Thermal State Quantum Key Distribution

Adam Walton[1], Ben Varcoe, David Jennings, Anne Ghesquière

University of Leeds

[1]pyaw@leeds.ac.uk

1. Introduction

- Current classical methods of key distribution assume that an attacker cannot solve certain mathematical problems in a reasonable time [1].
- Quantum Key Distribution (QKD) protocols instead base security on the laws of quantum mechanics [2-3].
- This allows for secure communication against an eavesdropper with arbitrarily large computing power.
- We use quadrature measurements from a thermal source, directed at two parties using a beam splitter, to produce a key.
- Such thermal sources are already commonly used in modern communication, such as in WiFi and Bluetooth.

2. Method

- Light from a thermal source is split at a beam splitter, with output beams directed at Alice and Bob, who wish to share a key for communication. This is shown in Figure 1.
- Eve intercepts Bob's beam with her own beam splitter of unknown transmittance, T.
- Double homodyne detection produces correlated measurements between each person, which are used to derive bit strings.
- A Monte Carlo simulation was used to model the protocol. Additionally, the covariance matrix at each point in the protocol was calculated. These are used to calculate Shannon and von Neumann entropy between each pair of people.
- Successful key distribution requires $I(A:B) > I(A:E)$ or $I(A:B) > I(B:E)$.

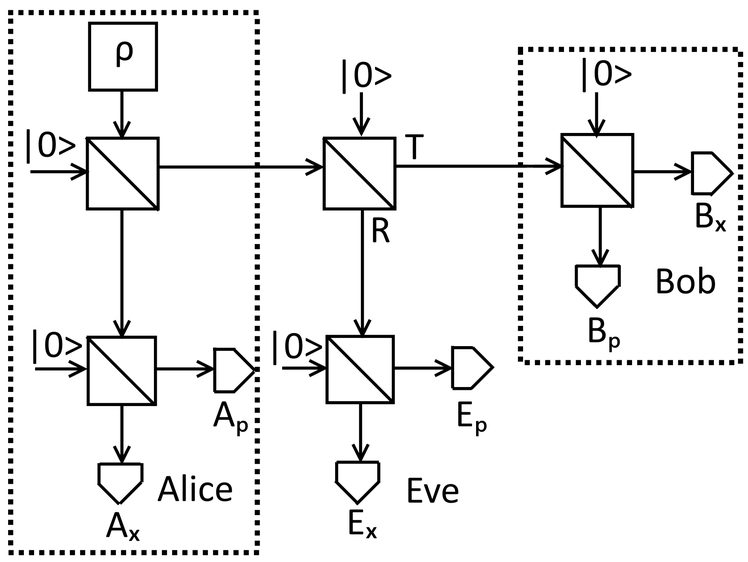

Fig. 1: **The thermal state protocol.** Thermal light described by the state ρ is split at a series of beam splitters. Alice, Bob, and Eve perform measurements on their received beams to produce bit strings.

3a. Results

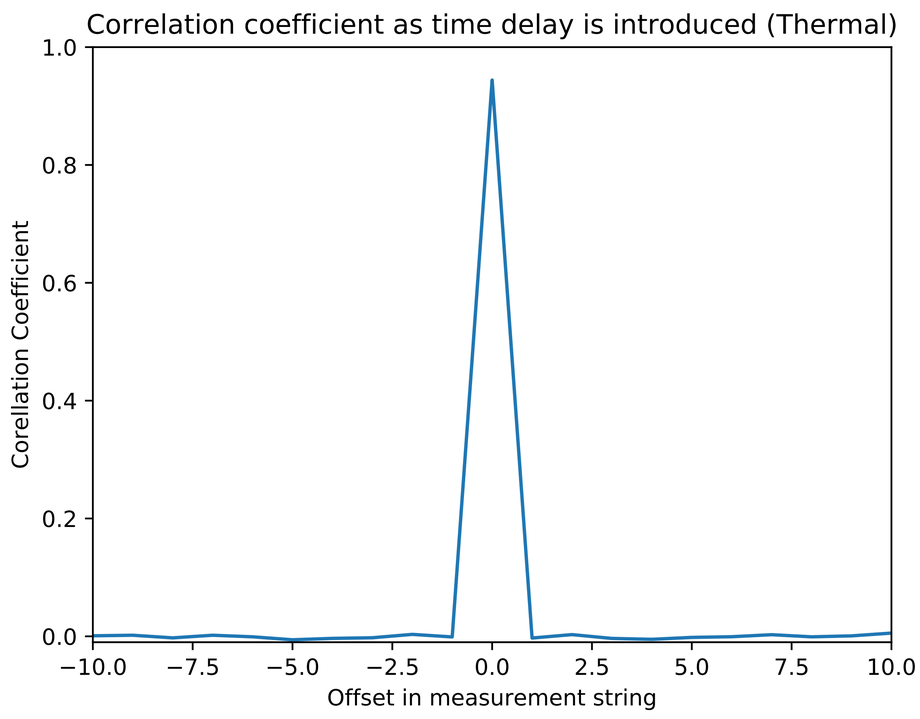

Fig. 2: **Correlations.** Correlation coefficients of measurement results as Alice and Bob's data streams are offset with respect to each other. Correlations in the beams are still detected after multiple beam splitters.

3b. Results

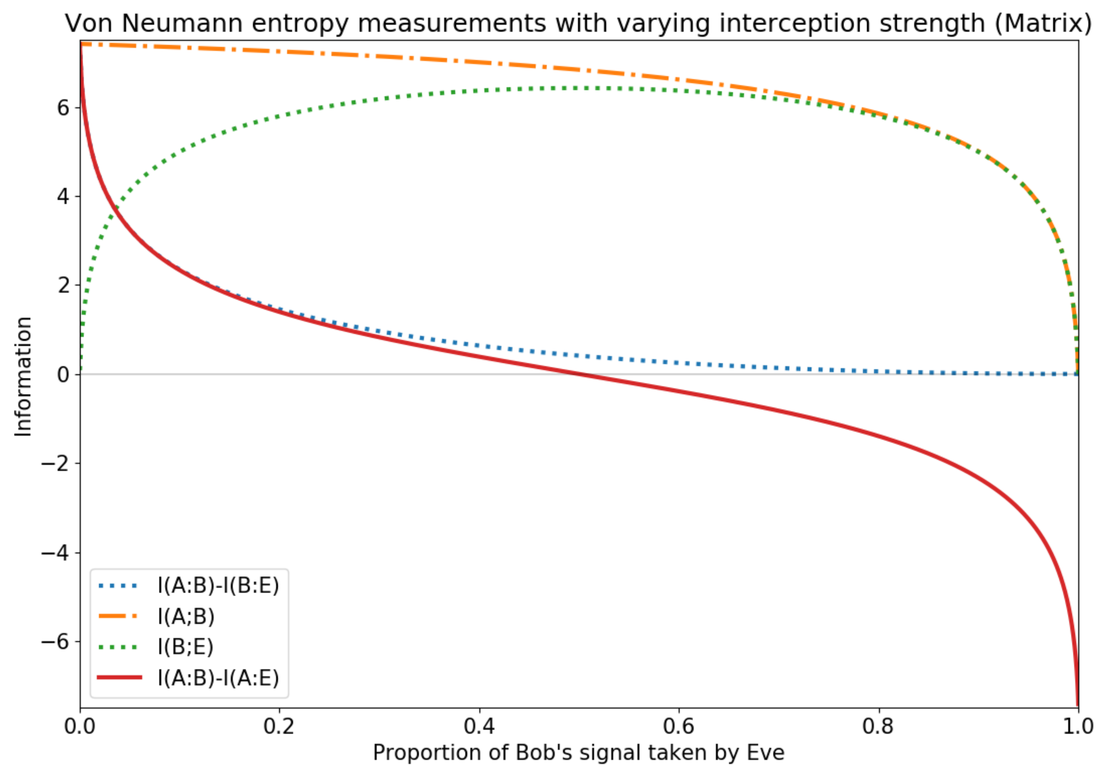

Fig. 3: **Eve's interception.** Mutual information changes as Eve's interception strength increases.

- Figure 2 shows that the correlations survive the protocol, and can therefore be used to produce keys. Coherent sources lack such correlations, and are not appropriate for this protocol [4].
- $I(A:B) - I(A:E) > 0$ only holds if Eve's beam splitter reflects less than 50% of Bob's beam.
- When calculating von Neumann entropy, $I(A:B) - I(B:E) > 0$ holds as long as Bob receives a nonzero proportion of the beam sent to them.
- Calculating Shannon mutual information through simulated bit strings produces similar behaviour as Eve's transmittance is changed.
- Bob can correct Alice's errors to ensure that they have the same bit string. Therefore Alice and Bob will be able to create usable keys using this protocol.

4. Conclusions

- With a perfect Eve, a lower bound on key rate remains positive provided Bob receives some of the beam sent to them.
- This is supported by two different methods of calculating mutual information.
- Thermal sources are already used in many forms of modern communication, providing an application for this protocol.
- Future work involves carrying out the protocol experimentally using transceivers and power splitters, and is able to produce correlated bit strings between Alice, Bob and Eve.
- Additional work also focused on adding loss or displacing the thermal source. Key distribution continued to be possible even with large loss on Bob's beam, before or after interception.

Acknowledgements

This project is undertaken under the supervision of Prof. Ben Varcoe and Dr. David Jennings. Simulation work was undertaken on ARC4, part of the High Performance Computing facilities at the University of Leeds, UK. This work was supported by the Northern Triangle Initiative Connecting capability fund as well as funding from the UK Quantum Technology Hub for Quantum Communications Technologies EP/M013472.

Citations

[1] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM, 21(2):120–126, Feb 1978.

[2] C. H. Bennett, F. Bessette, G. Brassard, Louis. Salvail, and J. Smolin. Experimental quantum cryptography. In Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology, EUROCRYPT '90, pages 253–265, Berlin, Heidelberg, 1991.

[3] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science, 560:7–11, Dec 2014.

[4] R. Loudon. Photon bunching and antibunching. Physics Bulletin, 27(1):21–23, Jan 1976.

UNIVERSITY OF LEEDS

LaTeX Tikzposter