One-Sided Device-Independent Certification of Unbounded Random Numbers

Brian Coyle, Matty J Hoban, Elham Kashefi

One-Sided Device-Independent Certification of Unbounded Random Numbers

Brian Coyle
School of Informatics, University of Edinburgh,
Edinburgh EH8 9AB, United Kingdom.
brian.coyle@ed.ac.uk

Matty J. Hoban
Department of Computer Science, University of Oxford,
Oxford OX1 3QD, United Kingdom.
matthew.hoban@cs.ox.ac.uk

Elham Kashefi
School of Informatics, University of Edinburgh,
Edinburgh EH8 9AB, United Kingdom.
Laboratoire dInformatique de Paris 6, CNRS,
Sorbonne Universite, 4 place Jussieu, 75005 Paris.
ekashefi@inf.ed.ac.uk

The intrinsic non-locality of correlations in Quantum Mechanics allow us to certify the behaviour of a quantum mechanism in a device independent way. In particular, we present a new protocol that allows an unbounded amount of randomness to be certified as being legitimately the consequence of a measurement on a quantum state. By using a sequence of non-projective measurements on single state, we show a more robust method to certify unbounded randomness than the protocol of [5], by moving to a *one-sided* device independent scenario. This protocol also does not assume any specific behaviour of the adversary trying to fool the participants in the protocol, which is an advantage over previous steering based protocols. We present numerical results which confirm the optimal functioning of this protocol in the ideal case. Furthermore, we also study an experimental scenario to determine the feasibility of the protocol in a realistic implementation. The effect of depolarizing noise is examined, by studying a potential state produced by a networked system of ion traps.

1 Introduction

Quantum mechanics is a theory that can exhibit, in some sense, fundamental randomness. This randomness can be extracted by measurements on a quantum system, but if the party preparing the quantum state and/or measurement apparatus is untrusted, how can we verify that a true measurement is occurring on a real quantum state? The seed of the answer was discovered by Bell in [1] in the form of Bell inequalities. The violation of these inequalities by certain quantum systems proved, along with the argument of Einstein, Podolsky and Rosen in 1935, [6], that quantum mechanics must be a non-local theory. Using these inequalities and non-local properties, it is possible to test the following about a process. If we acquire statistics produced by some procedure, and it can be shown that the statistics violate these Bell inequalities, then those statistics cannot have been produced by a local hidden variable theory. Using these ideas, it is possible to determine if randomness produced by a given apparatus was in fact the result of measurements on a quantum system, as opposed to being the result of a deterministic process. This 'Bell non-locality' has been utilized extensively in a situation referred to as *device independence*, where it is possible to certify quantum behaviours, even in a scenario where the party producing the device is untrusted, [13, 4].

In [5], the authors propose a scenario to generate and certify an unbounded amount of randomness

M. Cuffaro and P. Papayannopoulos (Eds.): 9th International Workshop on Physics and Computation (PC 2018)
EPTCS 273, 2018, pp. 14–26, doi:10.4204/EPTCS.273.2

using a sequence of non-projective measurements on a single quantum state. Non-projectivity is required to preserve some entanglement in the quantum state after the measurement, which is an essential resource in determining non-locality. In this scenario, Alice (A), and Bob (B), share an entangled state, possibly produced by a third party eavesdropper, Eve (E). Both halves of this state are contained in two separate devices and each sent to one of Alice or Bob. Alice (Bob) then chooses to measure in a particular basis, x (y), and record their measurement outcome, a (b). The randomness of one (local randomness), or both (global randomness) outcomes can be certified using a violation of a particular Bell inequality. Both inputs, x, y and outcomes a, b are assumed to be binary variables for simplicity, such that:

$$\overbrace{\begin{matrix} x \in \{0,1\} \\ y \in \{0,1\} \end{matrix}}^{\text{Measurements:}} \qquad \overbrace{\begin{matrix} a \in \{1,-1\} \\ b \in \{1,-1\} \end{matrix}}^{\text{Outcomes:}}$$

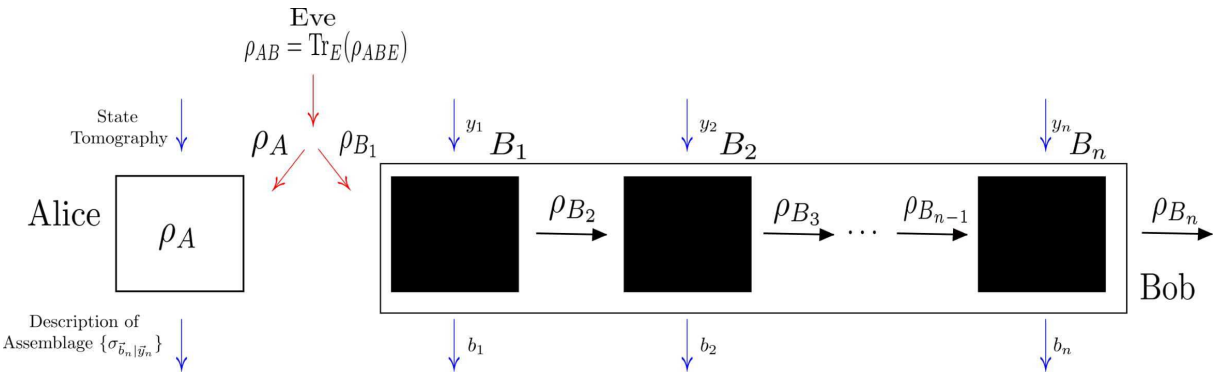


Figure 1: Illustration of Protocol 1. Bob makes a sequence of measurements on his state in a black box, and Alice certifies the randomness of the outcomes using the assemblage, $\{\sigma_{\vec{b}_n|\vec{y}_n}\}$

It is also possible to lift the trust restrictions on one of the parties, Alice say, so that she has full autonomy over her half of the shared state and measurement apparatus. This means that at any stage in the process, she has the ability to do quantum state tomography to determine the state she possesses and she is able to directly control her measurements. This is referred to as the *steering* or *one-sided device independent* scenario, because the results of Bob's measurements on his side of the shared state cause Alice to be '*steered*' into a certain state, which is dependent on Bob's measurement choice. Typically, in the fully device independent scenario, the joint probability distribution between Alice and Bob's outcomes given their measurement choices, $P(ab|xy)$, is the relevant quantity studied to enable certification of randomness. However, in the one-sided case, this is no longer relevant because we are not interested in Alice's measurement outcomes. Instead, we study the *assemblage*, $\{\sigma_{b|y}\}$, [14], which is the set of conditional unnormalized quantum states that one party can be steered into, given measurement choices of the other. In this paper, we will keep the convention of [5], where Bob makes measurements on his state, and Alice's state is the one which is steered. These assemblage elements, $\sigma_{b|y}$, are conditional on Bob's outcome, b, and his choice of measurement basis, y. The elements are defined by: $\sigma_{b|y} = p(b|y)\rho_{b|y} = \mathrm{tr}_B[(\mathbb{1}_A \otimes M_{b|y})\rho_{AB}]$, where $\rho_{AB} = \mathrm{tr}_E \rho_{ABE}$ is the state prepared by Eve and sent to Alice and Bob, and $\rho_{b|y}$ is the state that Alice is steered into conditional on Bob's input, y, and measurement outcome, b. $M_{b|y}$ are the POVM elements Bob expects to be able to measure by choosing his input y, such that $M_{b|y} \geq 0 \; \forall b, y$, and $\sum_b M_{b|y} = \mathbb{1}, \forall y$.

In the steering scenario, the certification of the local randomness of Bob's outcomes can be done by examining the assemblage elements, and their violation of '*steering inequalities*', analogous to the violation of Bell inequalities by the non-local probability distributions, $P(ab|xy)$. A maximal violation of steering inequalities corresponds to a maximally steerable state. The idea of producing certifiable randomness using steering was first studied by Law *et al.* [9], and then with the assistance of semi-definite programming by Passaro *et al.* [12]. Given an assemblage, a method was derived to determine the *steerability* of the assemblage via semi-definite programs (SDPs) by Skrzypczyk *et. al.*, [15]. The *steering weight* (SW) is given to be the solution to the following SDP, (1), and its dual program, (2):

$$
\begin{aligned}
SW = \quad & \min \quad 1 - \mathrm{tr}\sum_{\lambda} \sigma_\lambda \\
& \text{s.t.} \quad \sigma_{b|y} - \sum_{\lambda} D(b|y,\lambda)\sigma_\lambda \geq 0 \quad \forall b,y \\
& \qquad \sigma_\lambda \geq 0, \qquad\qquad\qquad \forall \lambda
\end{aligned}
\qquad (1)
$$

$$
\begin{aligned}
SW = \quad & \max \quad 1 - \mathrm{tr}\sum_{by} F_{b|y}\sigma_{b|y} \\
& \text{s.t.} \quad \sum_{by} D(b|y,\lambda)F_{b|y} - \mathbb{1} \geq 0 \quad \forall \lambda \\
& \qquad F_{b|y} \geq 0, \qquad\qquad\qquad \forall b,y
\end{aligned}
\qquad (2)
$$

The dual program, (2), is the most relevant for this paper because, as shown in [15], the dual variables of the SDP, (2), in fact define a steering inequality, $\{F_{b|y}\}$, for which the assemblage, $\{\sigma_{b|y}\}$, produces a maximal violation. $\{\sigma_\lambda\}$ is an assemblage that Eve could produce for Alice using hidden variables, λ, and the SDPs, (1), (2), test for the existence of such an assemblage. In the case where certifiable randomness is produced as a result of Bob's measurement, we want no such *local hidden state* (LHS) assemblages to exist. If Eve had the ability to reproduce the assemblage that Alice receives, by using her knowledge of these hidden variables then, from Eve's point of view, the outcomes that Bob receives are in fact deterministic, and not random.

The scenario that this work is presented in is similar to that of [5], where we assume Bob can implement non-projective measurements in rotated versions of the Pauli-X and Z bases, however Alice only needs the functionality to implement projective Pauli-X and Z basis measurements, since it is sufficient for her to do quantum state tomography to certify Bob's random outcomes. Also, [5] only considers the X basis measurement to be non-projective, and hence the random outcomes are obtained from a sequence of these X measurements. However, in this case, it is possible for Bob to also to choose to measure in a non-projective Z basis also. The motivation for this is the following. If Bob has the following state: $|0\rangle$, and makes a measurement in the Pauli-X basis, $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, he will get one of the outcomes $b_1 = \pm 1$, each with probability $1/2$. If he then makes a second measurement on the state, this time in the Pauli-Z basis, he will get one of the outcomes $b_2 = \pm 1$ each with probability $1/2$. However, if he had chosen his second measurement to be in the X basis, he would not get a random result, but a deterministic one. This example illustrates that measuring in (almost) orthogonal bases should give the maximal amount of randomness and will be further reinforced by numerical evidence shown in Figures (2c) and (3b) in Section 3.1 .

The following non-projective Kraus operators, $\Pi_{b|y}^{x(\theta)}$ are defined in [5]:

$$
\Pi_{\pm 1|1}^{x(\theta)} = \cos(\theta)\,|\pm\rangle\langle\pm| + \sin(\theta)\,|\mp\rangle\langle\mp| \qquad (3)
$$

These Kraus operators, which will be denoted by a measurement in the X_θ basis, reduce to the usual Pauli-X basis measurement operators for $\theta = 0$.

Introducing non-projective Z basis measurements corresponds to defining the following operators, denoted by Z_ϕ, which again reduce to the usual computational basis measurements for $\phi = 0$. The Kraus

operators for these non-projective measurements are given by:

$$\Pi^{z(\phi)}_{1|0} = \cos(\phi)\,|0\rangle\langle 0| + \sin(\phi)\,|1\rangle\langle 1| \qquad \Pi^{z(\phi)}_{-1|0} = \cos(\phi)\,|1\rangle\langle 1| + \sin(\phi)\,|0\rangle\langle 0| \tag{4}$$

Therefore, the POVM that Bob implements on his half of the shared state is:

$$M^{x(\theta)/z(\phi)}_{b|y} = (\Pi^{x(\theta)/z(\phi)}_{b|y})^{\dagger}(\Pi^{x(\theta)/z(\phi)}_{b|y}) \tag{5}$$

with $y = 1$ indicating that he has chosen to measure in the non-projective X_θ basis, and $y = 0$ indicates a measurement in the Z_ϕ basis. For a single measurement, if Alice wants to certify the randomness produced by Bob's non-projective X_θ measurements, the protocol should be repeated, with the same state produced by Eve, but in this 'test' run, Bob will choose to measure in the Z_0 basis. Alice will then do state tomography on the resulting states to determine them, and repeats until she has gathered enough statistics to reproduce the full assemblage with high enough confidence.

The quantifier of certifiable randomness that will be used is the *guessing probability* (GP), P_{G}. This quantifier was first discussed in [13] and was used in [5] for fully device-independent randomness certification. The SDP used in Protocol 1 is similar to that of [12], where the authors define the guessing probability in terms of the local hidden state (LHS) strategies that Eve could use to produce set of states for Alice and Bob which are determined by local hidden variables known only to her. However, this method uses an assumption about the fact that Eve creates these assemblage elements using local measurements on *her* side of the entangled state, effectively steering Alice and Bob into a given state, about which she could deduce certain properties. The ability for Eve to do this is clearly undesirable as this would enable her to have extra information about Bob's random outcomes. Essentially, this means his outcomes would be reproducible by some local hidden state model that Eve is using, as described above. However, the results of this paper make no assumptions about the specific actions of Eve. For clarity, we will study the case of a single measurement before giving the results for a sequence of measurements. With just a single measurement, the GP is given as the solution to the following SDP:

$$\begin{aligned} P_{\mathrm{G}}(y = y^*) = \quad & \max_{\{\sigma^E_{b|y}\}_{b,y}} && \mathrm{tr}_A[\sigma^E_{b|y^*}] \\ & \text{s.t.} && \sum_{b,y} F_{b|y}\sigma^E_{b|y} = v \\ & && \sum_b \sigma^E_{b|y} = \sum_b \sigma^E_{b|y'} \quad \forall e, y \neq y' \\ & && \sigma^E_{b|y} \succeq 0 \qquad\qquad \forall y, b \end{aligned} \tag{6}$$

The steering inequality $\{F_{b|y}\}$ is the one determined by the SDP, (2), which is maximally violated by the ideal assemblage, $\{\sigma_{b|y}\}$, that Alice expects to have access to if Eve follows the protocol honestly. The SDP, (6), allows Eve to create, for Alice, any assemblage, $\{\sigma^E_{b|y}\}$, as long as this assemblage obeys the constraints in the SDP. The first constraint enforces the fact that this assemblage should produce a violation of the steering inequality, $\{F_{b|y}\}$, with violation v that would be produced by the ideal assemblage. The second constraint enforces that Alice and Bob cannot communicate faster than the speed of light (no-signalling condition), while the last constraint enforces that Eve must produce a valid assemblage for Alice i.e. it must be a positive semidefinite matrix. We also assume Eve knows the measurement setting from which Bob wants to extract randomness, $y = y^*$.

Once Bob has made his measurement, Alice can then determine the state she then possesses as a

result. By repeating multiple runs of the protocol, Alice can determine the full statistics of Bob's measurement outcomes and hence the full assemblage. Once she knows the assemblage produced by the given initial state and measurement set, she can then calculate the optimal steering inequality for that assemblage, using (2), and the associated value of the violation, v, given by the steering inequality. Using this, she can calculate the GP with the SDP, (6). This guessing probability, as discussed in ([5], [13] , [9], [12]) is the optimal probability that Eve can guess Bob's outcome, b, given any information that she possesses. For example, if the assemblage is unsteerable (it has a steering weight of 0), then it is unsteerable with respect to any steering inequality and so the value of the violation, v, will reflect this. In this scenario, Eve could have engineered Bob's device to include some local hidden variables and hence produce deterministic outcomes. It is exactly this situation which we want to detect. For a single measurement, if the GP is equal to $1/2$, the outcome of the measurement is in fact random and Eve's only strategy is simply to guess randomly which outcome Bob received. However, if it is equal to 1, Eve knows the outcome exactly since, from her point of view, the process was deterministic. Clearly, to optimally certify randomness, we want the GP to be as close to the former situation as possible.

A further quantifier which is useful is the *min entropy*, H_{min}, [5]:

$$H_{min} = -\log_2(P_G) \tag{7}$$

The meaning of this quantity is clear. If $P_G = 1/2 \implies H_{min} = 1$ and so one certifiable random bit is produced by the measurement. If $P_G = 1 \implies H_{min} = 0$ and no randomness can be certified, i.e. the assemblage could have been produced by a LHS model.

2 One-Sided Device-Independent (1SDI) Protocol

As in [5], we can extend this scenario to one in which Bob implements a sequence of non-projective measurements on his half of the shared state. Defining the protocol for n rounds is therefore straightforward (n is predetermined by Alice and Bob), where on each round, Bob makes one measurement on the shared state. Bob will input his choice of measurement basis for the n rounds, denoted $\vec{y}_n = y_1 y_2 ... y_n \in \{0,1\}^n$, into the device and record his measurement outcomes, denoted $\vec{b}_n = b_1 b_2 ... b_n \in \{1,-1\}^n$. In round k, Bob chooses to measure in the '*noisy*' Pauli-X basis, X_{θ_k}, or the '*noisy*' Pauli-Z basis, Z_{ϕ_k}, using the Kraus operators defined by (3), (4) respectively. Of course, since the scenario is device independent, Bob does not know if these measurements were actually performed in the device, until the randomness is finally certified by the protocol.

If Alice wants to certify the randomness of the outcomes for all rounds up to round n, she must find the solution for the SDP, (8), for all $k < n$. This set of SDP's will give her the optimal steering inequality for each round k ($1 \leq k \leq n$), $\{F_{\vec{b}_k|\vec{y}_k}\}$, which is maximally violated by the assemblage $\{\sigma_{\vec{b}_k|\vec{y}_k}\}$.

$$\begin{aligned} SW(\sigma_{\vec{b}_k|\vec{y}_k}) = \quad & \max \quad 1 - \mathrm{tr} \sum_{\vec{b}_k,\vec{y}_k} F_{\vec{b}_k|\vec{y}_k} \sigma_{\vec{b}_k|\vec{y}_k} \\ & \text{s.t.} \quad \sum_{\vec{b}_k,\vec{y}_k} D(\vec{b}_k|\vec{y}_k,\vec{\lambda}_k) F_{\vec{b}_k|\vec{y}_k} - \mathbb{1} \geq 0 \quad \forall \vec{\lambda}_k \\ & \qquad F_{\vec{b}_k|\vec{y}_k} \geq 0, \qquad\qquad\qquad\quad \forall \vec{b}_k, \vec{y}_k \end{aligned} \tag{8}$$

This SDP calculates the steering weight for the assemblage created on measurement round k, however the actual value of this steering weight is not important for our purposes. Instead, we want to extract

the dual variables, $\{F_{\vec{b}_k|\vec{y}_k}\}$, which again define a steering inequality.

This SDP is adapted from [15] and as in that case, the primal SDP checks a given assemblage against all possible deterministic strategies, $D(\vec{b}_k|\vec{y}_k,\vec{\lambda}_k)$. This determines if the assemblage can be decomposed as a convex combination of assemblages, $\sigma_{\vec{\lambda}_k}$ that Eve could have created in some LHS model, given her possible knowledge of k hidden variables, $\vec{\lambda}_k = \lambda_1\lambda_2...\lambda_k$. Again, the steering inequality can be decomposed into a linear combination of these assemblage elements, with coefficients given by the variables $F_{\vec{b}_k|\vec{y}_k}$, which are the dual variables in the SDP, (8). Once Alice has this set of steering inequalities, she can determine the guessing probability for Eve, as the solution of the following SDP, (9):

$$P_{\mathrm{G}}(\vec{y}_n^*, F_{\vec{b}_n|\vec{y}_n}) = \max_{\vec{b}_n,\vec{y}_n} \mathrm{tr}_A\, \sigma^E_{\vec{b}_n|\vec{y}_n=\vec{y}_n^*} \tag{9}$$

s.t.

$$\begin{array}{ll|ll}
\sum_{\vec{b}_n,\vec{y}_n} F_{\vec{b}_n|\vec{y}_n}\sigma^E_{\vec{b}_n|\vec{y}_n} = v_n, & & \sum_{b_n}\sigma^E_{\vec{b}_n|\vec{y}_n} = \sigma^E_{\vec{b}_{n-1}|\vec{y}_{n-1}}, & \forall y_n \\
\sum_{\vec{b}_{n-1},\vec{y}_{n-1}} F_{\vec{b}_{n-1}|\vec{y}_{n-1}}\sigma^E_{\vec{b}_{n-1}|\vec{y}_{n-1}} = v_{n-1} & & \sum_{b_{n-1}}\sigma^E_{\vec{b}_{n-1}|\vec{y}_{n-1}} = \sigma^E_{\vec{b}_{n-2}|\vec{y}_{n-2}}, & \forall y_{n-1} \\
\vdots & \vdots & \vdots & \vdots \\
\sum_{b_1,y_1} F_{b_1|y_1}\sigma^E_{b_1|y_1} = v_1, & & \sum_{b_1}\sigma^E_{b_1|y_1} = \rho_A & \forall y_1 \\
\hline
\sum_{\vec{b}_n}\sigma^E_{\vec{b}_n|\vec{y}_n} = \sum_{b_n}\sigma^E_{\vec{b}_n|\vec{y}'_n}, & \forall \vec{y}_n,\vec{y}'_n & \sigma^E_{\vec{b}_n|\vec{y}_n} \succeq 0, & \forall \vec{y}_n,\vec{b}_n \\
\sum_{\vec{b}_{n-1}}\sigma^E_{\vec{b}_{n-1}|\vec{y}_{n-1}} = \sum_{b_{n-1}}\sigma^E_{\vec{b}_{n-1}|\vec{y}'_{n-1}}, & \forall \vec{y}_{n-1},\vec{y}'_{n-1} & \sigma^E_{\vec{b}_{n-1}|\vec{y}_{n-1}} \succeq 0, & \forall \vec{y}_{n-1},\vec{b}_{n-1} \\
\vdots & \vdots & \vdots & \vdots \\
\sum_{b_1}\sigma^E_{b_1|y_1} = \sum_{b_1}\sigma^E_{b_1|y'_1}, & \forall y_1,y'_1 & \sigma^E_{b_1|y_1} \succeq 0 & \forall y_1,b_1
\end{array}$$

Where the solution of this SDP is the guessing probability and the maximum over the trace of all the assemblages that Eve can create for Alice at the end of the protocol, $\sigma^E_{\vec{b}_n|\vec{y}_n=\vec{y}_n^*}$, for a particular input string, $\vec{y}_n^*$. Again, Eve knows from which measurement settings, $\vec{y}_n^*$, Bob wants to extract randomness. The steering inequality violations, $\vec{v}_n = v_1v_2\ldots v_n$ can be calculated by Alice once she has determined the associated steering inequality (if one exists). The constraints of the SDP are similar to the single measurement case except for the addition of one new set of constraints which are required for a sequence. These particular constraints enforce causality in the measurement sequence, so that, for example (for two measurement rounds):

$$\sum_{b_2}\sigma^E_{b_1b_2|y_1y_2} = \sigma^E_{b_1|y_1}, \qquad \forall y_2 \tag{10}$$

Simply put, this constraint means that Eve has no access to future events, i.e. in measurement round i, she only has access to information from rounds $j < i$ to aid in her attempts to guess the measurement outcomes.

For the final measurement round, the measurement operators become projective to end the protocol, i.e. $\theta_n = \phi_n = 0$ and the state at round $n-1$ is a pure entangled state. In this case, it is possible to define the steering inequality explicitly, as done in [15]:

$$F_{\vec{b}_n|\vec{y}_n} = \alpha\left(\mathbb{1} - \frac{\sigma_{\vec{b}_n|\vec{y}_n}}{\mathrm{tr}\left(\sigma_{\vec{b}_n|\vec{y}_n}\right)}\right) \tag{11}$$

where α is chosen sufficiently large. A choice of $\alpha = 100$ was chosen for all numerical results in this paper. Clearly, this choice of a steering inequality automatically gives a maximal violation value of $v_n = 0$.

Protocol 1 describes the full scenario in detail. If the guessing probability after n measurement rounds is sufficiently close to $1/2^n$, then Eve has followed the protocol faithfully and produced the required quantum state and measurement apparatus for Bob. This means that the probability of Eve guessing the sequence of bits that Bob has obtained decreases exponentially with the number of rounds in the protocol and we have true quantum randomness.

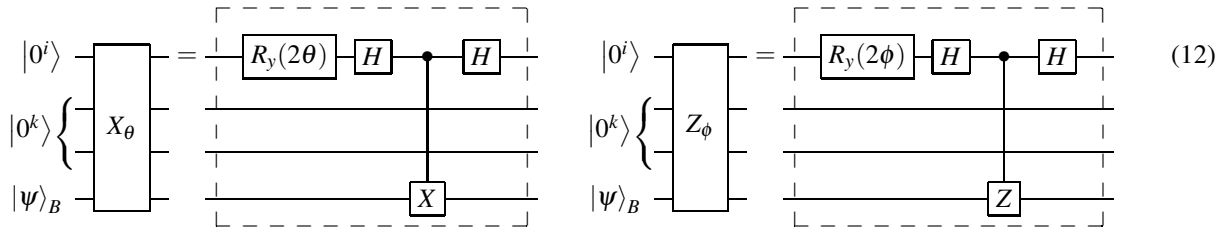
Protocol 1: 1SDI Randomness Certification

1. Eve prepares joint state ρ_{ABE} & sends state $\rho_{AB} = \mathrm{tr}_E(\rho_{ABE})$ to Alice and Bob. Bob's state is contained in a black box with the ability to implement a predetermined measurement sequence with angles, $\{\theta_1, \theta_2, \ldots, \theta_n\}, \{\phi_1, \phi_2, \ldots \phi_n\}$.
2. Bob chooses measurement y_1^* and makes measurement, $M_{b_1|y_1^*}$, on state corresponding to a measurement in either $X_{\theta_1}(y_1^* = 1)$, or $Z_{\phi_1}(y_1^* = 0)$ basis.
3. Alice's state is steered into $\sigma_{b_1|y_1^*}$, which she determines using state tomography.
4. Alice and Bob repeat step 2. and 3. up to n rounds to determine full assemblage for each round, k, $\{\sigma_{\vec{b}_k|\vec{y}_k^*}\}$ until Bob has made sufficient measurements to determine the measurement statistics accurately enough.
5. Alice determines the steering inequality for each assemblage generated by each measurement round, k, $\{F_{\vec{b}_k|\vec{y}_k^*}\}$ using SDP, (8), and the associated value of the steering inequality violation, v_k.
6. Alice uses SDP, (9), to determine the guessing probability for the assemblage after n rounds.
7. If the GP is sufficiently high, Alice and Bob abort the protocol and discard the measurement outcomes.

Figure (1) illustrates the protocol by writing Bob as a series of 'Bob's' to illustrate the causal structure of the protocol. In this picture, each B_i makes a single measurement on the state he receives from B_{i-1} by choosing a basis y_i, and receiving measurement outcome b_i before 'passing' the state onto B_{i+1}. As described above, each Bob has no access to the black box he receives, but Alice has full autonomy over her device.

2.1 Quantum Circuit for Protocol 1

The the following circuit, (13), was designed to implement Bob's half of the protocol, with his sequence of n measurements on his half of the shared state. First of all, the following two qubit unitary gates need to be introduced, that effectively implement the non-projective X_θ and Z_ϕ measurements, (12) respectively.

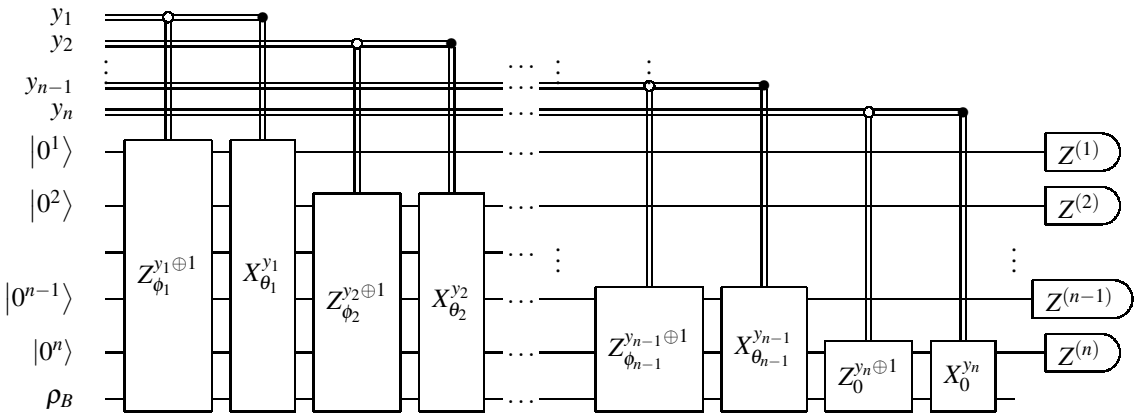


(12)

In each gate above, the control ancilla is the topmost one, labelled by i, where all the other (k) ancillas pass through the gate acted on by the identity. The index on the ancilla will represent the measurement

round it is used in. The input string, $\vec{y}_n$, for n measurement rounds is used as classical input to the circuit, and conditioned on this input for each round, either the noisy X or noisy Z measurement is implemented. As mentioned above, it is the topmost ancilla that is used as a control qubit for each gate in the circuit. At the end of the protocol, all ancillas can be measured in the usual computational basis, where $Z^{(k)}$ represents the measurement done in round k. Clearly, if the input $y_k = 0$, the noisy Z measurement is implemented, $Z_{\phi_k}^{y_k \oplus 1}$, while if $y_k = 1$, the noisy X measurement is implemented, $X_{\theta_k}^{y_k}$, and the other is not. In this fashion, only one quantum gate acts on the state per measurement round. Also, the state ρ_B is only Bob's half of the initial state.

This circuit is designed in the standard manner, in which all measurements are deferred to the end of the circuit. However, it could be further improved by using only a single ancilla. This ancilla would undergo multiple measurements, with the addition of a series of CNOT gates to the ancilla wire. These CNOT gates would return the ancilla to the usual $|0\rangle$ state conditioned on the previous measurement outcome.



(13)

3 Numerical Results

3.1 Ideal Case

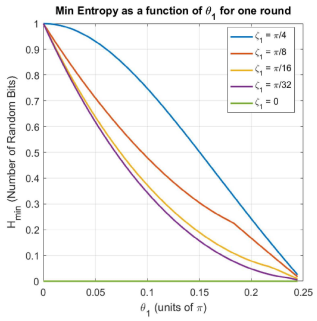
In this section, numerical results are presented to illustrate the performance of the protocol, in particular the SDP, (9), assuming ideal functionality of both devices. All numerical results were obtained using the Matlab convex optimization package, *cvx*, [2] and a package for managing quantum states, *qetlab*, [8]. The codes can be found at [3]. As a convention, it will be assumed that Bob always measures in the noisy X basis in the first round, with the final measurement round in the protocol being projective, $\theta_n = 0$ or $\phi_n = 0$, depending on whether n is odd or even. In all of the following, we assume the measurement statistics and runs of the protocol are i.i.d.

For completeness, the Min. Entropy for one round of measurement is plotted as a function of measurement angles used for the first round, with the noisy X measurements, X_{θ_1}, for a range of values of θ_1, as seen in Figure (2a). All measurements are applied on the initial state:

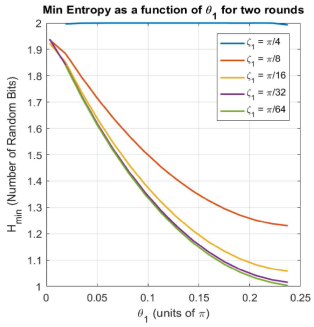
$$|\Psi(\zeta_1)\rangle = \cos(\zeta_1)|00\rangle + \sin(\zeta_1)|11\rangle \tag{14}$$

$|\Psi(\zeta_1)\rangle$ was measured for values of: $\zeta_1 \in \{0, \frac{\pi}{32}, \frac{\pi}{16}, \frac{\pi}{8}, \frac{\pi}{4}\}$. The solution of this SDP clearly reproduce the already known results for a single measurement round, as is done in [14, 12], but using our SDP which is

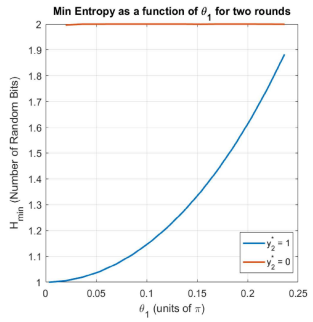
slightly different than the one derived in that paper and requires no assumption about the specific actions of the adversary, Eve. As expected, when $\zeta_1 = 0$, no randomness can be certified as the state becomes a product state, whereas for $\zeta_1 = \pi/4$, the maximal amount of randomness can be certified, since this state is maximally entangled between Alice and Bob.



(a) One round of measurements, for a range of initial states, ζ_1, as a function of initial measurement angle, θ_1



(b) H_{min} for two rounds of measurements, with a range of initial states, $\zeta_1 \in (0, \frac{\pi}{4}]$ and $\phi_1 = \theta_2 = \phi_2 = 0$.



(c) Difference in certified randomness when choosing between measurement settings $y_2^* = 1$ or $y_2^* = 0$ in the second measurement round.

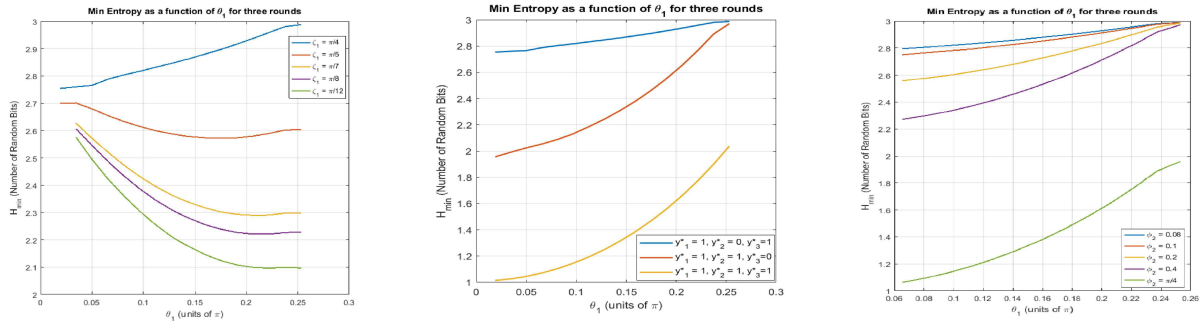
Figure 2: Min. Entropy, H_{min}, for one and two measurement rounds, as a function of initial measurement angle, θ_1.

Figures (2b) and (2c) show the results after two measurement rounds. In Figure (2b), the measurement in round one was taken to be in the noisy X basis, with a range of initial angles ζ_1, and the measurement in round two was taken to be in the usual computational basis, $\phi_2 = 0$. Figure (2c) illustrates the difference in choosing different measurement choices for the second round, i.e. between $y_2^* = 0$, or $y_2^* = 1$, with maximal randomness certified after sequential measurements in alternating bases, for example $y_1^* = 1, y_2^* = 0$.

Finally, Figure (3) shows numerical results for the protocol for three measurement rounds. The protocol proceeds in exactly the same manner as for one and two rounds. In particular, in the first round, Bob can choose between a non-projective measurement in the noisy X_{θ_1} basis, or if the particular run of the protocol is a test, he will measure in the projective Z^0 basis. In the second round, he will choose to measure in the noisy Z_{ϕ_2} basis, or the X_0 basis for a test run. In the final round, he will choose to measure in the projective ($\theta_3 = 0$) X_0 basis, or the projective ($\phi_3 = 0$) Z_0 basis for a test. Again, Figure (3b) reiterates the optimality of using an alternating sequence of non-projective measurements, with the most randomness produced with the setting $y_1^* = 1, y_2^* = 0, y_3^* = 1$ in this example. Figure (3c) shows the results for various second round measurement angles, and the amount of randomness that can be certified increases as the measurement angle, $\phi_2 \to 0$.

3.2 Networked Ion Trap Implementation

The framework in which we have designed this protocol, assuming a *malicious* adversary, Eve, is general enough to include the scenario in which she is not intentionally trying to interfere with our randomness generation, but instead we can imagine that Eve simply made some error in building the devices. This would correspond to introducing some noise, for example, in our state preparation and/or measurement apparatus. This noise assumption is clearly a sub-case of the malicious adversary scenario. This mentality allows us to use our protocol to evaluate the usefulness of some current available technologies



(a) H_{min} using various initial states, with initial angles, $\zeta_1 \in \{\frac{\pi}{4}, \frac{\pi}{5}, \frac{\pi}{7}, \frac{\pi}{8}, \frac{\pi}{12}\}$.

(b) H_{min} using various measurement settings, y_1^*, y_2^*, y_3^*.

(c) H_{min} using various angles in the second round, $\phi_2 \in \{0.08, 0.1, 0.2, 0.4, \frac{\pi}{4}\}$ rad.

Figure 3: H_{min} for three measurement rounds, as a function of initial measurement angle, θ_1.

for randomness generation purposes, in some simple cases. In particular, we will restrict to assuming we only have some noise in our state preparation, but all other parts of the device works perfectly. To do so, we test the state introduced in [11], which can be produced between two parties in a networked architecture of ion traps:

$$\rho_\varepsilon^{(0)} = (1-\varepsilon)\Phi^+ + \varepsilon/3\Phi^- + \varepsilon/3\Psi^+ + \varepsilon/3\Psi^- \tag{15}$$

where $\phi^+, \phi^-, \psi^+, \psi^-$ are the standard 2-qubit Bell states. The state, (15), is a mixed state assuming uniform depolarising noise. In [11], this state is assumed to be one produced by two ion traps entangled by a photonic link. The simple noise model is chosen to allow use of a technique to purify the state. In particular, after 3 rounds of this purification protocol, the resulting states are given by:

$$\rho_\varepsilon^{(1)} = \left(1 - 2/3\varepsilon - 2/3\varepsilon^2\right)\Phi^+ + \left(2/9\varepsilon + 2/9\varepsilon^2\right)\Phi^- + 2/9\varepsilon^2\Psi^+ + 2/9\varepsilon^2\Psi^- + O(\varepsilon^3) \tag{16}$$

$$\rho_\varepsilon^{(2)} = \left(1 - 8/9\varepsilon^2 - 8/27\varepsilon^3\right)\Phi^+ + 4/9\varepsilon^2\Phi^- + 4/9\varepsilon^2\Psi^+ + 8/27\varepsilon^3\Psi^- + O(\varepsilon^4) \tag{17}$$

$$\rho_\varepsilon^{(3)} = \left(1 - 2/9\varepsilon^2 - 16/27\varepsilon^3\right)\Phi^+ + 2/9\varepsilon^2\Phi^- + 8/27\varepsilon^3\Psi^+ + 8/27\varepsilon^3\Psi^- + O(\varepsilon^4) \tag{18}$$

where $\rho_\varepsilon^{(i)}$ is the state produced after i rounds of the purification protocol.

Currently, raw entanglement between two ion traps, connected with an entangling photon, has been achieved with a fidelity of about 85% $\implies \varepsilon \approx 0.15$, [7]. Starting with this level of raw infidelity, the purification protocol produces states of infidelity $\varepsilon \approx 0.1, 0.02, 0.005$ after one, two and three rounds respectively. The fidelity is given by (19), [10], and taken to be between the actual state $\rho^{(i)}$, and the pure Bell state, Φ^+:

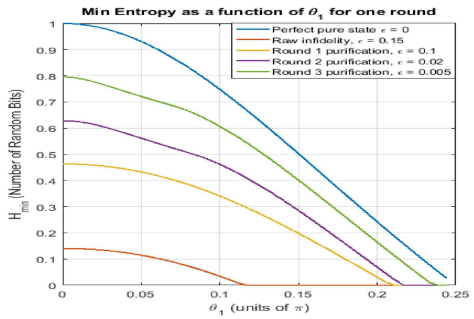
$$F(\rho_\varepsilon^{(i)}, \Phi^+) = \mathrm{Tr}\left(\sqrt{\sqrt{\rho_\varepsilon^{(i)}}\Phi^+\sqrt{\rho_\varepsilon^{(i)}}}\right) \tag{19}$$

Given the levels of entanglement present in the states above, we test the advantage of using a sequence of measurements vs. a single measurement on a noisy entangled state. Figure (4a) shows the result after a single X measurement on the states (choosing $y_1^* = 1$) (15, 16, 17, 18). Clearly, maximal

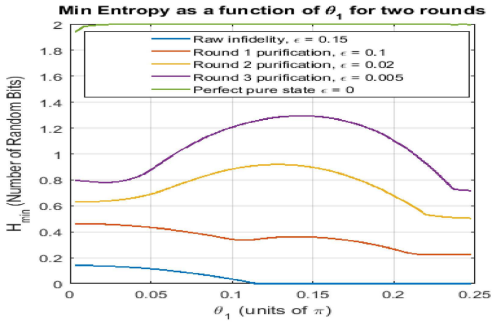
randomness can be certified in the case where the measurement is projective, as expected. It can also be seen that by using the raw entangled state, (15), very little randomness can be certified, with a maximum of approximately 0.15 bits.

Figure (4b) illustrates the results after two rounds of measurements, where the second round measurements are projective, $\theta_2 = \phi_2 = 0$. The case of $\theta_1 = 0$ gives the same result as the single measurement scenario, since in this case the first measurement is projective and hence no randomness can be certified in the second round.

Unfortunately, it can be seen that no extra randomness can be certified in two measurement rounds on the raw entangled state, (15). However, after two or more rounds of the purification protocol, indeed more randomness can be certified by using a sequence vs. a single measurement, as indicated by the peaks in Figure (4b). The infidelity for which the sequence becomes more useful than a single measurement can be seen to be approximately in the interval $\varepsilon \in (0.06, 0.07)$.



(a) Single measurement on the raw entangled state (15) ($\varepsilon = 0.15$), the states produced after three rounds of the purification protocol, (16, 17, 18), with $\varepsilon = 0.1, 0.02, 0.005$ respectively and a perfect pure state with $\varepsilon = 0$.



(b) Two rounds of measurement on the raw entangled state (15) ($\varepsilon = 0.15$), the states produced after three rounds of the purification protocol, (16, 17, 18), with $\varepsilon = 0.1, 0.02, 0.005$ respectively and a perfect pure state with $\varepsilon = 0$.

Figure 4: 1SDI protocol implemented for one and two measurement rounds on noisy states produced by a networked ion-trap architecture.

Finally, Figure (5a) shows the results after three rounds of measurements, where the third, and final round of measurements are projective with $\theta_3 = \phi_3 = 0$. The second round of measurements is chosen in this case to be a noisy Z measurement, with $\phi_2 = 0.08$ rad.

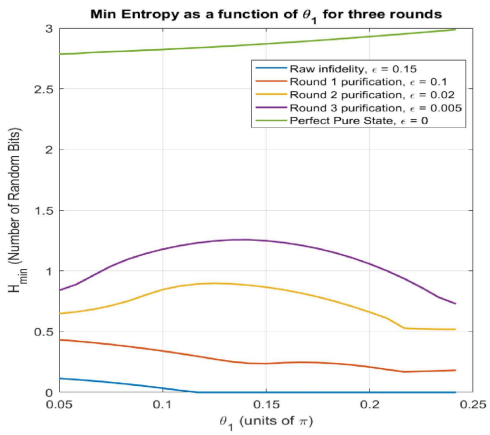
Unfortunately, it can be seen that no extra randomness can be certified by implementing three measurements, than with two rounds. This is even the case for the purified states, (16, 17, 18), so even these levels of purity are not sufficient to extract more randomness from a single state with three rounds of measurements. The perfect pure state, with $\varepsilon = 0$ is also plotted for comparison.

Clearly, there must be some level at which the state becomes pure enough to be useful so Figure (5b) shows the results of the protocol for very small infidelities, specifically:

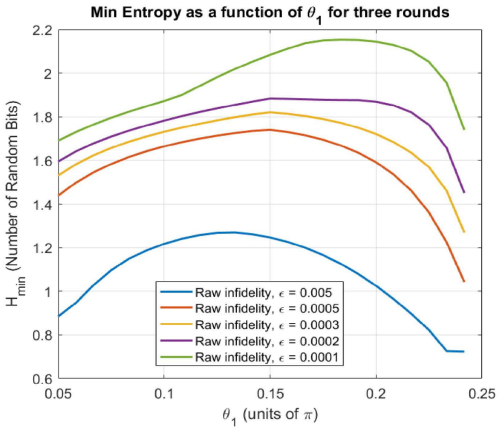
$$\varepsilon = \{5 \times 10^{-3}, 5 \times 10^{-4}, 3 \times 10^{-4}, 2 \times 10^{-4}, 1 \times 10^{-4}\}$$

It can be seen that for an infidelity approximately in the interval, $\varepsilon \in (1 \times 10^{-4}, 2 \times 10^{-4})$, the state is pure enough to be able to certify more randomness with three rounds of measurement, than with two. This corresponds to being able to create pure entangled states experimentally with fidelities of greater than 99.98%. This level could be reached by repeating the purification protocol more times but clearly

this decreases the efficiency of the protocol as many more extra qubits would need to be introduced to implement this purification. It is expected that for 4 and higher rounds of measurement, states which have an even higher level of purity would be required to make the protocol worthwhile, i.e. so that rounds of measurements on a single state would give better results than single measurements on new states each time.



(a) Three rounds of measurement on the raw entangled state, (15), ($\varepsilon = 0.15$), the states produced after three rounds of the purification protocol, (16, 17, 18), with $\varepsilon = 0.1, 0.02, 0.005$ respectively and a perfect pure state with $\varepsilon = 0$.



(b) Three rounds of measurement on raw entangled states with infidelities $\varepsilon = \{5\times10^{-3}, 5\times10^{-4}, 3\times10^{-4}, 2\times10^{-4}, 1\times10^{-4}\}$.

Figure 5: Three rounds of measurements on states with various levels of entanglement fidelity.

References

[1] J. S. Bell (1964): *On the Einstein Podolsky Rosen paradox*. *Physics Physique Fizika* 1(3), pp. 195–200, doi:10.1103/PhysicsPhysiqueFizika.1.195. Available at https://link.aps.org/doi/10.1103/PhysicsPhysiqueFizika.1.195.

[2] Stephen Boyd & Lieven Vandenberghe (2004): *Convex Optimization by Stephen Boyd*, doi:10.1017/CBO9780511804441. Available at /core/books/convex-optimization/17D2FAA54F641A2F62C7CCD01DFA97C4.

[3] BrianCoyle (2017): *TPMScProject2017: MSc Project Codes For 1SDI Certification of Random Numbers*. doi:10.5281/zenodo.1257182. Available at https://github.com/BrianCoyle/TPMScProject2017.

[4] Roger Colbeck (2009): *Quantum And Relativistic Protocols For Secure Multi-Party Computation*. *arXiv:0911.3814 [quant-ph]*. Available at http://arxiv.org/abs/0911.3814. ArXiv: 0911.3814.

[5] F. J. Curchod, M. Johansson, R. Augusiak, M. J. Hoban, P. Wittek & A. Acn (2017): *Unbounded randomness certification using sequences of measurements*. *Phys. Rev. A* 95(2), p. 020102, doi:10.1103/PhysRevA.95.020102. Available at https://link.aps.org/doi/10.1103/PhysRevA.95.020102.

[6] A. Einstein, B. Podolsky & N. Rosen (1935): *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?* *Phys. Rev.* 47(10), pp. 777–780, doi:10.1103/PhysRev.47.777. Available at https://link.aps.org/doi/10.1103/PhysRev.47.777.

[7] D. Hucul, I. V. Inlek, G. Vittorini, C. Crocker, S. Debnath, S. M. Clark & C. Monroe (2014): *Modular entanglement of atomic qubits using photons and phonons*. Nature Physics 11, p. 37. Available at http://dx.doi.org/10.1038/nphys3150.

[8] Nathaniel Johnston, Alessandro Cosentino & Vincent Russo (2016): *QETLAB: A MATLAB toolbox for quantum entanglement, version 0.9*, doi:10.5281/zenodo.44637. Available at http://qetlab.com.

[9] Y. Z. Law, L. P. Thinh, J.-D. Bancal & V. Scarani (2014): *Quantum randomness extraction for various levels of characterization of the devices*. J. Phys. A: Math. Theor. 47(42), p. 424028, doi:10.1088/1751-8113/47/42/424028. Available at http://stacks.iop.org/1751-8121/47/i=42/a=424028.

[10] Michael A. Nielsen & Isaac L. Chuang (2011): *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th edition. Cambridge University Press, New York, NY, USA.

[11] Ramil Nigmatullin, Christopher J. Ballance, Niel de Beaudrap & Simon C. Benjamin (2016): *Minimally complex ion traps as modules for quantum communication and computing*. New J. Phys. 18(10), p. 103028, doi:10.1088/1367-2630/18/10/103028. Available at http://stacks.iop.org/1367-2630/18/i=10/a=103028.

[12] Elsa Passaro, Daniel Cavalcanti, Paul Skrzypczyk & Antonio Acn (2015): *Optimal randomness certification in the quantum steering and prepare-and-measure scenarios*. New J. Phys. 17(11), p. 113010, doi:10.1088/1367-2630/17/11/113010. Available at http://stacks.iop.org/1367-2630/17/i=11/a=113010.

[13] S. Pironio, A. Acn, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning & C. Monroe (2010): *Random numbers certified by Bells theorem*. Nature 464(7291), p. 1021, doi:10.1038/nature09008. Available at https://www.nature.com/articles/nature09008.

[14] Paul Skrzypczyk (2016): *steeringreview: Code to accompany "Quantum steering: a short review with focus on semi-definite programming"*. Available at https://github.com/paulskrzypczyk/steeringreview.

[15] Paul Skrzypczyk, Miguel Navascus & Daniel Cavalcanti (2014): *Quantifying Einstein-Podolsky-Rosen Steering*. Phys. Rev. Lett. 112(18), p. 180404, doi:10.1103/PhysRevLett.112.180404. Available at https://link.aps.org/doi/10.1103/PhysRevLett.112.180404.