Stage M2 Recherche
Distilling Bell-nonlocality for quantum cryptography*

Jean-Daniel Bancal[1], Peter Brown[2], and Mirjam Weilenmann[3]

[1]CEA, Institut de physique théorique
[2]Télécom Paris, LTCI
[3]IQOQI Vienna

December 5, 2022

1 Motivation and context

Bell-nonlocality
Entangled quantum systems can exhibit a phenomenon known as *nonlocality.* Following Fig. 1, imagine an experiment in which two devices are given random and independent inputs X, Y from which they must produce outputs A, B (all coming from finite sets) and the two devices cannot communicate to each other. Running the experiment will lead to some conditional probability distribution $P_{AB|XY}$. Suppose the experiment is "classical", so prior to the experiment the devices shared some information (which we can model as a random variable Λ) and using this information, together with their respective inputs they produce an output. In this setting, the distribution will factorize as

$$P(a,b|x,y) = \sum_{\lambda \in \Lambda} P(\lambda) P(a|x,\lambda) P(b|y,\lambda) \tag{1}$$

and we call such a distribution *local* – the outputs A and B only depend on the local information available to the respective devices and any correlations we see between A and B can be explained by the shared past information Λ. Any probability distribution that we cannot write in the above form we refer to as *nonlocal.*

It turns out that there exist quantum systems that are not compatible with the above explanation, which shows that quantum theory is indeed nonlocal. This discovery, motivated by the EPR paradox [1] and solved by Bell [2] had a profound impact on our understanding of physics and was a large component of this year's Nobel prize in physics [3].

Application to cryptography
Imagine we run the above experiment and convince ourselves that the devices are producing nonlocal correlations. As a consequence, we have also proven that there is no classical description of our experiment and hence our devices must have been acting in a quantum way. Moreover, this is a black-box proof in the sense that we can convince ourselves of the nonlocality without the need to understand how the devices were locally operating.

It turns out that nonlocal statistics imply much more than this. In particular one can show that all nonlocal statistics are random and secret! If the devices are acting in a nonlocal manner then their outputs cannot be perfectly predicted by anybody (including any eavesdroppers). From this we can then build protocols to generate randomness that remain secure even when we do not trust the devices on which they operate. This

[*] Students interested are encouraged to contact any of the supervisors as soon as possible. Email addresses:
jdbancal.physics[[at]]gmail.com
peter.brown[[at]]telecom-paris.fr
mirjam.weilenmann[[at]]oeaw.ac.at

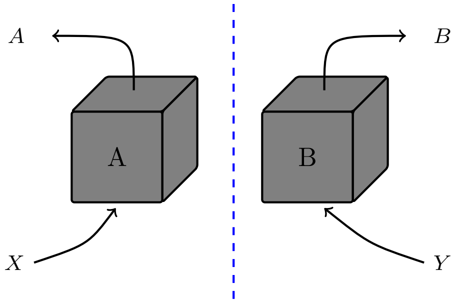

Figure 1: **A Bell experiment.** Two parties Alice and Bob are separated so they cannot communicate. They each receive random inputs X and Y respectively and must produce outputs A and B respectively. We are interested in what conditional probability distributions $p(a,b|x,y)$ the experiment can produce. Bell's theorem tells us that by sharing entanglement Alice and Bob can produce distributions that are more strongly correlated than any classical experiment. This is the key to device-independent quantum cryptography.

extreme level of security is known as device-independent security. Furthermore, we can extend this beyond the generation of randomness to settings where the two devices are generating a shared secret key (known as quantum key distribution) [4].

To classify the many different protocols one could come up with for this purpose, we can compare them in terms of the *rate* they achieve: in the case of randomness generation this is the number of random bits generated per round and in the case of key distribution the bits of key per round. The higher the rate, the better the protocol.

2 Project goal

The first experimental implementations of device-independent cryptography have recently been performed. However, current experiments are very noisy and so the rates of the protocols are very low and still far from practical. Therefore, one of the primary goals for theorists is to design device-independent protocols that have higher rates and are more robust to noise.

In this internship we will aim to do this by combining existing protocols with a type of classical probabilistic processing of the inputs and outcomes of the original protocol in different rounds of the experiment. This type of processing is colloquially known as a *wiring* and known as a useful way for concentrating the nonlocality of several resources into a single more powerful one [5, 6]. This is known as *nonlocality distillation*. The main advantage of this type of processing is that the new protocols are technologically not any more demanding than the original ones. There has furthermore been recent work showing that an even simpler type of classical processing can indeed be useful for improving current protocols [7].

Thus, by adapting these techniques from nonlocality distillation to distil the rates of our device-independent protocols instead, we hope to generate new protocols that outperform previous ones in the sense that they have higher rates, pushing device-independent cryptography towards practicality and having a strong impact on the future of quantum cryptography.

The specific contributions of the candidate would include:

1. Explore how nonlocality distillation can be applied to device-independent quantum key distribution protocols.
2. Implement numerical algorithms related to nonlocality distillation to demonstrate improved secret-key rates.
3. Compare these methods to the techniques of [7]

This project will include both analytical and numerical aspects, the numerics are based around linear and semidefinite programming and potentially other optimisations. No prior background in quantum cryptography is necessary but some background in quantum information is recommended. The internship will be physically based at either the IPhT, CEA Saclay or LTCI, Télécom Paris.

NB: The internship will be funded and there is a possibility of pursuing a PhD thesis afterwards on similar topics.

References

[1] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Physical Review*, vol. 47, no. 10, pp. 777–780, 1935.

[2] J. S. Bell, "On the Einstein-Podolsky-Rosen paradox," *Physics*, vol. 1, p. 195, 1964.

[3] A. Davour, "Nobel prize in physics 2022: Popular science background," 2022. Available at https://www.nobelprize.org/uploads/2022/10/popular-physicsprize2022-3.pdf.

[4] D. Nadlinger, P. Drmota, B. Nichol, G. Araneda, D. Main, R. Srinivas, D. Lucas, C. Ballance, K. Ivanov, E.-Z. Tan, *et al.*, "Experimental quantum key distribution certified by bell's theorem," *Nature*, vol. 607, no. 7920, pp. 682–686, 2022.

[5] M. Forster, S. Winkler, and S. Wolf, "Distilling nonlocality," *Physical review letters*, vol. 102, no. 12, p. 120401, 2009.

[6] N. Brunner and P. Skrzypczyk, "Nonlocality distillation and postquantum theories with trivial communication complexity," *Physical review letters*, vol. 102, no. 16, p. 160403, 2009.

[7] M. Ho, P. Sekatski, E.-Z. Tan, R. Renner, J.-D. Bancal, and N. Sangouard, "Noisy preprocessing facilitates a photonic realization of device-independent quantum key distribution," *Physical Review Letters*, vol. 124, no. 23, p. 230502, 2020.