Device-independent protocols from computational assumptions

Joint submission for arXiv:2001.09161 and arXiv:2010.04175.

Tony Metger, Yfke Dulek, Andrea Coladangelo, Rotem Arnon-Friedman, Thomas Vidick

Summary. Device-independent protocols use untrusted quantum devices to achieve a cryptographic task. Such protocols are typically based on Bell inequalities and require the assumption that the quantum device is composed of separated *non-communicating* components. In this submission, we present protocols for *self-testing* and *device-independent quantum key distribution* (DIQKD) that are secure even if the components of the quantum device can exchange arbitrary quantum communication. Instead, we assume that the device cannot break a standard post-quantum cryptographic assumption. Importantly, the computational assumption only needs to hold during the protocol execution and only applies to the (adversarially prepared) device in possession of the (classical) user, while the adversary herself remains unbounded. The output of the protocol, e.g. secret keys in the case of DIQKD, is information-theoretically secure.

For our self-testing protocol, we build on a recently introduced cryptographic tool [BCM+18, Mah18] to show that a classical user can enforce a bipartite structure on the Hilbert space of a black-box quantum device, and certify that the device has prepared and measured a state that is entangled with respect to this bipartite structure. This means that we are able to certify the existence of entanglement in a single quantum device, a result which may also be of interest for quantum foundations.

Using our self-testing protocol as a building block, we construct a protocol for DIQKD that leverages the computational assumption to produce information-theoretically secure keys. For this, we replace a non-local gate, being applied in the self-testing protocol, with gate teleportation, to allow an honest two-component device to succeed in the DIQKD protocol using only EPR pairs and local operations. The security proof of our DIQKD protocol uses the self-testing theorem in a black-box way to bound the relevant entropic quantities. Our self-testing theorem thus also serves as a first step towards a more general translation procedure for standard device-independent protocols to the setting of computationally bounded (but freely communicating) devices.

Introduction. In device-independent protocols, classical parties wish to use an untrusted black-box device prepared by an adversary to accomplish an information-processing or cryptographic task, e.g. key distribution. Because the device is untrusted and the classical parties only have black-box access, a device-independent protocol needs to certify that the device behaves as intended based solely on the classical input-output behaviour observed by the classical parties.

Most existing device-independent protocols achieve this certification by relying on Bell non-locality. For this, they assume that the device can be split into two (or more) possibly entangled components distributed to different classical parties, usually named Alice and Bob. Each classical party interacts with their component of the device. If the joint input-output behaviour of the device violates a Bell inequality, this can be used to certify properties of the device, e.g. that it must have produced a certain amount of entropy [Col06]. Crucially, since the certification is based on Bell non-locality, it is necessary to assume that the different components of the device do not communicate with each other during the protocol; otherwise, even classical devices could violate a Bell inequality, and the certification is rendered useless. We call this the *non-communication assumption* (also sometimes called the *locality assumption*).

In our work, we show that for two important device-independent tasks, self-testing and DIQKD, this non-communication assumption can be replaced by a computational assumption on the *device* (not the adversary). More precisely, we impose no partition into non-communicating components; instead, we assume that the device cannot efficiently solve the Learning with Errors (LWE) problem, a standard assumption in post-quantum cryptography [Reg09, Pei16]. Importantly, this computational assumption needs to hold *only during the protocol execution*: if the device is unable to break the LWE problem during the short time it takes to run the protocol, the classical parties can draw an information-theoretic conclusion, just like in Bell inequality-based device-independent protocols. For example, in the case of key distribution, the key generated at the end of the protocol will be information-theoretically secure, i.e. secure against unbounded quantum adversaries. This is known as *everlasting security* [Unr18].

Considering alternatives to the non-communication assumption is well-motivated by realistic implementations of device-independent protocols: in the standard non-communication setting, the different components of the device need to share entanglement to be able to succeed in the protocol; in practice, this entanglement is distributed "on the fly" *between* rounds of the protocol via a quantum channel connecting the two components, making it difficult to perfectly shield the components from each other *during* rounds of the protocol. Alternatively, one could enforce non-communication by the laws of special relativity; however, this requires Alice and Bob to be sufficiently far apart and is challenging to implement experimentally.[1]

In addition to suggesting an alternative approach towards device-independent cryptography, protocols such as ours may also be of foundational interest: device-independent entanglement certification is usually closely linked to non-local correlations arising from bipartite systems (as quantified by Bell inequality violations). In our work, no pre-existing bipartition of the system is present, but we are still able to certify entangled states and measurements in a device-independent way.

Self-testing. The goal of self-testing [SW87, PR92, MY04] is to certify that a device prepared a specific quantum state, e.g. an EPR pair, and measured this quantum state in specific bases chosen by the classical parties, e.g. a choice of computational or Hadamard basis for each qubit of the EPR pair. In the standard scenario with a two-component device, if the device succeeds in the self-testing protocol, we can conclude that there are *local* changes of basis for each component of the device (described by a local isometry) under which the device's actual state and measurements are mapped to the desired ones.

In our self-testing protocol, we drop the non-communication assumption, as we wish to allow quantum communication between the different components of the device. Hence, we can no longer assume a pre-existing tensor product structure on the device's global Hilbert space, and *local* changes of basis are not well-defined. To make a meaningful self-testing statement on a global Hilbert space, we note that self-testing certifies both the device's states and measurements, i.e., it certifies the relation between states and measurements, a basis-independent property that does not rely on a pre-existing tensor product structure.

Our protocol is a three-round interaction between a classical party and a quantum device, at the end of which the classical party decides to either "accept" or "reject" the device. Informally, the guarantee provided by our protocol is the following (for the formal statement, see [MV20, Theorem 4.38]):

Theorem (Informal)**.** *A device's strategy in the protocol is described by a quantum state and the measurements that the device makes on the state to obtain the (classical) answers received by the (classical) user. If a computationally bounded device is accepted in our protocol with probability* $1-\varepsilon$*, then there exists an isometry* V *such that for a universal constant* $c > 0$ *and under the isometry* V*:*

(i) *the device's state is* $O(\varepsilon^c)$*-close (in trace distance) to a Bell pair,*

(ii) *a subset of the device's measurements are* $O(\varepsilon^c)$*-close to single-qubit measurements in the computational or Hadamard basis, where the measurement bases are chosen by the user. Here, "closeness" is measured in a distance measure suitable for measurements acting on a state.*

This means that a device that succeeds with high probability must have prepared a Bell pair and performed single-qubit measurements on it, up to a small error and a global change of basis applied to both the device's state and measurements.

[1] It is possible to relax the non-communication assumption and allow a limited amount of communication between the components of the device [SPM13, TCB$^+$19, TCWP20]. However, this limit on the communication is a device-*dependent* assumption that cannot be certified as part of a device-independent protocol.

Device-independent quantum key distribution. In DIQKD, two honest classical parties, Alice and Bob, try to establish a secure key using a black-box device prepared by an adversary Eve. The device consists of two components, one given to Alice and one to Bob, and it is usually assumed that these components cannot communicate with each other during certain steps the protocol.

In our DIQKD protocol, similarly to our self-testing protocol, we replace the non-communication assumption by a computational assumption. This means that our setting explicitly includes the quantum channel between the different components that allows an honest device to distribute entanglement "on the fly". An adversarial device may use this channel in an arbitrary way, not just for entanglement distribution.

To use our self-testing protocol for DIQKD, we first make a key modification: if we directly translated the (single-device) self-testing protocol to the DIQKD setting (with two freely communicating components), the *honest* device would need to perform an entangling gate between its two components. However, we would like an honest device to be able to succeed in the protocol with the same non-local resources as those required in a standard DIQKD protocol, i.e., shared EPR pairs. To this end, we modify the self-testing protocol so that the *honest* device can use gate-teleportation [GC99, CLN05] instead of applying the non-local gate directly, and show that this does not compromise the soundness of the self-testing protocol against adversarial devices.

To generate the raw data from which a secure key can be extracted by classical post-processing, Alice and Bob repeatedly run the modified self-testing protocol and record the device's classical outputs. They then and use classical communication to check whether the device satisfies the conditions of the modified self-testing protocol.

If the device succeeded in a sufficiently high proportion of rounds, we can apply our self-testing theorem to the reduced state of the device (i.e., without Eve's system, since only the device prepared by Eve is computationally bounded, whereas Eve herself is not). This implies that (up to a change of basis) the states and measurements used by the device to generate Alice's and Bob's classical outputs must have been close to EPR states and computational/Hadamard basis single qubit measurements. Since the device must have approximately prepared an EPR state, Eve's system cannot be very entangled with the device's state. Hence, we can prove a lower bound on the key rate of our protocol, i.e., the rate at which Alice and Bob can produce shared bits that look uniformly random to Eve.

Main technical contributions. Our main technical contribution is the construction and security analysis of the self-testing protocol described above. The cryptographic primitive underlying this protocol is a so-called extended noisy trapdoor claw-free function family (ENTCF family), introduced in [Mah18, BCM+18]. In [GV19], ENTCF families were used for verifiable remote state preparation, a task which is reminiscent of self-testing, but only deals with single-qubit states and does not explicitly certify the device's measurements.

With [GV19] as a starting point, there are two main challenges in constructing a self-testing protocol for EPR pairs: firstly, we need a high level of control over the device's (a priori unstructured) Hilbert space to enforce a bipartite structure, a problem reminiscent of proving direct product theorems in theoretical computer science [GS00]. Secondly, we need to certify that the device has prepared a state that is entangled with respect to this bipartite structure, and that it has measured this entangled state in a basis chosen by the classical party. Such a fine control over the device's states and measurements was not achieved in previous works [BCM+18, Mah18, GV19] and is a prerequisite for our DIQKD protocol.

Specifically, we need to show that the device's actual measurement operators can be approximately mapped to the desired single-qubit computational and Hadamard basis measurements. This step, called operator rounding, is common in standard self-testing, but crucially relies on a pre-existing bipartition of the Hilbert space [MY04]. To perform operator rounding on a global Hilbert space without substructure, we combine the standard operator rounding techniques with the fact that the cryptographic assumptions allow for *blind* state preparation, meaning that the device does not know which state it has prepared. This "cryptographic operator rounding" is the main technical innovation of our work and allows us to establish a bipartite structure on the device's Hilbert space solely from the classical input-output behaviour. An additional check in the protocol then ensures that the entangling operation was applied correctly with respect to this bipartite structure.

References

[BCM$^+$18] Z. Brakerski, P. Christiano, U. Mahadev, U. Vazirani, and T. Vidick. "A Cryptographic Test of Quantumness and Certifiable Randomness from a Single Quantum Device", IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS), 320-331 (2018). arXiv:1804.00640v3.

[CLN05] A. M. Childs, D. W. Leung, and M. A. Nielsen. "Unified derivations of measurement-based schemes for quantum computation", Phys. Rev. A 71, 032318 (2005).

[Col06] R. Colbeck. *Quantum and relativistic protocols for secure multi-party computation*, PhD Thesis, University of Cambridge (2006). arXiv:0911.3814.

[GC99] D. Gottesman and I. L. Chuang. "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations", Nature 402, 390–393 (1999).

[GS00] O. Goldreich and S. Safra. "A combinatorial consistency lemma with application to proving the PCP theorem", SIAM Journal on Computing 29, 1132–1154 (2000).

[GV19] A. Gheorghiu and T. Vidick. "Computationally-secure and composable remote state preparation", *Preprint* (2019). arXiv:1904.06320v1.

[Mah18] U. Mahadev. "Classical Verification of Quantum Computations", IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS), 259-267 (2018). arXiv:1804.01082v2.

[MV20] T. Metger and T. Vidick. "Self-testing of a single quantum device under computational assumptions", *Preprint* (2020). arXiv:2001.09161.

[MY04] D. Mayers and A. Yao. "Self Testing Quantum Apparatus", Quantum Info. Comput. 4, 273-286 (2004). arXiv:quant-ph/0307205.

[Pei16] C. Peikert. "A decade of lattice cryptography", Foundations and Trends in Theoretical Computer Science 10, 283–424 (2016).

[PR92] S. Popescu and D. Rohrlich. "Which states violate Bell's inequality maximally?", Physics Letters A 169, 411–414 (1992).

[Reg09] O. Regev. "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography", J. ACM 56 (2009).

[SPM13] J. Silman, S. Pironio, and S. Massar. "Device-Independent Randomness Generation in the Presence of Weak Cross-Talk", Phys. Rev. Lett. 110, 100504 (2013).

[SW87] S. J. Summers and R. Werner. "Maximal violation of Bell's inequalities is generic in quantum field theory", Communications in Mathematical Physics 110, 247–259 (1987).

[TCB$^+$19] A. Tavakoli, E. Z. Cruzeiro, J. B. Brask, N. Gisin, and N. Brunner. "Informationally restricted quantum correlations", *Preprint* (2019). arXiv:1909.05656.

[TCWP20] A. Tavakoli, E. Z. Cruzeiro, E. Woodhead, and S. Pironio. "Characterising correlations under informational restrictions", *Preprint* (2020). arXiv:2007.16145.

[Unr18] D. Unruh. "Everlasting Multi-party Computation", Journal of Cryptology 31, 965–1011 (2018).