^2 protocol) or two heterodyne detectors (Het^2 protocol). The figure also shows a one-mode Gaussian attack, where the forward mode C_1 (from Bob to Alice) and the backward one A_2 (from Alice to Bob) are subject to the action of entangling cloners.

(only direct reconciliation can be compared, see Supplementary Information). It is evident that superadditivity holds almost everywhere also for these collective schemes, the only exception being $\otimes$Hom^2 above the same critical value T_c as before. We easily note that $\otimes$Hom coincides with Hom, whereas $\otimes$Hom^2 coincides with Hom^2. Then, in the case of disjoint decoding, the optimal coherent measurement asymptotically coincides with a sequence of incoherent homodyne detections. As a consequence, the collective protocols ($\otimes$Hom and $\otimes$Hom^2) collapse to the corresponding individual protocols (Hom and Hom^2), where there is no need for a quantum memory. In particular, this proves that $\otimes$Hom^2 admits an entanglement-free representation where infinitely squeezed states are sent to Alice through the forward path, and are then homodyned at the output of the backward path. The use of quantum memories does better in the case of joint decoding, because $\otimes$Het and $\otimes$Het^2 have much better performances than the corresponding individual protocols Het and Het^2. As a consequence, no simple entanglement-free representation is known for $\otimes$Het^2.

HYBRID PROTOCOLS

We remark that our previous quantitative cryptoanalysis concerns one-mode Gaussian attacks, which are the cryptographic analogue of a memoryless Gaussian channel. However, when a multiway scheme is considered, a single run of the protocol no longer corresponds to a single use of the channel. As a consequence, the most general collective attack against a multiway scheme, even if incoherent between separate runs, may involve quantum correlations between different channels. In general, an arbitrary collective attack against a two-way scheme can be called a two-mode attack. This is the general scenario of Fig. 4c where the action of this attack on a single round-trip of quantum communication is given by an arbitrary map $\mathcal{E}^2$. On the one hand, such an attack is said to be reducible to a one-mode attack if the map can be symmetrically decomposed as $\mathcal{E}^2 = \mathcal{E} \circ \mathcal{E}$ (the attack can be described by the scenario of Fig. 4b). On the other hand, the two-mode attack is called irreducible if $\mathcal{E}^2 \neq \mathcal{E} \circ \mathcal{E}$ (the attack of Fig. 4c cannot be described by Fig. 4b). The latter situation includes all attacks where some kind of correlation is exploited between the two paths, either if this correlation is classical (so that $\mathcal{E}^2 = \mathcal{E}_2 \circ \mathcal{E}_1$ with $\mathcal{E}_1 \neq \mathcal{E}_2$) or truly quantum (so that $\mathcal{E}^2 \neq \mathcal{E}_2 \circ \mathcal{E}_1$ for every $\mathcal{E}_1$ and $\mathcal{E}_2$).

To detect and handle an irreducible attack, the previous two-way protocols, Hom^2 and Het^2, must be modified into hybrid forms that we denote by Hom^{1,2} and Het^{1,2}. In this hybrid formulation, Alice randomly switches between a two-way scheme and the corresponding one-way scheme, where she simply detects the incoming mode and sends a new one back to Bob. We may describe this process by saying that Alice randomly closes (on) and opens (off) the quantum communication circuit with Bob, the effective switching sequence being communicated at the end of the protocol (Fig. 4d). By publicizing part of the exchanged data, Alice and Bob can carry out tomography of the quantum channels in both the on and off configurations. In particular, they can reconstruct the channel $\mathcal{E}^2$ affecting the two-way trip and the channels $\mathcal{E}_1$ and $\mathcal{E}_2$ affecting the forward and backward paths (see Fig. 4d). Then, they can check the reducibility conditions $\mathcal{E}_1 = \mathcal{E}_2$ and $\mathcal{E}^2 = \mathcal{E}_2 \circ \mathcal{E}_\alpha \circ \mathcal{E}_1$, where $\mathcal{E}_\alpha(\rho) = \hat{D}(\alpha)\rho\hat{D}^\dagger(\alpha)$ is Alice's publicized encoding map. If such conditions are satisfied then the two-mode attack is reducible, that is, Alice and Bob have excluded every kind of quantum and classical correlation between the two paths of the quantum communication (see Supplementary Information for an explicit description). In such a case, the honest users can therefore exploit the superadditivity of the two-way quantum communication. If the previous reducibility conditions are not met, then the honest users can always exploit the instances of one-way quantum communication. Notice that the verification of the reducibility conditions is easy in the Gaussian case, where the channels can be completely reconstructed by analysing the first and second statistical moments of the output states. Also notice that the reducibility conditions exclude every kind of quantum impersonation attack[32], where Eve short-circuits the channels of the two-way quantum communication.

In summary, the hybrid protocols constitute a safe implementation of two-way protocols, at least in the presence of collective Gaussian attacks (one-mode or two-mode). In the hybrid formulation, Alice and Bob can in fact optimize their security on both one-way and two-way quantum communication. The on–off manipulation of the quantum communication can be interpreted as if Alice had two orthogonal bases to choose from during the key distribution process. In the presence of this randomization, Eve is not able to optimize her Gaussian attack with respect to both kinds of quantum communication and the trusted parties can always make the *a posteriori* optimal choice. As a natural development of these results, we can consider a situation where Bob also carries out a random and independent on–off manipulation of the quantum communication. Such a scheme naturally leads to instances of n-way quantum communication (with $n > 2$) with security properties that would be interesting to inspect in future work. In general, our results pave the way for future investigations in the domain of secure multiple quantum communications, where quantum communication circuits can in principle grow to higher and higher complexity.

Received 3 September 2007; accepted 5 June 2008; published 11 July 2008.

References

1. Braunstein, S. L. & Pati, A. K. *Quantum Information Theory with Continuous Variables* (Kluwer–Academic, Dordrecht, 2003).
2. Braunstein, S. L. & van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **77**, 513–577 (2005).
3. Eisert, J. & Plenio, M. B. Introduction to the basics of entanglement theory in continuous-variable systems. *Int. J. Quantum Inf.* **1**, 479–506 (2003).

4. Ferraro, A., Olivares, S. & Paris, M. G. A. *Gaussian States in Quantum Information* (Bibliopolis, Napoli, 2005).
5. Hillery, M. Quantum cryptography with squeezed states. *Phys. Rev. A* **61**, 022309 (2000).
6. Ralph, T. C. Continuous variable quantum cryptography. *Phys. Rev. A* **61**, 010303(R) (2000).
7. Ralph, T. C. Security of continuous-variable quantum cryptography. *Phys. Rev. A* **62**, 062306 (2000).
8. Reid, M. D. Quantum cryptography with a predetermined key, using continuous-variable Einstein–Podolsky–Rosen correlations. *Phys. Rev. A* **62**, 062308 (2000).
9. Gottesman, D. & Preskill, J. Secure quantum key distribution using squeezed states. *Phys. Rev. A* **63**, 022309 (2001).
10. Cerf, N. J., Lévy, M. & Van Assche, G. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A* **63**, 052311 (2001).
11. Grosshans, F. & Grangier, Ph. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002).
12. Grosshans, F. *et al*. Quantum key distribution using Gaussian-modulated coherent states. *Nature* **421**, 238–241 (2003).
13. Iblisdir, S., Van Assche, G. & Cerf, N. J. Security of quantum key distribution with coherent states and homodyne detection. *Phys. Rev. Lett.* **93**, 170502 (2004).
14. Grosshans, F. & Cerf, N. J. Continuous-variable quantum cryptography is secure against non-Gaussian attacks. *Phys. Rev. Lett.* **92**, 047905 (2004).
15. Weedbrook, C. *et al*. Quantum cryptography without switching. *Phys. Rev. Lett.* **93**, 170504 (2004).
16. Lance, A. M. *et al*. No-switching quantum key distribution using broadband modulated coherent light. *Phys. Rev. Lett.* **95**, 180503 (2005).
17. Silberhorn, Ch. *et al*. Continuous variable quantum cryptography: Beating the 3 dB loss limit. *Phys. Rev. Lett.* **89**, 167901 (2002).
18. Namiki, R. & Hirano, T. Practical limitation for continuous-variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **92**, 117901 (2004).
19. Namiki, R. & Hirano, T. Security of continuous-variable quantum cryptography using coherent states: Decline of postselection advantage. *Phys. Rev. A* **72**, 024301 (2005).
20. Namiki, R. & Hirano, T. Efficient-phase-encoding protocols for continuous-variable quantum key distribution using coherent states and postselection. *Phys. Rev. A* **74**, 032302 (2006).
21. Heid, M. & Lütkenhaus, N. Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction. *Phys. Rev. A* **73**, 052316 (2006).
22. Grosshans, F., Cerf, N. J., Wenger, J., Tualle-Brouri, R. & Grangier, Ph. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Quantum. Inf. Comput.* **3**, 535–552 (2003).
23. Van Assche, G., Cardinal, J. & Cerf, N. J. Reconciliation of a quantum-distributed Gaussian key. *IEEE Trans. Inf. Theory* **50**, 394–400 (2004).
24. Navascués, M., Grosshans, F. & Acín, A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.* **97**, 190502 (2006).
25. García-Patrón, R. & Cerf, N. J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **97**, 190503 (2006).
26. Renner, R., Gisin, N. & Kraus, B. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A* **72**, 012332 (2005).
27. Renner, R. *Security of Quantum Key Distribution*. PhD thesis, Swiss Federal Institute of Technology (ETH) Zurich (2005).
28. Lodewyck, J. & Grangier, Ph. Tight bound on coherent states quantum key distribution with heterodyne detection. *Phys. Rev. A* **76**, 022332 (2007).
29. Sudjana, J., Magnin, L., García-Patrón, R. & Cerf, N. J. Tight bounds on the eavesdropping of a continuous-variable quantum cryptographic protocol with no basis switching. *Phys. Rev. A* **76**, 052301 (2007).
30. Grosshans, F. Collective attacks and unconditional security in continuous variable quantum key distribution. *Phys. Rev. Lett.* **94**, 020504 (2005).
31. Navascués, M. & Acín, A. Security bounds for continuous variables quantum key distribution. *Phys. Rev.Lett.* **94**, 020505 (2005).
32. Dušek, M., Haderka, O., Hendrych, M. & Myška, R. Quantum identification system. *Phys. Rev. A* **60**, 149–156 (1999).

Supplementary Information accompanies this paper on www.nature.com/naturephysics.

Acknowledgements

The research of S.P. was supported by a Marie Curie Outgoing International Fellowship within the 6th European Community Framework Programme (Contract No. MOIF-CT-2006-039703). S.P. thanks CNISM for hospitality at Università di Camerino and Gaetana Spedalieri for her moral and logistic support. S.L. was supported by the W.M. Keck centre for extreme quantum information processing (xQIT).

Author information

Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions.
Correspondence and requests for materials should be addressed to S.P.