Extremal Quantum Correlations and Cryptographic Security

T. Franz,* F. Furrer, and R. F. Werner

Institut für Theoretische Physik, Leibniz Universität Hannover, Appelstraße 2, 30167 Hannover, Germany

(Received 11 October 2010; published 24 June 2011)

We investigate a fundamental property of device-independent security in quantum cryptography by characterizing probability distributions which are necessarily independent of the measurement results of any eavesdropper. We show that probability distributions that are secure in this sense are exactly the extremal quantum probability distributions. This allows us to give a characterization of security in algebraic terms. We apply the method to common examples for two-party as well as multiparty setups and present a scheme for verifying security of probability distributions with two parties, two measurement settings, and two outcomes.

DOI: 10.1103/PhysRevLett.106.250502 PACS numbers: 03.67.Dd, 03.65.Ud

The idea of using quantum systems for secure communication has been around for more than 25 years now. But still the boundaries of quantum cryptography have not been fully understood. Only recently has a remarkable feature of quantum systems been realized, namely, that observed violations of a Bell inequality may imply cryptographic security, even if the measurements that lead to the violation are unknown to legitimate parties. This principle goes under the name "device-independent security" and has been proven against collective attacks [1] and, recently, against arbitrary attacks for memoryless measurement devices [2,3]. But still no proof for the most general situation is known. In this Letter, we focus on the question of when measurement outcomes obtained by the legitimate parties are independent of measurements performed by an eavesdropper. We give a necessary and sufficient condition for this under the assumption that the probability distributions are known without error.

We consider a quantum correlation experiment with N separated parties, each performing one of M different local measurements with K outcomes. We denote this situation by the triple (N, M, K). In a device-independent scenario, the parties (usually $N = 2$) want to extract a secret key from the observed correlations in which the security estimation is solely based on the measured probability distributions. There are no assumptions on the proper functioning of the measurement devices or the measured system, e.g., on their dimension. Probability distributions that are useful for cryptography have to feature certain properties. First, the obtained correlations should not permit a local hidden variable (LHV) model, as in this case a potential adversary can have full knowledge about the correlations. Second, the correlations should be only weakly correlated to any possible measurement of an adversary. The first property is well known to be equivalent to violating a Bell inequality (see below), but the latter still lacks a concrete characterization.

In this Letter, we address this problem by specifying all probability distributions which do not allow a LHV model and are provably statistically independent of the knowledge of any eavesdropper. We show that these probability distributions, which we call secure, can completely be characterized in geometric terms. Indeed, in the convex body $\mathcal{Q}$ of all quantum probability distributions, the secure points are precisely the nonclassical extremal points, i.e., those which are not deterministic and cannot be obtained as a proper convex combination of other points in $\mathcal{Q}$.

The characterization of extremal points in $\mathcal{Q}$ is of general interest, and numerical approaches to determine them are known [4,5]. In our examples, we provide and discuss different tools to certify and find extremal probability distributions for particular (N, M, K) cases. In many situations, it turns out to be easier to establish a stronger property, i.e., that the algebraic structure of the measurement operators is completely determined by the probability distributions. This also leads to a stronger notion of security. The most prominent example (see example 3) are correlations which maximally violate the Clauser-Horne-Shimony-Holt inequality [6].

Our results have links to previous results obtained in the framework of nonsignaling correlations, i.e., theories that are more general than quantum theory. One direction of our result, namely, that extremality implies security, was proven in Ref. [7] for nonsignaling theories in the bipartite case. In this Letter, we discuss only the quantum framework, although our proofs can in principle be adapted to any nonsignaling theory.

Definitions.—For simplicity, we consider the general (N, M, K) case, even though the results are also valid for different numbers of measurement settings and outcomes for each party. We denote the probability for obtaining a string of outcomes $\underline{x} = (x_1, \dots, x_N)$ given a string of measurement settings $\underline{s} = (s_1, \dots, s_N)$ by $\mathbb{P}(\underline{x} \mid \underline{s})$. These numbers are assumed to be known exactly; i.e., we do not consider the uncertainties involved in estimating such probabilities from a finite sample.

The set of probability distributions $\mathbb{P}$ conform to a LHV model, which can be realized by assuming the measurements reveal outcomes whose probabilities are predetermined, is called the set $\mathcal{C}$ of classical correlations. It is a polytope, i.e., generated by a finite number of extremal points, which are given by the assignment of definite outcomes to each measurement. The faces (of maximal dimension) correspond to inequalities, which are linear in $\mathbb{P}$, and are called (tight) Bell inequalities. In the $(2, 2, 2)$ case all tight Bell inequalities are equivalent to the Clauser-Horne-Shimony-Holt inequality [8]. A survey about Bell inequalities and further references can be found in Ref. [9].

We are interested in the set $\mathcal{Q}$ of quantum correlations, which is defined as the set of all probability distributions $\mathbb{P}$ that can be realized by a quantum representation

$$\mathbb{P}(\underline{x} \mid \underline{s}) = \mathrm{tr}[\rho F(\underline{x} \mid \underline{s})], \qquad (1)$$

where ρ is a density operator on a Hilbert space $\mathcal{H}$, whose dimension is not constrained and can be infinite, and $F(\underline{x} \mid \underline{s}) = F_1(x_1 \mid s_1) \dots F_N(x_N \mid s_N)$ is a product of commuting operators on $\mathcal{H}$. $\{F_i(x \mid s)\}_x$ are the measurement operators of the observable chosen by the ith party according to the measurement setting s. Thus the $F_i(x \mid s)$ are positive operators satisfying $\sum_{x=1}^{K} F_i(x \mid s) = \mathbb{1}$ and have to commute for different sites, since the parties are independent. As shown in Ref. [10], every $\mathbb{P}$ which can be realized in this way can also be realized in a simplified "standard" form, in which $\rho = |\Omega\rangle\langle\Omega|$ is a pure state and the operators $F_i(x \mid s)$ are projections. Moreover, in the standard form, $|\Omega\rangle$ is cyclic for the algebra $\mathcal{A}(F)$, which is obtained from the $F_i(x \mid s)$ by taking products, linear combinations, and limits of expectation values. Cyclic means that the vectors $A|\Omega\rangle$ with $A \in \mathcal{A}(F)$ span a dense subspace in $\mathcal{H}$.

The set $\mathcal{Q}$ is a closed convex set which has in contrast to $\mathcal{C}$ a continuum of extremal points (see, for instance, [11]). Bell inequalities define the boundary between $\mathcal{C}$ and $\mathcal{Q}$. The set $\mathcal{Q}$ can be characterized similarly by inequalities that are linear in $\mathbb{P}$, satisfied by all $\mathbb{P} \in \mathcal{Q}$, and tight for at least one $\mathbb{P} \in \mathcal{Q}$. We call them Tsirelson inequalities. For every linear expression in $\mathbb{P}$, there is a maximum on $\mathcal{C}$ and another, usually larger one on $\mathcal{Q}$ which leads to a Tsirelson inequality. Computational methods to derive such maximal violations in $\mathcal{Q}$ are derived in Refs. [4,5]. For the Clauser-Horne-Shimony-Holt expression in the $(2, 2, 2)$ case, these maxima are 2 [6] and $2\sqrt{2}$ [12], respectively. The value 4 is achieved on the set of "nonsignaling correlations" $\mathcal{P}$, defined by the property that the measurement of one party does not change the probabilities observed by another. Similar to $\mathcal{C}$, $\mathcal{P}$ is generated by finitely many extremal points [7]. It holds with proper inclusion $\mathcal{C} \subset \mathcal{Q} \subset \mathcal{P}$.

Secure probability distributions.—We model the eavesdropper by another quantum party, whose measurements must commute with all $F(\underline{x} \mid \underline{s})$. Accordingly, we call a probability distribution $\mathbb{P}$ secure if $\mathbb{P}$ does not factorize, i.e., $\mathbb{P}(\underline{x} \mid \underline{s}) \neq \prod_{j=1}^{N} \mathbb{P}_j(x_j \mid s_j)$, and for any quantum representation and any operator E commuting with all $F_i(x_i \mid s_i)$

$$\mathrm{tr}[\rho E F(\underline{x} \mid \underline{s})] = \mathrm{tr}(\rho E)\mathbb{P}(\underline{x} \mid \underline{s}). \qquad (2)$$

The operator E represents all possible measurements an eavesdropper could perform. The requirement that $\mathbb{P}$ is not a product is necessary to exclude classical deterministic points, i.e., the extremal points of $\mathcal{C}$, for which (2) is satisfied trivially. As we will see, this excludes all probability distributions which can be realized in LHV models.

In device-independent cryptography, our definition ensures that an attack of an eavesdropper can never be better than a classical guess. The number of extractable secure bits by classical postprocessing can then be characterized by the classical smooth min entropy [13].

Our first main result gives a geometric interpretation of secure probability distributions: A probability distribution $\mathbb{P}$ is secure if and only if it is extremal in $\mathcal{Q}\backslash\mathcal{C}$.

The argument is straightforward. Suppose $\mathbb{P}$ is secure but not extremal. Then there exists a direct sum representation and a convex decomposition with $\mathbb{P} = \lambda\mathbb{P}_1 + (1 - \lambda)\mathbb{P}_2$, $0 \leq \lambda \leq 1$. Now use the definition (2) with E being the projector onto the first or second summand to get $\mathbb{P} = \mathbb{P}_1$ and $\mathbb{P} = \mathbb{P}_2$, respectively. This shows that the convex combination is indeed trivial and $\mathbb{P}$ is extremal. As all extremal correlations in $\mathcal{C}$ are of product form, it follows that $\mathbb{P} \notin \mathcal{C}$. Conversely, suppose $\mathbb{P}$ is extremal and $\mathbb{P} \notin \mathcal{C}$. As before, we can conclude that $\mathbb{P}$ cannot be of product form. Take any commuting $0 \leq E < \mathbb{1}$ and set $\lambda = \mathrm{tr}(\rho E)$. Define $\mathbb{P}_1 = (1/\lambda)\mathrm{tr}[\rho E F(\underline{x} \mid \underline{s})]$ and $\mathbb{P}_2 = [1/(1 - \lambda)]\mathrm{tr}[\rho(\mathbb{1} - E)F(\underline{x} \mid \underline{s})]$ such that $\mathbb{P} = \lambda\mathbb{P}_1 + (1 - \lambda)\mathbb{P}_2$. As $\mathbb{P}$ is extremal, it holds that $\mathbb{P} = \mathbb{P}_1$, which is just Eq. (2), so $\mathbb{P}$ is secure.

The decision of whether a given probability distribution is secure has now been reduced to certifying extremality in $\mathcal{Q}$. This is, in general, a hard problem. Even in the $(2, 2, 2)$ case, no simple algebraic constraints are known to verify extremality of a given $\mathbb{P}$. In this Letter, we will provide an explicit, yet limited, certification scheme in example 3.

Algebraically secure probability distributions.—There is a straightforward way to strengthen the definition of secure probability distributions by extending the factorization property to a larger set of observables. The reason is that the stronger notion of security is often easier to verify.

A probability distribution $\mathbb{P}$ is called algebraically secure if it is secure and for any quantum representation and any operator E commuting with all $F_i(x_i \mid s_i)$

$$\mathrm{tr}(\rho E\tilde{F}) = \mathrm{tr}(\rho E)\mathrm{tr}(\rho\tilde{F}), \qquad (3)$$

for all $\tilde{F} \in \mathcal{A}(F)$.

They are characterized as follows: A probability distribution $\mathbb{P}$ is algebraically secure if and only if it is extremal in $\mathcal{Q}\backslash\mathcal{C}$ and has a unique quantum representation, up to unitary equivalence.

A sketch of the proof goes as follows. Assume first that $\mathbb{P}$ is algebraically secure and therefore extremal. Let $\rho = |\Omega\rangle\langle\Omega|$ together with $F_i(x_i \mid s_i)$ and $\rho' = |\Omega'\rangle\langle\Omega'|$ with $F_i'(x_i \mid s_i)$ be two representations of $\mathbb{P}$ on suitable Hilbert spaces $\mathcal{H}$ and $\mathcal{H}'$. Condition (3) implies that for all corresponding operators $\tilde{F} \in \mathcal{A}(F)$ and $\tilde{F}' \in \mathcal{A}(F')$, $\mathrm{tr}(\rho\tilde{F}) = \mathrm{tr}(\rho'\tilde{F}')$. Otherwise, the direct sum representation with E chosen as the projector on the first or second summand contradicts (3). Define then the unitary operator U via $U\tilde{F}|\Omega\rangle = \tilde{F}'|\Omega'\rangle$, which transforms one representation into the other. Because $|\Omega\rangle$ and $|\Omega'\rangle$ are cyclic, U can be extended to a unitary from $\mathcal{H}$ to $\mathcal{H}'$. Conversely, assume that $\mathbb{P}$ is extremal and all representations are unitarily equivalent. Let $0 \leq E \leq \mathbb{1}$ be an operator commuting with all $F_i(x_i \mid s_i)$. Since $\mathbb{P}$ is extremal, $\frac{1}{\mathrm{tr}(\rho E)} \times \sqrt{E}\rho\sqrt{E}$ together with the operators $F_i(x_i \mid s_i)$ is a valid quantum representation of $\mathbb{P}$. Hence, $E = \mathbb{1}$, which implies (3).

Secure vs algebraically secure.—It is now interesting to identify cases for which the notions of secure and algebraically secure coincide. To formalize the question, we can introduce a map Γ from all possible (unitary inequivalent) quantum representations $\mathcal{S}$ $[= \mathcal{S}(N, M, K)]$ to the set of probability distributions $\mathcal{Q}$. The set $\mathcal{S}$ can be considered as a convex set, and the map Γ is linear and surjective but not injective. The extremal points of $\mathcal{S}$ are exactly the irreducible quantum representations, which are defined by the property that the only invariant subspaces of $\mathcal{A}(F)$ are $\{0\}$ and $\mathcal{H}$. As shown in Ref. [14], each extremal probability distribution $\mathbb{P} \in \mathcal{Q}$ admits an irreducible quantum representation. Hence, a secure probability distribution $\mathbb{P}$ is algebraically secure if and only if $\Gamma^{-1}(\mathbb{P})$ is exactly one extremal point in $\mathcal{S}$. In Fig. 1, the point (a) corresponds to an algebraically secure probability distribution, while the point (b) and the end points of the line (c) are secure but not algebraically secure.

In the following, we discuss examples for which we provide methods to find extremal points and criteria to decide when they are also algebraically secure.

Example 1: The $(N, 2, 2)$ case.—The algebraic structure of the $(N, 2, 2)$ case is quite well understood (see, e.g., [15] and references therein). All irreducible quantum representations are in this case given on an N-qubit space $\mathcal{H} = \otimes_{i=1}^{N}\mathbb{C}^2$ with an arbitrary pure state $\psi \in \mathcal{H}$ and measurements, which are parameterized by N angles $\theta_1, \ldots, \theta_N$ $(\theta_i \in [0, \pi])$. The measurements are given at site i as $F_i(1, 1) = \frac{1}{2}(\mathbb{1} + \sigma_3)$ and $F_i(1, 2) = \frac{1}{2}[\mathbb{1} + \sin(\theta_i)\sigma_1 + \cos(\theta_i)\sigma_3]$, together with their complements $F_i(2, s) = \mathbb{1} - F_i(1, s)$. The σ_i denote the Pauli matrices, and we omitted the identities on the tensor factors for the other parties. This parametrization in $\{\theta_i\}$ and ψ is sufficient to determine the whole convex body $\mathcal{Q}$. An arbitrary $\mathbb{P}$ is a direct sum of at most $4^N + 1$ irreducible representations. Compare Ref. [16] for an alternative deviation of these results.

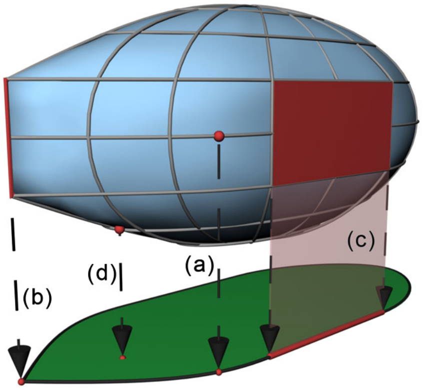

FIG. 1 (color online). Sketch of the set of quantum representations $\mathcal{S}$ (above) and the set of probability distributions $\mathcal{Q}$ (below). An extremal probability distribution can correspond either to a unique point (a) or to a face of $\mathcal{S}$ (b). Other faces of $\mathcal{S}$ can be mapped to faces of $\mathcal{Q}$ (c). Not all extremal points of $\mathcal{S}$ are also extremal for $\mathcal{Q}$ (d).

In order to find extremal points and test algebraic uniqueness, we combine the above parametrization with a maximization of a Tsirelson inequality. More explicitly, for each functional given by coefficients $\{c(\underline{x} \mid \underline{s})\}$, we can ask for the maximal quantum violation, i.e., $Q_c := \sup_{\mathbb{P}\in\mathcal{Q}} \sum_{\underline{x},\underline{s}} c(\underline{x} \mid \underline{s})\mathbb{P}(\underline{x} \mid \underline{s})$. In general, Q_c can be computed by a hierarchy of semidefinite programs [4,5]. Here, we follow another strategy by parameterizing the corresponding operator $C = \sum c(\underline{x} \mid \underline{s})F(\underline{x} \mid \underline{s}) = C(\theta_1, \ldots, \theta_N)$ by means of the irreducible representations. The maximization of $\langle\psi|C(\theta_1, \ldots, \theta_N)|\psi\rangle$ over all $\theta_i \in [0, \pi)$ and $\psi \in \mathbb{C}^{2^N}$ yields Q_c. Moreover, if there is exactly one set of parameters $\theta_1, \ldots, \theta_N$ and a unique state ψ for which the maximum is attained, the corresponding probability distribution $\mathbb{P}$ is algebraically secure. In the case where more than one possible choice of $\theta_1, \ldots, \theta_N$, ψ leads to a maximal violation, we can determine the convex span of the corresponding probability distributions. This corresponds to the face given by the intersection of $\mathcal{Q}$ and the hyperplane $\{\mathbb{P} \mid \sum_{\underline{x},\underline{s}} c(\underline{x} \mid \underline{s})\mathbb{P}(\underline{x} \mid \underline{s}) = Q_c\}$. Extremal points of that face are extremal points of $\mathcal{Q}$ and, thus, secure probability distributions.

As a straightforward application, one can deduce that the probability distributions leading to maximal violation of Mermin's inequalities [17] are algebraically secure.

Example 2: Certificate of extremality in the $(2, 2, 2)$ case.—The idea of the foregoing example was to find extremal $\mathbb{P}$'s by maximizing a given Tsirelson expression. Here, we start with a particular $\mathbb{P}$ and want to construct a Tsirelson inequality saturated by $\mathbb{P}$. If there exists such an inequality which is not trivial, i.e., cannot be saturated by any LHV model, and no other probability distribution in $\mathcal{Q}$ saturates it (or alternatively that just one quantum representation of $\mathbb{P}$ exists), extremality of $\mathbb{P}$ is certified.

We focus on the $(2, 2, 2)$ case and discuss a method for how to construct a maximally violated Tsirelson expression for a given $\mathbb{P}$. It comes along with a natural order of complexity for which we solve the lowest order explicitly. The main ingredient is again the parametrization of the irreducible quantum representations by a state $\psi \in \mathbb{C}^2 \otimes \mathbb{C}^2$ and two angles $\underline{\theta} = (\theta_A, \theta_B)$ (see the previous example) for which we denote the obtained probability distribution by $\mathbb{P}_{(\underline{\theta},\psi)}$. Because we are interested only in extremal $\mathbb{P}$'s, it is sufficient to consider $\mathbb{P}_{(\underline{\theta},\psi)}$ with a real ψ [10]. Since we have dichotomic measurements, we can equivalently work with ± 1 valued observables instead of measurement operators. We denote the observables on Alice's (Bob's) side by A_1 and A_2 (B_1 and B_2) and set $A_0 = B_0 = \mathbb{1}$.

Finding a Tsirelson inequality for $\mathbb{P}_{(\underline{\theta},\psi)}$ is equivalent to the following task: Construct a positive operator $T = \sum_k P_k(A_i, B_j)^\dagger P_k(A_i, B_j)$, with $P_k(A_i, B_j)$ polynomials in $A_i \otimes B_j$, $i, j = 0, 1, 2$, such that (i) $P_k[A_i(\theta_A), B_j(\theta_B)]\psi_0 = 0$ for all k and (ii) $T = \sum_{i,j=0}^{2} t_{ij} A_i \otimes B_j$ for all possible observables in $\mathcal{H}$. Here, $A_i(\theta_A)$ and $B_j(\theta_B)$ denote the observables of the representation $(\underline{\theta}, \psi)$. Condition (ii) implies that T can be interpreted as a linear functional of $\mathbb{P}$, (i) that it is 0 for $\mathbb{P}_{(\underline{\theta},\psi)}$, and the ansatz for T that T is a positive operator, and thus its associated functional on $\mathbb{P}$ is positive for each $\mathbb{P} \in \mathcal{Q}$.

In order to solve the problem, a constraint on the degree of the polynomials P_k in the ansatz for T has to be imposed. This introduces a natural hierarchy, where the order limits the possible $\mathbb{P}_{(\underline{\theta},\psi)}$ for which the method succeeds. For the simplest ansatz, $P_k = \sum_{j=1}^{2} (\alpha_{kj} A_j \otimes \mathbb{1} - \beta_{kj} \mathbb{1} \otimes B_j)$ ($\alpha_{kj}, \beta_{kj} \in \mathbb{R}$), the $\mathbb{P}$'s for which a Tsirelson inequality can be constructed are exactly the ones which correspond to a representation $(\phi_x^\pm, \theta_A, \theta_B)$ with maximally entangled state $\phi_x^\pm = (1/\sqrt{2})(\cos x, \mp \sin x, \sin x, \pm \cos x)$ ($x \in [0, \pi)$) for which

$$\frac{\sin(2x)\sin(2x \pm \theta_B)}{\sin(2x - \theta_A)\sin(2x - \theta_A \pm \theta_B)} < 0$$

holds. The corresponding Tsirelson inequality and the derivation can be found in Ref. [10].

Example 3: The $(2, M, 2)$ *case for full correlations.*— The difficulty of finding extremal points in the $(2, M, 2)$ scenario can be considerably reduced, as it is sufficient to consider only full correlations. This was shown by Tsirelson in Ref. [12], where he characterized all extremal points. In the following, let A_i and B_j, $i, j \in \{1, \ldots, M\}$, denote ± 1 valued observables located by Alice and Bob, respectively, and ρ a density operator. The set of quantum correlations $\mathcal{Q}_{\text{cor}}$ is given by all correlation tables $c_{ij} = \text{tr}(A_i B_j \rho)$ which can be obtained by means of a quantum representation. In Ref. [12] it was proven that all quantum representations of an extremal correlation table which is not deterministic have uniform marginal distributions $\text{tr}(A_i\rho) = \text{tr}(B_j\rho) = 0$. Thus, nondeterministic extremal correlations in $\mathcal{Q}_{\text{cor}}$ correspond to secure probability distributions in $\mathcal{Q}$. Furthermore, an extremal correlation table which allows just one quantum representation gives rise to an algebraically secure point.

For every correlation table c_{ij} exists a so-called c system, that is, a collection of vectors x_i, y_j ($i, j \in \{1, \ldots, M\}$) with $\|x_i\| \leq 1$, $\|y_j\| \leq 1$ in an Euclidian space with dimension M, such that $c_{ij} = \langle x_i, y_j \rangle$. If $\mathbb{P}$ is extremal, the corresponding c systems are isometric to each other, $\|x_i\| = \|y_j\| = 1$, and the linear hulls of the $\{x_i\}$ and $\{y_j\}$ coincide. Calling the dimension of the linear hull the rank r of the c system, it further follows that $\{x_i \otimes x_i, y_j \otimes y_j\}$ span the symmetric subspace of $\mathbb{R}^r \otimes \mathbb{R}^r$. The following inequalities hold: $r \leq M$, $r \leq -1/2 + \sqrt{1/4 + 4M}$, and $r(r+1)/2 \leq 2M - 1$. There are two cases to be distinguished. For c systems with even rank, the representation is unique (up to unitary equivalence), while for c systems with odd rank, there are exactly two nonequivalent representations.

With this, the question of secure versus algebraically secure is equivalent to determining the rank of the c system which corresponds to the given correlation table. According to the inequalities above, it follows directly that all probability distributions in the $(2, 2, 2)$ and $(2, 3, 2)$ cases which correspond to nonclassical extremal correlations in $\mathcal{Q}_{\text{cor}}$ are algebraically secure.

T. F. acknowledges support from the DFG under Grant No. WE-1240/12-1. F. F. acknowledges support from the Graduiertenkolleg 1463 of the Leibniz Universität Hannover. R. F. W. acknowledges the support of the EU FP7 project COQUIT (Contract No. 233747).

*torsten.franz@itp.uni-hannover.de

[1] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[2] E. Hänggi and R. Renner, arXiv:1009.1833.

[3] L. Masanes, S. Pironio, and A. Acín, Nature Commun. **2**, 238 (2011).

[4] A. Doherty, Y. Liang, B. Toner, and S. Wehner, in *Proceedings of the 23rd Annual IEEE Conference on Computational Complexity* (IEEE, New York, 2008), pp. 199–210.

[5] M. Navascues, S. Pironio, and A. Acin, New J. Phys. **10**, 073013 (2008).

[6] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[7] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, Phys. Rev. A **71**, 022101 (2005).

[8] A. Fine, Phys. Rev. Lett. **48**, 291 (1982).

[9] http://qig.itp.uni-hannover.de/qiproblems/1.

[10] See supplemental material at http://link.aps.org/supplemental/10.1103/PhysRevLett.106.250502 for proofs.

[11] L. Masanes, arXiv:quant-ph/0309137.

[12] B. S. Tsirelson, J. Sov. Math. **36**, 557 (1987).

[13] R. Impagliazzo, L. Levin, and M. Luby, Stoch. Proc. Appl. **89**, 12 (1989).

[14] W. Arveson, J. Am. Math. Soc. **21**, 1065 (2008).

[15] I. Raeburn and A. M. Sinclair, Math. Scand. **65**, 278 (1989).

[16] L. Masanes, arXiv:quant-ph/0512100.

[17] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).