Device-independent two-party cryptography secure against sequential attacks

2016 New J. Phys. 18 055004

(http://iopscience.iop.org/1367-2630/18/5/055004)

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
25 January 2016

REVISED
28 March 2016

ACCEPTED FOR PUBLICATION
12 April 2016

PUBLISHED
6 May 2016

PAPER

Device-independent two-party cryptography secure against sequential attacks

Jędrzej Kaniewski[1,2] and Stephanie Wehner[2]

[1] Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543
[2] QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands

E-mail: jkaniewski@math.ku.dk

Keywords: quantum cryptography, device-independent, two-party cryptography, CHSH inequality, uncertainty, nonlocality

Abstract

The goal of two-party cryptography is to enable two parties, Alice and Bob, to solve common tasks without the need for mutual trust. Examples of such tasks are private access to a database, and secure identification. Quantum communication enables security for all of these problems in the noisy-storage model by sending more signals than the adversary can store in a certain time frame. Here, we initiate the study of device-independent (DI) protocols for two-party cryptography in the noisy-storage model. Specifically, we present a relatively easy to implement protocol for a cryptographic building block known as weak string erasure and prove its security even if the devices used in the protocol are prepared by the dishonest party. DI two-party cryptography is made challenging by the fact that Alice and Bob do not trust each other, which requires new techniques to establish security. We fully analyse the case of memoryless devices (for which sequential attacks are optimal) and the case of sequential attacks for arbitrary devices. The key ingredient of the proof, which might be of independent interest, is an explicit (and tight) relation between the violation of the Clauser–Horne–Shimony–Holt inequality observed by Alice and Bob and uncertainty generated by Alice against Bob who is forced to measure his system before finding out Alice's setting (guessing with postmeasurement information). In particular, we show that security is possible for arbitrarily small violation.

1. Introduction

Quantum key distribution (QKD) [BB84, Eke91] allows two honest parties, Alice and Bob, to protect their communication from a nosy eavesdropper. Yet, there are many other tasks that Alice and Bob may wish to solve, in which they themselves do not trust each other and secure identification is one such example. Here, Alice wants to identify herself to Bob without revealing her password. Bit commitment and oblivious transfer constitute other well-known examples of such tasks.

It is intuitive that security for two-party cryptographic protocols is more difficult to achieve than for QKD, since Alice and Bob cannot help each other to check on the eavesdropper. Instead, every party has to fend for himself. It turns out that even using quantum communication Alice and Bob cannot achieve security without making additional assumptions [Col07, LC97, Lo97, May97]. Usually one relies on computational assumptions, i.e. that solving a computational puzzle requires a large amount of computing resources, namely more than is available to the adversary. Instead of relying on computational assumptions, however, it is possible to make physically motivated assumptions, for example that the adversary's ability to store information is limited. Introducing such storage restrictions was pioneered by Maurer [Mau91], who considered imposing a restriction on the adversary's ability to store *classical* bits known as the bounded-storage model. Unfortunately, the fact that (i) classical storage is cheap and plentiful and (ii) the gap between what the honest parties need to implement the protocol and what a dishonest party needs to break it is only polynomial [Cac97], renders this model less practical. In contrast, storing quantum information reliably is an extremely difficult problem, motivating the so-called bounded-quantum storage [DFSS05, DFR$^+$07] or more generally noisy-storage model

[KWW12, WST08]. The noisy-storage model admits protocols that require no quantum storage for the honest execution and that can be implemented in a manner similar to QKD using BB84 [DFW15, KWW12, WST08], six-state [BFW14] or continuous variable [FSW15] encodings. Significantly, security can always be achieved as long as the number of qubits n sent in the protocol is only slightly larger than the number of qubits r that the adversary can store, that is, whenever $r \lesssim n - O(\log n)$ [DFW15], which is essentially optimal. First implementations of bit commitment [NJM+12] and oblivious transfer [ENG+14] in the noisy-storage model have been demonstrated. Note that there exist other assumptions that make two-party cryptography possible, e.g. that the two parties are given access to guaranteed additional resources [Cré97,Riv99, WNI03,], or that they must delegate agents who cannot communicate during the protocol (which might be motivated by special relativity) [BGKW88, CSST11, KTHW13, Kan15, Ken05, Ken11, Ken12, Ken99, Sim07]. The noisy-storage model is particularly interesting since in contrast to computational or relativistic assumptions, security is preserved even if the assumption is invalidated at a later point. That is, security cannot be broken retroactively if the adversary acquires a larger quantum storage device in the future, making this assumption completely future-proof.

One of the central questions in (quantum) cryptography is finding the minimal assumptions which are sufficient to guarantee security. For example in the standard QKD scenario we assume that the quantum channel between Alice and Bob is untrusted (i.e. it is fully controlled by the eavesdropper) but the devices used by Alice and Bob inside their laboratories are fully characterised. Already early on, however, it was recognised that violation of a Bell inequality is intimately linked to cryptographic security [Eke91]. Mayers and Yao [MY04, MY98] went on to realise that quantum states can be *self-tested*, i.e. that certain quantum properties can be verified by a purely classical user, which started the field of *device-independent* (DI) quantum cryptography. In DI cryptography instead of assuming that we know how the devices work, we simply test them during the protocol by using them to exhibit Bell non-locality [BCP+14]. DI cryptography has been one of the most active research topics within quantum cryptography, predominantly in the context of QKD [AGM06, ABG+07, ARKP15, BHK05, BCK13, MS14a, MS14b, RUV13, VV14] and randomness expansion or amplification [BPPP14, CK10, CVY13, MS14a, MS14b, PAM+10,VV12].

DI two-party cryptography, on the other hand, remains a largely unexplored territory. Security of a protocol for imperfect coin flipping and bit commitment has been analysed in the DI regime [AMPS15, SCA+11]. Significantly, the setting considered by these works is different: since the authors do not impose any extra assumptions, they cannot hope to reach the perfect primitive so they aim for an imperfect implementation instead. Moreover, Adlam and Kent have recently proposed a DI relativistic bit commitment protocol [AK15], which allows security for a fixed amount of time under the assumption that each party is split into space-like separated agents.

Here, we take the very first step in proving DI security for two-party cryptographic protocols in the noisy-storage model. That is, we establish the security of these protocols even if the devices are not trusted under some extra assumptions (either we require the devices to behave identically in every round or we require the attack of the dishonest party to be sequential). To accomplish this, there are a number of conceptual as well as technical hurdles to cross.

(1) In QKD Alice and Bob are always honest, while Eve is always trying to break the protocol. In DI QKD it is therefore natural to give the power to prepare the devices to Eve. Analogously, we will assume here that all the devices used in the protocol are always prepared by the dishonest party.

(2) In the following section we will see that the protocol we start with uses quantum communication between Alice and Bob. This means that the adversary who prepared the devices will receive *quantum communication* coming back from the devices. This is in sharp contrast to DI QKD, in which Eve prepares the devices—with which she is possibly entangled—and then Alice and Bob simply push buttons on the devices to perform measurements. That is, there is no quantum communication going back to Eve. This feature introduces a significant difference between the security analysis of DI QKD and DI two-party cryptography protocol considered here and requires us to develop novel proof techniques.

1.1. Results

To establish DI security of two-party protocols, we will establish the DI security for a *universal* two-party primitive known as weak string erasure (WSE) [KWW12]. The most convenient manner of describing a new primitive is to specify its input–output behaviour. Such an abstract description is known as the *ideal functionality* and the ideal functionality of WSE is explained in figure 1. Universality means that a secure implementation of WSE can be used to construct *any* other two-party cryptographic primitive. In particular, the well-known primitive of bit commitment can be obtained from WSE using classical post-processing. Since classical post-

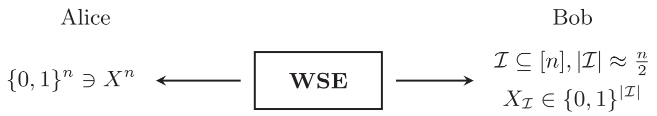
Alice
Bob
$\{0,1\}^n \ni X^n$
WSE
$\mathcal{I} \subseteq [n], |\mathcal{I}| \approx \frac{n}{2}$
$X_{\mathcal{I}} \in \{0,1\}^{|\mathcal{I}|}$

Figure 1. The ideal functionality of WSE [KWW12]: Alice gets a randomly chosen bit string X^n while Bob obtains a randomly chosen subset of indices $\mathcal{I} \subseteq [n] = \{1, 2, \ldots, n\}$ and the bits of X^n corresponding to the indices in $\mathcal{I}$, denoted by $X_{\mathcal{I}}$. Security means that if Bob is honest, then Alice cannot learn the index set $\mathcal{I}$. That is, she does not learn which bits of the string X^n are known to Bob. Conversely, if Alice is honest, then Bob finds it difficult to guess the *entire* string quantified by a lower bound on the min-entropy $\mathrm{H}_{\min}(X^n|\mathrm{Bob}) \geqslant \lambda n$ (equivalent to an upper bound on the guessing probability $\mathrm{p}_{\mathrm{guess}}(X^n|\mathrm{Bob}) \leqslant 2^{-\lambda n}$), where λ is a real parameter specified by the ideal functionality. Whenever $\lambda > 0$, WSE is useful for constructing other cryptographic primitives like bit commitment. We defer formal definitions until section 2.2.5.

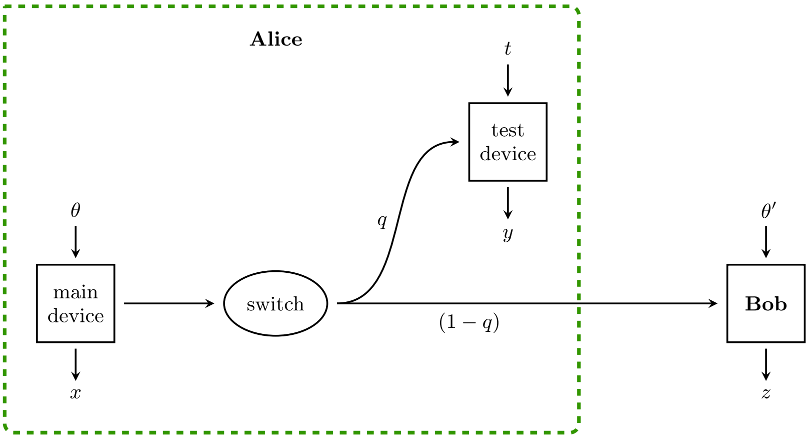

Figure 2. Honest execution of the DI WSE protocol. The main device prepares an EPR pair $|\Psi_{AB}\rangle$, measures the A system in either the computational $(\theta = 0)$ or Hadamard $(\theta = 1)$ basis (chosen uniformly at random) to produce $x \in \{0, 1\}$, while the B system is sent to the switch. Now, Alice chooses to either perform a test or play a live round. Whenever she decides to execute a test (with probability q), the switch directs B to the test device, and she performs a CHSH test between the main device and the test device. That is, she chooses a random input $t \in \{0, 1\}$ and checks the CHSH condition $x \oplus y = \theta \cdot t$ on the outputs $x, y \in \{0, 1\}$. Whenever, she decides to play a live round (with probability $1 - q$) she uses the switch to send B to Bob, who measures the incoming qubit in either the computational $(\theta' = 0)$ or Hadamard $(\theta' = 1)$ basis (chosen uniformly at random) to produce $z \in \{0, 1\}$, respectively. After n live rounds, both parties wait time Δt, which enforces the storage assumption, after which Alice announces her basis string $\theta^n = \theta_1\theta_2 \ldots \theta_n$. At the end Alice holds a random string $x^n = x_1x_2 \ldots x_n$, while Bob has an index set $\mathcal{I} = \{j \in [n] : \theta_j = \theta'_j\}$ and a substring $x_{\mathcal{I}} := (x_j)_{j\in\mathcal{I}}$.

processing is trusted in the model of DI quantum cryptography, this means that once we construct a DI protocol for WSE, we have obtained a protocol for any primitive that can be obtained from WSE using classical post-processing. Moreover, the final security bound (1) immediately implies the DI security of an oblivious transfer protocol in the bounded storage model (for details see section 4.3 of [DFR$^+$07]).

We propose a DI protocol for WSE whose security is certified by the violation of the Clauser–Horne–Shimony–Holt (CHSH) [CHSH69] inequality (see section 2.2.1 for details). We make the assumption that it is always the dishonest party that produced the devices. However, we will argue that dishonest Alice cannot gain any advantage by preparing Bob's devices so only the case of dishonest Bob requires detailed analysis. Before the protocol begins Bob provides Alice with two separate devices: a source of bipartite quantum states, combined with a measurement devices, plus one additional measurement devices that Alice can use for testing (see figure 2). According to the ideal specification this setup should be capable of producing the maximal violation of the CHSH inequality. In the protocol, Alice will use a switch to either send a quantum state to the test device or to Bob. That is, she sometimes uses her devices to violate the CHSH inequality (the test rounds) while sometimes she only measures one of the particles and passes the other one to Bob (the live rounds). Intuitively, observing a high CHSH violation in the test rounds implies that measurements performed by the devices are incompatible, which leads to uncertainty (against a classical adversary) in the live rounds. For completeness, let us stress the importance of the assumption that Alice has full control over the switch, i.e. she is free to choose which rounds are used for testing and which rounds are used in the protocol (sometimes referred to as the *free will* assumption). This assumption is crucial from the theoretical point (it implies that the sample used to assess the performance of the devices cannot be influenced by the dishonest party, which is important since in many cases even limited influence may completely break the security), but it is also reasonable from a practical point of view (a switch is a simple enough device to be prepared by Alice herself).

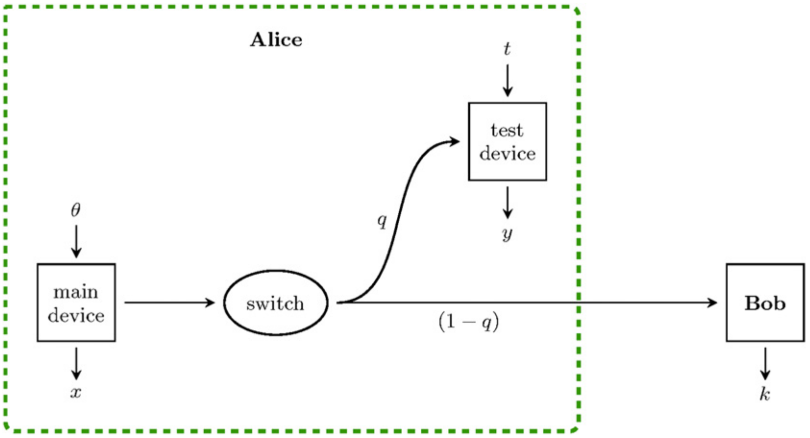

Figure 3. Dishonest Bob prepared all the devices. This means that the state generated by the source can be chosen arbitrarily by Bob, and similarly he can adjust the measurements performed by the main and test device. Alice has control of the correctly functioning switch to decide whether she wants to test or perform a live round. Honest Alice proceeds as before, however, Bob is not restricted to performing BB84 measurements on the returning quantum states. In sharp contrast to DI QKD, the dishonest party thus receives quantum communication coming back from the devices, which calls for new techniques. As we will show below, it will be enough to consider the case where Bob measures the resulting quantum states to obtain some classical information. We will then establish a bound on the min-entropy that Bob has about the string x^n, given this classical information k and the basis information received later. Using standard methods [KWW12], we can then turn this into a security statement in the noisy-storage model.

In the dishonest scenario we allow Bob to prepare all the devices and in addition he receives quantum communication from Alice during the protocol as depicted in figure 3. Here, we analyse two distinct security models.

- Memoryless devices (against an arbitrary attack)
  We call a device memoryless if its behaviour is identical every time it is used and there are no correlations between different uses. This is a convenient assumption because for such devices the observed CHSH violation β is a well-defined quantity and can be estimated to arbitrary precision. As explained in figure 1 the goal of WSE is to generate a string X^n that Bob is at least partially ignorant about as quantified by the min-entropy $\mathrm{H}_{\min}(X^n|\mathrm{Bob})$. In case of Bob whose quantum storage is restricted to be of dimension at most d we show that

$$\mathrm{H}_{\min}(X^n|\mathrm{Bob}) \geqslant nf(\beta) - \log d \tag{1}$$

  or equivalently

$$\mathrm{p}_{\mathrm{guess}}(X^n|\mathrm{Bob}) \leqslant d \cdot 2^{-nf(\beta)},$$

  where $f(\beta)$ is a simple function plotted in figure 4 and $\log \equiv \log_2$. Thus, to achieve security against such an adversary it suffices to choose n large enough to guarantee $nf(\beta) - \log d > 0$. For adversaries whose quantum storage is noisy rather than bounded the analysis is slightly more involved and can be found in section 2.3.1 (explicit security bound in proposition 5). In either case positive min-entropy rate implies that the protocol can be used for constructing more complicated primitives like bit commitment or oblivious transfer.

- General devices against a sequential attack
  In case of devices with memory (whose behaviour may change during the protocol and in particular there might be correlations between different rounds) the analysis is more involved both from the conceptual and technical point of view. First, we must realise that we cannot in advance test the devices (to estimate their quality) and use the results to make a security statement simply because the behaviour of the devices might change in time. In particular, it is clear that the devices must not know whether they are currently being tested or not. Therefore, the test rounds and the live rounds must be interspersed and we can only make a security statement about the combined performance. In this case the test rounds must be explicitly included in the protocol and we adapt the simplest solution in which before every round Alice flips a biased coin and either plays a test round (with probability q) or a live round (with probability $1 - q$). After n rounds she computes the fraction of successful CHSH rounds f_{CHSH} and checks whether it exceeds some previously chosen threshold γ. Note that estimating f_{CHSH} plays the role of estimating β in the memoryless scenario: once the devices are allowed to have memory and change behaviour from round to round, β is no longer a well-defined quantity and f_{CHSH} is the best approximation thereof. If $f_{\mathrm{CHSH}} \geqslant \gamma$ she declares the protocol to have

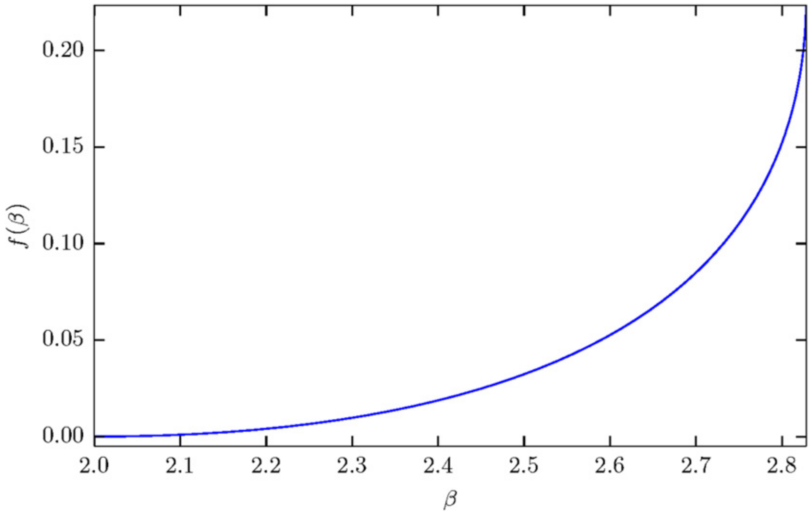

Figure 4. Lower bound on the min-entropy rate $f(\beta)$ as a function of the CHSH violation β. Crucially, we have $f(\beta) > 0$, whenever $\beta > 2$. This means that security can be achieved for arbitrarily small violation of the CHSH inequality.

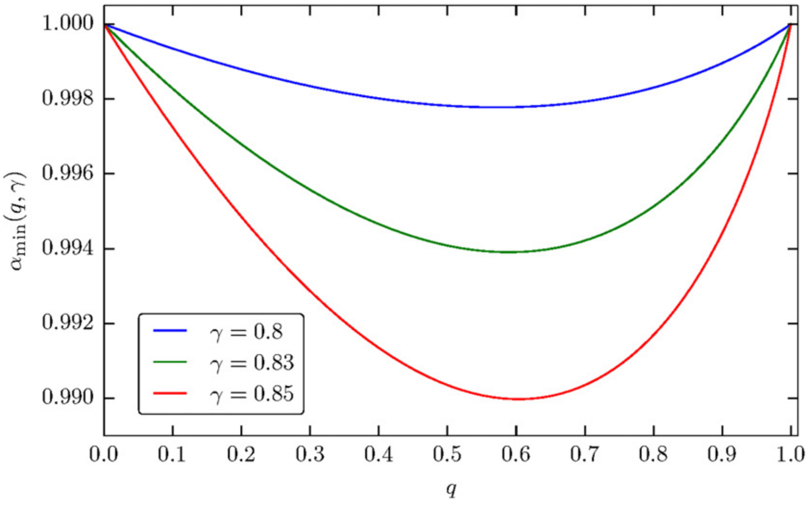

Figure 5. Values of the decay rate $\alpha_{\text{min}}(q, \gamma)$ calculated numerically as a function of q for various values of γ.

terminated successfully, otherwise she aborts. Intuitively, what we want to avoid is the situation in which Alice believes that the protocol has terminated correctly but nevertheless Bob actually knows the entire string x^n and we denote such an event by F (failure). Suppose n rounds are executed with parameters $q \in [0, 1]$ and $\gamma \in \left[\frac{3}{4}, 1\right]$. We call an attack sequential if after every round Bob is required to produce a classical outcome and his guess for that round is required to be a (classical) post-processing of that outcome combined with the basis information and any information from the previous rounds (see section 2.3.2 for a more detailed explanation). It is worth noting that this assumption removes the need to restrict Bob's storage capabilities: since he is forced to commit to his guess immediately after the round is over, storing the quantum system does not help). We show that in the sequential scenario the probability of failure is bounded by

$$\Pr[F] \leqslant [\alpha_{\text{min}}(q, \gamma)]^n , \tag{2}$$

where $\alpha_{\text{min}}(q, \gamma)$ can be easily calculated for any (valid) choice of q and γ (see figure 5). Alternatively, we can write $\Pr[F]$ in terms of the probability of passing the test p_{pass} and the probability of successfully guessing the entire 'live' string (restricted to sequential guessing strategies, see section 2.2.2 for a precise definition) conditioned on passing the test $\mathrm{p}_{\text{guess}}^{\text{seq}}(X^{\mathcal{L}}|\text{Bob, pass})$

$$\Pr[F] = p_{\text{pass}} \cdot \mathrm{p}_{\text{guess}}^{\text{seq}}(X^{\mathcal{L}}|\text{Bob, pass}) \leqslant [\alpha_{\text{min}}(q, \gamma)]^n . \tag{3}$$

Our analysis is tight in the sense that it identifies correctly the pairs (q, γ) for which security is possible, i.e. we show that $\alpha_{\min}(q, \gamma) < 1$ unless $q = 0$ (Alice never tests), $q = 1$ (Alice never plays a live round) or $\gamma = \frac{3}{4}$ (the threshold can be achieved by a classical strategy). This means that the probability of the devices performing well in the test rounds *and* failing to implement a secure WSE decays exponentially in the total number of rounds. The technique we use to prove this result is generic and can be applied to any situation in which the combined performance of two (or more) games is assessed (as long as there is some non-trivial trade-off between them).

These two contributions should be seen as steps towards a security proof against the most general attack. The memoryless model might be of independent interest since it captures the case of devices which are faulty rather than malicious (e.g. due to some misalignment of optical components); such scenarios are usually modelled as permanent deviations from the ideal specification rather than time-dependent ones.

2. Methods

In section 2.1 we present the original protocol for WSE using trusted devices, in section 2.2 we introduce the relevant quantities and prove some technical lemmas, in section 2.3.1 we formalise the scenario of memoryless devices and prove security statement (1) and in section 2.3.2 we analyse the case of arbitrary devices against sequential attacks and prove security claim (2).

2.1. The original WSE protocol for trusted devices

To build intuition, let us first describe the original protocol for WSE [KWW12], which works under the assumption that the devices used by Alice and Bob are perfect and prepared in a trustworthy fashion. We sketch out a simple security argument and discuss how to make the protocol DI. Note that there exist more sophisticated arguments which give better security guarantees but they seem to be more difficult to adapt to the DI scenario.

Protocol 1. WSE in the noisy-storage model

(1) Alice chooses two uniform n-bit strings x^n, $\theta^n \in \{0, 1\}^n$, generates the n-qubit state

$$\bigotimes_{j=1}^{n} H^{\theta_j}|x_j\rangle,$$

where H is the Hadamard gate, and sends it to Bob. (Note that this just a sequence of n randomly chosen BB84 [BB84] states.)

(2) Bob chooses a uniform n-bit string $\theta'^n \in \{0, 1\}^n$ and measures the jth qubit in the computational (if $\theta'_j = 0$) or Hadamard (if $\theta'_j = 1$) basis.

(3) Alice waits a fixed amount of time (to enforce the restriction on Bob's quantum memory) and then sends θ^n to Bob.

(4) Bob determines the index set as

$$\mathcal{I} \coloneqq \{j \in [n] : \theta_j = \theta'_j\}$$

and obtains the corresponding substring $x_{\mathcal{I}}$.

Correctness of this protocol is easy to verify because the string x^n is chosen uniformly at random by Alice and with high probability Bob measures roughly half of the qubits in the correct basis. Security for honest Bob is a direct consequence of the fact that the index set is determined by the positions at which $\theta_j \oplus \theta'_j = 0$. Since θ'^n is chosen uniformly at random by Bob, every index set is equally likely (and Alice is fully ignorant about it). Therefore, the only non-trivial scenario is the case of honest Alice.

Let $\rho_{X^n\Theta^n B}$ be the state of the protocol after step (1), where X^n and Θ^n are the classical random variables generated by Alice and B is the quantum system received by Bob. The memory bound forces Bob to put the B subsystem through a quantum channel which outputs a classical register K and a quantum register Q, which gives rise to $\rho_{X^n\Theta^n KQ}$. Since Θ^n is eventually announced to Bob, our goal is to find a lower bound on $\mathrm{H}_{\min}(X^n|KQ\Theta^n)$. In the bounded-storage model we can use the following chain rule

$$\mathrm{H}_{\min}(X^n|KQ\Theta^n) \geqslant \mathrm{H}_{\min}(X^n|K\Theta^n) - \log \dim Q. \tag{4}$$

In case of noisy storage the argument is slightly more involved (see section 2.3.1 for details) but again the task reduces to establishing uncertainty against a classical adversary. This is possible because generating random

BB84 states is equivalent to creating EPR pairs and measuring them in either computational or Hadamard basis and we know that outcomes of incompatible measurements cannot be predicted (perfectly) by a classical adversary. Indeed, it has been shown (equation (18) in [KWW12]) that the resulting conditional min-entropy satisfies $\mathrm{H}_{\min}(X^n|K\Theta^n) \geqslant \alpha n$ for

$$\alpha = -\log\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) \approx 0.22.$$

Note that this bound is tight and is achieved if Bob measures every received qubit in the intermediate basis $\{|\alpha_0\rangle, |\alpha_1\rangle\}$, where

$$|\alpha_0\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle,$$
$$|\alpha_1\rangle = \sin(\pi/8)|0\rangle - \cos(\pi/8)|1\rangle.$$

In case of trusted devices placing a lower bound on $\mathrm{H}_{\min}(X^n|K\Theta^n)$ is possible because we know exactly the measurement operators on Alice's side. The main challenge in the DI scenario is to prove a lower bound which relies solely on properties that can be certified DI. Our approach follows the intuition that observing a Bell violation implies incompatibility of local observables which is sufficient to guarantee uncertainty. Previously, this approach has been used successfully in proving security of DI QKD [LPT+13, TH13].

2.2. Preliminaries

For an integer $n \in \mathbb{N}$ let $[n] := \{1, 2, \ldots, n\}$. Throughout this paper we assume that all random variables are discrete (they take a finite number of values) and that all quantum systems are finite-dimensional. Let $\mathscr{H}$ be a (finite-dimensional) Hilbert space and let $\mathcal{L}(\mathscr{H})/\mathcal{H}(\mathscr{H})$ be the set of linear/Hermitian operators acting on $\mathscr{H}$. The Schatten ∞-norm of an operator X is denoted by $||X||$. The square root of a positive semidefinite operator X, denoted by $\sqrt{X}$, is defined as the unique positive semidefinite operator Y satisfying $Y^2 = X$. The modulus of an operator X, denoted by $|X|$, is defined as $Y = \sqrt{X^\dagger X}$. It is easy to verify that for arbitrary operators X and Y we have

$$|X + Y|^2 + |X - Y|^2 = 2(X^\dagger X + Y^\dagger Y). \tag{5}$$

The commutator of X and Y is defined as $[X, Y] = XY - YX$, while the anticommutator is defined as $\{X, Y\} = XY + YX$.

A quantum state ρ is a Hermitian operator $\rho \in \mathcal{H}(\mathscr{H})$ which is positive semidefinite ($\rho \geqslant 0$) and of unit trace ($\mathrm{tr}\rho = 1$). An observable is a Hermitian operator $A \in \mathcal{H}(\mathscr{H})$ which satisfies $-\mathbb{1} \leqslant A \leqslant \mathbb{1}$ (or equivalently $||A|| \leqslant 1$). Plugging $X = AB$ and $Y = BA$ into equation (5) gives

$$|\{A, B\}|^2 + |[A, B]|^2 = 2(AB^2A + BA^2B) \leqslant 4 \cdot \mathbb{1}, \tag{6}$$

where the upper bound follows from the fact that $A^2, B^2 \leqslant \mathbb{1}$.

2.2.1. *The CHSH inequality*

In 1964 John Bell showed that measuring quantum systems leads to stronger-than-classical correlations [Bel64]. In 1969 Clauser, Horne, Shimony and Holt spelt out the simplest scenario in which this can be observed [CHSH69]. Let $\mathscr{H}_A$ and $\mathscr{H}_B$ be Hilbert spaces and let $A_0, A_1 \in \mathcal{H}(\mathscr{H}_A)$ and $B_0, B_1 \in \mathcal{H}(\mathscr{H}_B)$ be binary observables. The CHSH operator is defined as

$$W = A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1$$

and the CHSH value equals $\beta = \mathrm{tr}(W\rho_{AB})$, where ρ_{AB} is a bipartite quantum state on $\mathscr{H}_A \otimes \mathscr{H}_B$. It is known that there exist a state and observables that yield $\beta = 2\sqrt{2}$. On the other hand, if we restrict ourselves to classical systems (which can be enforced by requiring the observables to commute, i.e. $[A_0, A_1] = [B_0, B_1] = 0$) we can only reach $\beta = 2$. This scenario can be equivalently cast as a two-player game in which Alice receives x, Bob receives y (both chosen uniformly at random) and are required to output a and b, respectively. The game is won if $a \oplus b = x \cdot y$ and it is straightforward to show that the winning probability of this game $\mathrm{p}_{\mathrm{win}}$ and the CHSH value β are related by

$$\mathrm{p}_{\mathrm{win}} = \frac{1}{2} + \frac{\beta}{8}.$$

Therefore, the optimal classical winning probability equals $\frac{3}{4}$, while the optimal quantum winning probability equals $\frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85$.

2.2.2. Guessing with postmeasurement information

We start by defining the guessing probability and min-entropy for a classical-quantum (cq) state (we denote the quantum register by B to be consistent with the protocol in which it is the dishonest Bob who faces the task of guessing).

Definition 1. Let ρ_{XB} be a cq-state

$$\rho_{XB} = \sum_x p_x |x\rangle\langle x| \otimes \rho_x^B,$$

where ρ_x^B are (normalised) quantum states and $\sum_x p_x = 1$. The optimal guessing probability of X given access to B is defined as

$$\mathrm{p_{guess}}(X|B) := \max_{\{M_x\}_x} \sum_x p_x \cdot \mathrm{tr}(M_x \rho_x^B),$$

where the maximisation is taken over all POVMs. The conditional min-entropy of X given B is defined as

$$\mathrm{H_{min}}(X|B) := -\log \mathrm{p_{guess}}(X|B).$$

Note that computing the guessing probability can be written as a semidefinite program, i.e. it can be computed efficiently (in the input dimension). For a classical probability distribution P_{XY} the expression simplifies to

$$\mathrm{p_{guess}}(X|Y) = \sum_y P_Y(y) \cdot \max_x P_{X|Y}(x|y).$$

Alternatively, this maximisation can be written more compactly as

$$\mathrm{p_{guess}}(X|Y) = \max_f \Pr[X = f(Y)],$$

where the maximisation is taken over deterministic functions $f: \mathcal{Y} \to \mathcal{X}$. It can be shown [Weh08] that the min-entropy is additive on tensor products, i.e. given two uncorrelated cq-states $\rho_{X_1B_1} \otimes \rho_{X_2B_2}$ we have

$$\mathrm{H_{min}}(X_1X_2|B_1B_2) = \mathrm{H_{min}}(X_1|B_1) + \mathrm{H_{min}}(X_2|B_2).$$

We also need the notion of smooth min-entropy.

Definition 2. For $\varepsilon \geqslant 0$ let $\mathcal{B}^\varepsilon(\rho_{XB})$ be the ball of cq-states of radius ε around ρ_{XB}, i.e. $\sigma_{XB} \in \mathcal{B}^\varepsilon(\rho_{XB})$ iff σ_{XB} is a cq-state and

$$\frac{1}{2}||\sigma_{XB} - \rho_{XB}||_1 \leqslant \varepsilon,$$

where $|| \cdot ||_1$ denotes the trace norm (Schatten 1-norm). Then, the smooth min-entropy of a cq-state ρ_{XB} is defined as

$$H_{\min}^\varepsilon(X|B)_\rho := \sup_{\sigma_{XB} \in \mathcal{B}^\varepsilon(\rho_{XB})} \mathrm{H_{min}}(X|B)_\sigma.$$

Security analysis of two-party cryptography in the bounded or noisy storage model leads to the task of *guessing with postmeasurement information* originally considered by Ballester, Wehner and Winter [BWW08]. Let ρ_{XYB} be a tripartite ccq-state, where X is a classical register taking values in $\mathcal{X}$, Y is a classical register taking values in $\mathcal{Y}$ and B is the quantum system of Bob. In the postmeasurement information scenario Bob is forced to measure his subsystem B to obtain some classical information F before learning Y. Later he learns the postmeasurement information Y and must produce a guess for X. We will later show that without loss of generality we can assume that the outcomes of Bob's measurement (i.e.the possible values of F) are labelled by functions $f: \mathcal{Y} \to \mathcal{X}$ such that Bob's optimal guess upon receiving y is $f(y)$. Equivalently we can think of the outcome of the measurement as a sequence of guesses: one for *every possible value* of the postmeasurement information.

Definition 3. Let ρ_{XYB} be a ccq-state

$$\rho_{XYB} = \sum_{xy} p_{xy} |x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho_{xy}^B.$$

The optimal guessing probability of X given access to B with Y as postmeasurement information is defined as

$$\mathrm{p_{guess}}(X|BY^*) := \max_{\{M_f\}_f} \sum_{\substack{x,y,f\\ x=f(y)}} p_{xy} \cdot \mathrm{tr}(M_f \rho_{xy}^B),$$

where the maximisation is taken over all POVMs with $|\mathcal{X}|^{|\mathcal{Y}|}$ outcomes labelled by functions $f: \mathcal{Y} \to \mathcal{X}$ and the star (*) indicates that Y is only available *after* the measurement. The conditional min-entropy of X given B with Y as postmeasurement information is defined as

$$\mathrm{H}_{\min}(X|BY^{*}) := -\log \mathrm{p}_{\mathrm{guess}}(X|BY^{*}).$$

This is a useful formulation because defining

$$\sigma_{f}^{B} = \sum_{\substack{x,y\\ x=f(y)}} p_{xy}\rho_{xy}^{B}$$

allows us to rewrite the objective function as

$$\sum_{\substack{x,y,f\\ x=f(y)}} p_{xy}\cdot \mathrm{tr}(M_{f}\rho_{xy}^{B}) = \sum_{f}\mathrm{tr}(M_{f}\sigma_{f}^{B}),$$

which is equivalent to the standard guessing probability $\mathrm{p}_{\mathrm{guess}}(F|B)$ for the (unnormalised) state

$$\rho_{FB} = \sum_{f}|f\rangle\langle f|\otimes\sigma_{f}^{B}.$$

Therefore, this problem can also be solved efficiently using semidefinite programming techniques [BWW08]. Moreover, just like in the standard guessing scenario, the min-entropy is additive over tensor products, i.e. given two uncorrelated ccq-states $\rho_{X_1Y_1B_1}\otimes\rho_{X_2Y_2B_2}$ we have

$$\mathrm{H}_{\min}(X_1X_2|B_1B_2Y_1^{*}Y_2^{*}) = \mathrm{H}_{\min}(X_1|B_1Y_1^{*}) + \mathrm{H}_{\min}(X_2|B_2Y_2^{*}). \tag{7}$$

The following proposition gives an alternative (but equivalent) formulation of the min-entropy with postmeasurement information.

Proposition 1. *Let ρ_{XYB} be a ccq-state and let $\mathcal{P}$ be the set of tripartite probability distributions over X, Y and K which can be obtained by measuring subsystem* B, *i.e. $P_{XYK}\in\mathcal{P}$ iff there exists a measurement $\{N_k\}_k$ such that*

$$\Pr[X=x,\ Y=y,\ K=k] = p_{xy}\cdot\mathrm{tr}(N_k\rho_{xy}^{B}).$$

Then, the following relation holds

$$\mathrm{p}_{\mathrm{guess}}(X|BY^{*}) = \sup_{P_{XYK}\in\mathcal{P}}\mathrm{p}_{\mathrm{guess}}(X|KY). \tag{8}$$

Proof. Let us first show that the left-hand side is never larger than the right-hand side. Let $\{M_f\}_f$ be the POVM which saturates the left-hand side and let P_{XYF} be the resulting probability distribution. Then

$$\begin{aligned}\mathrm{p}_{\mathrm{guess}}(X|BY^{*}) &= \sum_{\substack{x,y,f\\ x=f(y)}} p_{xy}\cdot\mathrm{tr}(M_f\rho_{xy}^{B}) = \sum_{\substack{x,y,f\\ x=f(y)}} P_{XYF}(xyf) = \sum_{y,f}P_{YF}(yf)\cdot P_{X|YF}(f(y)|yf)\\ &\leqslant \sum_{y,f}P_{YF}(yf)\cdot\max_{x}P_{X|YF}(x|yf) = \mathrm{p}_{\mathrm{guess}}(X|FY)\leqslant\sup_{P_{XYK}\in\mathcal{P}}\mathrm{p}_{\mathrm{guess}}(X|KY).\end{aligned}$$

To prove the other direction consider an arbitrary measurement $\{N_k\}_k$ (with a finite number of outcomes) which leads to the probability distribution P_{XYK}. For every value of k we define a function $g_k:\mathcal{Y}\to\mathcal{X}$ such that

$$g_k(y) = \arg\max_{x}P_{X|YK}(x|yk).$$

This allows us construct a new measurement whose outcomes are labelled by functions $f:\mathcal{Y}\to\mathcal{X}$

$$M_f = \sum_{k:g_k=f}N_k.$$

Using this measurement gives

$$\begin{aligned}\mathrm{p}_{\mathrm{guess}}(X|BY^{*}) &\geqslant \sum_{\substack{x,y,f\\ x=f(y)}} p_{xy}\cdot\mathrm{tr}(M_f\rho_{xy}) = \sum_{\substack{x,y,f\\ x=f(y)}}\sum_{k:g_k=f}p_{xy}\cdot\mathrm{tr}(N_k\rho_{xy}) = \sum_{\substack{x,y,k\\ x=g_k(y)}}P_{XYK}(xyk)\\ &= \sum_{y,k}P_{YK}(yk)\cdot P_{X|YK}(g_k(y)|ky) = \sum_{y,k}P_{YK}(yk)\cdot\max_{x}P_{X|YK}(x|yk) = \mathrm{p}_{\mathrm{guess}}(X|KY).\end{aligned}$$

By considering measurements that approach the optimal guessing probability we conclude that equation (8) holds. In particular, this implies that the supremum can be replaced by a maximum. □

The final security statement in the scenario of devices with memory is phrased in terms of *sequential guessing probability*. Intuitively, this corresponds to the situation in which Bob is required to guess a sequence of random variables but before each guess he gains access to an extra 'advice variable'.

Definition 4. Let $P_{X_1X_2\ldots X_nY_1Y_2\ldots Y_n}$ be a probability distribution of $2n$ variables, where X_j and Y_j take values in some arbitrary finite sets $\mathcal{X}$ and $\mathcal{Y}$, respectively. The sequential guessing probability of $X^n = X_1X_2\ldots X_n$ given $Y^n = Y_1Y_2\ldots Y_n$ is defined as

$$\mathrm{p}_{\mathrm{guess}}^{\mathrm{seq}}(X^n|Y^n) = \max_{\{f_j\}_j} \Pr[\bigwedge_{j=1}^{n} X_j = f_j(Y_1 Y_2 \ldots Y_j)],$$

where the maximisation is taken over deterministic functions $\{f_j\}_j$ such that $f_j : \mathcal{Y}^{\times j} \to \mathcal{X}$.

The sequential character of this quantity makes it meaningful to talk about a subset of rounds, e.g. the probability of successfully guessing the first j variables $\mathrm{p}_{\mathrm{guess}}^{\mathrm{seq}}(X^j|Y^j)$ is a well-defined quantity that depends only on $P_{X^j Y^j}$. This stands in contrast to the usual guessing probability in which evaluating the probability of successfully guessing the first bit requires the knowledge of the complete set of 'advice variables'. Thanks to this property the sequential guessing probability behaves well under conditioning

$$\mathrm{p}_{\mathrm{guess}}^{\mathrm{seq}}(X^n|Y^n) = \mathrm{p}_{\mathrm{guess}}^{\mathrm{seq}}(X^{n-1}|Y^{n-1}) \cdot \mathrm{p}_{\mathrm{guess}}(X_n|Y^n, \mathcal{S}),$$

where the second term is just the standard guessing probability of the last bit *conditional* on event $\mathcal{S}$, which corresponds to (sequentially) guessing the first $n - 1$ bits correctly.

2.2.3. Relation between transmitting classical information and uncertainty against noisy storage

Let $\mathcal{F} : \mathcal{L}(\mathscr{H} Q_{\mathrm{in}}) \to \mathcal{L}(\mathscr{H} Q_{\mathrm{out}})$ be a quantum channel (a completely positive, trace preserving map) and suppose we want to use it to transmit k bits of information. The following definition captures how well this can be achieved.

Definition 5. The optimal probability of successfully transmitting k bits of information through the channel $\mathcal{F}$ is defined as

$$\mathrm{P}_{\mathrm{succ}}^{\mathcal{F}}(k) = \max_{\{\rho_x\}_x, \{M_x\}_x} \frac{1}{2^k} \sum_{x \in \{0,1\}^k} \mathrm{tr}[M_x \mathcal{F}(\rho_x)],$$

where $\{\rho_x\}_x$ represents the encoding procedure (a set of 2^k normalised states on Q_{in}) while $\{M_x\}_x$ is the decoding measurement (a measurement on Q_{out} with 2^k outcomes).

The following lemma by König, Wehner and Wullschleger relates the success probability to the maximal decrease in entropy in the noisy storage setting [KWW12].

Lemma 1 (Lemma II.2, [KWW12]). *Let $\mathcal{F} : \mathcal{L}(\mathscr{H}_Q) \to \mathcal{L}(\mathscr{H}_{Q_{\mathrm{out}}})$ be a CPTP map. Consider an arbitrary ccq-state ρ_{XTQ} and define*

$$\sigma_{XTQ_{\mathrm{out}}} := (\mathrm{id}_{XT} \otimes \mathcal{F}_{Q \to Q_{\mathrm{out}}})(\rho_{XTQ}),$$

where id stands for the identity channel. For any $\varepsilon > 0$ we have

$$H_{\min}^{\varepsilon}(X|TQ_{\mathrm{out}})_{\sigma} \geqslant -\log \mathrm{P}_{\mathrm{succ}}^{\mathcal{F}}(\lfloor \mathrm{H}_{\min}(X|T) - \log(1/\varepsilon) \rfloor).$$

2.2.4. Trade-off between non-locality and uncertainty against classical adversaries

As mentioned before a crucial component of our analysis is the trade-off between how well a pair of devices can perform in the CHSH test and how unpredictable the output of a single device is against a classical adversary. It turns out that such a (tight) trade-off can be established by finding the right measure of incompatibility of binary observables. In our previous work we have used the effective anticommutator as a measure of incompatibility [KTW14]. Unfortunately, this quantity does not allow us to bound uncertainty against classical side information (see appendix A for a counterexample) so here we consider a more refined quantity: the *absolute effective anticommutator*. Proposition 2 shows that observing a CHSH violation places an upper bound on the absolute effective anticommutator.

Proposition 2. *Let $\rho_{AB} \in \mathcal{H}(\mathscr{H}_A \otimes \mathscr{H}_B)$ be a bipartite quantum state and let $A_0, A_1 \in \mathcal{H}(\mathscr{H}_A)$ and $B_0, B_1 \in \mathcal{H}(\mathscr{H}_B)$ be observables. The absolute effective anticommutator on Alice's side is defined as*

$$\varepsilon_+ := \frac{1}{2}\mathrm{tr}(|\{A_0, A_1\}|\rho_A).$$

The CHSH value of the setup is defined as $\beta := \mathrm{tr}(W\rho_{AB})$ for

$$W = A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1.$$

The following relation holds

$$|\beta| \leqslant 2\sqrt{1 + \sqrt{1 - \varepsilon_+^2}}. \tag{9}$$

Proof. The proof is a sequence of elementary inequalities (either at the level of numbers or operators). We will repeatedly use the Cauchy–Schwarz inequality, which says that for arbitrary operators X and Y we have

$$|\mathrm{tr}(X^{\dagger}Y)|^2 \leqslant \mathrm{tr}(X^{\dagger}X) \cdot \mathrm{tr}(Y^{\dagger}Y).$$

We start by setting $X^{\dagger} = W\sqrt{\rho_{AB}}$ and $Y = \sqrt{\rho_{AB}}$ which gives

$$\beta^2 = [\mathrm{tr}(W\rho_{AB})]^2 \leqslant \mathrm{tr}(W^2\rho_{AB}). \tag{10}$$

Writing out W^2 explicitly gives

$$W^2 = A_0^2 \otimes (B_0 + B_1)^2 + A_1^2 \otimes (B_0 - B_1)^2 + \{A_0, A_1\} \otimes (B_0^2 - B_1^2) - [A_0, A_1] \otimes [B_0, B_1].$$

Let us first focus on the first three terms. Upperbounding A_0^2 and A_1^2 by $\mathbb{1}$ gives

$$\begin{aligned} &A_0^2 \otimes (B_0 + B_1)^2 + A_1^2 \otimes (B_0 - B_1)^2 + \{A_0, A_1\} \otimes (B_0^2 - B_1^2) \\ &\leqslant \mathbb{1} \otimes 2(B_0^2 + B_1^2) + \{A_0, A_1\} \otimes (B_0^2 - B_1^2). \end{aligned}$$

Writing the identity in the eigenbasis of the anticommutator $\{A_0, A_1\} = \sum_k \lambda_k |e_k\rangle\langle e_k|$ gives

$$\mathbb{1} \otimes 2(B_0^2 + B_1^2) + \{A_0, A_1\} \otimes (B_0^2 - B_1^2) = \sum_k |e_k\rangle\langle e_k| \otimes [(2 + \lambda_k)B_0^2 + (2 - \lambda_k)B_1^2] \leqslant 4 \cdot \mathbb{1} \otimes \mathbb{1},$$

where the last inequality comes from upperbounding B_0^2 and B_1^2 by $\mathbb{1}$ (note that $|\lambda_k| \leqslant 2$). We have therefore established that

$$W^2 \leqslant 4 \cdot \mathbb{1} \otimes \mathbb{1} + (-[A_0, A_1] \otimes [B_0, B_1]).$$

We bound the second term by its (operator) modulus

$$-[A_0, A_1] \otimes [B_0, B_1] \leqslant |[A_0, A_1] \otimes [B_0, B_1]| = |[A_0, A_1]| \otimes |[B_0, B_1]|.$$

Neglecting the anticommutator term in inequality (6) leads to

$$|[B_0, B_1]|^2 \leqslant 4 \cdot \mathbb{1},$$

which implies that $|[B_0, B_1]| \leqslant 2 \cdot \mathbb{1}$. Therefore,

$$W^2 \leqslant 4 \cdot \mathbb{1} \otimes \mathbb{1} + 2\,|[A_0, A_1]| \otimes \mathbb{1}$$

and

$$\mathrm{tr}(W^2\rho_{AB}) \leqslant 4 + 2\mathrm{tr}(|[A_0, A_1]|\rho_A). \tag{11}$$

To upperbound $\mathrm{tr}(|[A_0, A_1]|\rho_A)$ we again use the Cauchy–Schwarz inequality with $X^{\dagger} = |[A_0, A_1]|\sqrt{\rho_A}$ and $Y = \sqrt{\rho_A}$ which gives

$$[\mathrm{tr}(|[A_0, A_1]|\rho_A)]^2 \leqslant \mathrm{tr}(|[A_0, A_1]|^2\rho_A). \tag{12}$$

Inequality (6) implies that

$$\mathrm{tr}(|[A_0, A_1]|^2\rho_A) \leqslant 4 - \mathrm{tr}(|\{A_0, A_1\}|^2\rho_A). \tag{13}$$

Using the Cauchy–Schwarz inequality one last time with $X^{\dagger} = |\{A_0, A_1\}|\sqrt{\rho_A}$ and $Y = \sqrt{\rho_A}$ gives

$$[\mathrm{tr}(|\{A_0, A_1\}|\rho_A)]^2 \leqslant \mathrm{tr}(|\{A_0, A_1\}|^2\rho_A). \tag{14}$$

Since the left-hand side of equation (14) equals $4\varepsilon_+^2$ combining it with inequalities (10)–(13) gives

$$\beta^2 \leqslant 4(1 + \sqrt{1 - \varepsilon_+^2}\,).$$

Taking a square root leads to the desired result. □

It is easy to verify that this relation is in fact tight (it suffices to consider projective rank-1 measurements on the maximally entangled state of two qubits). In proposition 3 we show that the absolute effective anticommutator being small implies uncertainty against classical adversaries.

Proposition 3. *Let ρ_{AK} be a quantum–classical state*

$$\rho_{AK} = \sum_k p_k \rho_k^A \otimes |k\rangle\langle k|$$

and let A_0 and A_1 be two observables acting on the register A. Let $\varepsilon_+ = \frac{1}{2}\mathrm{tr}(|\{A_0, A_1\}|\rho_A)$ for $\rho_A = \sum_k p_k \rho_k^A$. Measuring the observable chosen by a uniformly random register Θ and storing the outcome in the register X leads to the following probability distribution.

$$\Pr[X = x, \Theta = \theta, K = k] = \frac{1}{2} \cdot p_k \cdot \frac{1 + \mathrm{tr}(A_\theta \rho_k^A)}{2}.$$

Then, the guessing probability satisfies

$$p_{\text{guess}}(X|K\Theta) \leqslant \frac{1}{2} + \frac{1}{2}\sqrt{\frac{1+\varepsilon_+}{2}}. \tag{15}$$

Proof. Let the effective anticommutator conditional on $K = k$ be $\varepsilon_k = \frac{1}{2}\text{tr}(\{A_0, A_1\}\rho_k^A)$. As shown in [KTW14] the guessing probability averaged over the two bases satisfies

$$p_{\text{guess}}(X|K = k, \Theta) \leqslant \frac{1}{2} + \frac{1}{2}\sqrt{\frac{1+|\varepsilon_k|}{2}}.$$

Averaging over different values of K

$$p_{\text{guess}}(X|K\Theta) = \sum_k p_k p_{\text{guess}}(X|K = k, \Theta) \leqslant \frac{1}{2} + \sum_k \frac{p_k}{2}\sqrt{\frac{1+|\varepsilon_k|}{2}} \leqslant \frac{1}{2} + \frac{1}{2}\sqrt{\frac{1+\sum_k p_k|\varepsilon_k|}{2}},$$

where we have used the concavity of the square root. For any Hermitian operator A we have $|\text{tr}(A\rho)| \leqslant \text{tr}(|A|\rho)$ which implies

$$\sum_k p_k|\varepsilon_k| = \frac{1}{2}\sum_k p_k|\text{tr}(\{A_0, A_1\}\rho_k^A)| \leqslant \frac{1}{2}\sum_k p_k \text{tr}(|\{A_0, A_1\}|\rho_k^A) = \frac{1}{2}\text{tr}(|\{A_0, A_1\}|\rho_A) = \varepsilon_+.$$

Therefore, the final bound is

$$p_{\text{guess}}(X|K\Theta) \leqslant \frac{1}{2} + \frac{1}{2}\sqrt{\frac{1+\varepsilon_+}{2}}.$$

□

It turns out that this relation is tight and can be saturated by the same setup as before, which implies that the resulting trade-off between the CHSH violation and uncertainty against classical adversaries is tight.

2.2.5. Security definitions for WSE

Let X^n be the classical register representing the n-bit string given to Alice and let I be the classical register representing the subset of indices given to Bob. Using the notation introduced in section 1 security for honest Alice means that Bob should find it difficult to guess the entire string X^n.

Definition 6. Let B be the register containing all the information that Bob might acquire during the protocol. Let $\mathcal{S}_A$ be the set of states on registers X^n, B that (dishonest) Bob may enforce at the end of the protocol. A WSE protocol is (λ, ε)-secure for honest Alice if the smooth min-entropy satisfies

$$H_{\min}^{\varepsilon}(X^n|B) \geqslant \lambda n$$

for all $\sigma_{X^nB} \in \mathcal{S}_A$.

Security for honest Bob, on the other hand, requires that the string X^n takes a particular value (which Alice cannot influence anymore) and that Alice remains ignorant about the index set $\mathcal{I}$ that Bob received.

Definition 7. Let $\mathcal{S}_B$ be the set of states on registers X^n, I, A that (dishonest) Alice may enforce at the end of the protocol. A WSE protocol is (perfectly) secure for honest Bob if every state $\sigma_{X^nIA} \in \mathcal{S}_B$ can be written as

$$\sigma_{X^nIA} = \sigma_{X^nA} \otimes \frac{\mathbb{1}_I}{2^n}$$

for some cq-state σ_{X^nA}.

2.3. Protocol for DI WSE and security analysis

Since DI security can only be certified by observing some Bell violation we must make two modifications to protocol 1: (i) we have to turn it into an entanglement-based scheme and (ii) we must introduce some way of testing the devices. The protocol we propose requires four devices in total: three for Alice and one for Bob. Below we describe the devices available to Alice.

(1) The source emits bipartite quantum states ρ_{AB}. According to the ideal specification, it should emit the maximally entangled state of two qubits, i.e. $\rho_{AB} = |\Phi_+\rangle\langle\Phi_+|_{AB}$ for $|\Phi_+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$.

(2) The main device performs one out of two binary measurements represented by observables A_0, A_1. According to the ideal specification, these should correspond to the computational and Hadamard basis measurements, $A_0 = \sigma_z, A_1 = \sigma_x$.

(3) The test device performs one out of two binary measurements represented by observables B_0, B_1. According to the ideal specification, these should correspond to $B_0 = \frac{1}{\sqrt{2}}(\sigma_z + \sigma_x), B_1 = \frac{1}{\sqrt{2}}(\sigma_z - \sigma_x)$.

The only device available to Bob is a measurement device with two settings whose ideal specification coincides precisely with that of the main device of Alice (so that the outcome are identical if the measurement settings coincide).

2.3.1. Security analysis for memoryless devices

We call a device memoryless if it acts in the same manner every time we use it: the source always emits the same state and the measurement devices always perform the same measurements (and there are no correlations between different uses). This greatly simplifies the security analysis for several reasons: (i) we may assume that the state, measurement operators (and all quantities derived from them) are well-defined objects, (ii) probabilities can be estimated (to arbitrary precision) by repeating the experiment multiple times and (iii) testing can be completely separated from the actual protocol. In particular, the last point means that testing can be done beforehand and does need to be explicitly included in the protocol. In our protocol Alice tests her three devices by using them to violate the CHSH inequality. More specifically, she estimates the CHSH value

$$\beta = \mathrm{tr}[(A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1)\rho_{AB}].$$

We know that if $\beta \leqslant 2$ (no violation is observed), no security can be guaranteed and the devices cannot be used for DI cryptography. Therefore, from now on we assume that $\beta > 2$. While no finite set of statistical data allows Alice to determine the *exact value* of β, she can estimate it to arbitrary precision which is sufficient for our analysis. Since dealing with finite statistics is not the main focus of this paper, we assume that she can actually determine β exactly.

Recall that proposition 2 establishes a connection between the observed CHSH violation and the local incompatibility of observables (on either side). Since the test device will not take part in the actual protocol, we want to estimate the incompatibility of the main device. If ε_+ is the absolute effective anticommutator of the main device

$$\varepsilon_+ := \frac{1}{2}\mathrm{tr}(|\{A_0, A_1\}|\rho_A),$$

then from proposition 2 we know that

$$\varepsilon_+ \leqslant \frac{\beta}{4}\sqrt{8 - \beta^2}. \tag{16}$$

Our goal is to show that having an upper bound on ε_+ suffices to prove security (for honest Alice) of the following DI WSE protocol.

Protocol 2. DI WSE in the bounded/noisy storage model

(1) Alice uses the source to generate n bipartite states. She chooses a uniform n-bit string $\theta^n \in \{0, 1\}^n$ and uses the main device to measure the A register generated in the jth run with θ_j as the input. All the B registers are passed to Bob.

(2) Bob chooses a uniform n-bit string $\theta'^n \in \{0, 1\}^n$ and measures the jth subsystem using θ'_j as the input to his measurement device.

(3) Alice waits a fixed amount of time (this waiting time motivates the restriction on Bob's quantum memory) and then sends θ^n to Bob.

(4) Bob determines the index set as

$$\mathcal{I} := \{j \in [n] : \theta_j = \theta'_j\} \tag{17}$$

and obtains the corresponding substring $x_{\mathcal{I}}$.

It is easy to see that if the devices comply with the ideal specification, this is exactly the entanglement-based variant of protocol 1, hence, correctness follows straightforwardly. Security argument for honest Bob is closely related to the simulation argument given in the original paper [KWW12] so we just describe it informally. The correct way of defining the string X^n is by lifting the noisy memory restriction, i.e. we allow Bob to store all the states, wait until the receipt of the basis information and only then perform all the measurements in the correct bases. This uniquely specifies the state $\sigma_{X^n A}$ needed for definition 7. At the same time Bob generates a random n-bit string θ'^n and determines the index set $\mathcal{I}$ through relation (17). It is easy to check that this results in a uniform distribution over all possible subsets uncorrelated from the outside world (because θ'^n was chosen uniformly at random).

Security analysis for honest Alice turns out to be more challenging.

Proposition 4. *Protocol 2 executed against Bob whose quantum storage is bounded to be of dimension at most* d *implements WSE which is* (λ, ε)*-secure for honest Alice for* $\varepsilon = 0$ *and*

$$\lambda \geqslant h(\varepsilon_+) - \frac{\log d}{n},$$

where

$$h(x) := 1 - \log\left(1 + \sqrt{\frac{1+x}{2}}\right).$$

Proof. Using the source n times produces $\rho_{A^n B^n} = \bigotimes_{j=1}^n \rho_{A_j B_j}$. Alice measures all her subsystems using the main device (which produces $\rho_{X^n \Theta^n B^n} = \bigotimes_{j=1}^n \rho_{X_j \Theta_j B_j}$) and then Bob measures his subsystems to obtain K (which gives $P_{X^n \Theta^n K}$). It is important to emphasise that this final probability distribution is no longer of product form because Bob's measurement can introduce correlations between different rounds. First note that from proposition 1 we have

$$\mathrm{H}_{\min}(X^n|K\Theta^n) \geqslant \mathrm{H}_{\min}(X^n|B^n\Theta^{n*}), \tag{18}$$

where the left-hand side is evaluated on the probability distribution $P_{X^n\Theta^n K}$, while the right-hand side is evaluated on the quantum state $\rho_{X^n\Theta^n B^n}$. Because this quantum state is of tensor product form we have

$$\mathrm{H}_{\min}(X^n|B^n\Theta^{n*}) = \sum_{j=1}^{n} \mathrm{H}_{\min}(X_j|B_j\Theta_j^*) = n \cdot \mathrm{H}_{\min}(X_1|B_1\Theta_1^*), \tag{19}$$

where the first equality comes from the fact that the min-entropy is additive over tensor products (see equation (7)) and the second simply expresses the fact that all the rounds are identical. Now we need the bound the entropy produced while measuring a single copy of ρ_{AB}. Suppose that Bob measures the subsystem B to produce a classical random variable K. From proposition 3 we know that the min-entropy of the probability distribution $P_{XK\Theta}$ satisfies

$$\mathrm{H}_{\min}(X|K\Theta) \geqslant h(\varepsilon_+).$$

Since this bound is valid *for all measurements that Bob might perform*, it also holds for the optimal measurement which achieves $\mathrm{H}_{\min}(X|B\Theta^*) = \mathrm{H}_{\min}(X|K\Theta)$ (see proposition 1). Therefore, we also have

$$\mathrm{H}_{\min}(X|B\Theta^*) \geqslant h(\varepsilon_+). \tag{20}$$

Combining expressions (18)–(20) gives

$$\mathrm{H}_{\min}(X^n|K\Theta^n) \geqslant nh(\varepsilon_+). \tag{21}$$

Finally, including the quantum memory of Bob (of dimension d) leads to

$$\mathrm{H}_{\min}(X^n|KQ\Theta^n) \geqslant nh(\varepsilon_+) - \log d.$$

□

Clearly, if the dimension of Bob's memory is fixed, choosing large enough n brings the min-entropy rate arbitrarily close to $h(\varepsilon_+)$.

Proposition 5. *Protocol 2 executed against Bob whose quantum storage is represented by a quantum channel* $\mathcal{F}$ *implements WSE which is* (λ, ε)*-secure for honest Alice, where* $\varepsilon > 0$ *is an arbitrary positive constant and*

$$\lambda \geqslant -\frac{1}{n}\log \mathrm{P}_{\mathrm{succ}}^{\mathcal{F}}(\lfloor nh(\varepsilon_+) - \log(1/\varepsilon)\rfloor).$$

Proof. Applying lemma 1 to equation (21) (identify $X^n \leftrightarrow X$ and $K\Theta^n \leftrightarrow T$) gives

$$H_{\min}^{\varepsilon}(X^n|KQ_{\mathrm{out}}\Theta^n) \geqslant -\log \mathrm{P}_{\mathrm{succ}}^{\mathcal{F}}(\lfloor nh(\varepsilon_+) - \log(1/\varepsilon)\rfloor).$$

Since in the noisy storage scenario K, Q_{out} and Θ^n are the only registers available to Bob this coincides precisely with definition 6. □

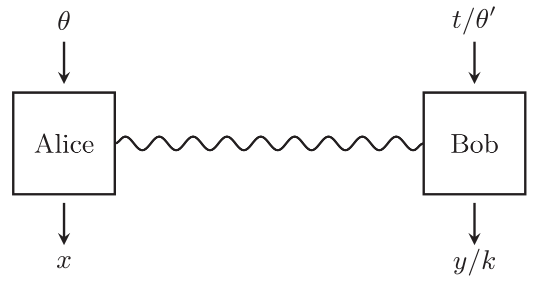

Figure 6. The key to the security proof against sequential attacks is to combine the CHSH game between the main device and the test device with the postmeasurement game between the main device and Bob's device. As already noted in [Weh08], if the postmeasurement game can be won perfectly, then the CHSH inequality cannot be violated. Here, we establish a complete trade-off between winning the CHSH game and the postmeasurement game. If the CHSH game can be won well, then the probability for Bob to succeed in the postmeasurement guessing game is low and hence the min-entropy about Alice's resulting string given classical information is high.

2.3.2. Security analysis for general devices against sequential attacks

As mentioned before in order to test devices that might behave differently in different rounds one must intersperse the test rounds with the live rounds. The natural solution is to introduce a biased coin-flip at the beginning of every round whose outcome determines whether the following round will be a test round (with probability q) or a live round (with probability $1 - q$). In the previous scenario test rounds happened entirely within Alice's laboratory (using the three devices provided by Bob) and only live rounds required Alice and Bob to interaction. To make the sequential analysis conceptually simpler we give Bob even more power and allow him to operate the test box (the device used for the CHSH test), i.e. if Alice wants to play a test round she simply sends the second input (the one she would previously use for the test device) to Bob who comes back with the outcome. Note that in this model the second part of the quantum state generated by the source always ends up with Bob (regardless of whether it is a test round or a live round), which brings us closer to the familiar scenario of two-player non-local games as shown in figure 6.

Let us stress that the interaction with the main device is always the same: regardless of whether the jth round is a test round or a live round Alice always inputs a uniformly random bit θ_j. This guarantees that the device remains ignorant whether it is currently being tested or used for a live round. On the other hand, Bob's interaction does depend on the type of round performed. Let q_j be the bit which specifies whether the jth round is a live round ($q_j = 0$) or a test round ($q_j = 1$). If Alice decides to test the devices, she will choose a random bit t_j and request Bob to use it as an input in the CHSH game and return the outcome y_j. On the other hand, if Alice decides to play a live round, she will simply announce it to Bob and (according to the original protocol) she will not expect a response. Indeed, in the most general adversarial scenario Bob would leave his quantum system untouched and only at the end of the protocol (immediately before the memory bound) would he measure his entire system to produce some classical information k. Once he has received the basis information, he computes his guess as a deterministic function of k and $\theta_1, \theta_2, \ldots, \theta_n$. In the sequential model we force Bob to produce some classical side information k_j in every round and we require that his guess in the jth round is a deterministic function (chosen before the protocol begins) of k_j, θ_j and any information from the previous rounds. In other words, for the jth round (which we assume to be a live round) the probability of winning equals

$$\Pr[X_j = f_j(K^j, \Theta^j)],$$

where $f_j : (\mathcal{K} \times \{0, 1\})^{\times j} \to \{0, 1\}$ is an arbitrary function chosen by Bob before the protocol begins. The summary of random variables generated in each round is presented in table 1. Note that in this model the requirement of immediately producing the relevant classical information essentially replaces the need to restrict Bob's storage capabilities. The fact that success (or failure) can be assessed *immediately* after every round makes such a model well-suited for a standard martingale-style analysis. It turns out that the only quantum component of such an analysis is the trade-off between the winning probabilities of the live round and the test round denoted by p_{L} and p_{T}, respectively. Conveniently, we have already investigated this trade-off since both probabilities can be bounded through the absolute effective anticommutator ε_+. More specifically, since the probability of passing the test p_{T} is related to the CHSH violation β inequality (9) implies

$$p_{\mathrm{T}} \leqslant \frac{1}{2} + \frac{1}{4}\sqrt{1 + \sqrt{1 - \varepsilon_+^2}}\,. \tag{22}$$

On the other hand, probability of winning the test round cannot exceed the optimal guessing probability of a classical adversary. Therefore, inequality (15) implies

Table 1. The random variables generated in the jth round in every round Alice chooses the round type Q_j, generates a random input Θ_j and obtains an outcome X_j. If $Q_j = 0$ (live round) Bob generates some classical information K_j (taking values in $\mathcal{K}$). On the other hand, if $Q_j = 1$ (test round) Alice generates another random input T_j and passes it to Bob who must produce an output Y_j.

Every round	Live round ($Q_j = 0$)	Test round ($Q_j = 1$)
Q_j, Θ_j, X_j	K_j	T_j, Y_j

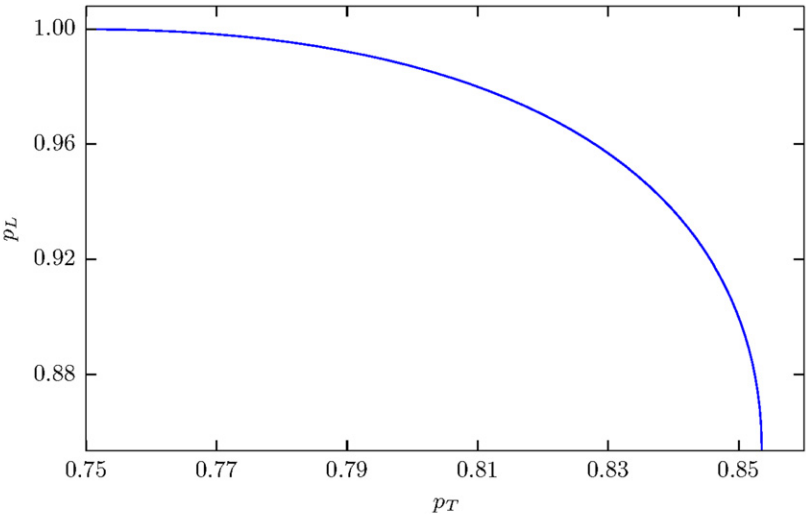

Figure 7. The (tight) trade-off between the winning probabilities of live and test rounds.

$$p_{\mathrm{L}} \leqslant \frac{1}{2} + \frac{1}{2}\sqrt{\frac{1+\varepsilon_+}{2}}. \tag{23}$$

Combining inequalities (22) and (23) and treating ε_+ as a parameter taking values in $[0, 1]$ we determine the admissible pairs $(p_{\mathrm{L}}, p_{\mathrm{T}})$. The optimal trade-off is plotted in figure 7.

The protocol takes three parameters: the probability of testing $q \in [0, 1]$, the CHSH threshold $\gamma \in \left[\frac{3}{4}, 1\right]$ and the number of rounds $n \in \mathbb{N}$. At the end of the protocol Alice calculates the fraction of successful CHSH rounds denoted by f_{CHSH}. If $f_{\mathrm{CHSH}} < \gamma$ she aborts the protocol, otherwise she declares the execution correct. The security statement in this model is simply a bound on the probability that Alice believes the protocol has terminated correctly *and* all the guesses of Bob are correct. We define the following random variables

$$R_l \coloneqq \sum_{j=1}^{l} Q_j \quad \text{(number of test rounds within the first } l \text{ rounds)},$$

$$S_l \coloneqq \sum_{j=1}^{l} (X_j \oplus Y_j \oplus \Theta_j T_j \oplus 1) Q_j \quad \text{(number of successful test rounds within the first } l \text{ rounds)}.$$

Let $\mathcal{L} \coloneqq \{j \in [n] : Q_j = 0\}$ be the set of live rounds and for $j \in \mathcal{L}$ let G_j be the event corresponding to Bob guessing the outcome correctly, i.e.

$$G_j \iff X_j = f_j(K^j, \Theta^j). \tag{24}$$

Moreover, let H_l be the event of guessing all the live rounds within the first l rounds

$$H_l \iff \bigwedge_{j \in [l] \bigcap \mathcal{L}} G_j. \tag{25}$$

The failure event is defined as a conjunction of exceeding the CHSH threshold and Bob guessing all the live bits correctly

$$F \iff S_n \geqslant \gamma R_n \wedge H_n. \tag{26}$$

Before we delve into the proof, let us show why finding an upper bound on $\Pr[F]$ is equivalent to proving security claim (3). Let P be the event of passing, i.e. $P \iff S_n \geqslant \gamma R_n$ and let $p_{\text{pass}} \coloneqq \Pr[P]$. Writing

$$\Pr[F] = p_{\text{pass}} \cdot \Pr[H_n|P] \tag{27}$$

allows us to identify the last term with the sequential guessing probability conditioned on passing the test. Indeed, since

$$H_n \iff \bigwedge_{j\in\mathcal{L}} X_j = f_j(K^j, \Theta^j) \tag{28}$$

and assuming that Bob has chosen the optimal set of functions $\{f_j\}_j$, we see that

$$\Pr[H_n] = \mathrm{p}_{\text{guess}}^{\text{seq}}(X^{\mathcal{L}}|Y^{\mathcal{L}}) \tag{29}$$

with $Y_j = (K_j, \Theta_j)$ being the jth advice variable.

To improve clarity of the proof it is convenient to define a variable which evaluates the test threshold after l rounds $X_l = S_l - \gamma R_l$. Note that the transition $l \to (l+1)$ is governed by the following equation

$$\begin{aligned}\Pr[X_{l+1} \geqslant x \wedge H_{l+1}] = \Pr[X_l \geqslant x \wedge H_l] \cdot (1-q)p_{\text{L}} + \Pr[X_l \geqslant x - (1-\gamma) \wedge H_l] \cdot qp_{\text{T}} \\ + \Pr[X_l \geqslant x + \gamma \wedge H_l] \cdot q(1-p_{\text{T}}),\end{aligned} \tag{30}$$

where the three terms correspond to a successful live round, a successful test round and an unsuccessful test round, respectively. In the following proposition we establish a recursive upper bound on the probability of failure.

Proposition 6. *Let $k \geqslant 0$ be an arbitrary real constant. For all $l \in \mathbb{N}$ the following inequality holds*

$$\Pr[X_l \geqslant x \wedge H_l] \leqslant [\alpha(q, \gamma, k)]^l e^{-kx}, \tag{31}$$

where $\alpha(q, \gamma, k)$ is a real constant defined as

$$\alpha(q, \gamma, k) := \max_{(p_{\text{L}}, p_{\text{T}})} [(1-q)p_{\text{L}} + q\mathrm{e}^{k(1-\gamma)}p_{\text{T}} + q\mathrm{e}^{-k\gamma}(1-p_{\text{T}})] \tag{32}$$

and the maximisation is taken over all admissible pairs $(p_{\text{L}}, p_{\text{T}})$.

Proof. Proof by induction. The statement is trivial for $l = 0$ and the second induction step follows directly from applying the ansatz (31) to equation (30) (and we directly obtain the form of $\alpha(q, \gamma, k)$ given in equation (32)). □

As an immediate corollary (set $x = 0$) we get a bound on the desired probability

$$\Pr[F] = \Pr[S_n \geqslant \gamma R_n \wedge H_n] = \Pr[X_n \geqslant 0 \wedge H_n] \leqslant [\alpha(q, \gamma, k)]^n. \tag{33}$$

Since this holds for any $k \geqslant 0$, we choose the tightest bound

$$\alpha_{\min}(q, \gamma) := \min_{k\geqslant 0} \alpha(q, \gamma, k), \tag{34}$$

which leads to the final bound

$$\Pr[F] \leqslant [\alpha_{\min}(q, \gamma)]^n . \tag{35}$$

While we do not know how to find $\alpha_{\min}(q, \gamma)$ analytically, numerical evaluation is straightforward as explained in appendix B. Some numerical results are plotted in figure 5.

3. Conclusions

We have proposed a protocol implementing DI WSE and proved security in two scenarios. In the memoryless scenario the device is first extensively tested which allows to estimate the incompatibility between the two measurements. This turns out to be sufficient to show a lower bound on the min-entropy of the output (against a classical adversary), which happens to be tight. Due to the SDP formulation of the min-entropy we can show that the lower bound is additive when multiple rounds are played (which is not obvious since Bob's attack could introduce correlations between different rounds). Moreover, we have considered a model in which the devices used by Alice might have memory but Bob is restricted to sequential attacks. In this case a martingale-style approach leads to an explicit security statement.

A secure implementation of WSE leads directly to bit commitment since the reduction involves classical post-processing only (which is trusted even in the DI setting). To turn WSE into some arbitrary universal functionality (e.g. oblivious transfer) one needs to add trusted quantum communication or a secure (quantum proof) implementation of another cryptographic primitive called interactive hashing (for explicit security bounds for such constructions see sections IV and V of [KWW12]). Alternatively, one can use our techniques to directly prove security of an oblivious transfer protocol (in the bounded storage model) proposed in [DFR+07].

While this work constitutes a significant progress in the field of DI two-party cryptography, many open questions remain. In the memoryless case we only obtain bounds on the min-entropy, while it is often advantageous to derive bounds on other Rényi entropies. The problematic step in this case is the additivity of lower bounds if multiple rounds are played. In case of the min-entropy additivity is a direct consequence of the SDP formulation (the same observation holds for the collision entropy corresponding to the pretty good measurement) but we do not know if additivity holds in general. While this problem might seem purely technical, it is of practical relevance as it would lead to significantly better security guarantees.

Another important open question is the analysis of devices with memory. In our analysis we have assumed that Bob's attack is sequential. Unfortunately, we know that sequential attacks are not always optimal (even if Alice's behaviour is sequential, see appendix C for a simple counterexample). A security proof for devices with memory in this scenario is arguably the most important open question related to DI two-party cryptography.

Finally, we note that in the realm of the noisy-storage model there are much more sophisticated analyses [DFW15], which do not rely on the fact that we will first bound the adversary's information about the string X^n when he is holding classical information, and subsequently relate this to his information about X^n *including* quantum information. Instead, one establishes a direct link between the adversary's quantum information and his uncertainty about X^n [DFW15]. It remains an interesting open question whether these techniques can be applied in the DI setting.

Acknowledgments

We thank Rotem Arnon-Friedman, Matthias Christandl, Yfke Dulek, David Elkouss, Serge Fehr, Fabian Furrer, Iordanis Kerenidis, Le Phuc Thinh, Christian Schaffner, Florian Speelman, Marco Tomamichel, Gonzalo de la Torre and Thomas Vidick for interesting discussions. JK is supported by Ministry of Education, Singapore. SW is funded by STW, NWO VIDI and an ERC Starting Grant.

Appendix A. Effective anticommutation is not sufficient against classical side information

Let $\{|j\rangle\}_{j=0}^{3}\}$ be a basis for a four-dimensional Hilbert space. Consider the state

$$\rho_A = \frac{1}{2}(|0\rangle\langle 0| + |2\rangle\langle 2|)$$

and binary observables

$$A_0 = |0\rangle\langle 0| - |1\rangle\langle 1| + |2\rangle\langle 2| - |3\rangle\langle 3|,$$
$$A_1 = |0\rangle\langle 0| - |1\rangle\langle 1| - |2\rangle\langle 2| + |3\rangle\langle 3|.$$

It is easy to check that the anticommutator equals

$$\{A_0, A_1\} = 2(|0\rangle\langle 0| + |1\rangle\langle 1| - |2\rangle\langle 2| - |3\rangle\langle 3|),$$

which implies that the effective anticommutator equals $\frac{1}{2}\mathrm{tr}(\{A_0, A_1\}\rho_A) = 0$. While observable A_0 leads to no uncertainty, it is easy to verify that if we measure observable A_1 we obtain a uniform outcome. Indeed, it is possible to show non-trivial lower bound on $H_\alpha(X|\Theta)$.

Now, suppose that somebody holds an extra bit of classical information about the system. More specifically, we consider

$$\rho_{AK} = \frac{1}{2}(|0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_K + |2\rangle\langle 2|_A \otimes |1\rangle\langle 1|_K).$$

Measuring observable A_1 now leads to an outcome which is still uniform but it is perfectly correlated with the classical register K. Therefore, $H_\alpha(X|K\Theta) = 0$, which demonstrates that effective anticommutation does not imply uncertainty against classical side information. This is consistent with evaluating the absolute effective anticommutator $\frac{1}{2}\mathrm{tr}(|\{A_0, A_1\}|\rho_A) = 1$, which does not yield a non-trivial uncertainty bound.

Appendix B. Numerical evaluation of $\alpha_{\min}(q, \gamma)$

Recall that our goal is to evaluate

$$\alpha_{\min}(q, \gamma) := \min_{k \geqslant 0} \max_{(p_{\mathrm{L}}, p_{\mathrm{T}})} [(1 - q)p_{\mathrm{L}} + q\mathrm{e}^{k(1-\gamma)}p_{\mathrm{T}} + q\mathrm{e}^{-k\gamma}(1 - p_{\mathrm{T}})].$$

We first show that the maximisation over the admissible pairs $(p_{\mathrm{L}}, p_{\mathrm{T}})$ can be performed analytically. Since the expression inside the square bracket is increasing in both p_{L} and p_{T} the optimal point lies at the boundary, which can be parametrised by the effective absolute anticommutator $t = \frac{1}{2}\mathrm{tr}(|\{A_0, A_1\}|\,\rho_A) \in [0,\ 1]$. Let us restate equations (22) and (23)

$$p_{\mathrm{L}}(t) = \frac{1}{2} + \frac{1}{2\sqrt{2}}\sqrt{1+t},$$
$$p_{\mathrm{T}}(t) = \frac{1}{2} + \frac{1}{4}\sqrt{1+\sqrt{1-t^2}} = \frac{1}{2} + \frac{1}{4\sqrt{2}}(\sqrt{1+t} + \sqrt{1-t}).$$

Solving the maximisation problem corresponds to calculating $g(k) := \max_{t\in[0,1]} f_k(t)$ for

$$f_k(t) := A\sqrt{1+t} + B\sqrt{1-t} + C$$

with

$$A = \frac{1}{4\sqrt{2}}[2(1-q) + q\mathrm{e}^{-k\gamma}(\mathrm{e}^k - 1)],$$
$$B = \frac{q\mathrm{e}^{-k\gamma}(\mathrm{e}^k - 1)}{4\sqrt{2}},$$
$$C = \frac{1-q}{2} + \frac{q\mathrm{e}^{-k\gamma}(\mathrm{e}^k + 1)}{2}.$$

The first two terms can be written as an inner product $\langle u, v\rangle$ for $u = (A, B)$ and $v = (\sqrt{1+t}, \sqrt{1-t})$. Applying the Cauchy–Schwarz inequality leads to the following upper bound

$$g(k) \leqslant \sqrt{2(A^2 + B^2)} + C, \tag{B1}$$

which can be achieved by choosing $t = (A^2 - B^2)/(A^2 + B^2)$.

We do not know how to minimise $g(k)$ over $k \geqslant 0$ analytically but numerically it is an easy task because for all valid (q, γ) we have $g(0) = 1$ and $\lim_{k\to\infty} g(k) = \infty$ and the function is convex. Therefore, there is a unique minimum which corresponds precisely to $\alpha_{\min}(q, \gamma)$.

There are three cases in which we should not be able to prove security:

- Alice never tests: $q = 0$.
- Alice always tests: $q = 1$.
- The threshold is classical: $\gamma = \frac{3}{4}$.

Here, we show that in all other cases we get $\alpha_{\min}(q, \gamma) < 1$. Assuming that $q \neq 1$ (if $q = 1$ there is no security possible anyway) we find the Taylor expansion around $k = 0$

$$\sqrt{2(A^2 + B^2)} = \frac{1-q}{2} + \frac{q}{4}k + O(k^2),$$
$$C = \frac{1+q}{2} + \frac{q(1-2\gamma)}{2}k + O(k^2)$$

and therefore

$$g(k) = 1 + \left(\frac{3}{4} - \gamma\right)qk + O(k^2).$$

This shows that whenever $q > 0$ and $\gamma > \frac{3}{4}$ setting k small enough leads to $g(k) < 1$, which concludes the argument.

Appendix C. Sequential guessing is not necessarily optimal

Consider a device which can be used twice and recall that we use Θ_k and X_k to denote the input and output in the kth round, respectively. Alice's subsystem consists of two qubits while Bob's subsystem is a qudit. The initial state is

$$\rho_{A_1A_2B} = \frac{1}{2}(|0\rangle\langle 0|_{A_1} \otimes |0\rangle\langle 0|_{A_2} + |1\rangle\langle 1|_{A_1} \otimes |1\rangle\langle 1|_{A_2}) \otimes \rho_B$$

for some fixed ρ_B. Since Bob's state is uncorrelated, it carries no useful information so we can ignore it and assume that Bob picks his 'guessing functions' deterministically. In the first round the device of Alice performs the computational basis measurement on the first qubit regardless of the value of Θ_1. Therefore, the state after the first round is

$$\rho_{X_1A_2} = \frac{1}{2}(|0\rangle\langle 0|_{X_1} \otimes |0\rangle\langle 0|_{A_2} + |1\rangle\langle 1|_{X_1} \otimes |1\rangle\langle 1|_{A_2}).$$

In the second round the device performs a projective measurement on the second qubit but the basis depends on Θ_2: if $\Theta_2 = X_1$ the qubit is measured in the computational basis (which ensures that $X_1 = X_2$, while if $\Theta_2 \neq X_1$ the qubit is measured in the Hadamard basis (which leads toX_1 and X_2 being uncorrelated). It is easy to verify that the resulting probability distribution $P_{X_1X_2\Theta_2}$ (we have ignored Θ_1 since it is uncorrelated from the other random variables) is

Θ_2	X_1	X_2	Pr
0	0	0	1/4
0	1	0	1/8
0	1	1	1/8
1	0	0	1/8
1	0	1	1/8
1	1	1	1/4

In the general scenario it is optimal for Bob to guess $X_1 = \Theta_2$ and $X_2 = \Theta_2$ which succeeds with probability $\frac{1}{2}$.

However, in the sequential scenario Bob must attempt to guess X_1 before he learns Θ_2. It is easy to verify that in this case his guessing probability is at most $\frac{3}{8}$.

References

[ABG+07] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 Device-independent security of quantum cryptography against collective attacks *Phys. Rev. Lett.* **98** 230501

[AGM06] Acín A, Gisin N and Masanes L 2006 From Bell's theorem to secure quantum key distribution *Phys. Rev. Lett.* **97** 120405

[AK15] Adlam E and Kent A 2015 Device-independent relativistic quantum bit commitment *Phys. Rev.* A **92** 022315

[AMPS15] Aharon N, Massar S, Pironio S and Silman J 2015 *Device-independent bit commitment based on the CHSH inequality*

[ARKP15] Aguilar E A, Ramanathan R, Kofler J and Pawłowski M 2015 Completely device independent quantum key distribution arXiv:1507.05752

[BB84] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Conf. on Computers, Systems and Signal Processing* online: http://cs.ucsb.edu/~chong/290N-W06/BB84.pdf

[BCK13] Barrett J, Colbeck R and Kent A 2013 Memory attacks on device-independent quantum cryptography *Phys. Rev. Lett.* **110** 010503

[BCP+14] Brunner N, Cavalcanti D, Pironio S, Scarani V and Wehner S 2014 Bell nonlocality *Rev. Mod. Phys.* **86** 419

[Bel64] Bell J S 1964 On the Einstein–Podolsky–Rosen paradox *Physics* **1** 195–200

[BFW14] Berta M, Fawzi O and Wehner S 2014 Quantum to classical randomness extractors *IEEE Trans. Inf. Theory* **60** 1168–92

[BGKW88] Ben-Or M, Goldwasser S, Kilian J and Wigderson A 1988 Multi-prover interactive proofs: how to remove intractability assumptions *Proc. 20th ACM STOC*

[BHK05] Barrett J, Hardy L and Kent A 2005 No signaling and quantum key distribution *Phys. Rev. Lett.* **95** 010503

[BPPP14] Bouda J, Pawłowski M, Pivoluska M and Plesch M 2014 Device-independent randomness extraction for arbitrarily weak min-entropy source *Phys. Rev.* A **90** 032313

[BWW08] Ballester M A, Wehner S and Winter A 2008 State discrimination with post-measurement information *IEEE Trans. Inf. Theory* **54** 4183–98

[Cac97] Cachin C 1997 Entropy measures and unconditional security in cryptography *PhD Thesis* ETH Zurich

[CHSH69] Clauser J F, Horne M A, Shimony A and Holt R A 1969 Proposed experiment to test local hidden-variable theories *Phys. Rev. Lett.* **23** 880

[CK11] Colbeck R and Kent A 2010 Private randomness expansion with untrusted devices *J. Phys. A: Math. Theor.* **44** 095305

[Col07] Colbeck R 2007 Impossibility of secure two-party classical computation *Phys. Rev.* A **76** 062308

[Cré97] Crépeau C 1997 Efficient cryptographic protocols based on noisy channels *Advances in Cryptology: Proc. EUROCRYPT '97 LNCS* vol 1233

[CSST11] Crépeau C, Salvail L, Simard J-R and Tapp A 2011 Two provers in isolation *Advances in Cryptology: Proc. ASIACRYPT '11 LNCS* vol 7073

[CVY13] Coudron M, Vidick T and Yuen H 2013 Robust randomness amplifiers: upper and lower bounds *Proc. 16th APPROX and 17th RANDOM LNCS* vol 8096

[DFR+07] Damgård I B, Fehr S, Renner R, Salvail L and Schaffner C 2007 A tight high-order entropic quantum uncertainty relation with applications *Advances in Cryptology: Proc. CRYPTO '07 LNCS* vol 4622

[DFSS05] Damgård I B, Fehr S, Salvail L and Schaffner C 2005 Cryptography in the bounded quantum-storage model *Proc. 46th IEEE FOCS*

[DFW15] Dupuis F, Fawzi O and Wehner S 2015 Entanglement sampling and applications *IEEE Trans. Inf. Theory* **61** 1093–112

[Eke91] Ekert A K 1991 Quantum cryptography based on Bell's theorem *Phys. Rev. Lett.* **67** 661

[ENG+14] Erven C, Ng N H Y, Gigov N, Laflamme R, Wehner S and Weihs G 2014 An experimental implementation of oblivious transfer in the noisy storage model *Nat. Commun.* **5** 3418

[FSW15] Furrer F, Schaffner C and Wehner S 2015 Continuous-variable protocols in the noisy-storage model arXiv:1509.09123

[Kan15] Kaniewski J 2015 Relativistic quantum cryptography *PhD Thesis* National University of Singapore arXiv:1512.00602

[Ken99] Kent A 1999 Unconditionally secure bit commitment *Phys. Rev. Lett.* **83** 1447

[Ken05] Kent A 2005 Secure classical bit commitment using fixed capacity communication channels *J. Cryptol.* **18** 313

[Ken11] Kent A 2011 Unconditionally secure bit commitment with flying qudits *New J. Phys.* **13** 113015

[Ken12] Kent A 2012 Unconditionally secure bit commitment by transmitting measurement outcomes *Phys. Rev. Lett.* **109** 130501

[KTHW13] Kaniewski J, Tomamichel M, Hänggi E and Wehner S 2013 Secure bit commitment from relativistic constraints *IEEE Trans. Inf. Theory* **59** 4687

[KTW14] Kaniewski J, Tomamichel M and Wehner S 2014 Entropic uncertainty from effective anticommutators *Phys. Rev.* A **90** 012332

[KWW12] König R, Wehner S and Wullschleger J 2012 Unconditional security from noisy quantum storage *IEEE Trans. Inf. Theory* **58** 1962

[LC97] Lo H-K and Chau H 1997 Is quantum bit commitment really impossible? *Phys. Rev. Lett.* **78** 3410

[Lo97] Lo H-K 1997 Insecurity of quantum secure computations *Phys. Rev.* A **56** 1154

[LPT+13] Lim C C W, Portmann C, Tomamichel M, Renner R and Gisin N 2013 Device-independent quantum key distribution with local Bell test *Phys. Rev.* X **3** 031006

[Mau91] Maurer U M 1991 A provably-secure strongly-randomized cipher *Advances in Cryptology: Proc. EUROCRYPT '90 LNCS* (Berlin: Springer) pp 361–73

[May97] Mayers D 1997 Unconditionally secure quantum bit commitment is impossible *Phys. Rev. Lett.* **78** 3414

[MS14a] Miller C A and Shi Y 2014 Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices *Proc. 46th ACM STOC* **2014** 417

[MS14b] Miller C A and Shi Y 2014 Universal security for randomness expansion from the spot-checking protocol arXiv:1411.6608

[MY98] Mayers D and Yao A C-C 1998 Quantum cryptography with imperfect apparatus *Proc. 39th IEEE FOCS*

[MY04] Mayers D and Yao A C-C 2004 Self testing quantum apparatus *Quantum. Inf. Comput.* (arXiv:quant-ph/0307205)

[NJM+12] Ng N H Y, Joshi S K, Ming C C, Kurtsiefer C and Wehner S 2012 Experimental implementation of bit commitment in the noisy-storage model *Nat. Commun.* **3** 1326

[PAM+10] Pironio S *et al* 2010 Random numbers certified by Bell's theorem *Nature* **464** 1021

[Riv99] Rivest R L 1999 *Unconditionally secure commitment and oblivious transfer schemes using private channels and a trusted initializer* http://people.csail.mit.edu/rivest/pubs/Riv99d.pdf.

[RUV13] Reichardt B W, Unger F and Vazirani U 2013 Classical command of quantum systems *Nature* **496** 456

[SCA+11] Silman J, Chailloux A, Aharon N, Kerenidis I, Pironio S and Massar S 2011 Fully distrustful quantum bit commitment and coin flipping *Phys. Rev. Lett.* **106** 220501

[Sim07] Simard J-R 2007 Classical and quantum strategies for bit commitment schemes in the two-prover model *Masters Thesis* McGill University (http://crypto.cs.mcgill.ca/~crepeau/PDF/memoire-JR.pdf)

[TH13] Tomamichel M and Hänggi E 2013 The link between entropic uncertainty and nonlocality *J. Phys. A: Math. Theor.* **46** 055301

[VV12] Vazirani U and Vidick T 2012 Certifiable quantum dice: or, true random number generation secure against quantum adversaries *Proc. 44th ACM STOC*

[VV14] Vazirani U and Vidick T 2014 Fully device-independent quantum key distribution *Phys. Rev. Lett.* **113** 140501

[Weh08] Wehner S 2008 Cryptography in a quantum world *PhD Thesis* Universiteit van Amsterdam

[WNI03] Winter A, Nascimento A C A and Imai H 2003 Commitment capacity of discrete memoryless channels *Cryptography and Coding LNCS* **2898** 35

[WST08] Wehner S, Schaffner C and Terhal B 2008 Cryptography from noisy storage *Phys. Rev. Lett.* **100** 220502