Limits of privacy amplification against non-signalling memory attacks (QCrypt 2013)

Rotem Arnon-Friedman and Amnon Ta-Shma

The Blavatnik School of Computer Science, Tel-Aviv University, Israel

Abstract

The task of privacy amplification, in which Alice holds some partially secret information with respect to an adversary Eve and wishes to distill it until it is completely secret, is known to be solvable almost optimally in both the classical and quantum worlds. Unfortunately, when considering an adversary who is limited only by non-signalling constraints such a statement cannot be made in general. We consider systems which violate the chained Bell inequality and prove that under the natural assumptions of a time-ordered non-signalling system, which allow past subsystems to signal future subsystems (using the device's memory for example), super-polynomial privacy amplification by any hashing is impossible. This is of great relevance when considering practical device independent key distribution protocols which assume a super-quantum adversary.

Full paper: Physical Review A, Vol.86, No.6. DOI: 10.1103/PhysRevA.86.062333
`http://pra.aps.org/abstract/PRA/v86/i6/e062333`

Motivation - the path to protocols with minimal assumptions

As already quite known, due to the difficulty in fully characterising the device on which a protocol is being executed one would like to consider device independent protocols, for which the security proof is not based on the internal functioning of the device. An example for this is the scenario of device independent quantum key distribution (DIQKD). In DIQKD we assume that the system on which the protocol is being executed was made and given to the honest parties Alice and Bob by a malicious adversary Eve. We therefore ought to consider the system, which we know nothing about, as a black box, and impose no assumptions on it.

Taking another step forward in constructing a protocol with minimal assumptions, one can also consider removing the assumption that the adversary is limited by quantum physics and instead consider a non-signalling adversary. When considering the presence of a non-signalling adversary we assume that the only thing which limits the adversary is the non-signalling principle. That is, the adversary has super-quantum power; however, if Alice and Bob enforce some local non-signalling constraints on their devices then these cannot be broken by the adversary. Such constraints can be enforced by shielding and isolating the devices or by placing them in a space-like separated way. For example, if Alice and Bob perform their measurements in a space-like separated way, then according to relativity theory, Alice cannot use her system in order to signal Bob and vice-versa.

Time-ordered non-signalling conditions

Is it possible to construct such DIQKD protocols when considering a non-signalling adversary? It appears that the answer depends on the specific local non-signalling conditions that Alice and Bob enforce on the system. It was proven in [1, 2] that if Alice and Bob enforce full non-signalling conditions, i.e., any subsystem cannot signal any other subsystem, then DIQKD is possible. The main drawback is that the full non-signalling conditions are hard to enforce (shielding each subsystem is impractical for example), and therefore such protocols are impractical. On the other extreme, it was already proven in [3] that the task of privacy amplification, which is easier than QKD, is impossible if we impose non-signalling conditions only between Alice and Bob, i.e., Alice and Bob cannot signal each other, while signalling within their systems is possible.

A more realistic non-signalling condition that one can consider is that in addition to the non-signalling condition between Alice and Bob, within the system of the parties signalling is possible only from the past to the future and not the other way around. These time-ordered non-signalling conditions are natural assumptions when considering a protocol in which Alice and Bob each use just one device with memory. In that case, the inputs and outputs of past measurements (which were saved in the memory of the device) can affect the outputs of future measurements.

In contrast to the full non-signalling conditions, the time-ordered non-signalling conditions are easy to ensure. Alice and Bob can both shield their entire system (as has to be done anyhow in order to make sure that no information leaks straight to the adversary) and therefore signalling will be impossible between them. Moreover, when running the protocol, they will perform their measurements in a sequential manner; the first system will be measured in the beginning, then the second one and so on. This will make sure (as long as we believe that messages cannot be sent from the future to the past) that signalling is possible only in the forward direction of time. In fact, these are the non-signalling conditions that one "gets for free" when performing an experiment of QKD. For example, an entanglement-based protocol in which Alice and Bob receive entangled photons and measure them one after another using the same device will lead to the time-ordered non-signalling conditions. If Alice's and Bob's devices have memory then information from past measurements can be available for future measurements, i.e., signalling is possible from the past to the future but not the other way around.

Our question

We consider the task of privacy amplification (PA). In the privacy amplification problem Alice holds some information which is only partially secret with respect to an adversary, Eve. Alice's goal is to distill her information, to a shorter string, which is completely (or almost completely) secret. Note that in the PA problem we only want Alice to have a secret key with respect to the adversary, while in the task of key distribution we also want Bob to hold the same key as Alice. Therefore PA is easier than key distribution.

In order to understand what exactly is the PA problem, consider the following scenario. Assume that Alice has a system, a black box, which produces for her a partially secret bit or a string, X. By saying that X is partially secret we mean that there is some entropy in X conditioned on Eve's knowledge about X. One would hope that by letting Alice use several such systems, which will produce several partially secret bits X_1, X_2..., X_n, she will have enough entropy in order to produce a more secret bit or a string, K, out of them, or in other words, she will be able to amplify the privacy of her key. The idea behind PA protocols is to apply some hash function $f : \{0,1\}^n \rightarrow \{0,1\}^{|K|}$ (for $|K| < n$) to X_1, X_2..., X_n in order to receive a shorter, but more secret, bit string K. The amount of secrecy is usually measured by the distance of the actual system of Alice and Eve from an ideal system, in which K is uniformly distributed and uncorrelated to Eve's system.

In our paper we ask the following question. Under the assumptions of time-ordered non-signalling system, is PA against non-signalling adversaries possible? In particular, we consider systems which violate the chained Bell inequality [4, 5]. All known DIQKD protocols, such as [6, 7], are based on the violation of some chained Bell inequality and cannot tolerate a reasonable amount of noise. This suggests the need for a privacy amplification protocol in such scenarios, and therefore one would like to know if PA is possible in such systems under the time-ordered non-signalling assumptions.

Our contribution

We give an example for a system which fulfils all the time-ordered non-signalling conditions, and in which super-polynomial PA is impossible. More precisely, we prove that for protocols which are based on a violation of chained Bell inequalities, under the assumption of a time-ordered non-signalling system, super-polynomial PA is impossible by any hashing. That is, when using n black boxes, each producing a partially secret bit, the adversary can always get a great amount of information about the hashing result; at least as high as $\Omega\left(\frac{1}{n}\right)$.

We prove this by giving a simple adversarial strategy which biases the result of any hash function by $\Omega\left(\frac{1}{n}\right)$ by using the memory of the device, or in other words, by using the possibility to send signals from a previously measured system to the next one. The lower bound on the information of the adversary is proven using ideas from the field of boolean function analysis.

Interestingly, our result holds independently of how high the violation of the Bell inequality is (as long as it is not maximal). This suggests that, in contrast to the full non-signalling scenario, when considering other non-signalling conditions the amount of the violation of the Bell inequality does not quantify the available secrecy which can be extracted from the system.

To summarise, the assumption of time-ordered non-signalling system is the relevant assumption, from a practical point of view, when considering device independent protocols for cryptographic tasks. Our result shows that under this assumption one can not expect to have an exponentially good privacy amplification protocol against non-signalling adversaries (in contrast to the case of quantum adversaries [8]). It is not yet clear whether our result is tight, therefore the question whether linear privacy amplification is possible or not remains open.

References

[1] E. Hänggi, R. Renner, and S. Wolf. Quantum cryptography based solely on Bell's theorem. *Arxiv preprint arXiv:0911.4171*, 2009.

[2] L. Masanes. Universally composable privacy amplification from causality constraints. *Physical Review Letters*, 102(14):140501, 2009.

[3] E. Hänggi, R. Renner, and S. Wolf. The impossibility of non-signaling privacy amplification. http://arxiv.org/abs/0906.4760.

[4] S.L. Braunstein and C.M. Caves. Wringing out better Bell inequalities. *Annals of Physics*, 202(1):22–56, 1990.

[5] J. Barrett, A. Kent, and S. Pironio. Maximally nonlocal and monogamous quantum correlations. *Phys. Rev. Lett.*, 97:170409, Oct 2006.

[6] J. Barrett, L. Hardy, and A. Kent. No signaling and quantum key distribution. *Physical Review Letters*, 95(1):10503, 2005.

[7] J. Barrett, R. Colbeck, and A. Kent. Unconditionally secure device-independent quantum key distribution with only two devices. *Arxiv preprint arXiv:1209.0435*, 2012.

[8] Umesh Vazirani and Thomas Vidick. Fully device independent quantum key distribution. *arXiv preprint arXiv:1210.1810*, 2012.