Research Statement

Andrea W. Coladangelo

February 2019

Outline

In section 1, I introduce the driving theme of my research so far, the problem of *testing quantum devices*. In section 2, I take the reader on a journey through my previous work. In section 3, I discuss future research directions.

1 Testing quantum devices

It is widely believed that quantum computers have the potential to speed up a wide range of computational tasks (see, for example, [Mon16]), and provable advantages are known in restricted models [BGK18]. Moreover, the ongoing race for building a universal quantum computer has fueled important experimental advances. The current setting inevitably raises the following basic question: once we have a universal quantum computer, how do we test that it is functioning correctly? Or more generally, how can a classical verifier test any quantum device at all? This verifier could be an experimentalist with specialized knowledge about a certain experimental setup and the technical equipment involved, or it could be a consumer who has purchased a purported quantum device and has nothing but a laptop and the quantum device itself. In both cases, the verifier would like to certify that the quantum device is behaving as intended. There are several possible ways to approach this problem. For example, the experimentalist may attempt to verify the correct behaviour of the quantum apparatus by performing a series of measurements, and doing some statistical analysis on the outcomes by applying techniques from state and process tomography [Par09] or randomized benchmarking [KLR$^+$08]. However, both of these approaches assume that the measurement apparatus is trusted. This might be a fine assumption for the experimentalist with access to her own trusted setup. However, for the layman consumer, any measurement apparatus is just as untrusted as the quantum device to be tested. For a classical verifier to truly test and certify a quantum system, that system should be modeled in a *device-independent* way, i.e. as a black-box having classical inputs (e.g. measurement settings) and classical outputs (e.g. measurement results).

Remarkably, a single, a priori very modest, physical assumption about the black-box to be tested allows to obtain very strong guarantees about the quantum apparatus it contains. More precisely, if one knows merely that the black-box consists of two spatially isolated (but possibly entangled) components, then it is possible, in some cases, to characterize uniquely the quantum apparatus inside the black-box by just observing the input-output statistics. Spatially isolated here means that the two components are formally modelled as being in tensor product and each component acts locally on one tensor factor. It is precisely the entanglement between the two components that makes this characterization possible. This realization has led to important advances in the field of quantum cryptography, including the first full device-independent security proofs for quantum key-distribution [VV14, MS16], randomness expansion [MS16] and delegated quantum computation [RUV13].

The problem of certifying the behaviour of quantum devices in the device-independent scenario is not only compelling from a practical standpoint, but also fascinating: one can think of such a certificate (or certification procedure), whenever

it exists, as a "classical signature" of a quantum system, in the sense that the classical witness or transcript obtained by the verifier's classical interaction with the quantum device singles out a unique quantum apparatus that is compatible with it. It is not obvious at all that such a certificate exists, and it is remarkable that nature allows its existence even in special cases.

2 Contributions

Several natural questions arise when thinking about device-independent certification of quantum devices: Does the set of quantum apparatus that can be certified by a classical verifier consist of a few exceptions, or is such a certification a more general phenomenon? If so, can it be exploited not only to certify a fixed quantum apparatus, but to orchestrate a full-fledged quantum computation in a verifiable way? As mentioned earlier, it is entanglement that makes this certification possible at all. Does the answer to these questions yield a more refined understanding of entanglement as a fundamental resource in quantum information? My work makes progress on these questions, and provides a resolution to some of them. Before proceeding, I will informally introduce the framework in which I study these questions.

2.1 The framework: device-independent self-testing

The framework that I work in was first introduced by Bell [Bel64], who at the time was not explicitly concerned with the problem of certifying quantum devices, but rather with exhibiting the non-locality of quantum mechanics. The setup consists of a verifier, who wishes to certify properties of an uncharacterized quantum system by interacting classically with it (by probing it with classical questions and expecting classical answers in return). As mentioned earlier, we make just one physical assumption about the system to be tested: that it consists of two spatially isolated components (usually referred to as the provers, or Alice and Bob) that are unable to communicate throughout the experiment. The behaviour of the provers is captured by the joint distribution of their answers as a function of their questions. We refer to this data as a *bipartite correlation*. Formally, a bipartite correlation captures the scenario where there is one round of interaction between the verifier and the provers, but this notion can be generalized naturally to more rounds of interaction. Typically, the two provers are thought of as cooperatively playing a game refereed by the verifier. In some cases, subject to the constraint that they do not share any entanglement, one can upper bound the expected score of the provers in the game. Such a bound is referred to as a Bell inequality. Thus, the violation of a Bell inequality can be seen as a certificate of entanglement.

The area of device-independent self-testing seeks to make even stronger statements about *which measurements* are being performed, and on *which state*. The device-independent approach exploits the fact that certain correlations can be uniquely achieved (up to local isometries) by particular measurements on a particular quantum state. When this is the case, we say that the correlation self-tests those measurements on that quantum state. The term "self-testing", in the context of Bell experiments, was coined by Mayers and Yao [MY04], and the most popular example of a self-test is given by the CHSH game [CHSH69]: it is well-known that a correlation attaining maximal winning probability in the CHSH game can only be induced by specific measurements on a maximally entangled pair of qubits (also known as an EPR pair). Importantly, this self-testing statement also holds "approximately" [MYS12, RUV13], meaning that a close-to-maximal winning probability still implies that the underlying state and measurements are close to ideal. This property is often referred to as "robustness", and is important in practice since one inevitably only observes close-to-ideal correlations.

Next, I will address the question of how a classical verifier can exploit self-testing results to orchestrate full-fledged quantum computations in this setup. I will lead up to this question by discussing a necessary ingredient for such a task: certification of many copies of EPR pairs.

2.2 Parallel self-tests

A natural question to ask is: can the self-test of a single EPR pair via the CHSH game be extended to a self-test of many EPR pairs? Indeed, the ability to test many EPR pairs in sequence or in parallel is essential in practice, since most meaningful protocols would require the use of many EPR pairs, rather than a single one. The first work to consider this question was by Reichardt et al. [RUV13], and showed that one can self-test many EPR pairs by playing many copies of the CHSH game *in sequence* and observing a high-enough fraction of games being won.

One might wonder if it is possible instead to certify many EPR pairs by playing many copies of the CHSH game at the same time, i.e. *in parallel*, as opposed to in sequence. In practice, this would likely yield improvements in the round complexity of the protocol employing the EPR pairs. The study of amplification and parallel repetition in cryptography suggests that while a parallel self-test might hold, it is unlikely to be easy to prove. Nonetheless, McKague gave the first parallel self-test of many EPR pairs [McK16b], but his self-test involved a more complicated game than CHSH.

My contribution was to analyze the direct parallel repetition of the CHSH game, and to show that n EPR pairs can be self-tested by playing n copies of the CHSH game in parallel. Similarly, I showed that $2n$ EPR pairs can be self-tested by playing n copies of the magic square game in parallel [Col17]. In a different work [CS17a], Jalex Stark and I obtained a general self-testing result for a broad and well-studied class of non-local games, called linear-constraint-system games, and parallel versions thereof. The main technical ingredient that we employed was the representation-theoretic framework for linear-constraint-system games introduced by Cleve, Liu and Slofstra [CLS17], which considerably simplifies the analysis of the parallel self-tests.

The significance of these results stems primarily from their applications. In the next subsection, I discuss how these parallel self-tests are employed in protocols to delegate quantum computations. Another direction of application of these tests is to the study of interactive proofs with entangled provers (see [NV18] for the latest progress).

2.3 Applications to delegated quantum computation

For the foreseeable future, we can expect quantum computers to be owned exclusively by specialized research centers. Use of a quantum computer by regular clients will likely require delegating the computation to a potentially untrusted cloud service, such as that announced by IBM [Cas17]. Informally, a delegated quantum computation protocol is carried out between a verifier, who has in mind a quantum circuit Q and an input $|x\rangle$, and one or more servers. The protocol consists of several rounds of interaction between the verifier and the servers, at the end of which the verifier outputs $c \in \{1, 0, \perp\}$. The protocol is said to be verifiable if the verifier outputs the correct outcome of the computation with high probability (whenever she doesn't output $\perp$).

In 2012, Reichardt, Unger and Vazirani [RUV13] gave the first protocol for a completely classical verifier to delegate her computation to two non-communicating servers in a verifiable way. This was based on a robust self-testing theorem for playing n CHSH games in sequence, and it was the first to demonstrate how powerful tools from self-testing can be exploited by a classical verifier to control quantum devices and orchestrate a computation.

Unfortunately, the complexity overhead of the delegation protocol from [RUV13], in terms of both the number of EPR pairs needed for the provers and the overall time complexity of the provers as well as the (classical) verifier, while polynomial, is prohibitively large: $\Omega(g^{8192})$ for delegating a circuit of size g. One can envision utilizing more robust, and parallel, self-tests to improve this scaling. In fact, a series of subsequent works [McK16a, GKW15, HPDF15, FH15, NV17] has improved the efficiency to $\Omega(g^4)$, but also requiring more than two provers.

In [CGJV17], we overcome the efficiency limitations of multi-prover delegation protocols by introducing a new robust self-testing theorem for certifying measurements of single-qubit Clifford observables on shared EPR pairs. Our self-testing theorem builds upon and extends a previous work of Natarajan and Vidick [NV17]. Employing our new self-testing theorem we obtain an efficient two-prover classical-verifier protocol in which the complexity overhead of verifiably delegating a g-gate quantum circuit is near-optimal, scaling as $O(g \log g)$.

2.4 Self-testing as a more general phenomenon

As hinted at earlier, the study of self-testing is also important from a foundational perspective. A major unanswered question in the field is whether self-testing is a property of a few special states, for example EPR pairs or copies of EPR pairs, or the latter is just an instance of a more general phenomenon. A number of special cases have been solved over several years, providing examples of states that can be self-tested [YN13, BP15, SAT$^+$16, YVB$^+$14, WCY$^+$14, PVN14, McK11]. These include all partially entangled pairs of qubits, some particular states of qutrits, and a few multipartite states. Hence, while it seems clear that self-testing is not an exclusive characteristic of maximally entangled states nor qubit states, for some time little was known about self-testing higher-dimensional entangled states (i.e. pairs of entangled qudits for $d > 2$). In particular, one natural question remained open: is it possible to self-test all pure bipartite entangled states?

In 2017, Koon Tong Goh, Valerio Scarani and I answered this question affirmatively by proving that all pure bipartite entangled states of any finite local dimension can be self-tested [CGS17], thereby settling the bipartite case. In other words, for each pure bipartite entangled state, one can write down a correlation that can be attained exclusively by measuring this state. As I mentioned in section 1, I like to think of this correlation as a "classical signature" of the quantum state.

In a subsequent collaboration [SCAA17], we showed that all multipartite entangled states that possess a Schmidt decomposition can also be self-tested, giving the first self-test for a large class of multipartite states. In a more recent work [Col18] that extends some of these ideas, I introduce a generalization of the CHSH inequality, and I show that maximal violation of this inequality self-tests the maximally entangled state of local dimension d.

2.5 Separation of finite and infinite-dimensional quantum correlations

My investigations have been primarily motivated by questions in quantum cryptography, but they have often intersected with foundational questions about quantum correlation sets and entanglement. This should not come as a surprise, since the primary tool that propels the results I described so far is the study of quantum correlations. However, our understanding of these is far from complete, and several fundamental questions about quantum correlation sets remain unanswered. One example of a very basic question that has remained elusive is the following: does the set of attainable correlations change if we allow the provers to share infinite-dimensional entanglement, as opposed to just finite-dimensional entanglement? In other words, are finite-dimensional quantum correlations just as expressive as infinite-dimensional quantum correlations? This is part of a set of questions about the relationship between different variants of quantum correlation sets which have sometimes been collectively referred to as Tsirelson's problem in the literature.

In a sequence of two works, [CS17b] and [CS18], Jalex Stark and I settle this question. By building on insight developed in the previous work [CGS17], we first made partial progress [CS17b] by showing that the two sets are distinct *if* one allows question or answer sets to have infinite size. Note that question and answer sets are typically taken to be finite, and allowing for infinite-sized question or answer sets makes the result much weaker. Intuitively, one can think that the smaller the question and answer sets are, the harder it is for the power of infinite-dimensions to be expressed. In fact, it is well-known that in the case where question and answer sets are both of size 2 there is no separation between finite and infinite-dimensional quantum correlations.

In [CS18], we settle the full question by showing that there exist correlations on question sets of size 4 and 5 and answer sets of size 3 that can be attained exactly with infinite-dimensional, but not finite-dimensional, entanglement. To give some insight into our result, the state that produces our separating correlation is of the form $|\Psi\rangle \propto \sum_{i=1}^{\infty} \alpha^i |ii\rangle$, for some $\alpha \in (0, 1)$. A crucial idea in the construction of the separating correlation is to design one that enforces a certain scale-invariance in the Schmidt coefficients of any state that achieves it. This scale-invariance should be consistent only with *infinitely* many Schmidt coefficients, and should mimic that of $|\Psi\rangle$: namely any two neighbouring Schmidt coefficients are in ratio α, and this is true at any scale. The main obstacle that we overcome in constructing such a correlation is how to enforce this scale-invariance with such few questions and answers.

3 Future directions

There are several research directions that I wish to pursue:

(i) Certifying the behaviour of multipartite quantum systems. Compared to the bipartite case, much less is known about device-independently certifying multipartite systems. As mentioned earlier, in [SCAA17] we show that all multipartite states that possess a Schmidt decomposition can be self-tested, but not much else is known about robust certifications, or certification procedures that allow to certify generic measurements on generic multipartite states. This problem becomes relevant in the light of recent efforts to build a "quantum internet" [WEH18], which opens up the possibility of running larger-scale multi-party protocols in a device-independent way.

(ii) Our correlation separating finite and infinite-dimensional quantum correlations exhibits precisely, although on slightly larger question and answer sets, the behaviour that is conjectured to be possessed by the famous I3322 Bell inequality (which concerns question sets of size 3 and answer sets of size 2, as the name suggests). There is extensive numerical evidence [PV10] which suggests that finite dimensions are not enough to attain the maximal violation of the I3322 inequality but infinite dimensions suffice, yet an analytical proof has remained elusive. The similarities between the structure of our $(4, 5, 3, 3)$ separating correlation and the correlation that is conjectured to maximally violate the I3322 inequality are striking. Armed with a stronger understanding of how certain kinds of structures that appear in correlations require infinite-dimensions to attain, I hope to make progress on the I3322 conjecture. Or otherwise, gain more insight into how nature can so neatly pack enough structure in such few question and answers to make infinite-dimensional entanglement necessary.

(iii) One might wonder and be surprised at how a classical verifier is able to control the behaviour of non-communicating quantum provers in delegation protocols. Intuitively, the power of the client comes from the fact that she knows more than the provers (she knows both of the questions being asked). If non-communicating provers are replaced by a single prover, then this power vanishes. The recent sequence of breakthrough works [Mah17, Mah18] by Mahadev has shown how computational assumptions can be utilized to "restore" a balance of power between the client (who knows a trapdoor to some one-way function) and the single prover. These ideas fuel the exploration of quantum cryptographic protocols that leverage computational assumptions. More concrete directions that I wish to explore include: finding schemes for verifiable delegation that improve on the efficiency of the one proposed by Mahadev; finding a public-key quantum money scheme [Aar09] or a quantum lightning scheme [Zha17] that is secure under a well-studied cryptographic assumption; investigate the possibility of using quantum tools to extend the class of (classical or quantum) circuits that we can obfuscate.

(iv) A more speculative route that I am interested in exploring is the use of financial incentives in quantum cryptography. The idea of introducing financial incentives has led to interesting applications in classical cryptography via the study of rational proofs [AM12, GHRV14, GHRV16, CMS16, AGP16]. Recently, the notion of "smart-contract" on a blockchain has gained popularity as a tool that allows to enforce these monetary incentives in a trust-less way, i.e. without having to trust a central entity, or that the verifier pays the correct rewards to the provers. Informally, smart-contract are contracts whose consequences are enforced automatically upon fulfillment of certain algorithmically-checkable conditions. Smart-contracts have recently found several applications in the design of classical multi-party cryptographic primitives like secure multi-party computation [BK14], secure lotteries [BK14], and protocols for playing card-games [BKM17, DDL17, DDL18]. I believe that there is the potential for something very exciting to emerge from the combination of classical smart-contracts and quantum cryptography. In [Col19], I attempt to bridge this gap, by providing an example of an application that shows the interplay between the two. One open avenue that I am particularly interested in exploring is the generation of trusted public randomness, i.e. randomness which can be agreed upon by parties that do not necessarily trust each other, and that cannot be influenced by dishonest parties.

Classical proposals for this task have a number of shortcomings. Given that randomness is inherent in quantum systems, there is the potential for quantum tools to provide an edge for this task.

References

[Aar09] Scott Aaronson. Quantum copy-protection and quantum money. In *Computational Complexity, 2009. CCC'09. 24th Annual IEEE Conference on*, pages 229–242. IEEE, 2009.

[AGP16] Pablo Daniel Azar, Shafi Goldwasser, and Sunoo Park. How to incentivize data-driven collaboration among competing parties. In *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science*, pages 213–225. ACM, 2016.

[AM12] Pablo Daniel Azar and Silvio Micali. Rational proofs. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 1017–1028. ACM, 2012.

[Bel64] John S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[BGK18] Sergey Bravyi, David Gosset, and Robert Koenig. Quantum advantage with shallow circuits. *Science*, 362(6412):308–311, 2018.

[BK14] Iddo Bentov and Ranjit Kumaresan. How to use bitcoin to design fair protocols. In *International Cryptology Conference*, pages 421–439. Springer, 2014.

[BKM17] Iddo Bentov, Ranjit Kumaresan, and Andrew Miller. Instantaneous decentralized poker. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 410–440. Springer, 2017.

[BP15] Cédric Bamps and Stefano Pironio. Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing. *Phys. Rev. A*, 91:052111, May 2015.

[Cas17] Davide Castelvecchi. IBM's quantum cloud computer goes commercial. *Nature News*, 543(7644), 6 March 2017.

[CGJV17] Andrea Coladangelo, Alex Grilo, Stacey Jeffery, and Thomas Vidick. Verifier-on-a-leash: new schemes for verifiable delegated quantum computation. *arXiv preprint* `arXiv:1708.07359`, 2017.

[CGS17] Andrea Coladangelo, Koon Tong Goh, and Valerio Scarani. All pure bipartite entangled states can be self-tested. *Nature Communications 8*, page 15485, 2017.

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23:880–884, 1969.

[CLS17] Richard Cleve, Li Liu, and William Slofstra. Perfect commuting-operator strategies for linear system games. *Journal of Mathematical Physics*, 58(1):012202, 2017.

[CMS16] Jing Chen, Samuel McCauley, and Shikha Singh. Rational proofs with multiple provers. In *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science*, pages 237–248. ACM, 2016.

[Col17] Andrea W. Coladangelo. Parallel self-testing of (tilted) epr pairs via copies of (tilted) chsh and the magic square game. *Quantum Information and Computation*, 17:831–865, 2017.

[Col18] Andrea Coladangelo. Generalization of the clauser-horne-shimony-holt inequality self-testing maximally entangled states of any local dimension. *Physical Review A*, 98(5):052115, 2018.

[Col19] Andrea Coladangelo. Smart contracts meet quantum cryptography. *arXiv preprint arXiv:1902.05214*, 2019.

[CS17a] Andrea Coladangelo and Jalex Stark. Robust self-testing for linear constraint system games. *arXiv preprint* `arXiv:1709.09267`, 2017.

[CS17b] Andrea Coladangelo and Jalex Stark. Separation of finite and infinite-dimensional quantum correlations, with finite question or answer sets. *arXiv preprint* `arXiv:1708.06522`, 2017.

[CS18] Andrea Coladangelo and Jalex Stark. Unconditional separation of finite and infinite-dimensional quantum correlations. *arXiv preprint arXiv:1804.05116*, 2018.

[DDL17] Bernardo David, Rafael Dowsley, and Mario Larangeira. Kaleidoscope: An efficient poker protocol with payment distribution and penalty enforcement. Technical report, Cryptology ePrint Archive, Report 2017/899, 2017. http://eprint. iacr. org/2017/899, 2017.

[DDL18] Bernardo David, Rafael Dowsley, and Mario Larangeira. 21-bringing down the complexity: fast composable protocols for card games without secret state. In *Australasian Conference on Information Security and Privacy*, pages 45–63. Springer, 2018.

[FH15] Joseph F. Fitzsimons and Michal Hajdušek. Post hoc verification of quantum computation, 2015. arXiv preprint `arXiv:1512.04375`.

[GHRV14] Siyao Guo, Pavel Hubáček, Alon Rosen, and Margarita Vald. Rational arguments: single round delegation with sublinear verification. In *Proceedings of the 5th conference on Innovations in theoretical computer science*, pages 523–540. ACM, 2014.

[GHRV16] Siyao Guo, Pavel Hubáček, Alon Rosen, and Margarita Vald. Rational sumchecks. In *Theory of Cryptography Conference*, pages 319–351. Springer, 2016.

[GKW15] Alexandru Gheorghiu, Elham Kashefi, and Petros Wallden. Robustness and device independence of verifiable blind quantum computing. *New Journal of Physics*, 17, 2015.

[HPDF15] Michal Hajdušek, Carlos A. Pérez-Delgado, and Joseph F. Fitzsimons. Device-independent verifiable blind quantum computation, 2015. arXiv preprint `arXiv:1502.02563`.

[KLR+08] Emanuel Knill, Dietrich Leibfried, Rolf Reichle, Joe Britton, R Brad Blakestad, John D Jost, Chris Langer, Roee Ozeri, Signe Seidelin, and David J Wineland. Randomized benchmarking of quantum gates. *Physical Review A*, 77(1):012307, 2008.

[Mah17] Urmila Mahadev. Classical homomorphic encryption for quantum circuits. *arXiv preprint arXiv:1708.02130*, 2017.

[Mah18] Urmila Mahadev. Classical verification of quantum computations. *arXiv preprint arXiv:1804.01082*, 2018.

[McK11] Matthew McKague. Self-testing graph states. In *Conference on Quantum Computation, Communication, and Cryptography*, pages 104–120. Springer, 2011.

[McK16a] Matthew McKague. Interactive proofs for BQP via self-tested graph states. *Theory of Computing*, 12(3):1–42, 2016. arXiv preprint `arXiv:1309.5675`.

[McK16b] Matthew McKague. Self-testing in parallel. *New Journal of Physics*, 18(4):045013, 2016.

[Mon16] Ashely Montanaro. Quantum algorithms: an overview. *npj Quantum Information*, 2(15023), 2016.

[MS16] Carl A Miller and Yaoyun Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *Journal of the ACM (JACM)*, 63(4):33, 2016.

[MY04] Dominic Mayers and Andrew Yao. Self testing quantum apparatus. *Quantum Information & Computation*, 4:273–286, 2004.

[MYS12] Matthew McKague, Tzyh Haur Yang, and Valerio Scarani. Robust Self Testing of the Singlet. *J. Phys. A: Math. Theor.*, 45:455304, 2012.

[NV17] Anand Natarajan and Thomas Vidick. A quantum linearity test for robustly verifying entanglement. In *Proceedings of the Forty-ninth Annual ACM SIGACT Symposium on Theory of Computing (STOC 2017)*, pages 1003–1015, 2017.

[NV18] Anand Natarajan and Thomas Vidick. Low-degree testing for quantum states. *arXiv preprint arXiv:1801.03821*, 2018.

[Par09] Matteo GA Paris. Quantum estimation for quantum technology. *International Journal of Quantum Information*, 7(supp01):125–137, 2009.

[PV10] Károly F Pál and Tamás Vértesi. Maximal violation of a bipartite three-setting, two-outcome bell inequality using infinite-dimensional quantum systems. *Physical Review A*, 82(2):022116, 2010.

[PVN14] Károly F Pál, Tamás Vértesi, and Miguel Navascués. Device-independent tomography of multipartite quantum states. *Phys. Rev. A*, 90(4):042340, 2014.

[RUV13] Ben W. Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496:456–460, 2013. Full version `arXiv:1209.0448`.

[SAT+16] Alexia Salavrakos, Remigiusz Augusiak, Jordi Tura, Peter Wittek, Antonio Acín, and Stefano Pironio. Bell inequalities for maximally entangled states. *arXiv preprint arXiv:1607.04578*, 2016.

[SCAA17] Ivan Supić, Andrea Coladangelo, Remik Augusiak, and Toni Acín. A simple approach to self-testing multipartite states. *arXiv preprint* `arXiv:1707.06534`, 2017.

[VV14] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Physical review letters*, 113(14):140501, 2014.

[WCY+14] Xingyao Wu, Yu Cai, Tzyh Haur Yang, Huy Nguyen Le, Jean-Daniel Bancal, and Valerio Scarani. Robust self-testing of the three-qubit W state. *Phys. Rev. A*, 90(4):042339, 2014.

[WEH18] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412):eaam9288, 2018.

[YN13] Tzyh Haur Yang and Miguel Navascués. Robust self-testing of unknown quantum systems into any entangled two-qubit states. *Phys. Rev. A*, 87:050102, May 2013.

[YVB+14] Tzyh Haur Yang, Tamás Vértesi, Jean-Daniel Bancal, Valerio Scarani, and Miguel Navascués. Robust and Versatile Black-Box Certification of Quantum Devices. *Phys. Rev. Lett.*, 113:040401, Jul 2014.

[Zha17] Mark Zhandry. Quantum lighning never strikes the same state twice. *arXiv preprint arXiv:1711.02276*, 2017.