cryptography

MDPI

Article

Certified Randomness From Steering Using Sequential Measurements †

Brian Coyle [1,*], Elham Kashefi [1,2] and Matty J. Hoban [3]

1 School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, UK
2 Laboratoire d'Informatique de Paris 6, CNRS, Sorbonne Université, 4 Place Jussieu, 75005 Paris, France; ekashefi@gmail.com
3 Department of Computing, Goldsmiths, University of London, New Cross, London SE14 6NW, UK; matty.hoban@googlemail.com
* Correspondence: brian.coyle@ed.ac.uk
† This paper is an extended version of our paper published in the Proceedings of the 9th International Workshop on Physics and Computation.

Received: 1 October 2019; Accepted: 28 November 2019; Published: 6 December 2019

Abstract: The generation of certifiable randomness is one of the most promising applications of quantum technologies. Furthermore, the intrinsic non-locality of quantum correlations allow us to certify randomness in a device-independent way, i.e., we do not need to make assumptions about the devices used. Due to the work of Curchod et al. a single entangled two-qubit pure state can be used to produce arbitrary amounts of certified randomness. However, the obtaining of this randomness is experimentally challenging as it requires a large number of measurements, both projective and general. Motivated by these difficulties in the device-independent setting, we instead consider the scenario of one-sided device independence where certain devices are trusted, and others are not; a scenario motivated by asymmetric experimental set-ups such as ion-photon networks. We show how certain aspects of previous works can be adapted to this scenario and provide theoretical bounds on the amount of randomness that can be certified. Furthermore, we give a protocol for unbounded randomness certification in this scenario, and provide numerical results demonstrating the protocol in the ideal case. Finally, we numerically test the possibility of implementing this scheme on near-term quantum technologies, by considering the performance of the protocol on several physical platforms.

Keywords: one-sided device independence; randomness generation; randomness certification; quantum cryptography; semi-definite programming; self testing

1. Introduction

Quantum physics has the potential to make a great impact upon information technology, especially through the development of universal quantum computers. However, near-term quantum devices will not be capable of fault-tolerant, universal quantum computation. Luckily these devices will still be of use for information processing tasks, in particular as genuine random number generators. Certifiable (private) random numbers can then be used for cryptography, the simulation of physical systems, or other randomised algorithms. By certifiable we mean that there is a certificate guaranteeing that the randomness is private and unpredictable from any external agent (who is not directly using the device). This certificate may be predicated on certain assumptions, which could be computational or physical in nature, depending on the degree of security desired.

It is now well established that quantum systems are capable of producing data that is unpredictable, and thus random to any external agent, even when one has perfect knowledge of the quantum system. Unfortunately, in practice it can be difficult to have perfect knowledge of quantum

systems, especially if they are somewhat noisy, as near-term quantum devices will be. These (often classical) sources of noise can appear as unpredictable as the randomness resulting from the quantum systems, so one must have an excellent characterisation of the sources of noise to extract the true quantum randomness. Indeed, if the noise is just classical data then it could have been generated by some external process and thus an external agent could, in principle, keep a copy of this data and use it to predict the output data of a quantum device.

There does exist a convenient approach to certifiable quantum random number generation, which is *device-independent randomness certification*. In this scenario one does not need a complete characterisation of a device; genuine randomness is certified by the violation of a Bell inequality [1] between two, or more, devices. That is, certification is achieved via the statistics produced in a Bell test, without any specific assumptions made on the devices producing the statistics.The kind of assumption made in this approach is to assume that devices are quantum mechanical or that there multiple, non-communicating devices that might share some resource. Furthermore, there are no computational assumptions made about the device producing the randomness. The downside of this approach is that a genuine violation of a Bell inequality is experimentally daunting, with the first loophole-free demonstrations emerging very recently [2].

Given the experimental challenges of device-independent random number generation, [3,4] a promising and practical route to certifiable randomness generation is within the scope of one-sided device-independent quantum information [5]. In this setting, certain devices are assumed to be perfectly characterised (through trusted and characterised measurement devices) while others are not. Randomness can be certified based on the violation of a steering inequality [6], which is the analogue of a Bell inequality for this new setting.

Within the framework of device-independent randomness certification it was shown that a single entangled pair of qubits (in a pure state) can be a source of “unbounded" random numbers, one qubit for each wing of the Bell experiment [7]. That is, one can fix a value N of random bits that one would like to obtain, and then construct a scheme with sequences of measurements on the two-qubit state that will produce N bits of randomness. Thus by using a sequence of measurements, one can exceed the randomness possible from a single general measurement, which for a qubit is 2 bits [8]. One issue is that this randomness certification scheme involves a large number of measurements (exponential in the size of the output random string) for one of the parties and limits its utility for various protocols.

In this work, we study the adaptation of the above sequential measurement scenario to the one-sided device independent scenario. In doing so, we develop a more robust scheme no longer requiring exponentially many measurements for one of the parties. We present an analytical bound on the min entropy of our randomness generation scheme. We then go on to give numerical results to derive more optimal rates of randomness generation. Furthermore, we discuss how the scheme could be implemented in current architectures for networked quantum information processing. This is an extended version of the following conference paper [9].

Related Work

In Table 1 we compare our work with that of [7], showing how, by trusting one party’s measurements, we exponentially reduce the number of measurements required. In work by Skrzypczyk and Cavalcanti, it was shown how, by increasing the local Hilbert space dimension of the quantum state held by Alice and Bob, more randomness can be certified in the one-sided device-independent scenario [10]. In particular, for a local dimension d, then $\Omega(\log d)$ bits can be certified. This work is built on a series of works in one-sided device-independent randomness certification, with [11] establishing tools based on semi-definite programming.

Our cryptographic scenario is intermediate between the device-independent and the device-dependent scenarios. Another such example of an intermediate scenario is that of semi-device-independent quantum information [12,13], where one bounds the dimension (or energy) of the Hilbert space of the systems involved. Randomness certification has been shown in this scenario,

with experimental implementations of various protocols [14,15]. This scenario is not comparable with that of one-sided device-independence due to the different assumptions, but it demonstrates that such intermediate scenarios are of broad interest.

Table 1. Comparison between the device-independent and one-sided device-independent sequential randomness generation between our work and the work in [7]. The positive integer n is the number of measurements made in a sequence of measurements. Here we see that there is an exponential improvement in the number of measurements required.

	Our Work	[7]
Alice	Trusted	Untrusted
Bob	Untrusted	Untrusted
Randomness certified	$\Omega(n)$	$\Omega(n)$
Number of measurements required	$O(n)$	$O(2^n)$
Method	Steering inequality violation	Bell inequality violation
Relevant Quantity	Steerable assemblage $\{\sigma_{\vec{b}\|\vec{y}}\}$	Non-local probability distribution $\{P(\vec{ab}\|x\vec{y})\}$

2. One-Sided Device Independence and Randomness Certification

Before introducing the scenario it is worthwhile briefly motivating it first from an experimental point-of-view. One particular kind of experimental set-up we have in mind is an atom-photon hybrid experiment, where one system is an atom in a cavity, and the other system is a photon, which is emitted from the atom. Instead of an atom in a cavity, an ion in a trap is another possibility. Photons are convenient for long-range communication, and ion trap technology is associated with high fidelity operations and excellent system control. As a result the detection efficiency in an ion trap is very close to perfect, but in spite of recent advances, photo-detectors are not. In a device-independent scheme, a lower detection efficiency can compromise the security of a protocol, so to circumvent these issues we can resort to the one-sided device-independent setting (1sDI). In this setting, the photonic system is taken to be trusted and well characterised thus ruling out detector-based attacks, and the atomic system is treated as a black box.

An extra motivation for this 1sDI scenario will be when one wants to consider sequences of measurements on the same system, as we will do. We need our technology to allow for the possibility of returning a quantum system after a measurement (thus being a non-trivial quantum instrument). This is experimentally challenging for photonic systems, but feasible within ion trap technology. Ideally we would thus like our trusted system to make very simple operations, such as a single measurement that does not return a quantum state as an output. In this way, we can see one-sided device independence as exploiting the best features of a hybrid quantum information experiment. This will be pertinent when we come to discuss implementations of our randomness certification scheme.

The idea of producing certifiable randomness using steering was first studied by Law et al. [16], and then by Passaro et al. [11], who utilised the techniques of semi-definite programming. The broad scenario considered in 1sDI information processing for randomness generation is the following. There are two parties, Alice (A), and Bob (B), who can share some resource. We allow for the possibility of a third party, Eve (E), having prepared the shared quantum resource. Alice's share of the resource is assumed to be a quantum system with a known Hilbert space, upon which Alice can perform arbitrary (characterised) quantum operations. In particular, Alice can perform tomographically complete measurements. Bob's share of the resource is contained within a black box and he can only input classical data into the box and retrieve more classical data; he does not have any knowledge of the inner workings of the black box, only that it has a quantum description. Bob can only collect statistics of the input and output data.

Given this scenario, the way in which we certify the randomness generated is through a (slightly modified) non-local guessing game [11,17]. We give a schematic of this guessing game in Figure 1. In this game, in each round, Eve prepares a quantum state $|\psi\rangle_{ABE}$, which we can assume to be pure

through the Stinespring dilation (we could dilate the Hilbert spaces of Bob and Eve, for example). Then one subsystem is each distributed to Alice and Bob so that they share the joint state $\rho_{AB} = \mathrm{tr}_E|\psi\rangle\langle\psi|_{ABE}$. Since Alice has access to her respective subsystem she is able to characterise $\rho_A = \mathrm{B}\rho_{AB}$, but Bob does not have direct access to his subsystem. Inside Bob's device if he inputs the classical variable y, which is his choice of measurement, and gets the output b then a measurement is made on Bob's subsystem, which is described by the positive operator $M^B_{b|y}$ such that $\sum_b M^B_{b|y} = \mathbb{I}_B$ for all y. Eve will then in each round perform a measurement that will generate an outcome z, which will be her guess of Bob's outcome b; this measurement will be described by a positive operator N^E_z such that $\sum_z N^E_z = \mathbb{I}_E$.

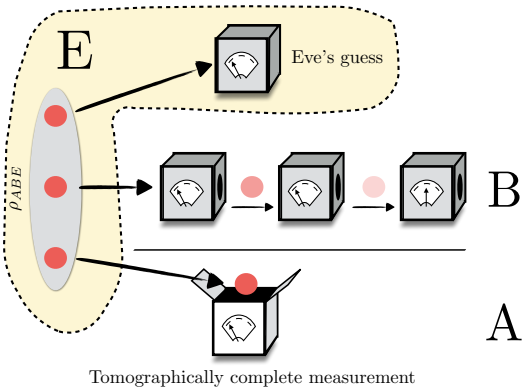


Figure 1. Illustration of the tripartite scenario between Alice, Bob, and Eve, in which Bob also makes a sequence of measurements and Alice can make trusted measurements. Eve tries to guess the outcomes of Bob's measurements.

In this setting, Eve's goal is to optimise over the state $|\psi\rangle_{ABE}$ and measurements N^E_z that will give her the best chance to guess the outcome of Bob's measurement. Importantly, Eve's strategy has to be compatible with the observed statistics of what Alice and Bob observe. Note that in this game, the most compact way of describing what Alice and Bob observe (assuming Alice performs tomography on her system) is described by the *assemblage* $\{\sigma_{b|y}\}_{b,y}$, which is a set where each element can be described as

$$\sigma_{b|y} = \mathrm{tr}_B\left(\mathbb{I}_A \otimes M^B_{b|y}\rho_{AB}\right), \tag{1}$$

which can be viewed as a sub-normalised density matrix describing the state of Alice's system after the measurement $M^B_{b|y}$ is made such that $\sum_b \sigma_{b|y} = \rho_A$ for all y. This assemblage is merely Alice's and Bob's observed assemblage, but really every element is obtained in the following way:

$$\sigma_{b|y} = \mathrm{tr}_{BE}\left(\sum_z \mathbb{I}_A \otimes M^B_{b|y} \otimes N^E_z|\psi\rangle\langle\psi|_{ABE}\right) \tag{2}$$

$$= \sum_z \sigma_{z,b|y} \tag{3}$$

where we have course-grained over all of Eve's measurement outcomes, or guesses, and introduced the identity

$$\sigma_{z,b|y} = \mathrm{tr}_{BE}\left(\mathbb{I}_A \otimes M^B_{b|y} \otimes N^E_z|\psi\rangle\langle\psi|_{ABE}\right), \tag{4}$$

which can be seen as the sub-normalised state of Alice's system conditioned on Bob's and Eve's particular measurement outcomes.

Returning to the game, we quantify Eve's ability to guess Bob's outcome with the guessing probability. We first assume that that Bob will aim to generate randomness from only one particular

input, denoted by y^*, and Eve knows y^*. The guessing probability for Eve's output z to correctly guess Bob's output b for choice y^* is then

$$p_{\text{guess}}(y^*) = \sum_z \delta_{b,z} \text{tr}_A \sigma_{z,b|y^*}. \tag{5}$$

This can be seen as the sum over z of the probabilities $p(z, b|y^*)$ when $b = z$ [11].

We will now expand upon this set-up to allow for Bob's measurement to be a sequence of measurements. That is, we describe Bob's input y and output b to be tuples of length n, so that $y := (y_1, y_2, y_3, ..., y_n)$ and $b := (b_1, b_2, b_3, ..., b_n)$. That is, Bob makes a sequence of measurements where each ith measurement in the sequence corresponds to the measurement choice y_i with output b_i. We assume that the output b_i is obtained before the choice y_{i+1} is made, and thus we impose a constraint of causality: Measurement outcomes in the past are independent of future measurement choices. A consequence of this, for example, is that $p(b_1|y_1, y_2) = p(b_1|y_1)$, i.e., the probability of observing b_1 given y_1 is independent of the future choice of y_2. Since $\text{tr}_A \sigma_{b|y} = p(b|y)$ for $y := (y_1, y_2, y_3, ..., y_n)$ and $b := (b_1, b_2, b_3, ..., b_n)$, this then has consequences for the assemblage. For example, for $n = 2$,

$$\sum_{b_2} \sigma_{b_1,b_2|y_1,y_2} = \sigma_{b_1|y_1,y_2} = \sigma_{b_1|y_1}, \tag{6}$$

and likewise for larger n. At this point it is worthwhile pointing out that any assemblage that satisfies these causality constraints in addition to non-signalling constraints, i.e., $\sum_b \sigma_{b|y} = \rho_A$ for all y, can be realised by Alice and Bob sharing a quantum state and Bob making an appropriate sequence of measurements, as proven in [18].

These are all of the constraints in the scenario that we are considering when allowing for sequences of measurements on a state. The goal is given all of these constraints, to give bounds on the guessing probability $p_{\text{guess}}(y^*)$ given an observed assemblage $\{\sigma_{b|y}\}_{b,y}$. One method for doing this is through semi-definite programming [11], and we will return to this technique when it comes to presenting numerical results. We will also give analytical results based on self-testing in the steering scenario [19]. One unifying aspect to our results is that instead of certifying randomness given the observed assemblages, we can certify randomness based on the violation of steering inequalities, which are analogous to Bell inequalities. More generally, a steering inequality violation results directly from some observed statistics for Alice. Therefore we can certify randomness based on statistical tests given particular (known) measurements made by Alice. Within this work, it will be made clear how $p_{\text{guess}}(y^*)$ is being calculated.

Given the guessing probability $p_{\text{guess}}(y^*)$, we can compute a related quantity, which is the certifiable min entropy of Bob's outcomes:

$$H_{min}(b|y^*, z) := -\log_2 p_{\text{guess}}(y^*) \tag{7}$$

As we can see this is directly related to the guessing probability. That is, if the set of possible outcomes b has cardinality 2^m and $p_{\text{guess}}(y^*) = 2^{-m}$ then the min entropy associated with Bob's outcomes is m bits. In this way, Bob's device is a source of m bits of certifiable randomness.

3. A Scheme for Unbounded Randomness Generation

In this section we will describe an honest strategy, in which a sequence of measurements made upon half of a two-qubit entangled state can result in a large amount of observed randomness. In the subsequent sections we will give methods to certify that this is genuine randomness, but for now we will not concern ourselves with certification.

The scheme is similar to that of [7]. We will call this scheme the two-qubit sequential measurement (TQSM) scheme. We have that Bob can implement non-projective measurements in "rotated versions" of the Pauli-X and Z bases, and Alice has the functionality implement a tomographically complete set

of measurements, for example to measure the Pauli observables, X, Y, Z since this is sufficient for her to do quantum state tomography to certify Bob's random outcomes.

First, for simplicity, we will consider Bob just making one sequence, i.e., a sequence of n measurements for $n = 1$ so that $y := y_1$ and $b := b_1$. We have that Bob can make a choice between two dichomotic measurements, so that $y, b \in \{0, 1\}$. When Bob makes choice $y = 0$ ($y = 1$), he will make a (possibly non-projective) rotated version of a measurement in the Pauli-Z (Pauli-X) basis.

We will now describe these "rotated" measurements in terms of their associated Kraus operators. These operators are of the form $\Pi^{\omega}_{b|y}$ where ω is an angle and b, y are the bits as defined above. Consider the following operators:

$$\begin{aligned}
\Pi^{\phi}_{0|0} &= \cos(\phi)|0\rangle\langle 0| + \sin(\phi)|1\rangle\langle 1| \\
\Pi^{\phi}_{1|0} &= \cos(\phi)|1\rangle\langle 1| + \sin(\phi)|0\rangle\langle 0| \\
\Pi^{\theta}_{0|1} &= \cos(\theta)|+\rangle\langle +| + \sin(\theta)|-\rangle\langle -| \\
\Pi^{\theta}_{1|1} &= \cos(\theta)|-\rangle\langle -| + \sin(\theta)|+\rangle\langle +|.
\end{aligned} \tag{8}$$

The positive operator valued measure (POVM) constructed from these Kraus operators that Bob implements on his half of the shared state will be of the form

$$M^{\omega}_{b|y} = \left(\Pi^{\omega}_{b|y}\right)^{\dagger}\left(\Pi^{\omega}_{b|y}\right).$$

These Kraus operators reduce to the usual projective Pauli-X and Pauli-Z basis projectors for $\theta = \phi = 0$. Therefore, if Alice and Bob share the pure quantum state $|\psi\rangle_{AB}$ and Bob makes a measurement in, say, the rotated Pauli-X basis, and gets the outcome $b = 1$, the post-measurement state will be

$$\rho_{AB} = \frac{\mathbb{I}_A \otimes \Pi^{\phi}_{1|1}|\psi\rangle\langle\psi|\mathbb{I}_A \otimes \Pi^{\phi}_{1|1}}{|\mathbb{I}_A \otimes \Pi^{\phi}_{1|1}|\psi\rangle|^2}$$

Very similar expressions are then obtained for the other Kraus operators. It should be noted that for all pure states $|\psi\rangle_{AB} = \alpha|00\rangle + \beta|11\rangle$ the post-measurement state ρ_{AB} will also be pure [7]. The post-measurement pure state shared by Alice and Bob after outcome b for input y will be

$$|\psi_{b|y}\rangle = U^{b|y}_A \otimes U^{b|y}_B \left(\cos(\zeta_{b|y})|00\rangle + \sin(\zeta_{b|y})|11\rangle\right). \tag{9}$$

where unitaries $U^{b|y}_A$ and $U^{b|y}_B$, and angle $\zeta_{b|y}$ depend on the initial quantum state and the angle of the rotated measurement. We point out that such an angle and unitaries exist (and can be calculated).

What is the probability of getting the outcome b given y? This will be $p(b|y) = |\mathbb{I}_A \otimes \Pi^{\phi}_{b|y}|\psi\rangle|^2$. We will only care about the case where $y = 1$, since for this case if $|\psi\rangle = \alpha|00\rangle + \beta|11\rangle$ we have that

$$p(b|y) = |\mathbb{I}_A \otimes \Pi^{\phi}_{b|y=1}|\psi\rangle|^2 = \frac{1}{2}.$$

Therefore, assuming that Alice and Bob share that state and Bob makes that measurement (in the honest setting) then Bob's outcome for $y = 1$ will be perfectly random. This will then be the basis of the certified randomness in this scheme.

The above is what happens for a sequence consisting of one measurement. For sequences of measurements of length n for $n \geq 2$, the post-measurement state $|\psi_b\rangle$ as described in (9) will be relevant. Note that up to the unitaries $U^{b|y}_A$ and $U^{b|y}_B$, the state $|\psi_{b|y}\rangle$ is of the form $\alpha|00\rangle + \beta|11\rangle$.

Therefore, if after his first measurement, Bob applies the unitary $(U_B^{b|y})^\dagger$ to his share of the state, the joint state will be

$$|\psi_{b|y}\rangle = U_A^{b|y} \otimes \mathbb{I} \left(\cos(\zeta_{b|y})|00\rangle + \sin(\zeta_{b|y})|11\rangle \right).$$

Now after applying this unitary, Bob can make another measurement that is a rotated Pauli measurement. Now Bob's input y will be a tuple of length 2, i.e., $y = (y_1, y_2)$. For the second round, Bob's choices of measurements are again between two rotated Pauli basis measurements, where $y_2 = 0$ is for the Z basis and $y_2 = 1$ is for the X basis.

If $y_1 = y_2 = 1$, then Bob performs the rotated X measurement, followed by a correcting unitary, then another rotated X measurement and another corrective unitary. The post-measurement state after this second measurement (and unitary) will be

$$|\psi_{b_1,b_2|1,1}\rangle = U_A^{b_1,b_2|y_1=1,y_2=1} \otimes \mathbb{I}_B \left(\cos(\zeta_{b_1,b_2|1,1})|00\rangle + \sin(\zeta_{b_1,b_2|1,1})|11\rangle \right),$$

again for appropriately chosen unitaries and angles.

The probability of getting the outcomes $b := (b_1, b_2)$ for inputs $y = (1, 1)$ is straightforwardly calculated to be $p(b_1, b_2|1, 1) = \frac{1}{4}$. Thus for a sequence of two measurements with each being the rotated X basis measurement, we have two perfectly random outcomes (b_1, b_2). In general, for this sequence of rotated measurement, correcting unitary, rotated measurement, and so on, if there n measurements, then the probability $p(b_1, b_2, ..., b_n|y = (1, 1, ..., 1)) = 2^{-n}$.

This TQSM scheme thus gives us randomness assuming a particular state and sequence of measurements made by Bob. In subsequent sections the goal will be to remove the assumptions of the state and measurements but certify (almost) the same amount of randomness in the 1sDI scenario. It turns out that the randomness in the TQSM scheme can be certified. That is, to reproduce the observed assemblage (or statistics) between Alice and Bob, Eve would have to prepare devices that implement something equivalent to, or extremely close to, the TQSM scheme. Since this scheme produces a great deal of randomness, so will the certified version.

Before moving on, it is worthwhile to point out how this scheme differs from that presented in [7]. The important distinction is that in the scheme of [7], in addition to Bob making a sequence of measurements, Alice had to choose from a number of measurements that increased with the length of the sequence. This is because the certification was done in the device-independent setting, and not the 1sDI setting. The number of measurements Alice makes will never depend on the number of measurements in the sequence; it will only depend on the dimension of Alice's Hilbert space since she only needs to do at most a tomographically complete measurement.

4. Certifiable Unbounded Randomness Generation

In this section we will give an analytical method for certifying the randomness in a sequential scenario that is suited to the TQSM scheme. In particular, we will show that the TQSM scheme can produce an unbounded amount of certifiable randomness: for an arbitrary integer N, there is a sequence of measurements that produces $\Omega(N)$ bits of certifiable randomness.

In order to certify randomness in the 1sDI setting, we cannot assume the initial state shared by Alice, Bob, and Eve nor the measurement sequence made by Bob; we can only assume the Hilbert space of Alice's system, which from now on will be assumed to be two, i.e., Alice holds a qubit system. As mentioned earlier, it can assume that the state $|\psi\rangle_{ABE}$ shared by Alice, Bob, and Eve is pure. We can additionally assume for cryptographic purposes that the measurements in Bob's sequence are all projective. For example, the non-projective measurements in the TQSM scheme can be simulated by projective measurements on a potentially larger Hilbert space (we outline such an approach in Appendix A).

We introduce notation to refer to Bob's measurements. In particular we will introduce observables for each of Bob's measurements in the sequence. For the first measurement in the sequence, the choice

of measurement corresponding to $y_1 = 0$ and $y_1 = 1$ will have the observable $Z_B = M^B_{0|y_1=0} - M^B_{1|y_1=0}$ and $X_B = M^B_{0|y_1=1} - M^B_{1|y_1=1}$ respectively, where $M^B_{b_1|y_1}$ being Bob's POVM corresponding to the outcome b_1 for input y_1. For subsequent measurements we will introduce a piece of notation that $b^i := (b_1, b_2, ..., b_i)$ and $y^i := (y_1, y_2, ..., y_i)$ will be the tuple of all values of b_i and y_i from 1 to i consecutively (and inclusive). The observable corresponding to the $(i+1)$th measurement in the sequence after obtaining the outcomes b^i for choices y^i will be denoted as $Z_B^{b^j|y^i} = M^B_{0|b^i,y^i,y_{i+1}=0} - M^B_{1|b^i,y^i,y_{i+1}=0}$ and $X_B^{b^j|y^i} = M^B_{0|b^i,y^i,y_{i+1}=1} - M^B_{1|b^i,y^i,y_{i+1}=1}$.

The method for certifying this randomness is for Alice to choose between three of the Pauli measurements. Note that Alice does not have to randomly choose between measurements. In each round of the guessing game, Alice can choose a different Pauli basis, but this can be chosen deterministically. Based on the statistics gathered from these three Pauli measurements and Bob's sequence of measurements. Note that every single-qubit observable can be written as a linear combination of Pauli matrices so it is sufficient to make Pauli measurements and calculate the statistics for an arbitrary observable a posteriori. As part of the certification we have statistical criteria that the statistics obtained by Alice and Bob need to satisfy. If the statistics satisfy the criteria then this is the certificate that the outcomes of Bob's sequence of measurements is random. To wit, Eve will not be able to perfectly predict the outcomes of Bob's measurements. The statistical criteria will be based on the TQSM scheme.

From the TQSM scheme we have that after the ith measurement and correctly unitary, the state of Alice and Bob's two-qubit state will be

$$|\psi_{b^i|y^i}\rangle = U_A^{b^i|y^i} \otimes \mathbb{I}_B \left(\cos(\zeta_{b^i|y^i})|00\rangle + \sin(\zeta_{b^i|y^i})|11\rangle\right). \tag{10}$$

We will use the unitaries and angles in this post-measurement state to outline the statistical criteria. For each measurement in a sequence, there will be statistical criteria that should be satisfied. For simplicity we will start with the first measurement in the sequence.

The statistical criteria we will use can be derived from considering Alice and Bob both making Pauli-X and Pauli-Z measurements on a two-qubit pure entangled state of the form $\alpha|00\rangle + \beta|11\rangle$. The criteria essentially compares the observed statistics with those that would be obtained from perfect Pauli measurements on such an entangled state. These criteria will be then be used for self-testing the devices by showing that their behaviour will not deviate from Pauli measurements on an entangled state. For future work, it would be of interest to use a steering inequality instead of these three seperate criteria. Recall that the TQSM scheme is very similar to pure Pauli measurements on a two-qubit pure entangled state, except for some rotation in the typically non-projective measurements. Hence we wish to leverage this fact to produce certifiable randomness. The statistical criteria is

$$\begin{aligned} |\langle \tau_Z^A \otimes Z_B\rangle - 1| &\leq \epsilon_1 \\ |\langle \tau_X^A \otimes X_B\rangle - \sin(2\zeta)| &\leq \epsilon_2 \\ |\langle \tau_Z^A\rangle - \cos(2\zeta)| &\leq \epsilon_1, \end{aligned} \tag{11}$$

where τ_Z and τ_X are the Pauli-Z and Pauli-X observables respectively and ϵ_1, ϵ_2 are real, positive numbers. The angle ζ just comes from the target pure state between Alice and Bob $|\psi\rangle = \cos(\zeta)|00\rangle + \sin(\zeta)|11\rangle$. For subsequent measurements in the sequence, after the ith measurement, we have the following criteria for the $(i+1)$th measurement in the sequence:

$$
\begin{aligned}
|\langle U_A^{b^i|y^i}\tau_Z^A\left(U_A^{b^i|y^i}\right)^\dagger\otimes Z_B^{b^i|y^i}\rangle-1| &\leq \epsilon_1^{i+1}\\
|\langle U_A^{b^i|y^i}\tau_X^A\left(U_A^{b^i|y^i}\right)^\dagger\otimes X_B^{b^i|y^i}\rangle-\sin(2\zeta_{b^i|y^i})| &\leq \epsilon_2^{i+1}\\
|\langle U_A^{b^i|y^i}\tau_Z^A\left(U_A^{b^i|y^i}\right)^\dagger\rangle-\cos(2\zeta_{b^i|y^i})| &\leq \epsilon_1^{i+1},
\end{aligned}
\tag{12}
$$

where the unitary $U_A^{b^i|y^i}$ and $\zeta_{b^i|y^i}$ are the same as in (11). Just as with (11), ϵ_1^{1+1} and ϵ_2^{1+1} are real, positive numbers. We will call the conjunction of the critera in (11) and all criteria (12) for all i the sequential steering criteria (SSC).

It should be emphasised again that in the SCC, Alice does not need to make a measurement corresponding to the observable $U_A^{b^i|y^i}\tau_Z^A\left(U_A^{b^i|y^i}\right)^\dagger$, say, since for a known unitary $U_A^{b^i|y^i}$, this observable can be written as a real linear combination of Pauli matrices. Thus Alice only needs to measure the Pauli observables to recover the relevant expectation values.

If we take the TQSM scheme and start introducing parameters for the rotated measurements, then we can adjust the SSC parameters to suit the TQSM scheme. For each measurement in the sequence for the measurement in the rotated Pauli Z basis, we will fix the angle ϕ to be equal to zero so that the POVM is for the outcome 0 (1) is $|0\rangle\langle 0|$ ($|1\rangle\langle 1|$). For the rotated Pauli X measurement we fix the angle to be θ_i for the ith measurement in the sequence, which we can fix later but it will be in the range $\theta_i \in]0, \frac{\pi}{4}[$. Therefore the POVM for $y_i = 1$, we have $M^{\theta_i}_{0|y_i=1} = \cos(\theta_i)|+\rangle\langle +| + \sin(\theta_i)|-\rangle\langle -|$ and $M^{\theta_i}_{1|y_i=1} = \cos(\theta_i)|-\rangle\langle -| + \sin(\theta_i)|+\rangle\langle +|$.

One point to make at this stage is for the choice parameters to give the criteria in (13), after Bob makes the measurement choice $y_1 = 0$ in any round then he makes a projective measurement. The problem with this is that the post-measurement state will be a product state, and no longer entangled; entanglement is necessary to certify randomness in the 1sDI scenario we have here. To get around this issue, we alter the scheme, as is suggested in [7], such that after any time Bob makes a projective measurement, he does not make any more measurements in the sequence. That is, a measurement in the $(i+1)$th round will only follow the measurement choice $y_i = 1$. Therefore, the only bit-strings y that will be produced by Bob will be consist of a bit-value (0 or 1) prefixed by all ones. When we look at numerical approaches to randomness certification we will relax this constraint to look for optimal amounts of randomness.

When we put these details and values for the measurements into the SSC we obtain the following bounds:

$$
\begin{aligned}
|\langle U_A^{b^i|y^i}\tau_Z^A\left(U_A^{b^i|y^i}\right)^\dagger\otimes Z_B^{b^i|y^i}\rangle-1| &= 0\\
|\langle U_A^{b^i|y^i}\tau_X^A\left(U_A^{b^i|y^i}\right)^\dagger\otimes X_B^{b^i|y^i}\rangle-\sin(2\zeta_{b^i|y^i})| &\leq 2\sin^2(\theta_i)\\
|\langle U_A^{b^i|y^i}\tau_Z^A\left(U_A^{b^i|y^i}\right)^\dagger\rangle-\cos(2\zeta_{b^i|y^i})| &= 0.
\end{aligned}
\tag{13}
$$

We will use these values to certify the randomness produced by the TQSM scheme.

Coming back to randomness certification, for a sequence of measurements, the sequence of inputs y^*, from which we will obtain a string of n random bits will be the all-ones string, i.e., $y^* = (1, 1, ..., 1)$. The following (informally stated) result gives an upper bound on the guessing probability for Eve to correctly guess Bob's sequence of measurement outcomes.

Theorem 1. *For Bob making a sequence of n measurements yielding the outcome bit-string b of length n, if Alice, Bob, and Eve share some initial state $|\psi\rangle_{ABE}$, and if Eve makes a measurement associated with operators $\{M_z\}_z$, where z is Eve's guess of Bob's outcome b, Eve's guessing probability is*

$$p_{guess}(y^*) = \sum_z \delta_{b,z} tr_A \sigma_{z,b|y^*}. \tag{14}$$

and if for each i, if the SSC is satisfied and for all ϵ_1^i and ϵ_2^i (with $\epsilon_1^1 = \epsilon_2$ and $\epsilon_1^1 = \epsilon_2$) from the statements of the SSC, then

$$p_{guess} \leq \prod_{i=1}^{n} \left(\frac{1}{2} + \sqrt{\epsilon_1^i} \left(3\sqrt{2} + 2 + \frac{5}{2\sin(\zeta_{b^{i-1}|y^{i-1}})} \right) + 3\sqrt{\epsilon_1^i + \epsilon_2^i} \left(\frac{1}{\sqrt{2}\sin(\zeta_{b^{i-1}|y^{i-1}})} + 1 \right) \right), \tag{15}$$

and if $\epsilon_1^i = 0$ for all i, then

$$P_{guess} \leq \prod_{i=1}^{n} \left(\frac{1}{2} + 3\sqrt{\epsilon_2^i} \left(\frac{1}{\sqrt{2}\sin(\zeta_{b^{i-1}|y^{i-1}})} + 1 \right) \right). \tag{16}$$

The proof of this theorem can be found in the Appendix A. This theorem uses techniques from self-testing in the 1sDI setting as developed in [19]. Of independent interest we present a method to self-test all partially entangled two-qubit states in a robust manner.

Given Theorem 1 we can certify an unbounded amount of randomness assuming all of the SSC is satisfied. In particular, for the TQSM scheme we can give bounds on the amount of bits that will be certified, as indicated in the following the result.

Theorem 2. *If all statistics satisfy the SSC with $\epsilon_1^i = 0$ and $\epsilon_2^i = 2\sin^2(\theta_i)$ for all i and θ_i as a free choice of angle that is assumed to be small, then the certifiable randomness $H_{min}(b|y^*, z)$ for Bob's sequence of n measurements is*

$$H_{min}(b|y^*, z) \geq (1 - c)n,$$

where $c \in]0, 1[$. Furthermore, the TQSM scheme achieves this asymptotic behaviour as its resulting statistics will satisfy the SSC for the chosen values $\epsilon_1^i = 0$ and $\epsilon_2^i = 2\sin^2(\theta_i)$ for all i.

Proof. If we take the result of Theorem 1 and convert the probability into a min entropy we have

$$\begin{aligned}
H_{min}(b|y^*, z) &\geq -\sum_{i=1}^{n} \log_2 \left(\frac{1}{2} + 3\sqrt{\epsilon_2^i} \left(\frac{1}{\sqrt{2}\sin(\zeta_{b^{i-1}|y^{i-1}})} + 1 \right) \right) \\
&= n - \sum_{i=1}^{n} \log_2 \left(1 + 6\sqrt{\epsilon_2^i} \left(\frac{1}{\sqrt{2}\sin(\zeta_{b^{i-1}|y^{i-1}})} + 1 \right) \right) \\
&\geq n - \frac{6}{\ln 2} \sum_{i=1}^{n} \sqrt{\epsilon_2^i} \left(\frac{1}{\sqrt{2}\sin(\zeta_{b^{i-1}|y^{i-1}})} + 1 \right) \\
&= n - \frac{6}{\ln 2} \sum_{i=1}^{n} \sin(\theta_i) \left(\frac{1}{\sin(\zeta_{b^{i-1}|y^{i-1}})} + \sqrt{2} \right) \\
&\geq n - \frac{6\sqrt{2}}{\ln 2} \sum_{i=1}^{n} \theta_i \left(\frac{1}{\zeta_{b^{i-1}|y^{i-1}}} + 1 \right) \\
&\geq n - \frac{12\sqrt{2}}{\ln 2} \sum_{i=1}^{n} \theta_i \left(\frac{1}{\zeta_{b^{i-1}|y^{i-1}}} \right),
\end{aligned}$$

where in the third line we have that $\ln(1+\alpha) \leq \alpha$, and in the fourth line we use the value of $\epsilon_2^i = 2\sin^2(\theta_i)$ from the statement of the theorem. In the fifth line we have that $\sin(\alpha) \geq \frac{\alpha}{\sqrt{2}}$ and $\sin(\alpha) \leq \alpha$ for $\alpha \in]0, \frac{\pi}{4}[$, which will always be the case by construction. Then in the sixth line, we used the fact that $(\frac{1}{\alpha}+1) \leq \frac{2}{\alpha}$ for $\alpha \in]0, \frac{\pi}{4}[$, which will always be the case by construction. In the conditions, we can choose $\theta_i = d\zeta_{b^{i-1}|y^{i-1}}$ for constant $d = \frac{c\ln 2}{12\sqrt{2}}$, such that $H_{\min}(\mathbf{B}|\mathbf{Y} = \mathbf{0}, E) \geq (1-c)N$, thus completing the proof. □

Note that by appropriate choice of the measurement parameters for the rotated Pauli-X basis measurement we can get arbitrarily close to the n bits of randomness by reducing the constant c in the statement of the theorem. We cannot reduce this constant to 0 since this would involve one of the rotated Pauli-X measurements would become projective, and we would not be able to certify randomness.

5. Numerical Results

The previous analytical results indicate that unbounded randomness is possible, but the methods employed are perhaps sub-optimal in extracting the most randomness from the TQSM scheme. In this section we will employ numerical techniques, similar to those developed in [11], to give an indication of how robust the scheme is for randomness generation.

The methods employed in this section are based in semi-definite programming (SDP). We will take the approach that given the violation of a steering inequality, can we certify the randomness. A violation of a steering inequality implies that there must be certifiable randomness present. In this way the violation of the steering inequality is the certificate for the randomness. First we will outline how to derive a steering inequality from assemblages.

Given an assemblage, a method was derived to determine the steerability of the assemblage via an SDP by Skrzypczyk et al. [20]. The steering weight (SW) is given to be the solution to the following SDP, (17):

$$\begin{aligned} SW(\{\sigma_{b|y}\}) = \quad & \min \quad 1 - \mathrm{tr}\sum_{\lambda}\sigma_{\lambda} & & \\ & \text{s.t.} \quad \sigma_{b|y} - \sum_{\lambda} D(b|y,\lambda)\sigma_{\lambda} \geq 0 & \forall b, y & \\ & \qquad \sigma_{\lambda} \geq 0, & \forall \lambda & \end{aligned} \tag{17}$$

where $\{\sigma_{\lambda}\}$ is an assemblage that Eve could produce for Alice using hidden variables λ. This SDP has a corresponding dual program given by:

$$\begin{aligned} SW(\{\sigma_{b|y}\}) = \quad & \max \quad 1 - \mathrm{tr}\sum_{by} F_{b|y}\sigma_{b|y} & & \\ & \text{s.t.} \quad \sum_{by} D(b|y,\lambda)F_{b|y} - \mathbb{1} \geq 0 & \forall \lambda & \quad . \\ & \qquad F_{b|y} \geq 0, & \forall b, y & \end{aligned} \tag{18}$$

The dual program, (18), is the most relevant for this work, as shown in [20], the dual variables of the SDP, (18), in fact define a steering inequality, $\{F_{b|y}\}$, for which the assemblage, $\{\sigma_{b|y}\}$, produces an optimal violation, if one exists. We will use these steering inequalities as the fundamental building block for our sequential certification scheme.

We now return to calculating the certifiable randomness in terms of the guessing probability for Eve to guess Bob's measurement outcomes. For simplicity, we will first study the case of a single

measurement before giving the results for a sequence of measurements. With just a single measurement, the maximum guessing probability is given as the solution to the following SDP:

$$\begin{aligned} p_{\text{guess}} = \quad & \max_{\{\sigma^E_{b|y}\}_{b,y}} && \text{tr}_A \sigma^E_{b|y^*} \\ & \text{s.t.} && \sum_{b,y} F_{b|y}\sigma^E_{b|y} = v \\ & && \sum_b \sigma^E_{b|y} = \sum_b \sigma^E_{b|y'} \quad \forall z, y \neq y' \\ & && \sigma^E_{b|y} \succeq 0 \qquad\quad \forall y, b \end{aligned} . \tag{19}$$

The steering inequality $\{F_{b|y}\}$ is the one determined by the SDP (18), which is optimally violated by the observed assemblage. The SDP (19) 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 the observed violation of the steering inequality, $\{F_{b|y}\}$, which is found as a result of Alice computing the optimal values for the steering weight SDP (18). Of course, if the assemblage that Alice observes is not steerable, i.e., it produces a steering weight of 0, then this will be reflected in the observed violation of a steering inequality, i.e., there will not be one for any steering inequality. 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 can now extend this scenario to one in which Bob implements a sequence of measurements on his half of the shared state. Defining the protocol for n rounds is therefore straightforward. The idea will be that for each measurement in the sequence there will be a steering inequality, and an observed violation. The steering inequalities and violations will be obtained from the assemblages produced by the TQSM scheme, where the SW is calculated and a steering inequality generated for each measurement round in the sequence of measurements. Once we have this set of steering inequalities, she can determine the guessing probability for Eve, as the solution of the following SDP:

$$p_{\text{guess}} = \max_{b,y} \text{tr}_A \sigma^E_{b|y=y^*} \quad \text{s.t.}$$

$$\begin{aligned} \sum_{b,y} F_{b|y}\sigma^E_{b|y} &= v_n, \\ \sum_{b^{n-1},y^{n-1}} F_{b^{n-1}|y^{n-1}}\sigma^E_{b^{n-1}|y^{n-1}} &= v_{n-1} \\ \vdots \quad & \quad \vdots \\ \sum_{b_1,y_1} F_{b_1|y_1}\sigma^E_{b_1|y_1} &= v_1, \end{aligned}$$

$$\begin{aligned} \sum_{b_n} \sigma^E_{b|y} &= \sigma^E_{b^{n-1}|y^{n-1}}, \quad \forall y_n \\ \sum_{b_{n-1}} \sigma^E_{b^{n-1}|y^{n-1}} &= \sigma^E_{b^{n-2}|y^{n-2}} \quad \forall y^{n-1} \\ \vdots \quad & \quad \vdots \quad \vdots \\ \sum_{b_1} \sigma^E_{b_1|y_1} &= \rho_A \quad \forall y_1 \end{aligned}$$

$$\begin{aligned} \sum_b \sigma^E_{b|y} &= \sum_b \sigma^E_{b|y'} && \forall y, y' \\ \sum_{b^{n-1}} \sigma^E_{b^{n-1}|y^{n-1}} &= \sum_{b^{n-1}} \sigma^E_{b^{n-1}|y^{n-1\prime}} && \forall y^{n-1}, y^{n-1\prime} \\ & \vdots && \vdots \\ \sum_{b_1} \sigma^E_{b_1|y_1} &= \sum_{b_1} \sigma^E_{b_1|y_1'} && \forall y_1, y_1' \end{aligned}$$

$$\begin{aligned} \sigma^E_{b|y} &\succeq 0 \quad \forall y, b \\ \sigma^E_{b^{n-1}|y^{n-1}} &\succeq 0 \quad \forall y^{n-1}, b^{n-1} \\ & \vdots \quad \vdots \\ \sigma^E_{b_1|y_1} &\succeq 0 \quad \forall y_1, b_1 \end{aligned}$$

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, $\sigma^E_{b|y=y^*}$, for a particular input string, y^*. Again, Eve knows from which measurement settings, y^*, Bob wants to extract randomness. The steering inequality violations can be calculated by Alice for the assemblage she observes. The constraints of the SDP are similar to the single measurement case except for the addition of one new set of constraints that are required for a sequence. These particular constraints enforce causality in the measurement sequence, as mentioned earlier. Recall that, as mentioned earlier,

any assemblage satisfying these constraints can be implemented by Alice and Bob sharing a quantum state and by Bob making appropriate measurements [18].

To obtain the most amount of randomness, for the final measurement round, the measurement operators will become projective, i.e., $\theta_n = \phi_n = 0$ and the state at round $n-1$ should be a pure entangled state. In this case, it is possible to define the steering inequality explicitly, as done in [20]:

$$F_{b|y} = \alpha \left(\mathbb{1} - \frac{\sigma_{b|y}}{\mathrm{tr}(\sigma_{b|y})} \right) \tag{20}$$

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 violation value of $v_n = 0$.

Ideal Case

In this section, we present numerical results to illustrate the performance of the TQSM scheme assuming ideal functionality of devices. 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. We will also allow for the possibility that both of Bob's possible measurements for each measurement in the sequence can be non-projective.

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 rotated X measurements for a range of values of θ_1, as seen in Figure 2. All measurements are applied on the following initial pure state:

$$|\Psi(\zeta_1)\rangle = \cos(\zeta_1)|00\rangle + \sin(\zeta_1)|11\rangle. \tag{21}$$

$|\Psi(\zeta_1)\rangle$ 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 reproduces the already known results for a single measurement round, as is done in [11,21], but using our SDP, which is slightly different than the one derived in those works. As expected, when $\zeta_1 = 0$, no randomness can be certified as the state becomes a product state. In the opposite end of the spectrum, for $\zeta_1 = \pi/4$, the maximal amount of randomness can be certified, since this state is maximally entangled between Alice and Bob.

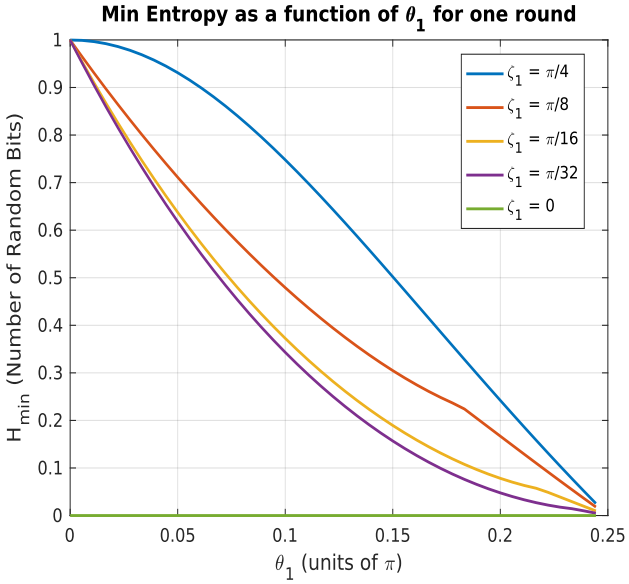
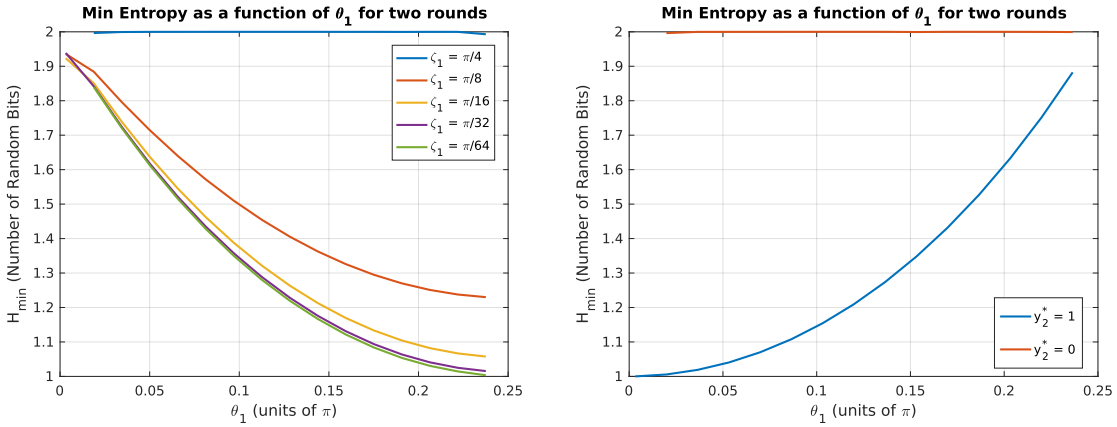


Figure 2. H_{min} for one round of measurements, using a range of initial states, ζ_1, as a function of initial measurement angle, θ_1.

Figure 3a,b shows the results after two measurement rounds. In Figure 3a, 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 3b 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, $y_1^* = 1, y_2^* = 0$. We cut the graphs at the extremes of the measurement angles ($\theta_1 = \{0, \pi/4\}$) in order to avoid the discontinuity that occurs as soon as the first round measurement undergoes the transition from projective to non-projective.

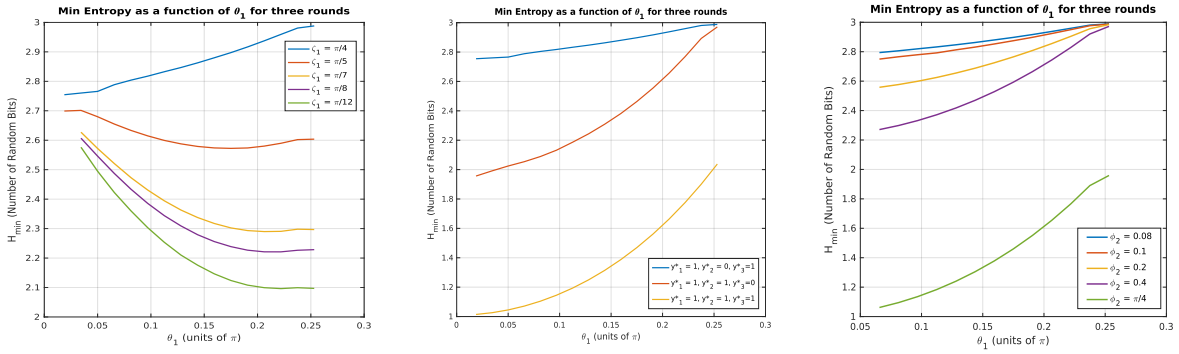
An interesting feature of the protocol can be seen in Figure 3a, for the case of $\zeta_1 = \pi/4$. It turns out that in this case a maximal amount of randomness can be certified, for all initial measurement angles, θ_1. This behaviour illustrates the fundamental difference between the steering, and fully device independent scenario and the more robust nature of quantum steering. In the latter, one observes the amount of certifiable randomness decreases monotonically as ($\theta_1 \to 0$), corresponding to the first round measurement becoming non-interactive. We leave a further analysis of this phenomenon to future work.



(**a**) (**b**)

Figure 3. (**a**) H_{min} for two rounds of measurements, with a range of initial states, $\zeta_1 \in (0, \frac{\pi}{4}]$ and $\phi_1 = \theta_2 = \phi_2 = 0$. (**b**) Difference in certified randomness when choosing between measurement settings $y_2^* = 1$ or $y_2^* = 0$ in the second measurement round.

Finally, Figure 4 illustrates numerical results for the protocol with 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 4b 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 4c shows the results for various second round measurement angles, and the amount of randomness that can be certified increases as the measurement angle, $\phi_2 \to 0$.



(**a**) (**b**) (**c**)

Figure 4. (**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.

In these results we see that the amount of randomness that can be certified using the numerics is quite robust. This then could make this scheme amenable to experiment. In the next section we will adapt these numerical techniques to look at experimental feasibility of this randomness certification scheme.

6. Towards Experimental Implementations

6.1. 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 subcase of the malicious adversary scenario. This mentality allows us to use our protocol to evaluate the usefulness of some current available technologies 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 [22], which can be produced between two parties in a networked architecture of ion traps:

$$\rho_\epsilon = (1-\epsilon)\Phi^+ + \frac{\epsilon}{3}\Phi^- + \frac{\epsilon}{3}\Psi^+ + \frac{\epsilon}{3}\Psi^- \tag{22}$$

where ϕ^+, ϕ^-, ψ^+, and ψ^- are the standard 2-qubit Bell states. The state, (22), is a mixed state assuming uniform depolarising noise. In [22], 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 three rounds of this purification protocol, the resulting states are given by:

$$\rho_\epsilon^{(0)} = (1-\epsilon)\Phi^+ + \frac{\epsilon}{3}\Phi^- + \frac{\epsilon}{3}\Psi^+ + \frac{\epsilon}{3}\Psi^- \tag{23}$$

$$\rho_\epsilon^{(1)} = \left(1 - \frac{2}{3}\epsilon - \frac{2}{3}\epsilon^2\right)\Phi^+ + \left(\frac{2}{9}\epsilon + \frac{2}{9}\epsilon^2\right)\Phi^- + \frac{2}{9}\epsilon^2\Psi^+ + \frac{2}{9}\epsilon^2\Psi^- + O(\epsilon^3) \tag{24}$$

$$\rho_\epsilon^{(2)} = \left(1 - \frac{8}{9}\epsilon^2 - \frac{8}{27}\epsilon^3\right)\Phi^+ \frac{4}{9}\epsilon^2\Phi^- + \frac{4}{9}\epsilon^2\Psi^+ + \frac{8}{27}\epsilon^3\Psi^- + O(\epsilon^4) \tag{25}$$

$$\rho_\epsilon^{(3)} = \left(1 - \frac{2}{9}\epsilon^2 - \frac{16}{27}\epsilon^3\right)\Phi^+ \frac{2}{9}\epsilon^2\Phi^- + \frac{8}{27}\epsilon^3\Psi^+ + \frac{8}{27}\epsilon^3\Psi^- + O(\epsilon^4) \tag{26}$$

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

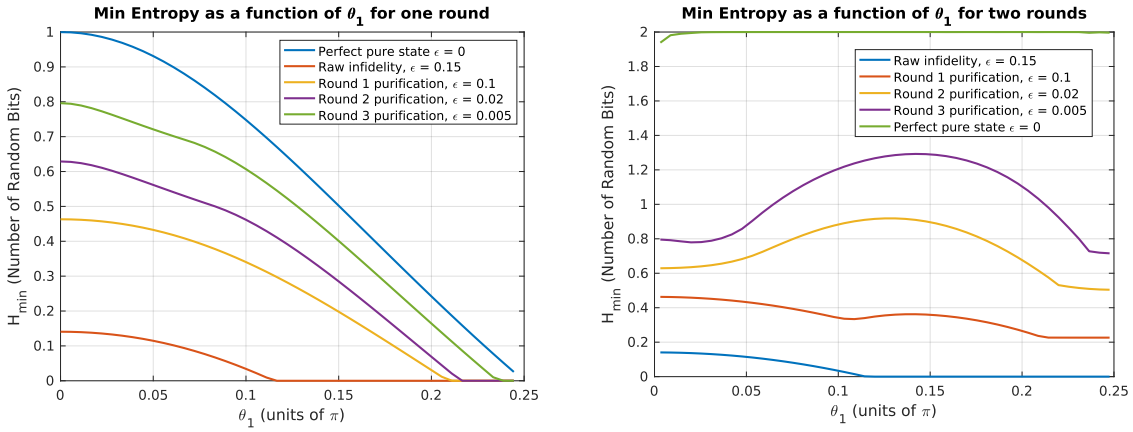
Currently, raw entanglement between two ion traps, connected with an entangling photon, has been achieved with a fidelity of about 85% $\implies \epsilon \approx 0.15$ [23]. Starting with this level of raw infidelity, the purification protocol produces states of infidelity $\epsilon \approx 0.1, 0.02$, and 0.005 after one, two, and three rounds respectively. The fidelity is given by (27) [24], and taken to be between the actual state $\rho^{(i)}$, and the pure Bell state, Φ^+:

$$F(\rho_\epsilon^{(i)}, \Phi^+) = \mathrm{Tr}\left(\sqrt{\sqrt{\rho_\epsilon^{(i)}}\Phi^+\sqrt{\rho_\epsilon^{(i)}}}\right) \tag{27}$$

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 5a shows the result after a single X measurement on the states (choosing $y_1^* = 1$) (23)–(26). 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, (23), very little randomness can be certified, with a maximum of approximately 0.15 bits.

Figure 5b 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, (22). 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 5b. The infidelity for which the sequence becomes more useful than a single measurement can be seen to be approximately in the interval $\epsilon \in (0.06, 0.07)$.



(**a**) (**b**)

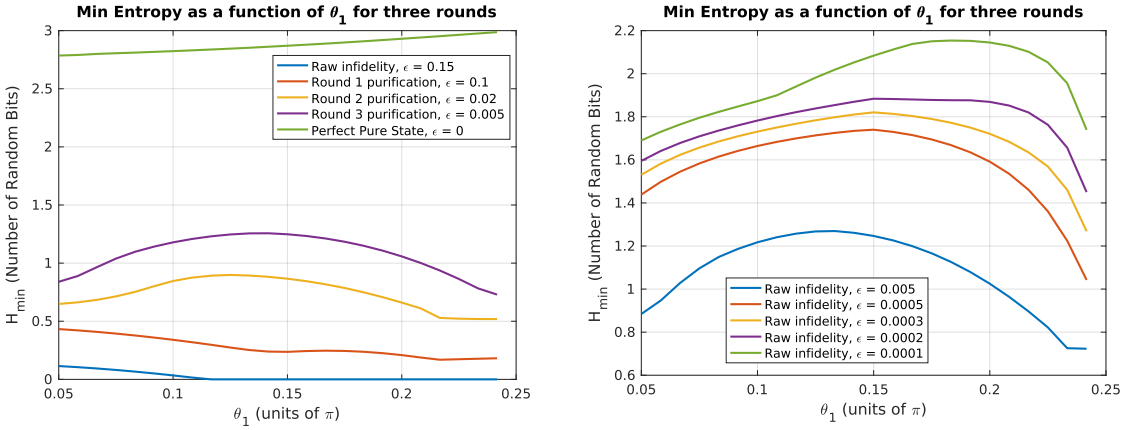
Figure 5. (**a**) Single measurement on the raw entangled state (22) ($\epsilon = 0.15$), the states produced after three rounds of the purification protocol, (24)–(26), with $\epsilon = 0.1, 0.02$, and 0.005 respectively and a perfect pure state with $\epsilon = 0$. (**b**) Two rounds of measurement on the raw entangled state (22) ($\epsilon = 0.15$), the states produced after three rounds of the purification protocol, with the same parameters as (**a**).

Finally, Figure 6a 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, (24)–(26), 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 $\epsilon = 0$ is also plotted for comparison.

Clearly, one would expect the existence of *some* level at which the state becomes pure enough to be useful so Figure 6b shows the results of the protocol for very small infidelities, specifically:

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



(**a**) (**b**)

Figure 6. (**a**) Three rounds of measurement on the raw entangled state, (22), ($\epsilon = 0.15$), the states produced after three rounds of the purification protocol, (24)–(26), with $\epsilon = 0.1, 0.02$, and 0.005 respectively and a perfect pure state with $\epsilon = 0$. (**b**) Three rounds of measurement on raw entangled states with infidelities $\epsilon = \{5 \times 10^{-3}, 5 \times 10^{-4}, 3 \times 10^{-4}, 2 \times 10^{-4}, 1 \times 10^{-4}\}$.

It can be seen that for an infidelity approximately in the interval, $\epsilon \in (1 \times 10^{-4}, 2 \times 10^{-4})$, 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. Furthermore, for four and higher rounds of measurement, states that 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.

6.2. Atom–Photon Implementation

We also examined a potential state arising from an atom–photon (AP) interaction. This case is even more applicable to the above 1sDI scenario as discussed in Section 1. In light of this, it makes sense to consider a situation where an entangled state is produced by some process between an atom, and a coherent photon state. As an example, we investigate the state produced in [25], which is the simplest for our purposes since it only involves single photon and vacuum states. However, an alternative method, using coherent photon states, such as the approach of [26,27] could be studied. These scenarios are particularly relevant as the authors have the aim of performing a Bell test, and observing a violation of a Bell inequality.

It is possible to examine two possible cases in this scenario, since the setup is asymmetric. We can either consider noise introduced in either imperfections in the atom side, or on the photon side.

The ideal case considered in [25] is given by (keeping our notation):

$$|\Psi^{\zeta_1}\rangle = \cos(\zeta_1)|0, g\rangle + \sin(\zeta_1)|1, s\rangle \tag{28}$$

where $|g\rangle, |s\rangle$ are two atomic states (held by Bob) and $|0\rangle, |1\rangle$ are the photon vacuum and single photon state respectively, held by Alice.

For simplicity, we will consider two of the cases presented in [25] as sources of imperfections. The first error is introduced in the transmission efficiency, and we also consider the possibility that the photon was lost during the transmission. The transmission inefficiency is given by η_t, and if the photon is lost, we get an extra contribution to the overall state corresponding to $|0,s\rangle$, with a weight of $\sin^2(\zeta_1)(1-\eta_t)$, such that the final state is given by:

$$\rho_{\eta_t} = N|\Psi_{\eta_t}^{\zeta_1}\rangle\langle\Psi_{\eta_t}^{\zeta_1}| + \sin^2(\zeta_1)(1-\eta_t)|s,0\rangle\langle s,0| \tag{29}$$

where:

$$|\Psi_{\eta_t}^{\zeta_1}\rangle = \frac{1}{N}(\cos(\zeta_1)|0,g\rangle + \sin(\zeta_1)\sqrt{\eta_t}|1,s\rangle), \tag{30}$$

$$N = \cos^2(\zeta_1) + \sin^2(\zeta_1)\eta_t. \tag{31}$$

Since both sets of atomic, (A), and photonic, (P), states are orthogonal to each other, we can make the translation to 'logical' basis states: $|g\rangle \to |0\rangle_A, |s\rangle \to |1\rangle_A, |0\rangle \to |0\rangle_P, |1\rangle \to |1\rangle_P$ the state is given in the computational basis by:

$$\rho_{\eta_t} = \begin{pmatrix} c^2 & 0 & 0 & \sqrt{\eta_t}cs \\ 0 & s^2(1-\eta_t) & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \sqrt{\eta_t}cs & 0 & 0 & \eta_t s^2 \end{pmatrix}. \tag{32}$$

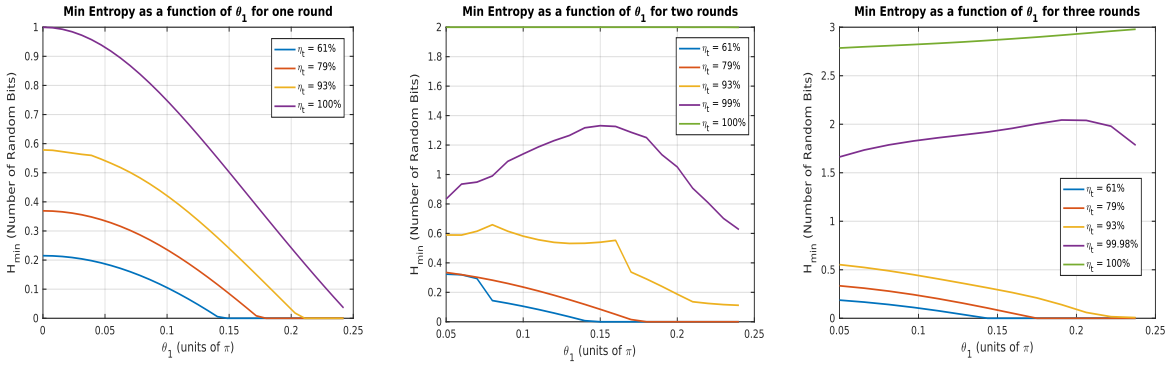
Where we have defined $c = \cos(\zeta_1)$, $s = \sin(\zeta_1)$ Figure 7 illustrates the results after one, two, and three measurement rounds for an atom–photon state (29) with $\zeta_1 = \pi/4$. Values of the transmission efficiency, η_t were chosen for interest to correspond with those described in [26]. In that paper, the authors examine Bell inequality violations where Bob (Alice in our case) has access to the photonic system, and can make either homodyne measurements or photon counting to determine his Bell statistics. This intuitively corresponds in our case to his choice of measurement basis. Alternatively, Bob might not use photon counting, but instead choose between homodyne measurements in two different quadratures. Values of $\eta_t = \{61\%, 79\%\}$ are the required levels of efficiency to produce a Bell violation, if the measurements on the photonic side are either homodyne and photon counting, or both homodyne respectively. It should be noted that in our case, we would not need to distinguish between these two cases as we do not need to reproduce statistics for binary outcomes on Alice's side, since she is fully trusted, and needs only to do state tomography on the photonic mode. As such, the measurement scheme that allows her to more easily do tomography is the one that should be chosen in the actual implementation of our protocol. Also, a value of $\eta_t = 93\%$ was plotted as this is the level that would be required to close the locality loophole in the Bell violation, as stated in [26].

From Figure 7a, it can be seen that for a value of $\eta_t = 61\%$, more randomness can be certified with a single measurement with the AP state, than with the one produced in two ion traps, with a fidelity of $\epsilon = 85\%$, as in the latter case, only about 0.15 random bits could be certified, but in the former over 0.2 random bits can be certified.

In this implementation, we see once again see the same general trends as with the ion trap apparatus. At some level of transmission efficiency, illustrated by $\eta_t = 99\%, \eta_t = 99.98\%$ in Figure 7b,c respectively, the state becomes pure enough for a sequence to become worthwhile. In particular, for $\eta_t = 99\%$, two measurements on the state generates more certifiable randomness than is possible with one, and for $\eta_t = 99.98\%$, we can get more than two certifiable random bits.

As a result, we can see that this particular atom photon model has more promise for randomness certification than the ion trap model, although it may be an unfair comparison to directly compare transmission efficiency in the former case to state fidelity in the latter. However, while the state in [22] only takes into account a very simple depolarising noise model, which may be unrealistic in practice, the atom–photon state, (29), of [26] takes into account all coupling errors in the state preparation

between Alice and Bob. Another interesting property to investigate would be the detection efficiency of the photons and how this effects the protocol.



(**a**) (**b**) (**c**)

Figure 7. (**a**) H_{min} for one round, for various levels of η_t. (**b**) H_{min} for two rounds, for various levels of η_t. (**c**) H_{min} for three rounds, for various levels of η_t. The second round measurement angle is $\phi_2 = 0.08$ rad.

6.3. Nitrogen-Vacancy Center Implementation

Next, we consider an entangled state produced between Alice and Bob using qubits based on electronic spins of nitrogen-vacancy defect centers in diamond. In particular, we examine the state used in the first loophole free Bell test, [2,28]. This state is again relevant due to its use in the Bell test, and as mentioned in [2], the setup could readily be used for randomness certification, albeit in a fully device independent scenario. The shared state between Alice and Bob in this experiment is given by the following density matrix:

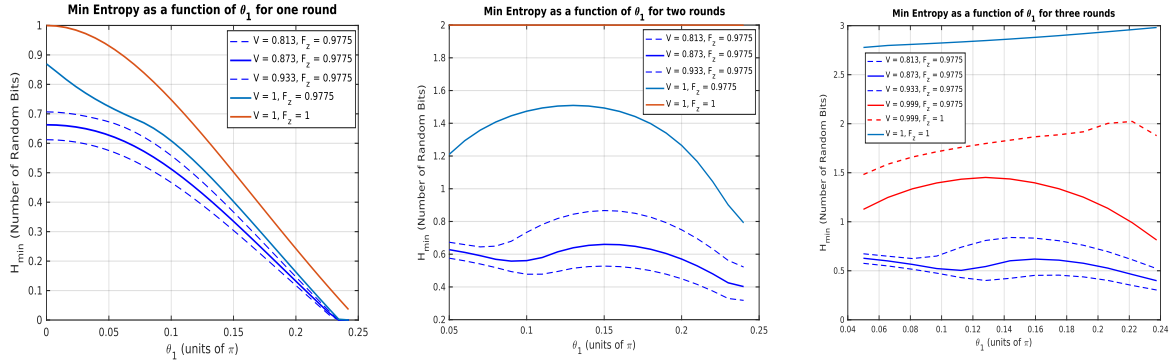
$$\rho_{NV} = \frac{1}{2}\begin{pmatrix} 1-F_z & 0 & 0 & 0 \\ 0 & F_z & -V & 0 \\ 0 & -V & F_z & 0 \\ 0 & 0 & 0 & 1-F_z \end{pmatrix} \tag{33}$$

where, $F_z = 1/2[(1-e^A_{\text{early}})(1-e^B_{\text{late}}) + (1-e^B_{\text{early}})(1-e^A_{\text{late}})]$, and V is the visibility that describes the indistinguishability of the photons used to create entanglement. The residual errors, $e^{A/B}_{early/late}$, are due to the spin-photon coupling, as described in [2]. In this case, the ideal case is not particular Bell state we have assumed above, Φ^+, instead it is another Bell state, $\Psi^- = |\psi^-\rangle\langle\psi^-|, |\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. The best estimate for the visibility is given to be $V = 0.873 \pm 0.060$, and the residual errors are found to be $e^A_{\text{early}} = 1.4 \pm 0.2\%, e^B_{\text{early}} = 1.6 \pm 0.2\%, e^A_{\text{late}} = 0.8 \pm 0.4\%, e^B_{\text{late}} = 0.7 \pm 0.4\%$. For these values, the fidelity of the state used in their Bell test is reported to be $\langle\psi^-|\rho_{NV}|\psi^-\rangle = 0.92 \pm 0.03$, and $F_z \approx 0.9775$.

Figure 8 shows the results of the protocol when the electronic spin state, (33), is used. In the experiment described in [2], a very pure state was required to implement a reliable Bell test, and due to this, the state is substantially better for randomness certification than that available in the ion trap, or atom–photon implementation, with it being possible to certify 0.65 ± 0.05 random bits using electronic spins with a single measurement. Also, in both Figure 8b,c, the effect of the residual errors can be seen to have a large consequence when it comes to randomness certification, and ultimately the state purity. For example, in Figure 8b with a perfect visibility of $V = 1$ and using a value of $F_z = 0.9775$ a maximum of 1.5 bits can be certified with two measurements, which is substantially less than then maximal amount of 2 bits that can certified with a perfect pure state. A similar feature can be seen in Figure 8c for three measurement rounds. It would also be interesting to study the effect of the,

ΔF_z, derived from the statistical uncertainties on $e^{A/B}_{early/late}$, on the amount of randomness producible by the state. $\Delta F_z = 0$ was assumed in our numerical results for clarity.

The sensitivity of the randomness certification to errors is especially apparent in Figure 8c. For a reduction in visibility, V, by only 0.1%, the amount of random bits drops by almost a full unit. Similarly, a reduction in F_z by 0.023 leads to a loss of 1/2 a random bit, and even with this small drop, the situation changes from one in which a sequence of three measurements can do better than is ever possible with two, to a scenario in which two measurement rounds produce a very similar amount of certifiable randomness, and the third measurement is almost unnecessary.

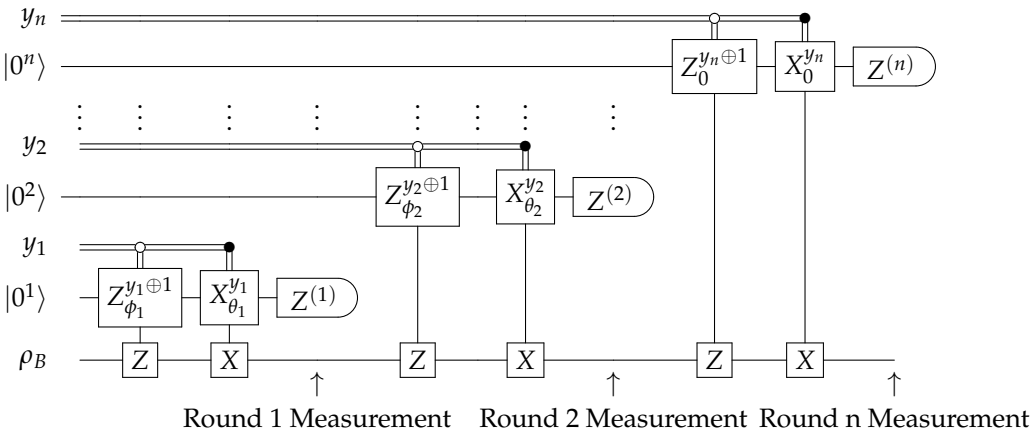


(**a**) (**b**) (**c**)

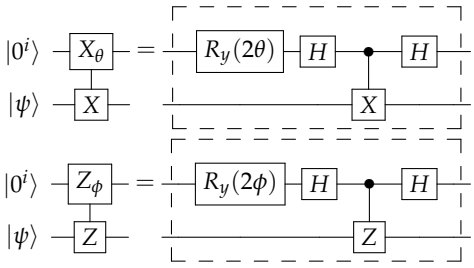
Figure 8. H_{min} using NV center state. The full blue line in each figure represents the best experimental estimate of [2] corresponding to $V = 0.873, F_z = 0.9775$. The dashed blue lines represent the effect of the error in the visibility, corresponding to states with $\Delta V = \pm 0.060$. Also, states with perfect visibility, $V = 1$, but with residual errors, $F_z = 0.9775$, along with a perfect pure Bell state, Ψ^-, are also plotted for comparison. Results for: (**a**) a single measurement, (**b**) two measurements, and (**c**) for three measurement rounds, with a second round measurement angle of $\phi_2 = 0.08$ rad, all with various θ_1 values.

6.4. Implementation on Rigetti Forest Platform

As a final example, we implement the protocol using Rigetti's Forest Platform [29]. This is done in a proof of principle way using the following circuit:



where we have defined the following two qubit unitary gates, that effectively implement the non-projective measurements in the X and Z bases, denoted as X^θ, respectively.



The index on the ancilla represents the measurement round it is used in. The input string, y, 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 each round of the protocol, a single 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 $|\psi\rangle_B$ is only Bob's initial reduced state.

The circuit could be further improved since it is possible to only use a single ancilla. This ancilla would undergo multiple measurements, with the addition of a series of CNOT gates to the ancilla wire in order to reset the ancilla post measurement. These CNOT gates would return the ancilla to the usual $|0\rangle$ state conditioned on the previous measurement outcome. It is actually essential that the measurements occur in a sequential manner, i.e., it is Bob's post-measurement state, which is rotated in the next round of the protocol. In this way, the measurements actually cannot be deferred to the end of the circuit since if this was done, there would be a cheating strategy for Eve. Causality is essential for the proper security of the protocol. However, since the quantum hardware prohibits intermediate measurements in a quantum circuit, and instead it is necessary to defer all measurements to the end of the circuit. While this would not be sufficient for security against a malicious adversary, it is useful as a proof-of principle, assuming any deviation occurs from noise errors alone.

To implement the protocol, we proceed as described above and perform tomography on Alice's qubit, ρ_A after the sequence of measurements on Bob's qubit, ρ_B (deferred onto the ancillary qubits). We proceed using the simulator of the `Aspen` quantum processing unit (QPU) with the sublattice `Aspen-4-3Q-A`. With this scheme, we require an $2 + n$ qubit chip to implement n sequential measurements. We perform direct inversion tomography [30] by measuring the expectation values of the Pauli Observables, X, Y, Z to reconstruct the state:

$$\rho_A = \frac{1}{2}\left(\mathbb{1} + r_x X + r_y Y + r_z Z\right). \tag{34}$$

Direct inversion tomography is the simplest method of state tomography, and compensates for the fact that, due to measurement errors, the state which is estimated naively may lie outside the Bloch Sphere (i.e., it has a norm greater than 1). If this is the case, the vector, $\mathbf{r} = (r_x, r_y, r_z)$ is simply rescaled by its norm in the following way:

$$\hat{\mathbf{r}} = \begin{cases} \mathbf{r} & \text{if } ||\mathbf{r}||_2 \leq 1 \\ \mathbf{r}/||\mathbf{r}||_2 & \text{if } ||\mathbf{r}||_2 > 1 \end{cases} \tag{35}$$

where $||\mathbf{x}||_2 = \left(|x_1|^2 + |x_2|^2 + |x_3|^2\right)^{1/2}$ is the ℓ_2 norm. The original vector is estimated by approximating the expectation values, $(\mathrm{tr}(X\rho_A), \mathrm{tr}(Y\rho_A), \mathrm{tr}(Z\rho_A))$. This is achieved by counting

the number of times the positive eigenvalue is observed, minus the number of times the negative eigenvalue is observed and normalising the answer, for each operator.

However, when implementing the protocol on the simulator, Alice can use her foreknowledge that Bob makes measurements only in the noisy X/Z bases. In this case, the steered states, ρ_A, would have no Y contribution so Alice would only be required to estimate $(\mathrm{tr}(X\rho_A), \mathrm{tr}(Z\rho_A))$. However, if the protocol was to run on the physical hardware, it would be necessary to include measurements of the Y observable also. To generate the full assemblage, this must be done for each of Bob's measurement choices and outcomes, $\sigma_{b|y}$. The full protocol requires the assemblage after each round, $\sigma_{b^i|y^i} \forall i \leq n$, but it is sufficient to compute these from the final round assemblages elements. This is due to the causality relationship $\sum_{b_i} \sigma_{b^i|y^i} = \sigma_{b^{i-1}|y^{i-1}}$.

Figure 9 illustrates the protocol using Rigetti's Simulator of sublattices of the QPU containing three, four, and five qubits to implement one, two, and three measurement rounds in Figure 9a, Figure 9b, and Figure 9c respectively. For a single measurement, the results are encouraging, but this is because 100,000 measurements allows a good characterisation of the four assemblage elements received by Alice. It is apparent that the exponential scaling quickly overtakes the number of measurements such that three measurement rounds do not increase the randomness certified over two, it actually reduces it. Unfortunately, we were not able to get sensible results when running the protocol on the QPU versions of the corresponding simulators in Figure 9, even for a single measurement, due to noise. Potentially, this could be mitigated by using more sophisticated tomography techniques.

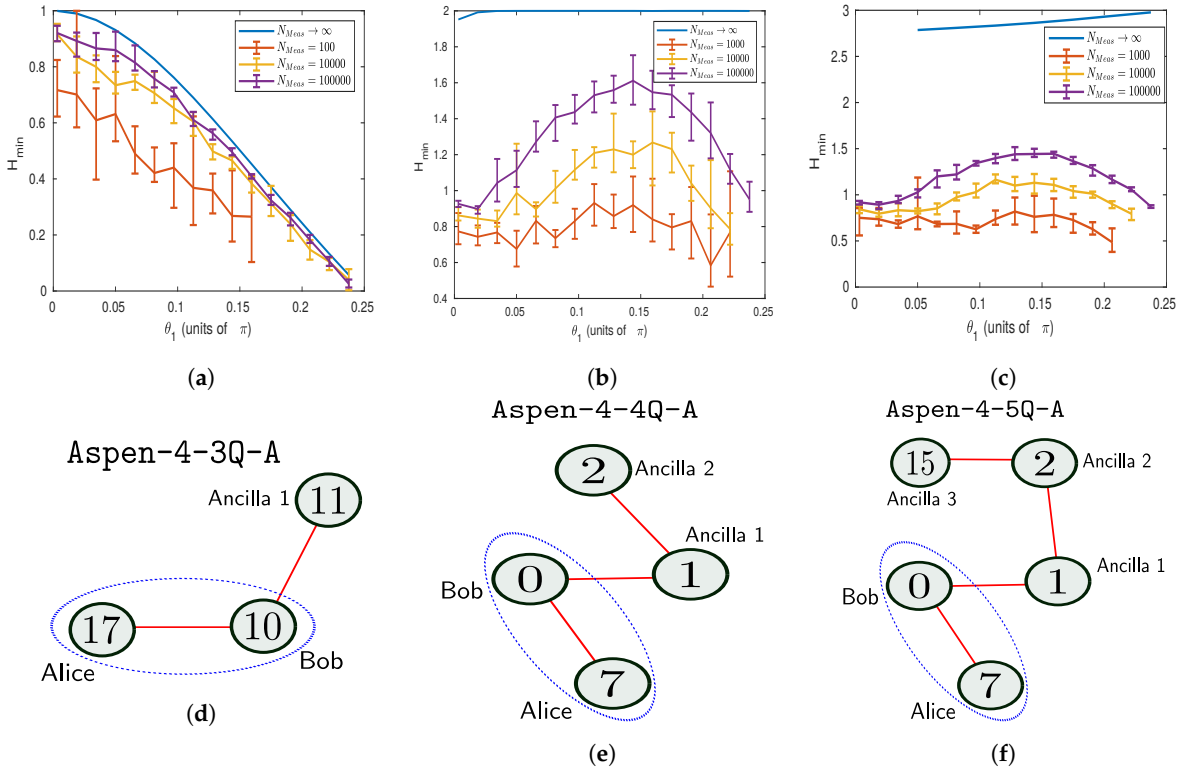


Figure 9. H_{min} for (**a**) one, (**b**) two, and (**c**) three measurement rounds on Rigetti `Aspen` Simulator using the pure entangled state (21), with $\zeta_1 = \pi/4$. N_{meas} is the number of measurements taken when estimating each of the expectations values required to approximate (34). Also plotted for comparison is the limit of infinite measurements, such that the ideal assemblage elements are obtained. In each case, the protocol is run five times, with the average H_{min} plotted, and the error bars represent the maximum and minimum values obtained over the five runs. Figures (**d**–**f**) illustrate the chip simulator topology used for one, two, and three measurements respectively. The qubits shared between Alice and Bob are indicated also.

7. Discussion

We presented a novel protocol to certify an unbounded amount of random numbers from sequential measurements on one half of a quantum state shared by two parties, building on the work of [7,11,21]. The 'certificate' in this case can be a set of statistical criteria or the states into which the other party is 'steered' as a result of the sequence of well-chosen measurements. We studied the behaviour of the scheme both in the ideal setting, and in experimentally realistic settings, [22], including those which have actually been implemented [2,25]. We also demonstrated the feasibility of the scheme in being able to certify multiple random bits produced from a single quantum state, rather than multiple states each producing only one bit. This distinction is important given the valuable nature of controlled quantum systems, and hence represents an important step in resource reduction.

Our scheme could be readily turned into a protocol for randomness expansion, especially now that we have improved upon the work of [7] in reducing the number of measurements required. We leave this to future work.

Interesting future work would be to investigate the reason behind the apparent anomaly in the steering scenario with two sequential measurements on a maximally entangled state, as discussed in Section 5. Given our focus in this work on studying the behaviour of the protocol in realistic experimental implementations, it would be insightful to actually implement the protocol in a physical system, similar to those carried out in Bell testing, [2].

8. Materials and Methods

All numerical results in this work were obtained using the Matlab convex optimisation package, *cvx*, [31] and a package for managing quantum states, *qetlab*, [32]. The resulting code required to produce all images in this work is available at [33].

Author Contributions: B.C. and M.J.H. devised the scheme. B.C. wrote the code and produced the numerical results. M.J.H. derived the theorems. E.K. supervised the work.

Funding: This work was supported by the Engineering and Physical Sciences Research Council (grant EP/L01503X/1), EPSRC Centre for Doctoral Training in Pervasive Parallelism at the University of Edinburgh, School of Informatics and Entrapping Machines, (grant FA9550-17-1-0055).

Acknowledgments: B.C. thanks Atul Mantri and Niraj Kumar for useful discussions. We also thank Rigetti Computing for the use of their quantum compute resources, and views expressed in this paper are those of the authors and do not necessarily reflect the views or policies of Rigetti Computing.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Appendix A. Proof of Theorem 1

We will at first consider the case of a single round of the scheme outlined in this paper, that is, when Bob's first measurement is his only one. Recall that Eve has created a quantum state $|\psi_{ABE}\rangle$ with sub-systems denoted by A, B, and E, which are Alice, Bob, and Eve's respective subsystems.

We want to bound Eve's guessing probability of the outcome b of Bob's measurement. In order to do this we will constrain what form $|\psi_{ABE}\rangle$ takes, and if the dichotomic observable corresponding to Bob's measurement is denoted X_B, we will also constrain the form of $\mathbb{I}_A \otimes X_B \otimes \mathbb{I}_E|\psi_{ABE}\rangle$. In particular, we will use the techniques of self-testing in the one-sided device-independent setting [19] to show that there exists a local isometry acting on Bob's systems that map the state $|\psi_{ABE}\rangle$ to the state $|\zeta\rangle_{AB'}|\text{anc}\rangle_{E'}$, where B' denotes a virtual qubit system held by Bob respectively such that $|\zeta\rangle_{AB'} = \cos(\zeta)|00\rangle + \sin(\zeta)|11\rangle$, and E' is an arbitrary virtual system held by Eve. We also show something analogous for $\mathbb{I}_A \otimes X_B \otimes \mathbb{I}_E|\psi_{ABE}\rangle$.

To rigorously establish our self-testing results, we first need to establish the statistical conditions that need to be satisfied. Bob's aforementioned observable X_B has two eigenvalues taking the values ± 1 (corresponding to the binary outcomes b). Without loss of generality, Bob's observable can be

taken to be sharp with eigenvalues $+1$ and -1 being associated with projectors Σ_B^0 and Σ_B^1 respectively such that $\Sigma_B^0 + \Sigma_B^1 = \mathbb{I}_B$ and $\Sigma_B^0 - \Sigma_B^1 = X_B$. In addition to X_B, Bob has a second sharp observable Z_B with eigenvalues $+1$ and -1 being associated with projectors Π_B^0 and Π_B^1 respectively such that $\Pi_B^0 + \Pi_B^1 = \mathbb{I}_B$ and $\Pi_B^0 - \Pi_B^1 = Z_B$. In addition to Bob's measurement, we denote Alice's Pauli X and Z matrices as τ_X and τ_Z respectively. Now we can state the statistical criteria that Alice and Bob need to satisfy:

$$\begin{aligned} \left|\langle \tau_Z^A \otimes Z_B \rangle - 1\right| &\leq \epsilon_1 \\ \left|\langle \tau_X^A \otimes X_B \rangle - \sin(2\zeta)\right| &\leq \epsilon_2 \\ \left|\langle \tau_Z^A \rangle - \cos(2\zeta)\right| &\leq \epsilon_1 \end{aligned} \tag{A1}$$

with ϵ_1 and ϵ_2 being small error terms, i.e., a positive real number. We chose the errors to have this symmetry motivated by our original scheme, as will hopefully be clear.

We can now state the self-testing result we will need:

Theorem A1. *If Alice and Bob's statistics satisfy the criteria in (A1) and $\zeta \in]0, \frac{\pi}{4}]$, then there exist a quantum state $|anc\rangle \in \mathcal{H}_{E'}$ in Hilbert space $\mathcal{H}_{E'}$ and local isometry Φ_B such that*

$$\begin{aligned} \|\mathbb{I}_A \otimes \Phi_B \otimes \mathbb{I}_E(|\psi_{ABE}\rangle) - |\zeta\rangle_{AB'}|anc\rangle_{E'}\| &\leq \sqrt{\epsilon_1}(\sqrt{2}+1) + \sqrt{\epsilon_1+\epsilon_2} \\ \left\|\mathbb{I}_A \otimes \Phi_B \otimes \mathbb{I}_E(\mathbb{I}_A \otimes X_B \otimes \mathbb{I}_E|\psi_{ABE}\rangle) - \mathbb{I}_A \otimes \tau_X^{B'}|\zeta\rangle_{AB'}|anc\rangle_{E'}\right\| &\leq \sqrt{\epsilon_1}\left(2\sqrt{2}+1+\frac{5}{2\sin(\zeta)}\right) \\ &+ \sqrt{\epsilon_1+\epsilon_2}\left(\frac{3}{\sqrt{2}\sin(\zeta)}+2\right). \end{aligned}$$

To prove this result we need to state a few lemmas. Before doing this, we will simplify notation to have to have $|\psi\rangle := |\psi_{ABE}\rangle$ and we will suspend denoting tensor products and identities when it is clear from context. The lemmas we need now follow.

Lemma A1. *If (A1) is satisfied and $\zeta \in]0, \frac{\pi}{4}]$ the following is true:*

$$\|(|x\rangle\langle x|_A - \Pi_B^x)\,|\psi\rangle\| \leq \sqrt{\frac{\epsilon_1}{2}},$$

for $x \in \{0,1\}$ and $\{|x\rangle\}_x$ being the computational basis, i.e., the eigenstates of τ_Z.

Proof. We will proof the case where $x = 0$, but the proof for $x = 1$ is essentially the same. Note that by definition:

$$\begin{aligned} \|\left(|0\rangle\langle 0|_A - \Pi_B^0\right)|\psi\rangle\| &= \sqrt{|\langle\psi|0\rangle_A|^2 + \langle\Pi_B^0\rangle - 2\langle\psi|0\rangle\langle 0|_A\Pi_B^0|\psi\rangle} \\ &= \sqrt{\frac{1}{2} - \frac{1}{2}\left(\langle\psi|(2|0\rangle\langle 0|_A - \mathbb{I}_A)\otimes(2\Pi_B^0 - \mathbb{I}_B)|\psi\rangle\right)} \\ &= \sqrt{\frac{1}{2} - \frac{1}{2}\langle\tau_Z^A Z_B\rangle} \\ &\leq \sqrt{\frac{\epsilon_1}{2}}, \end{aligned}$$

where the first line of (A1) was used in the final inequality. □

Lemma A2. *If (A1) is satisfied and $\zeta \in]0, \frac{\pi}{4}]$ the following is true:*

$$\begin{aligned} \| \left(\sin(\zeta)|1\rangle\langle 0|_A - \cos(\zeta)|1\rangle\langle 1|_A X_B\right)|\phi\rangle\| &\leq \sqrt{\frac{\epsilon_1+\epsilon_2}{2}} \\ \| \left(\cos(\zeta)|0\rangle\langle 1|_A - \sin(\zeta)|0\rangle\langle 0|_A X_B\right)|\phi\rangle\| &\leq \sqrt{\frac{\epsilon_1+\epsilon_2}{2}}. \end{aligned}$$

Proof. We will prove the first case as the second case has essentially the same proof. By definition we have

$$\begin{aligned} &\| \left(\sin(\zeta)|1\rangle\langle 0|_A - \cos(\zeta)|1\rangle\langle 1|_A X_B\right)|\phi\rangle\| = \\ &\sqrt{\sin^2(\zeta)|\langle 0|\psi\rangle_A|^2 + \cos^2(\zeta)|\langle 1|\psi\rangle_A|^2 - \sin(\zeta)\cos(\zeta)\langle\psi|\tau_X^A X_B|\psi\rangle} \\ &\leq \sqrt{\sin^2(\zeta)(\cos^2(\zeta)+\frac{\epsilon_1}{2}) + \cos^2(\zeta)(\sin^2(\zeta)+\frac{\epsilon_1}{2}) - \sin(\zeta)\cos(\zeta)(\sin(2\zeta)-\epsilon_2)} \\ &\leq \sqrt{\frac{\epsilon_1+\sin(2\zeta)\epsilon_2}{2}} \leq \sqrt{\frac{\epsilon_1+\epsilon_2}{2}}, \end{aligned}$$

where in the first inequality the second and third line of (A1) were utilised. In particular, we utilised the fact that

$$\langle\psi|Z_A|\psi\rangle = 2|\langle 0|\psi\rangle_A|^2 - 1 = 1 - 2|\langle 1|\psi\rangle_A|^2, \tag{A2}$$

which concludes the proof. □

Lemma A3. *If (A1) is satisfied and $\zeta \in]0, \frac{\pi}{4}]$ the following is true:*

$$\begin{aligned} \left\| \left(\sin(\zeta)|1\rangle\langle 0|_A - \cos(\zeta)X_B\Pi_B^1\right)|\phi\rangle\right\| &\leq \sqrt{\frac{\epsilon}{2}} + \cos(\zeta)\sqrt{\frac{\epsilon_1}{2}} \\ \left\| \left(\cos(\zeta)|0\rangle\langle 1|_A - \sin(\zeta)X_B\Pi_B^0\right)|\phi\rangle\right\| &\leq \sqrt{\frac{\epsilon}{2}} + \sin(\zeta)\sqrt{\frac{\epsilon_1}{2}}, \end{aligned}$$

for $\epsilon := \epsilon_1 + \epsilon_2$, and thus

$$\left\| \left(X_B - \frac{\sin(\zeta)}{\cos(\zeta)}|1\rangle\langle 0|_A - \frac{\cos(\zeta)}{\sin(\zeta)}|0\rangle\langle 1|_A\right)|\phi\rangle\right\| \leq \sqrt{2\epsilon_1} + \sqrt{\frac{\epsilon}{2}}\left(\frac{1}{\sin(\zeta)} + \frac{1}{\cos(\zeta)}\right).$$

Proof. We address the first line in the lemma as the proof of the second line is essentially the same:

$$\begin{aligned} &\left\| \left(\sin(\zeta)|1\rangle\langle 0|_A - \cos(\zeta)X_B\Pi_B^1\right)|\phi\rangle\right\| \\ =&\left\| \left(\sin(\zeta)|1\rangle\langle 0|_A - \cos(\zeta)|1\rangle\langle 1|_A X_B + \cos(\zeta)|1\rangle\langle 1|_A X_B - \cos(\zeta)X_B\Pi_B^1\right)|\phi\rangle\right\| \\ \leq&\sqrt{\frac{\epsilon_1+\epsilon_2}{2}} + \cos(\zeta)\sqrt{\frac{\epsilon_1}{2}}, \end{aligned}$$

where the inequality uses the triangle inequality and the results from the previous two lemmata. For the second part of the proof, we have

$$\begin{aligned} &\left\| \left(X_B - \frac{\sin(\zeta)}{\cos(\zeta)}|1\rangle\langle 0|_A - \frac{\cos(\zeta)}{\sin(\zeta)}|0\rangle\langle 1|_A\right)|\phi\rangle\right\| \\ &\left\| \left(X_B(\Pi_B^0+\Pi_B^1) - \frac{\sin(\zeta)}{\cos(\zeta)}|1\rangle\langle 0|_A - \frac{\cos(\zeta)}{\sin(\zeta)}|0\rangle\langle 1|_A\right)|\phi\rangle\right\| \\ \leq&\sqrt{2\epsilon_1} + \sqrt{\frac{\epsilon}{2}}\left(\frac{1}{\sin(\zeta)} + \frac{1}{\cos(\zeta)}\right), \end{aligned}$$

thus completing the proof. □

Lemma A4. *If (A1) and $\zeta \in]0, \frac{\pi}{4}]$ is satisfied the following is true:*

$$\begin{aligned}\left\| \left(\frac{\sin(\zeta)}{\cos(\zeta)} |1\rangle\langle 0|_A - \Pi_B^0 X_B \right) |\phi\rangle \right\| &\leq \sqrt{2\epsilon_1} \left(1 + \frac{1}{\sin(2\zeta)} \right) + \sqrt{\frac{\epsilon}{2}} \left(\frac{1}{\sin(\zeta)} + \frac{1}{\cos(\zeta)} \right) \\ \left\| \left(\frac{\cos(\zeta)}{\sin(\zeta)} |0\rangle\langle 1|_A - \Pi_B^1 X_B \right) |\phi\rangle \right\| &\leq \sqrt{2\epsilon_1} \left(1 + \frac{1}{\sin(2\zeta)} \right) + \sqrt{\frac{\epsilon}{2}} \left(\frac{1}{\sin(\zeta)} + \frac{1}{\cos(\zeta)} \right),\end{aligned}$$

for $\epsilon := \epsilon_1 + \epsilon_2$, and thus

$$\left\| \left(|0\rangle\langle 0|_A - X_B \Pi_B^1 X_B \right) |\phi\rangle \right\| \leq \sqrt{\frac{\epsilon_1}{2}} \left(\frac{\cos(\zeta)}{\sin(\zeta)} + 2 \left(1 + \frac{1}{\sin(2\zeta)} \right) \right) + \sqrt{\frac{\epsilon}{2}} \left(\frac{2}{\sin(\zeta)} + \frac{1}{\cos(\zeta)} \right).$$

Proof. We address the first line in the lemma as the proof of the second line is essentially the same:

$$\begin{aligned}\| \left(\frac{\sin(\zeta)}{\cos(\zeta)} |1\rangle\langle 0|_A - \Pi_B^0 X_B \right) |\phi\rangle \| &= \| \left(\frac{\sin(\zeta)}{\cos(\zeta)} |1\rangle\langle 0|_A - \left(\frac{\sin(\zeta)}{\cos(\zeta)} |1\rangle\langle 0|_A + \frac{\cos(\zeta)}{\sin(\zeta)} |0\rangle\langle 1|_A \right) \Pi_B^0 + \\ &\quad \left(\frac{\sin(\zeta)}{\cos(\zeta)} |1\rangle\langle 0|_A + \frac{\cos(\zeta)}{\sin(\zeta)} |0\rangle\langle 1|_A \right) \Pi_B^0 - \Pi_B^0 X_B \right) |\psi\rangle \| \\ &\leq \| \left(\frac{\sin(\zeta)}{\cos(\zeta)} |1\rangle\langle 0|_A - \left(\frac{\sin(\zeta)}{\cos(\zeta)} |1\rangle\langle 0|_A + \frac{\cos(\zeta)}{\sin(\zeta)} |0\rangle\langle 1|_A \right) \Pi_B^0 \right) |\psi\rangle \| \\ &\quad + \sqrt{2\epsilon_1} + \sqrt{\frac{\epsilon}{2}} \left(\frac{1}{\sin(\zeta)} + \frac{1}{\cos(\zeta)} \right),\end{aligned}$$

where Lemma A3 was used in the inequality along with the fact that $\|\Pi_B^0\|_\infty \leq 1$. We now need to provide a bound on the remaining norm, which we now do:

$$\begin{aligned}&\left\| \left(\frac{\sin(\zeta)}{\cos(\zeta)} |1\rangle\langle 0|_A - \left(\frac{\sin(\zeta)}{\cos(\zeta)} |1\rangle\langle 0|_A + \frac{\cos(\zeta)}{\sin(\zeta)} |0\rangle\langle 1|_A \right) \Pi_B^0 \right) |\psi\rangle \right\| \\ \leq\ & \frac{\sin(\zeta)}{\cos(\zeta)} \left\| \left(\left(|1\rangle\langle 0|_A \right) |0\rangle\langle 0|_A - \left(|1\rangle\langle 0|_A \right) \Pi_B^0 \right) |\psi\rangle \right\| + \\ & \frac{\cos(\zeta)}{\sin(\zeta)} \left\| \left(\left(|1\rangle\langle 0|_A \right) |0\rangle\langle 0|_A - \left(|1\rangle\langle 0|_A \right) \Pi_B^0 \right) |\psi\rangle \right\| \\ \leq\ & \left(\frac{\sin(\zeta)}{\cos(\zeta)} + \frac{\cos(\zeta)}{\sin(\zeta)} \right) \sqrt{\frac{\epsilon_1}{2}} = \frac{1}{\sin(2\zeta)} \sqrt{2\epsilon_1},\end{aligned}$$

thus proving the first claim. To prove the final claim we first observe that $X_B \Pi_B^1 X_B = X_B \Pi_B^1 \Pi_B^1 X_B$ and thus

$$\begin{aligned}&\| \left(|0\rangle\langle 0|_A - \frac{\cos(\zeta)}{\sin(\zeta)} |0\rangle\langle 1|_A X_B \Pi_B^1 + \frac{\cos(\zeta)}{\sin(\zeta)} |0\rangle\langle 1|_A X_B \Pi_B^1 - X_B \Pi_B^1 \Pi_B^1 X_B \right) |\psi\rangle \| \\ \leq\ & \| \left(|0\rangle\langle 0|_A - \frac{\cos(\zeta)}{\sin(\zeta)} |0\rangle\langle 1|_A X_B \Pi_B^1 \right) |\psi\rangle \| + \sqrt{2\epsilon_1} \left(1 + \frac{1}{\sin(2\zeta)} \right) + \sqrt{\frac{\epsilon}{2}} \left(\frac{1}{\sin(\zeta)} + \frac{1}{\cos(\zeta)} \right),\end{aligned}$$

where the inequality utilises the first part of the lemma and the fact that $\|X_B\Pi_B^1\|_\infty \leq 1$, and we have that

$$\begin{aligned}
& \left\| \left(|0\rangle\langle 0|_A - \frac{\cos(\zeta)}{\sin(\zeta)} |0\rangle\langle 1|_A X_B \Pi_B^1 \right) |\psi\rangle \right\| \\
= & \left\| \left(|0\rangle\langle 0|_A + (|0\rangle\langle 1|_A |1\rangle\langle 0|_A - |0\rangle\langle 1|_A |1\rangle\langle 0|_A) - \frac{\cos(\zeta)}{\sin(\zeta)} |0\rangle\langle 1|_A X_B \Pi_B^1 \right) |\psi\rangle \right\| \\
= & \left\| \left((|0\rangle\langle 1|_A) |1\rangle\langle 0|_A - \frac{\cos(\zeta)}{\sin(\zeta)} |0\rangle\langle 1|_A X_B \Pi_B^1 \right) |\psi\rangle \right\| \\
\leq & \frac{1}{\sin(\zeta)} \left(\sqrt{\frac{\epsilon}{2}} + \cos(\zeta) \sqrt{\frac{\epsilon_1}{2}} \right),
\end{aligned}$$

where we used Lemma A3 and $\||0\rangle\langle 1|_A\|_\infty \leq 1$ in the last inequality, thus concluding the proof. □

Now we have the useful lemmas, we are in a position to prove Theorem A1. To outline the structure of the proof, we will explicitly construct an isometry Φ_B acting on Bob's system, which introduces an auxiliary qubit system B', and then is a unitary acting on B and B'.

Proof of Theorem A1. We first will explicitly construct the isometry Φ_B that acts upon Bob's system in the statement of the theorem. The isometry introduces an auxiliary qubit system B' in the state $|+\rangle_{B'} = \frac{1}{\sqrt{2}}(|0\rangle_{B'} + |1\rangle_{B'})$ and then applies a unitary $U_{BB'}$ jointly to Bob's system B and B'. The unitary is constructed as $U_{BB'} = \Lambda^X_{BB'}(\mathbb{I}_B \otimes H_{B'})\Lambda^Z_{BB'}$ where $\Lambda^P_{BB'} = |0\rangle\langle 0|_{B'} \otimes \mathbb{I}_B + |1\rangle\langle 1|_{B'} \otimes P_B$ for $P \in \{X, Z\}$ and $H_{B'}$ is the Hadamard applied to qubit B'. Since X_B and Z_B can be shown to be unitaries, one can show that $U_{BB'}$ is unitary. We now take the state $|\psi\rangle$ and apply $\Phi_{BB'}$ to get

$$\begin{aligned}
U_{BB'}|\psi\rangle|+\rangle_{B'} &= \frac{1}{2}\left[|\psi\rangle|0\rangle_{B'} + X_B|\psi\rangle|1\rangle_{B'} + Z_B|\psi\rangle|0\rangle_{B'} - X_BZ_B|\psi\rangle|1\rangle_{B'}\right] \\
&= \Pi_B^0|\psi\rangle|0\rangle_{B'} + X_B\Pi_B^1|\psi\rangle|1\rangle_{B'},
\end{aligned}$$

using the fact that $\Pi_B^x = \frac{1}{2}\left(\mathbb{I}_B + (-1)^x Z_B\right)$ for $x \in \{0, 1\}$. Therefore, in the first line of the statement of the theorem, we need to bound

$$\|\Phi_B(|\psi\rangle) - |\zeta\rangle_{AB'}|\text{anc}\rangle_{E'}\| = \|\Pi_B^0|\psi\rangle|0\rangle_{B'} + X_B\Pi_B^1|\psi\rangle|1\rangle_{B'} - |\zeta\rangle_{AB'}|\text{anc}\rangle_{E'}\|, \tag{A3}$$

and from Lemmata A1 and A3, we have the following useful identity:

$$\|(\Pi_B^0 - |0\rangle\langle 0|_A)|\psi\rangle|0\rangle_{B'} + (X_B\Pi_B^1 - \tan(\zeta)|1\rangle\langle 0|_A)|\psi\rangle|1\rangle_{B'}\| \leq \sqrt{2\epsilon_1} + \frac{1}{\cos(\zeta)}\sqrt{\frac{\epsilon}{2}}.$$

We can use this identity to give the bound on (A3) of

$$\begin{aligned}
& \|(\Pi_B^0|0\rangle_{B'} + X_B\Pi_B^1|1\rangle_{B'})|\psi\rangle - |\zeta\rangle_{AB'}|\text{anc}\rangle_{E'}\| \\
\leq & \sqrt{2\epsilon_1} + \frac{1}{\cos(\zeta)}\sqrt{\frac{\epsilon}{2}} + \|(|0\rangle\langle 0|_A|\psi\rangle|0\rangle_{B'} + (\tan(\zeta)|1\rangle\langle 0|_A)|\psi\rangle|1\rangle_{B'} - |\zeta\rangle_{AB'}|\text{anc}\rangle_{E'}\|,
\end{aligned}$$

and by the Schmidt decomposition we also have $|\psi\rangle = \alpha|0\rangle_A|\psi_0\rangle_{BE} + \beta|1\rangle_A|\psi_1\rangle_{BE}$ for α and β being real positive numbers and $|\psi_0\rangle$ being orthogonal to $|\psi_1\rangle$. Utilising this fact we have

$$\begin{aligned}
|0\rangle\langle 0|_A|\psi\rangle|0\rangle_{B'} + (\tan(\zeta)|1\rangle\langle 0|_A)|\psi\rangle|1\rangle_{B'} &= \alpha|0\rangle_A|\psi_0\rangle_B|0\rangle_{B'} + \alpha\tan(\zeta)|1\rangle_A|\psi_0\rangle_B|1\rangle_{B'} \\
&= (|00\rangle + \tan(\zeta)|11\rangle)_{AB'}(\alpha|\psi_0\rangle) \\
&:= |\zeta'\rangle(\alpha|\psi_0\rangle),
\end{aligned}$$

where $\langle\zeta'|\zeta\rangle = 1+\tan^2(\zeta)$ and $\langle\zeta|\zeta'\rangle = \langle\zeta'|\zeta\rangle = \cos(\zeta)+\sin(\zeta)\tan(\zeta)$. Therefore, if we set $|\text{anc}\rangle_{E'}|\psi_0\rangle_{BE}$ then:

$$\begin{aligned}
& \|(|0\rangle\langle 0|_A|\psi\rangle|0\rangle_{B'} + (\tan(\zeta)|1\rangle\langle 0|_A)|\psi\rangle|1\rangle_{B'} - |\zeta\rangle_{AB'}|\text{anc}\rangle_{E'}\| \\
= & \sqrt{1+\alpha^2(1+\tan^2(\zeta)) - 2\alpha(\cos(\zeta)+\sin(\zeta)\tan(\zeta))} \\
= & 1-\alpha\sec(\zeta) \\
\leq & 1-\sec(\zeta)\sqrt{\cos^2(\zeta)-\frac{\epsilon_1}{2}} \\
= & 1-\sqrt{1-\frac{\epsilon_1}{2\cos^2(\zeta)}} \\
\leq & \frac{\sqrt{\epsilon_1}}{\sqrt{2}\cos(\zeta)},
\end{aligned}$$

where in the second line we use the fact that $\langle\tau_Z^A\rangle = 2\langle\psi|(|0\rangle\langle 0|_A)|\psi\rangle - 1 = 2\alpha^2 - 1$ and thus by virtue of (A1) being satisfied we have $|\alpha^2 - \cos^2(\zeta)| \leq \frac{\epsilon_1}{2}$. In principle this allows the system BE to be isomorphic to the system E' under the action of this isometry. Putting all of this together we have

$$\|\Phi_B(|\psi\rangle) - |\zeta\rangle_{AB'}|\text{anc}\rangle_{E'}\| \leq \sqrt{\epsilon_1}\left(\sqrt{2}+\frac{1}{\sqrt{2}\cos(\zeta)}\right) + \frac{1}{\cos(\zeta)}\sqrt{\frac{\epsilon}{2}} \leq \sqrt{\epsilon_1}(\sqrt{2}+1)+\sqrt{\epsilon},$$

where in the final inequality we used the fact that $\cos(\zeta) \geq \frac{1}{\sqrt{2}}$ for $\zeta \in]0, \frac{\pi}{4}]$, thus concluding the proof for the first line of Theorem A1.

For the second line of the proof for Theorem A1, thus we need to bound the following expression:

$$\|\Phi_B(X_B|\psi\rangle) - |\zeta\rangle_{AB'}|\text{anc}\rangle_{E'}\| = \|\Pi_B^0 X_B|\psi\rangle|0\rangle_{B'} + X_B\Pi_B^1 X_B|\psi\rangle|1\rangle_{B'} - \tau_X^{B'}|\zeta\rangle_{AB'}|\text{anc}\rangle_{E'}\|.$$

To provide an upper bound to the right-hand-side we have that

$$\begin{aligned}
& \|\Pi_B^0 X_B|\psi\rangle|0\rangle_{B'} + X_B\Pi_B^1 X_B|\psi\rangle|1\rangle_{B'} - \tau_X^{B'}|\zeta\rangle_{AB'}|\text{anc}\rangle_{E'}\| \\
\leq & \left\| \left(\Pi^0 X_B - \frac{\sin(\zeta)}{\cos(\zeta)}|1\rangle\langle 0|_A\right)|\psi\rangle|0\rangle_{B'}\right\| + \left\| \left(X_B\Pi_B^1 X_B - |0\rangle\langle 0|_A\right)|\psi\rangle|1\rangle_{B'}\right\| \\
+ & \left\|\frac{\sin(\zeta)}{\cos(\zeta)}|1\rangle\langle 0|_A|\psi\rangle|0\rangle_{B'} + |0\rangle\langle 0|_A|\psi\rangle|1\rangle_{B'} - \tau_X^{B'}|\zeta\rangle_{AB'}|\text{anc}\rangle_{E'}\right\| \\
\leq & \sqrt{\epsilon_1}\left[2\sqrt{2}\left(1+\frac{1}{\sin(2\zeta)}\right)+\frac{\cos(\zeta)}{2\sin(\zeta)}\right] + \sqrt{\frac{\epsilon}{2}}\left[\frac{3}{\sin(\zeta)}+\frac{2}{\cos(\zeta)}\right] \\
+ & \left\|\frac{\sin(\zeta)}{\cos(\zeta)}|1\rangle\langle 0|_A|\psi\rangle|0\rangle_{B'} + |0\rangle\langle 0|_A|\psi\rangle|1\rangle_{B'} - \tau_X^{B'}|\zeta\rangle_{AB'}|\text{anc}\rangle_{E'}\right\|,
\end{aligned}$$

where the first inequality is just resulting from the triangle inequality and the second inequality is an application of Lemma A4. The final term we need to bound is

$$\begin{aligned}
& \left\|\frac{\sin(\zeta)}{\cos(\zeta)}|1\rangle\langle 0|_A|\psi\rangle|0\rangle_{B'} + |0\rangle\langle 0|_A|\psi\rangle|1\rangle_{B'} - \tau_X^{B'}|\zeta\rangle_{AB'}|\text{anc}\rangle_{E'}\right\| \\
= & \left\|\tau_X^{B'}\left(\alpha(\tan(\zeta)|11\rangle_{AB'} + |00\rangle_{AB'})|\psi_0\rangle_B - |\zeta\rangle_{AB'}|\text{anc}\rangle_{E'}\right)\right\| \\
= & \left\|\left[(\tan(\zeta)|11\rangle_{AB'} + |00\rangle_{AB'})(\alpha|\psi_0\rangle_B) - |\zeta\rangle_{AB'}|\text{anc}\rangle_{E'}\right]\right\| \\
\leq & \frac{\sqrt{\epsilon_1}}{\sqrt{2}\cos(\zeta)},
\end{aligned}$$

where the first inequality is a consequence of the aforementioned Schmidt decomposition and the second equality results from the fact that $\tau_X^{B'}$ is a unitary, and the final inequality is just the bound derived earlier for the same norm. Putting all of this together we then get the bound

$$\begin{aligned} & \|\Phi_B(\otimes X_B|\psi\rangle) - \tau_X^{B'}|\zeta\rangle_{AB'}|\text{anc}\rangle_{E'}\| \\ \leq\ & \sqrt{\epsilon_1}\left[2\sqrt{2}\left(1+\frac{1}{\sin(2\zeta)}\right)+\frac{\cos(\zeta)}{2\sin(\zeta)}+\frac{1}{\sqrt{2}\cos(\zeta)}\right]+\sqrt{\frac{\epsilon}{2}}\left[\frac{3}{\sin(\zeta)}+\frac{2}{\cos(\zeta)}\right] \\ \leq\ & \sqrt{\epsilon_1}\left(2\sqrt{2}+1+\frac{5}{2\sin(\zeta)}\right)+\sqrt{\epsilon}\left(\frac{3}{\sqrt{2}\sin(\zeta)}+2\right), \end{aligned}$$

where the last inequality utilised the fact that $1 > \cos(\zeta) \geq \frac{1}{\sqrt{2}}$ as outlined earlier. □

Corollary A1. *For Alice, Bob, and Eve sharing the state $|\psi\rangle$ then for Bob making the measurement associated with the observable X_B and for Eve making a dichotomic measurement $\{M_z, \mathbb{I}_E - M_z\}$ with M_z being the POVM associated with Eve's guess z of Bob's measurement outcome, then Eve's maximum probability of guessing Bob's outcome is*

$$p_{guess} = \max_{\{|\psi\rangle, M_z, X_B\}} \sum_{z\in\{0,1\}} \frac{1}{2}\langle\psi|(1+(-1)^z X_B)M_z|\psi\rangle,$$

and if Alice and Bob's statistics satisfy the criteria in (A1) and $\zeta \in]0, \frac{\pi}{4}]$, then

$$p_{guess} \leq \frac{1}{2} + \sqrt{\epsilon_1}\left(3\sqrt{2}+2+\frac{5}{2\sin(\zeta)}\right)+3\sqrt{\epsilon_1+\epsilon_2}\left(\frac{1}{\sqrt{2}\sin(\zeta)}+1\right).$$

Proof. Starting with the definition of p_{guess} and $\sum_z M_z = \mathbb{I}_E$ in the statement we have that

$$p_{\text{guess}} = \frac{1}{2} + \frac{1}{2}\max_{\{|\psi\rangle, M_z, X_B\}} \langle\psi|X_B \otimes (M_0 - M_1)|\psi\rangle.$$

Since the statistics of Alice and Bob satisfy (A1) then Theorem A1 implies that there exists an isometry that (up to some error) maps $|\psi\rangle$ to $|\zeta\rangle|\text{anc}\rangle$ and $X_B|\psi\rangle$ to $\tau_X|\zeta\rangle|\text{anc}\rangle$. Isometries do not change probabilities so we have that

$$\begin{aligned} p_{\text{guess}} &= \frac{1}{2} + \frac{1}{2}\max_{\{|\psi\rangle, M_z, X_B\}} \Phi_B^\dagger(\langle\psi|) \otimes (M_0 - M_1)\Phi_B(X_B|\psi\rangle) \\ &\leq \frac{1}{2} + \sqrt{\epsilon_1}\left(3\sqrt{2}+2+\frac{5}{2\sin(\zeta)}\right)+3\sqrt{\epsilon_1+\epsilon_2}\left(\frac{1}{\sqrt{2}\sin(\zeta)}+1\right) \\ &+ \langle\zeta_{AB'}|\tau_X^{B'}|\zeta_{AB'}\rangle \max_{\{|\psi\rangle, M_z\}} \langle\text{anc}|(M_0 - M_1)|\text{anc}\rangle \\ &\leq \frac{1}{2} + \sqrt{\epsilon_1}\left(3\sqrt{2}+2+\frac{5}{2\sin(\zeta)}\right)+3\sqrt{\epsilon_1+\epsilon_2}\left(\frac{1}{\sqrt{2}\sin(\zeta)}+1\right), \end{aligned}$$

where the inequality in the second line is through applying (via the triangle inequality) both of the self-testing results in Theorem A1 along with the fact that $\|(M_0 - M_1)\|_\infty \leq 1$, and the second inequality comes from the fact that $\|(M_0 - M_1)\|_\infty \leq 1$ and that $\langle\zeta_{AB'}|\tau_X^{B'}|\zeta_{AB'}\rangle = 0$. □

If we consider one round of our particular scheme then (up to local unitaries) Alice and Bob share the state $|\zeta\rangle = \cos(\zeta)|00\rangle + \sin(\zeta)|11\rangle$ and Bob makes a measurement from two possible measurements with observables Z_B and X_B, where $Z = \tau_Z$ and X is associated with

POVM elements $\{\cos^2(\xi)|+\rangle\langle+| + \sin^2(\xi)|-\rangle\langle-|, \cos^2(\xi)|-\rangle\langle-| + \sin^2(\xi)|+\rangle\langle+|\}$ such that Bob's observable is $X = \cos(2\xi)\tau_X$. Given this scheme, we have the following correlations:

$$\begin{aligned} \langle \tau_Z^A \otimes Z_B \rangle &= 1 \\ \langle \tau_X^A \otimes X_B \rangle &= \sin(2\zeta)\cos(2\xi) \\ \langle \tau_Z^A \rangle &= \cos(2\zeta). \end{aligned}$$

Thus this scheme will pass the statistical criteria in (A1) with $\epsilon_1 = 0$ and $\epsilon_2 = 2\sin^2(\xi)$, and a guessing probability of

$$p_{\text{guess}} \leq \frac{1}{2} + 3\sin(\xi)\left(\frac{1}{\sin(\zeta)} + \sqrt{2}\right).$$

We will return to this observation later on, but first we need to now consider the case of Bob making a sequence of measurements. Recall that in our scheme described in Section 4, after each ith measurement made by Bob, the state shared between Alice and Bob is (after Bob's post-measurement unitary corrections)

$$|\psi_{b^i|y^i}\rangle = U_A^{b^i|y^i} \otimes \mathbb{I}_B \left(\cos(\zeta_{b^i|y^i})|00\rangle + \sin(\zeta_{b^i|y^i})|11\rangle\right), \tag{A4}$$

where $b^i|y^i$ is the bit-string of outcomes of Bob's sequence of measurements from round 1 to round i, also $U_A^{b^i|y^i}$ and $\zeta_{b^i|y^i}$ depend on the initial state shared by Alice and Bob and Bob's sequence of measurement outcomes (and the type of measurement). By convention, we have that b^0 is the empty string. The important thing is that we know in an honest implementation of our scheme what the values of $U_A^{b^i|y^i}$ and $\zeta_{b^i|y^i}$ will be. If we want to certify randomness from the sequence of measurements we need statistical criteria for Alice and Bob such that if they pass, we are guaranteed randomness. This statistical criteria will be that in round $i+1$ of the sequence of measurements, Alice and Bob's statistics need to satisfy:

$$\begin{aligned} |\langle U_A^{b^i|y^i} \tau_Z^A \left(U_A^{b^i|y^i}\right)^\dagger \otimes Z_B^{b^i|y^i} \rangle - 1| &\leq \epsilon_1^{i+1} \\ |\langle U_A^{b^i|y^i} \tau_X^A \left(U_A^{b^i|y^i}\right)^\dagger \otimes X_B^{b^i|y^i} \rangle - \sin(2\zeta_{b^i|y^i})| &\leq \epsilon_2^{i+1} \\ |\langle U_A^{b^i|y^i} \tau_Z^A \left(U_A^{b^i|y^i}\right)^\dagger \rangle - \cos(2\zeta_{b^i|y^i})| &\leq \epsilon_1^{i+1}. \end{aligned} \tag{A5}$$

We can now state a useful corollary of Theorem A1 (and Corollary A1).

Corollary A2. *After Bob makes i measurements yielding the outcomes $b^i|y^i$, Alice, Bob and Eve share some quantum state $|\phi_{b^i|y^i}\rangle$, then for Bob making the measurement associated with the observable X_B and for Eve making a dichotomic measurement $\{M_z, \mathbb{I}_E - M_z\}$ with M_z being the POVM associated with Eve's guess z of Bob's measurement outcome, then Eve's probability of guessing Bob's outcome is*

$$p_{guess} = \max_{\{|\phi_{b^i|y^i}\rangle, M_z, X_B\}} \sum_{z\in\{0,1\}} \frac{1}{2}\langle\phi_{b^i|y^i}|(1+(-1)^z X_B)M_z|\phi_{b^i|y^i}\rangle,$$

and if Alice and Bob's statistics satisfy the criteria in (A5), then

$$p_{guess} \leq \frac{1}{2} + \sqrt{\epsilon_1^{i+1}}\left(3\sqrt{2} + 2 + \frac{5}{2\sin(\zeta_{b^i|y^i})}\right) + 3\sqrt{\epsilon_1^{i+1} + \epsilon_2^{i+1}}\left(\frac{1}{\sqrt{2}\sin(\zeta_{b^i|y^i})} + 1\right).$$

Proof. First notice that the statistical criteria in (A5) is equivalent to (A1) up to a local unitary $U_A^{b^i|y^i}$ on Alice's system. This local unitary can be simulated by applying the inverse of this operation to Alice's part of the state that Alice and Bob share. The self-testing results in Theorem A1 will now hold for the state $U_A^{b^i|y^i} \otimes \mathbb{I}_{B'}|\zeta\rangle_{AB'}$ instead of $|\zeta\rangle_{AB'}$ since the norms are invariant under the action of unitaries. Given this, one can apply the result from Corollary A1 to complete the proof. □

This result quantifies the randomness of each round of our scheme. Now, if we consider the scheme in general, there is a sequence of measurements made by Bob, and we want to bound Eve's probability to guess the total string b of Bob's outcomes. The following result gives us a bound on this probability.

Corollary A3. *For Bob making a sequence of measurements yielding the outcome bit-string b, if Alice, Bob, and Eve share some initial state $|\psi\rangle$, Bob's measurement in round i is associated with observable $X_B^{b^i|y^i}$, and Eve makes a measurement associated with operators $\{M_z\}_z$, where z is Eve's guess of Bob's outcome b, the probability of guessing it correctly is*

$$p_{guess} = \max_{\{|\psi\rangle, M_z, \{X_B^{b^i|y^i}\}\}} \sum_{b,z} \delta_z^b P_{|\psi\rangle}(z, b|\{X_B^{b^i|y^i}\}_i),$$

and if for each i, there exist unitaries $U_A^{b^i|y^i}$ and angles $\zeta_{b^i|y^i}$ such that the statistical criteria in (A5) is satisfied, then

$$p_{guess} \leq \prod_{i=1}^{n} \left(\frac{1}{2} + \sqrt{\epsilon_1^i} \left(3\sqrt{2} + 2 + \frac{5}{2\sin(\zeta_{b^{i-1}|y^{i-1}})} \right) + 3\sqrt{\epsilon_1^i + \epsilon_2^i} \left(\frac{1}{\sqrt{2}\sin(\zeta_{b^{i-1}|y^{i-1}})} + 1 \right) \right), \quad \text{(A6)}$$

and if $\epsilon_1^i = 0$ for all i, then

$$p_{guess} \leq \prod_{i=1}^{n} \left(\frac{1}{2} + 3\sqrt{\epsilon_2^i} \left(\frac{1}{\sqrt{2}\sin(\zeta_{b^{i-1}|y^{i-1}})} + 1 \right) \right). \quad \text{(A7)}$$

Proof. First we can rewrite p_{guess} as

$$\max_{\{|\psi\rangle, M_z, \{X_B^i\}\}} \sum_{b_1,z} \delta_{z_1}^{b_1} P_{|\psi\rangle}(b_1, z|X_B^1) \sum_{b_2} \delta_{z_2}^{b_2} P_{|\psi\rangle}(b_2, z|\{X_B^i\}_{i\leq 2}, b_1) \ldots \sum_{b_n} \delta_{z_n}^{b_n} P_{|\psi\rangle}(b_n, z|\{X_B^i\}_{i\leq n}, b^{n-1}),$$

by applying Bayes' theorem and then the constraints from causality; roughly that outcome b_i cannot be affected by outcome b_j if $j > i$. Using this structure we have that

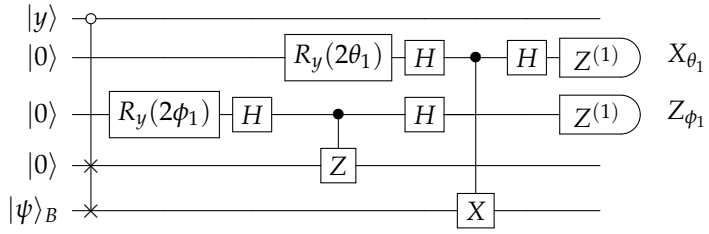
$$p_{\text{guess}} \leq \prod_{j=1}^{n} \left(\max_{\{|\psi\rangle, M_z, \{X_B^i\}\}} \sum_{b_j,z} \delta_{z_j}^{b_j} P_{|\psi\rangle}(b_j, z|\{X_B^i\}_{i\leq j}, b^{j-1}) \right),$$

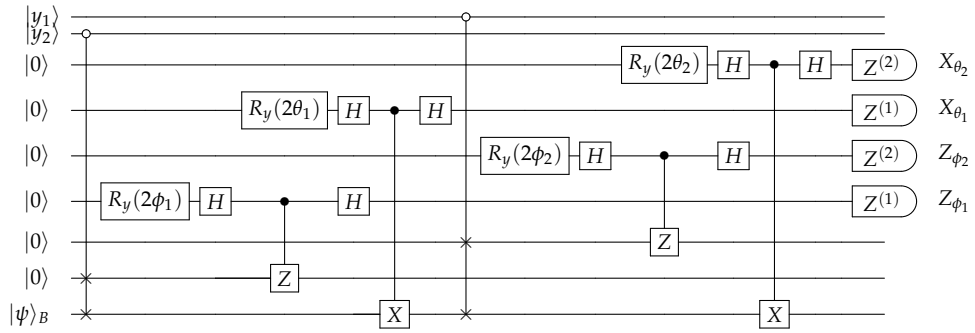
where there are now multiple maximizations, essentially for each summand of p_{guess}. Now notice that the sum over strings z along with the probability in the summand can be interpreted as a coarse-grained measurement by Eve. To wit, Eve makes a measurement with outcomes corresponding to each string z, and for each b_j, Eve will produce a guess of this based on the value of z_j. For example, if Eve generates a string z such that $z_j = 0$ then Eve's guess of b_j is 0. This then reduces each maximisation to the guessing probability for each round, and thus from Corollary A3 we have the statement. □

This final corollary gives us the proof of Theorem 1 in the main body of the paper.

Appendix B. Alternative Quantum Circuit for Sequences of Measurements

The following circuit can be used to implement the sequence of non-projective measurements in Bob's device, in which the measurement choices are encoded in quantum states in the computational basis, as an alternative to the classically controlled version given in the main text. This circuit only implement Bob's half of the protocol on his quantum state denoted by ρ_B, which is prepared for him by Eve. Alice's part in the protocol is simply to do state tomography on her steered state so this is excluded from the circuit. These circuits measure the state for one, and two rounds respectively with a generalisation to higher rounds straightforward.





References

1. Bell, J.S. On the Einstein Podolsky Rosen paradox. *Phys. Phys. Fiz.* **1964**, *1*, 195–200, doi:10.1103/PhysicsPhysiqueFizika.1.195. [CrossRef]
2. Hensen, B.; Bernien, H.; Dréau, A.E.; Reiserer, A.; Kalb, N.; Blok, M.S.; Ruitenberg, J.; Vermeulen, R.F.L.; Schouten, R.N.; Abellán, C.; et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* **2015**, *526*, 682–686, doi:10.1038/nature15759. [CrossRef]
3. Pironio, S.; Acín, A.; Massar, S.; Giroday, A.B.d.l.; Matsukevich, D.N.; Maunz, P.; Olmschenk, S.; Hayes, D.; Luo, L.; Manning, T.A.; Monroe, C. Random numbers certified by Bell's theorem. *Nature* **2010**, *464*, 1021, doi:10.1038/nature09008. [CrossRef] [PubMed]
4. Colbeck, R. Quantum And Relativistic Protocols For Secure Multi-Party Computation. *arXiv* **2009**, arXiv:0911.3814.
5. Cavalcanti, D.; Skrzypczyk, P. Quantum steering: A review with focus on semidefinite programming. *Rep. Prog. Phys.* **2017**, *80*, 024001, doi:10.1088/1361-6633/80/2/024001. [CrossRef] [PubMed]
6. Wiseman, H.M.; Jones, S.J.; Doherty, A.C. Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox. *Phys. Rev. Lett.* **2007**, *98*, 140402, doi:10.1103/PhysRevLett.98.140402. [CrossRef]
7. Curchod, F.J.; Johansson, M.; Augusiak, R.; Hoban, M.J.; Wittek, P.; Acín, A. Unbounded randomness certification using sequences of measurements. *Phys. Rev. A* **2017**, *95*, 020102, doi:10.1103/PhysRevA.95.020102. [CrossRef]
8. Acín, A.; Pironio, S.; Vértesi, T.; Wittek, P. Optimal randomness certification from one entangled bit. *Phys. Rev. A* **2016**, *93*, 040102, doi:10.1103/PhysRevA.93.040102. [CrossRef]
9. Coyle, B.; Hoban, M.J.; Kashefi, E. One-Sided Device-Independent Certification of Unbounded Random Numbers. *Electron. Proc. Theor. Comput. Sci.* **2018**, *273*, 14–26. doi:10.4204/EPTCS.273.2. [CrossRef]

10. Skrzypczyk, P.; Cavalcanti, D. Maximal Randomness Generation from Steering Inequality Violations Using Qudits. *Phys. Rev. Lett.* **2018**, *120*, 260401, doi:10.1103/PhysRevLett.120.260401. [CrossRef]
11. Passaro, E.; Cavalcanti, D.; Skrzypczyk, P.; Acín, A. Optimal randomness certification in the quantum steering and prepare-and-measure scenarios. *New J. Phys.* **2015**, *17*, 113010, doi:10.1088/1367-2630/17/11/113010. [CrossRef]
12. Pawłowski, M.; Brunner, N. Semi-device-independent security of one-way quantum key distribution. *Phys. Rev. A* **2011**, *84*, 010302, doi:10.1103/PhysRevA.84.010302. [CrossRef]
13. Van Himbeeck, T.; Woodhead, E.; Cerf, N.J.; García-Patrón, R.; Pironio, S. Semi-device-independent framework based on natural physical assumptions. *Phys. Rev. A* **2011**, *84*, 010302, doi:10.1103/PhysRevA.84.010302. [CrossRef]
14. Rusca, D.; van Himbeeck, T.; Martin, A.; Brask, J.B.; Pironio, S.; Brunner, N.; Zbinden, H. Quantum random number generation with partially characterized devices based on bounded energy. In Proceedings of the Quantum Information and Measurement (QIM) V: Quantum Technologies, Rome Italy, 4–6 April 2019.
15. Lunghi, T.; Brask, J.B.; Lim, C.C.W.; Lavigne, Q.; Bowles, J.; Martin, A.; Zbinden, H.; Brunner, N. Self-Testing Quantum Random Number Generator. *Phys. Rev. Lett.* **2015**, *114*, 150501, doi:10.1103/PhysRevLett.114.150501. [CrossRef] [PubMed]
16. Law, Y.Z.; Thinh, L.P.; Bancal, J.D.; Scarani, V. Quantum randomness extraction for various levels of characterization of the devices. *J. Phys. A Math. Theor.* **2014**, *47*, 424028, doi:10.1088/1751-8113/47/42/424028. [CrossRef]
17. Nieto-Silleras, O.; Pironio, S.; Silman, J. Using complete measurement statistics for optimal device-independent randomness evaluation. *New J. Phys.* **2014**, *16*, 013035, doi:10.1088/1367-2630/16/1/013035. [CrossRef]
18. Sainz, A.B.; Hoban, M.J.; Skrzypczyk, P.; Aolita, L. Bipartite post-quantum steering in generalised scenarios. *arXiv* **2019**, arXiv:1907.03705.
19. Šupić, I.; Hoban, M.J. Self-testing through EPR-steering. *New J. Phys.* **2016**, *18*, 075006, doi:10.1088/1367-2630/18/7/075006. [CrossRef]
20. Skrzypczyk, P.; Navascués, M.; Cavalcanti, D. Quantifying Einstein-Podolsky-Rosen Steering. *Phys. Rev. Lett.* **2014**, *112*, 180404, doi:10.1103/PhysRevLett.112.180404. [CrossRef]
21. Code to Accompany "Quantum Steering: A Short Review with Focus on Semi-Definite Programming". Available online: https://github.com/paulskrzypczyk/steeringreview (accessed on 1 October 2019).
22. Nigmatullin, R.; Ballance, C.J.; Beaudrap, N.D.; Benjamin, S.C. Minimally complex ion traps as modules for quantum communication and computing. *New J. Phys.* **2016**, *18*, 103028, doi:10.1088/1367-2630/18/10/103028. [CrossRef]
23. Hucul, D.; Inlek, I.V.; Vittorini, G.; Crocker, C.; Debnath, S.; Clark, S.M.; Monroe, C. Modular entanglement of atomic qubits using photons and phonons. *Nat. Phys.* **2014**, *11*, 37–42. [CrossRef]
24. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed.; Cambridge University Press: New York, NY, USA, 2011.
25. Sangouard, N.; Bancal, J.D.; Gisin, N.; Rosenfeld, W.; Sekatski, P.; Weber, M.; Weinfurter, H. Loophole-free Bell test with one atom and less than one photon on average. *Phys. Rev. A* **2011**, *84*, 052122, doi:10.1103/PhysRevA.84.052122. [CrossRef]
26. Teo, C.; Araújo, M.; Quintino, M.T.; Minář, J.; Cavalcanti, D.; Scarani, V.; Terra Cunha, M.; França Santos, M. Realistic loophole-free Bell test with atom–photon entanglement. *Nat. Commun.* **2013**, *4*, 2104, doi:10.1038/ncomms3104. [CrossRef] [PubMed]
27. Teo, C.; Minář, J.; Cavalcanti, D.; Scarani, V. Analysis of a proposal for a realistic loophole-free Bell test with atom-light entanglement. *Phys. Rev. A* **2013**, *88*, 053848, doi:10.1103/PhysRevA.88.053848. [CrossRef]
28. Pfaff, W.; Hensen, B.; Bernien, H.; van Dam, S.B.; Blok, M.S.; Taminiau, T.H.; Tiggelman, M.J.; Schouten, R.N.; Markham, M.; Twitchen, D.J.; et al. Unconditional quantum teleportation between distant solid-state qubits. *Science* **2014**, *345*, 532–535, doi:10.1126/science.1253512. [CrossRef] [PubMed]
29. Smith, R.S.; Curtis, M.J.; Zeng, W.J. A Practical Quantum Instruction Set Architecture. *arXiv* **2016**, arXiv:1608.03355.
30. Schmied, R. Quantum state tomography of a single qubit: Comparison of methods. *J. Mod. Opt.* **2016**, *63*, 1744–1758, doi:10.1080/09500340.2016.1142018. [CrossRef]

31. Grant, M.; Boyd, S. Graph implementations for nonsmooth convex programs. In *Recent Advances in Learning and Control*; Blondel, V., Boyd, S., Kimura, H., Eds.; Lecture Notes in Control and Information Sciences; Springer, London, UK, 2008; pp. 95–110.
32. Johnston, N. QETLAB: A MATLAB Toolbox for Quantum Entanglement, Version 0.9. 2016. Available online: http://www.qetlab.com/Main_Page (accessed on 1 October 2019). [CrossRef]
33. MSc Project Codes For 1SDI Certification of Random Numbers. 2017. Available online: https://github.com/BrianCoyle/TPMScProject2017 (accessed on 1 October 2019).

© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).