Quantum cryptography with an ideal local relay

Spedalieri, Gaetana; Ottaviani, Carlo; Braunstein, Samuel L.; Gehring, Tobias; Jacobsen, Christian Scheffmann; Andersen, Ulrik Lund; Pirandola, Stefano

Published in:
Electro-Optical and Infrared Systems: Technology and Applications XII; and Quantum Information Science and Technology

Link to article, DOI:
10.1117/12.2202662

Publication date:
2015

Document Version
Publisher's PDF, also known as Version of record

Invited Paper

Quantum cryptography with an ideal local relay

Gaetana Spedalieri[a], Carlo Ottaviani[a], Samuel L. Braunstein[a], Tobias Gehring[b], Christian S. Jacobsen[b], Ulrik L. Andersen[b], and Stefano Pirandola[a]

[a]Computer Science and York Centre for Quantum Technologies,University of York, Deramore Lane, York YO10 5GH, United Kingdom

[b]Department of Physics, Technical University of Denmark, Fysikvej, 2800 Kongens Lyngby, Denmark

ABSTRACT

We consider two remote parties connected to a relay by two quantum channels. To generate a secret key, they transmit coherent states to the relay, where the states are subject to a continuous-variable (CV) Bell detection. We study the ideal case where Alice's channel is lossless, i.e., the relay is locally in her lab and the Bell detection is perfomed with unit efficiency. This configuration allows us to explore the optimal performances achievable by CV measurement-device-independent quantum key distribution. This corresponds to the limit of a trusted local relay, where the detection loss can be re-scaled. Our theoretical analysis is confirmed by an experimental simulation where 10^{-4} secret bits per use can potentially be distributed at 170km assuming ideal reconciliation.

1. INTRODUCTION

Quantum key distribution (QKD)[1,2] is a central area in quantum information science.[3,4] A typical QKD protocol involves two parties, Alice and Bob, who generate secret keys by exchanging quantum systems over an insecure communication channel. Another scenario involves a swapping-like protocol[5] where secret correlations are established by the measurement of a third untrusted party (relay). This idea of 'measurement-device independence' (MDI)[5–15] has been extended to continuous-variable (CV) systems,[16,17] with the possibility of much higher key rates.

In this paper, we study consider a limit configuration for CV-MDI-QKD, where the relay is in Alice's lab and performs an ideal Bell detection. This is an extrapolation which allows us to investigate the maximal rate/distance performances achievable by CV-MDI-QKD. Experimentally, this is equivalent to consider a local relay where the loss associated with the various technical imperfections (such as the detector inefficiencies) can be re-scaled and therefore neglected. As a matter of fact, this limit case corresponds to the case where the loss of the relay is trusted.

Our theoretical analysis, confirmed by an experimental simulation, shows that 10^{-2} secret bits per relay use can be distributed at 10dB loss in Bob's channel, equivalent to 50km of standard optical fibre (at the loss rate of 0.2dB/km). Assuming ideal reconciliation, a potential rate of about 10^{-4} secret bits per relay use can be distributed over a very lossy link, i.e., 34dB loss corresponding to 170km of fibre.

2. PROTOCOL

The scheme is depicted in Fig. 1. At one side, Alice prepares a mode A in a coherent state $|\alpha\rangle$ with Gaussian-modulated amplitude α; at the other side, Bob prepares mode B in another coherent state $|\beta\rangle$ with Gaussian-modulated amplitude β (Gaussian distributions have zero mean and large variance). Modes A and B are sent to the relay, which performs a CV Bell detection,[18] by mixing the modes in a balanced beam splitter whose output ports are conjugately homodyned with outputs q_- and p_+. The complex variable $\gamma := (q_- + ip_+)/\sqrt{2}$ is then communicated to Alice and Bob via a classical public channel. Since $\gamma \simeq \alpha - \beta^*$, each party may infer the variable of the other party by postprocessing.

Further author information: Send correspondence to G.S. (gae.spedalieri@york.ac.uk)

Electro-Optical and Infrared Systems: Technology and Applications XII; and Quantum Information Science and Technology, edited by David A. Huckridge, Reinhard Ebert, Mark T. Gruneisen, Miloslav Dusek, John G. Rarity, Proc. of SPIE Vol. 9648, 96480Z · © 2015 SPIE · CCC code: 0277-786X/15/$18 · doi: 10.1117/12.2202662

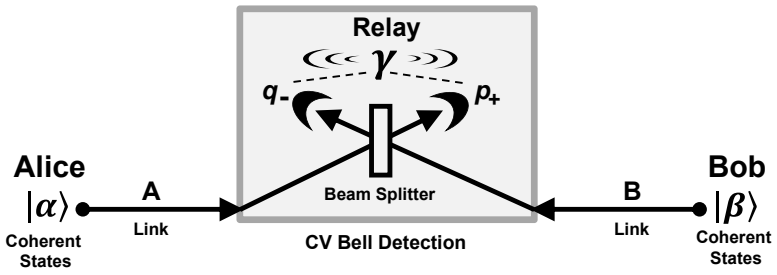

Figure 1. Basic protocol. See text for explanations.

The most general eavesdropping strategy is a joint attack involving both the relay and the two links.[16,17] Here we consider the simple case where Eve attacks Bob's link B only, by means of a Gaussian attack[19] which introduces loss and thermal noise. The travelling mode B is mixed with an ancillary mode E by a beam splitter with transmissivity τ. The ancilla introduces thermal noise with variance ω and belongs to a reservoir of ancillas under Eve's control. This kind of entangling-cloner attack[4] is repeated for each use of the relay and the output ancillas are finally detected by Eve by means of an optimized collective quantum measurement.

3. SECRET-KEY RATE

By specializing the formulas of CV-MDI-QKD,[16] we can derive the secret-key rate for the scenario depicted in Fig. 2. Assuming ideal reconciliation efficiency and large modulation, the key rate is given by

$$R = h\left(\frac{\chi}{1+\tau}-1\right) - h\left[\frac{\tau\chi-(1+\tau)^2}{1-\tau^2}\right] + \log_2\left[\frac{2(1+\tau)}{e(1-\tau)\chi}\right], \tag{1}$$

where

$$h(x) := \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2}, \tag{2}$$

and χ is the equivalent noise, decomposable as $\chi = \chi_{\rm loss} + \varepsilon$, where $\chi_{\rm loss} = 2(1+\tau)/\tau$ is the noise due to loss, while ε is the 'excess noise'. The maximum theoretical performance of the protocol, with respect to the loss present in Bob's link, is reached for $\varepsilon = 0$. In this case, we have

$$R_{\rm loss} = h[(2-\tau)/\tau] + \log_2[\tau/(1-\tau)e], \tag{3}$$

which goes to zero only for $\tau \to 0$, corresponding to Bob arbitrarily far from the relay. It is easy to convert transmissivity τ to distance d in optical fibre, by considering the standard loss rate of 0.2dB/km.

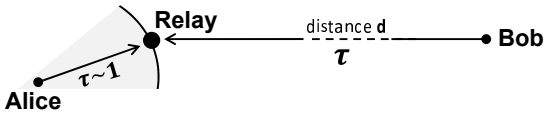

Figure 2. Key-distribution via an ideal local relay. This is locally in Alice's lab and it is assumed to work perfectly (unit quantum efficiency). By contrast, Bob's link has transmissivity $\tau < 1$ corresponding to some distance d in standard optical fibre. Bob's channel can also be affected by thermal/excess noise.

In the scenario of Fig. 2, Bob can be very far from the relay also in the presence of non-zero excess noise $\varepsilon \neq 0$, with potential distances beyond 100 km of simulated fibre. This can be seen from the numerical results shown in Fig. 3, where the solid line represents the case of a pure-loss attack ($\varepsilon = 0$), while the dashed curve corresponds to an attack with non-zero excess noise, in particular $\varepsilon = 0.02$. We can see the robustness of the key rate with respect to the excess noise.

This theoretical analysis is also confirmed by a proof-of-principle experiment where we have realized the local ideal relay by suitably re-scaling the loss in Alice's link in the post-processing of the data. We have reproduced the

extreme asymmetric configuration of Fig. 2, with variable Bob's transmissivity τ, down to 4×10^{-4} corresponding to about 170km in standard optical fibre. For every experimental point, we have evaluated the key rate R assuming ideal reconcilation efficiency $\xi = 1$. Experimental results are plotted in Fig. 3 and compared with the theoretical predictions, with excellent agreement. The extrapolated experimental rate approaches the theoretical limit of the pure-loss attack. Due to imperfections, we have an excess noise $\varepsilon \lesssim 0.02$. Note that we can potentially reach $R \simeq 10^{-4}$ secret bits per relay use over a link with 34dB loss, equivalent to 170km of optical fibre.

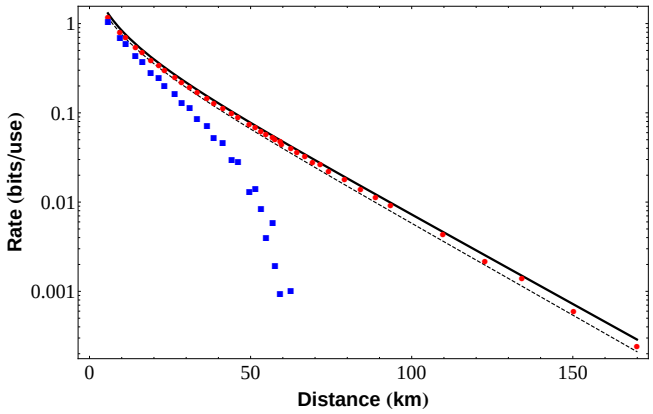

Figure 3. Secret-key rate R versus Bob's distance d from the relay. Experimental points refer to ideal reconciliation ($\xi = 1$, red circles) and realistic reconciliation ($\xi \simeq 0.97$, blue squares). For comparison, we also plot the theoretical rates for a pure-loss attack (solid line) and a Gaussian attack with excess noise $\varepsilon = 0.02$ (dashed line).

Note that the current reconciliation procedures for CV protocols do not have unit efficiency (indeed this is one of the main factors limiting the distance of CV-QKD). By taking this limitation into account[20] ($\xi \simeq 0.97$), we can still reach remarkably high rates over distances well beyond the typical connection lengths of a network. As we can see from Fig. 3, one can potentially achieve $R \simeq 10^{-2}$ secret bits per relay use over a link with 10dB loss, equivalent to 50km of optical fibre.

4. CONCLUSION

In this work, we have explored the maximal performances in terms of rates and distances achievable by CV-MDI-QKD with coherent states. We have considered the extreme configuration where the relay is in Alice's lab and the Bell detection is ideally performed. An important feature of this protocol is the simplicity of the relay, which does not possess any quantum source but just performs a standard optical measurement, with all the heavy procedures of data post-processing left to the end-users, fulfilling the idea behind the end-to-end principle.[21] CV Bell detection involves highly efficient photodetectors plus linear optics, whereas the discrete-variable version of this measurement needs nonlinear elements to operate deterministically. This feature combined with the use of coherent states makes the scheme very attractive, guaranteeing both cheap implementation and extremely high rates.

Our study also shows how improvements in the classical reconciliation techniques (from $\xi \simeq 0.97$ to $\xi = 1$) have a dramatic impact on the performances of the protocol, which means that the development of more efficient classical codes for error correction and privacy amplification is a central task in CV-QKD. Finally, future investigations could involve the explicit security analysis of mixed technology environments where some of the connections are established at low frequencies (infrared or microwave) where thermal effects become important.[22–24]

Acknowledgments

This work was supported by EPSRC (Grants EP/J00796X/1 and EP/L011298/1) and the Leverhulme Trust.

REFERENCES

1. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).
2. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dusek, M., Lutkenhaus, N. & Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).
3. Wilde, M. M. *Quantum Information Theory* (Cambridge University Press, Cambridge, 2013).
4. Weedbrook, C., Pirandola, S., Garcia-Patron, R., Cerf, N. J., Ralph, T. C., Shapiro, J. H. & Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621 (2012).
5. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).
6. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
7. Ma, X., Fred Fung, C.-H. & Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 052305 (2012).
8. Ma, X. & Razavi, M. Alternative schemes for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 062319 (2012).
9. Wang, X.B. Three-intensity decoy state method for device independent quantum key distribution with basis dependent errors. *Phys. Rev. A* **87**, 012320 (2013).
10. Branciard, C., Rosset, D., Liang, Y.-C. & Gisin, N. Measurement-device-independent entanglement witnesses for all entangled quantum states. *Phys. Rev. Lett.* **110**, 060405 (2013).
11. Tomamichel, M., Fehr, S., Kaniewski, J. & Wehner, S. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New J. Phys.* **15**, 103002 (2013).
12. Ci Wen Lim, C., Portmann, C., Tomamichel, M., Renner, R. & Gisin, N. Device-independent quantum key distribution with local Bell test. *Phys. Rev. X* **3**, 031006 (2013).
13. Abruzzo, S., Kampermann, H., & Bruß D. Measurement-device-independent quantum key distribution with quantum memories. *Phys. Rev. A* **89**, 012301 (2014).
14. Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I. & Tittel, W. Real-World two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.* **111**, 130501 (2013).
15. Ferreira da Silva, T., Vitoreti, D., Xavier, G. B., do Amaral, G. C., Temporão, G. P. & von der Weid, J. P. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A* **88**, 052303 (2013).
16. Pirandola, S., et al. High-rate measurement-device-independent quantum cryptography. Nature Photon. **9**, 397–402 (2015).
17. Ottaviani, C., Spedalieri, G., Braunstein, S. L. & Pirandola, S. Continuous-variable quantum cryptography with an untrusted relay: Detailed security analysis of the symmetric configuration. Phys. Rev. A **91**, 022320 (2015).
18. Spedalieri, G., Ottaviani, C. & Pirandola, S. Covariance matrices under Bell-like detections. *Open Syst. Inf. Dyn.* **20**, 1350011 (2013).
19. Pirandola, S., Braunstein, S. L. & Lloyd, S. Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography. *Phys. Rev. Lett.* **101**, 200504 (2008).
20. Jouguet, P., Kunz-Jacques, S., & Leverrier, A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. *Phys. Rev. A* **84**, 062317 (2011).
21. Saltzer, J. H., Reed, D. P. & Clark, D. D. End-to-end arguments in system design. *Proceedings of the Second International Conference on Distributed Computing Systems* (Paris, France, April 8-10, 1981).
22. Weedbrook, C., Pirandola, S., Lloyd, S. & Ralph, T. C. Quantum cryptography approaching the classical limit. *Phys. Rev. Lett.* **105**, 110501 (2010).
23. Weedbrook, C., Pirandola, S. & Ralph, T. C. Continuous-variable quantum key distribution using thermal states. *Phys. Rev. A* **86**, 022318 (2012).
24. Weedbrook, C., Ottaviani, C., & Pirandola, S. Two-way quantum cryptography at different wavelengths. *Phys. Rev. A* **89**, 012309 (2014).