High-rate measurement-device-independent quantum cryptography

Stefano Pirandola,[1] Carlo Ottaviani,[1] Gaetana Spedalieri,[1] Christian Weedbrook,[2, 3] Samuel L. Braunstein,[1] Seth Lloyd,[4] Tobias Gehring,[5] Christian S. Jacobsen,[5] and Ulrik L. Andersen[5]

[1] *Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, UK*
[2] *Department of Physics, University of Toronto, Toronto M5S 3G4, Canada*
[3] *QKD Corporation, 112 College Street, Toronto M5G 1L6, Canada*
[4] *Department of Mechanical Engineering and Research Laboratory of Electronics,*
Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA
[5] *Department of Physics, Technical University of Denmark, Fysikvej, 2800 Kongens Lyngby, Denmark*

(Dated: June 29, 2015)

Quantum cryptography achieves a formidable task — the remote distribution of secret keys by exploiting the fundamental laws of physics. Quantum cryptography is now headed towards solving the practical problem of constructing scalable and secure quantum networks. A significant step in this direction has been the introduction of measurement-device independence, where the secret key between two parties is established by the measurement of an untrusted relay. Our protocol could be employed to build high-rate quantum networks where devices securely connect to nearby access points or proxy servers, while at the same time eliminating many possible side-channels, preventing their exploitation in in-field implementations.

PACS numbers: 03.67.Dd, 03.67.Hk, 03.67.-a
Keywords: quantum key distribution; continuous variables; quantum information

In a recent publication [1], we present a proof of the security of a measurement-device-independent quantum key distribution protocol using continuous variables, specifically coherent states, and we further present a proof-of-principle experiment, showing the feasibility of the protocol. This presents a significant advance of measurement-device independent (MDI) protocols [2–11], while also advancing the field of continuous variable quantum cryptography [12–20] from the conventional point-to-point structure, to an end-to-end structure.

More specifically we show, theoretically as well as experimentally, that Alice and Bob can communicate indirectly through an untrusted third party, while still maintaining security. Their respectively generated coherent states are sent to a relay controlled by this third party, which could very well be the eavesdropper. The relay performs a continuous variable Bell detection which, after having publicly announced the result, allows the relay to establish correlations between Alice and Bob, without correlating either of them with the relay. The proof-of-principle experiment was performed in free space at 1,064 nm, see fig. 1.

We find, see fig. 2, that the optimal configuration of the investigated protocol is an asymmetric one, that is low loss for Alice allows Bob to tolerate a high amount of loss, while still maintaining rates that surpass qubit-based MDI protocols [2, 9–11].

In conclusion we have demonstrated the security of a continuous variable measurement-device independent quantum key distribution protocol, discussed the applications of asymmetric network configurations and performed a proof-of-principle experiment which produces high transfer rates compared to previous work.

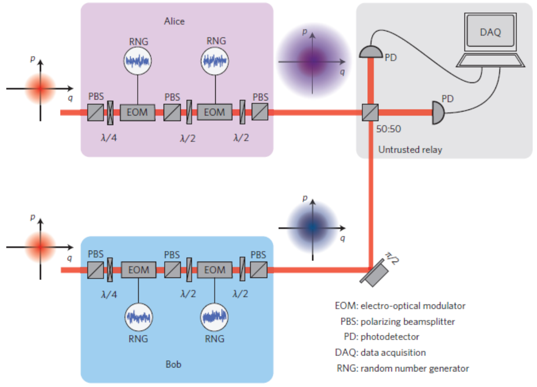

Figure 1. Free-space experimental set-up. Alice and Bob apply amplitude and phase modulators to a pair of identical classical phase-locked bright coherent beams. Alice's and Bob's stations are private spaces whose internal loss and noise are fully trusted. Losses in the links are simulated by suitably attenuating the variances of the modulations. At the relay, the modes are mixed in a balanced beamsplitter and the output ports photodetected. Photocurrents are finally processed to realise a CV Bell measurement.

[1] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nature Photonics **9**, 397 (2015)

[2] H.-K. Lo, M. Curty, and B. Qi, Physical Review Letters **108**, 1 (2012)

[3] X. Ma and M. Razavi, Physical Review A - Atomic, Molecular, and Optical Physics **86**, 1 (2012)

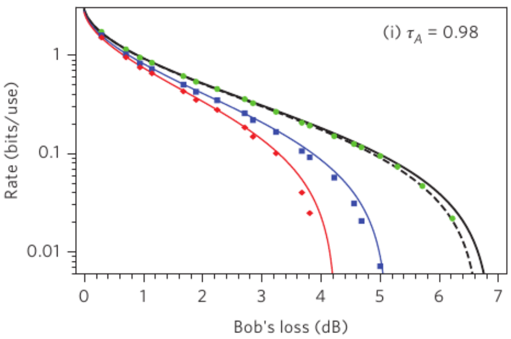

Figure 2. Experimental results (points) and comparison with theoretical predictions (lines), for varying reconciliation efficiencies. The dashed black line is the same as the black line, but with added excess noise which was also present in the experiment.

[4] X. B. Wang, Physical Review A - Atomic, Molecular, and Optical Physics **87**, 1 (2013)

[5] C. Branciard, D. Rosset, Y. C. Liang, and N. Gisin, Physical Review Letters **110**, 060405 (2013)

[6] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner, New Journal of Physics **15** (2013)

[7] C. C. W. Lim, C. Portmann, M. Tomamichel, R. Renner, and N. Gisin, Physical Review X **3**, 1 (2013)

[8] S. Abruzzo, H. Kampermann, and D. Bruß, Physical Review A - Atomic, Molecular, and Optical Physics **89**, 1 (2014)

[9] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Physical Review Letters **111**, 1 (2013)

[10] T. Ferreira Da Silva, D. Vitoreti, G. B. Xavier, G. C. Do Amaral, G. P. Temporão, and J. P. Von Der Weid, Physical Review A - Atomic, Molecular, and Optical Physics **88**, 1 (2013)

[11] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, Physical Review Letters **113**, 190501 (2014)

[12] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Reviews of Modern Physics **84**, 621 (2012)

[13] N. J. Cerf, M. Levy, and G. Van Assche, Physical Review A **63**, 052311 (2001)

[14] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003)

[15] J. Lodewyck and P. Grangier, Physical Review A **76**, 022332 (2007)

[16] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Physical Review Letters **93**, 170504 (2004)

[17] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Nature Physics **4**, 12 (2008)

[18] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, Physical Review Letters **105**, 110501 (2010)

[19] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, Nature Communications **3**, 1083 (2012)

[20] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nature Photonics **7**, 378 (2013)