Master 2 project: Entropic uncertainty relations and semi device-independent quantum key distribution

Advisor: Andreas Bluhm andreas.bluhm@univ-grenoble-alpes.fr

Length: 4-6 months

Deadline: Please get in touch before **November 24**

Keywords: Quantum information theory, quantum cryptography, uncertainty relations, quantum steering, quantum entropies

Desirable qualifications: Familiarity with the formalism of finite-dimensional quantum mechanics or quantum information, knowledge of linear algebra, ability to write mathematical proofs, programming skills

Quantum cryptography is special in the sense that it uses physical principles instead of computational assumptions in order to guarantee security of communication [1, 2]. One of the best known tasks is *quantum key distribution* (QKD) [3], in which two parties want to generate a secret key by performing measurements on a shared quantum state and communicating their choice of measurement basis publicly. The most famous such protocol is named after their inventors and the year of publication and therefore known as the BB84 protocol [4]. For this to work, however, the parties need to trust that their devices are doing what the manufacturers claim they do, otherwise the protocol is insecure.

However, quantum mechanics offers a way to avoid making this assumption. By verifying that the correlations between the measurement outcomes of the two parties satisfy certain inequalities, so-called Bell-inequalities, the two parties can be sure that their devices are doing what they are supposed to do and hence that the key they share at the end of the protocol is actually secret. These type of protocols are known as *device-independent quantum key distribution* (DIQKD) [5].

While DIQKD provides the highest level of security available, there is a price to pay. It turns out that the key rates, i.e., the number of secret random bits produced by the protocols, are much lower and experimental realizations are still far from being useful in practice. That is why it becomes interesting to study a compromise between security and key rates. The idea is the following: Imagine you want to do online banking. For that to work, you need to establish a secret key between you and your bank. While the bank has the money to invest in secure infrastructure, you most likely do not. Therefore, it is reasonable to assume that the bank's devices work as planned, but your own devices do not necessarily. This is known as *semi device-independent quantum key distribution* (semi DIQKD) (sometimes also called one-sided DIQKD) [6].

To prove security of such protocols, one can use *entropic uncertainty relations* [7]. These quantify the well-known fact that one cannot know precisely the position and momentum of a quantum particle at the same time. More general, if one has two incompatible measurements, it is not possible to have good knowledge about the outcomes of both these measurements at the same time. The notion of uncertainty about the outcome of a measurement is quantified using so called *entropies*, which are mathematical objects appearing all over information theory. The easiest entropic uncertainty relation is the one by Maassen and Uffink [7]:

$$H(X) + H(Z) \geq \log \frac{1}{c}\,. \tag{1}$$

In words, it says that the uncertainty about the oucome of measurement X and the outcome of measurement Z on the same particle cannot both be small, where the number c encodes how different X and Z are. While good entropic uncertainty relations (also taking into account possible quantum side information) exist for two measurements [8, 9], there are no analogous entropic uncertainty relations for three measurements.

The aim of the project is therefore to prove new entropic uncertainty relations for three measurements and to use them in order to find better protocols for semi DIQKD, meaning higher key rates. To achieve that, the idea will be to understand proofs of existing entropic uncertainty relations and based on this to develop a strategy to extend these proofs to three measurements. Subsequently, following the strategy in [6] gives security proofs for more complex semi DIQKD protocols.

This master project could potentially lead to a PhD project on quantum cryptography.

References

[1] Renner, R. & Wolf, R. Quantum advantage in cryptography. *AIAA Journal* **61**, 1895–1910 (2023). URL https://arxiv.org/abs/2206.04078.

[2] Vidick, T. & Wehner, S. *Introduction to Quantum Cryptography* (Cambridge University Press, 2023).

[3] Wolf, R. *Quantum Key Distribution. An Introduction with Exercises.* No. 988 in Lecture Notes in Physics (Springer, 2021).

[4] Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science* **560**, 7–11 (2014). URL https://arxiv.org/abs/2003.06557.

[5] Masanes, L., Pironio, S. & Acín, A. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature Communications* **2**, 238 (2011). URL https://www.nature.com/articles/ncomms1244.pdf.

[6] Branciard, C., Cavalcanti, E. G., Walborn, S. P., Scarani, V. & Wiseman, H. M. One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering. *Physical Review A* **85**, 010301 (2012). URL https://arxiv.org/abs/1109.1435.

[7] Coles, P. J., Berta, M., Tomamichel, M. & Wehner, S. Entropic uncertainty relations and their applications. *Reviews of Modern Physics* **89**, 015002 (2017). URL https://arxiv.org/abs/1511.04857.

[8] Berta, M., Christandl, M., Colbeck, R., Renes, J. M. & Renner, R. The uncertainty principle in the presence of quantum memory. *Nature Physics* **6**, 659–662 (2010). URL https://www.nature.com/articles/nphys1734.

[9] Tomamichel, M. & Renner, R. Uncertainty relation for smooth entropies. *Physical Review Letters* **106**, 110506 (2011). URL https://arxiv.org/abs/1009.2015.