Fully Device-Independent Quantum Key Distribution Using Synchronous Correlations

Nishant Rodrigues
Department of Computer Science, University of Maryland, College Park, MD, USA
Joint Center for Quantum Information and Computer Science, College Park, MD, USA

Brad Lackey
Microsoft Quantum, Redmond, WA, USA

Abstract

We derive a device-independent quantum key distribution protocol based on synchronous correlations and their Bell inequalities. This protocol offers several advantages over other device-independent schemes including symmetry between the two users and no need for pre-shared randomness. We close a "synchronicity" loophole by showing that an almost synchronous correlation inherits the self-testing property of the associated synchronous correlation. We also pose a new security assumption that closes the "locality" (or "causality") loophole: an unbounded adversary with even a small uncertainty about the users' choice of measurement bases cannot produce any almost synchronous correlation that approximately maximally violates a synchronous Bell inequality.

2012 ACM Subject Classification Theory of computation → Cryptographic protocols; Hardware → Quantum communication and cryptography; Theory of computation → Quantum information theory

Keywords and phrases quantum cryptography, device independence, key distribution, security proofs, randomness

Digital Object Identifier 10.4230/LIPIcs.TQC.2023.8

1 Introduction

Quantum key distribution (QKD) allows two parties to establish a shared classical secret key using quantum resources. The two main requirements of QKD are (1) Correctness: the two parties, Alice and Bob, get the same key; and (2) Security: an adversary Eve gets negligible information about the key. Device-independent quantum key distribution (DI-QKD) is entanglement-based, and aims to prove security of QKD based solely on the correctness of quantum mechanics, separation of devices used by the two parties, and passing of statistical tests known as Bell violations [23, 16]. These protocols are usually specified by a non-local game, characterized by a conditional probability distribution or *correlation* $p(y_A, y_B \,|\, x_A, x_B)$. Intuitively, Alice and Bob obtain or generate random inputs x_A and x_B respectively, and the correlation describes the likelihood their entangled quantum devices return outputs y_A and y_B to each respectively. We will be interested in symmetric correlations and so will take $x_A, x_B \in X$ and $y_A, y_B \in Y$ where X and Y are finite sets; for our protocol specifically $X = \{0, 1, 2\}$ and $Y = \{0, 1\}$.

In general, security of a DI-QKD scheme relies on the monogamy of entanglement. The key result is that maximally entangled quantum states are separable within any larger quantum system. In cryptographic terms, if Alice and Bob share a maximally entangled state then the results of measurements they make on this state will be uncorrelated to any other measurement results an adversary can perform. Hence, presuming the correctness of quantum mechanics, no adversary can have any information about key bits Alice and Bob may generate through this process. Generally, a DI-QKD protocol will involve two types of

18th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2023).
Editors: Omar Fawzi and Michael Walter; Article No. 8; pp. 8:1–8:22
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

rounds: testing rounds where Alice and Bob (publicly) share their inputs and output results for performing statistics tests, and data rounds where they obtain shared secret bits. The goal of the testing rounds is to produce a certificate that Alice and Bob are operating on maximally entangled states.

Most current DI-QKD schemes are based on the CHSH inequality, a linear inequality in $p(y_A, y_B \,|\, x_A, x_B)$, which if satisfied characterizes classical statistics within a quantum system. Hence a violation of this inequality is a certificate of quantum behavior. This inequality exhibits "rigidity" in that the only quantum state that produces a maximal violation of the inequality is (up to natural equivalences) a Bell pair. Thus the goal of the testing rounds in a DI-QKD protocol is to statistically verify that the system produces a maximal violation of the CHSH inequality.

In a non-local game Alice and Bob may preshare an entangled resource in each round, but are not allowed any communication between receiving or generating their inputs x_A and x_B and measuring the system to obtain their outputs y_A and y_B. This is typically called a "nonsignaling" condition, leading to *nonsignaling correlations* which include all quantum strategies. If (even classical) communication between Alice and Bob is possible, then it is simple to classically simulate a correlation that produces a maximal violation of the CHSH inequality, and hence any certificates of quantumness or entanglement are void [22]. This *locality* or *causality loophole* in the security proof is challenging to avoid; the only known means to close it is by having Alice and Bob acausally separated during each round: bounds on the speed of light prevent such communication [11, 9, 21].

A *synchronous correlation* is one such that $p(y_A, y_B \mid x, x) = 0$ whenever $y_A \neq y_B$ and $x \in X$. That is, whenever Alice and Bob input the same value they are guaranteed to receive the same outputs, although that value may be nondeterministic. These correlations have recently become popular owing to their use in the resolution of the Connes Embedding Conjecture and Tsirl'son's Problem [12], but have also been used to generalize combinatorial properties to the quantum setting [14, 17, 13].

We present a fully device-independent QKD protocol based on synchronous correlations. This protocol is symmetric, in that roles of Alice and Bob are completely interchangeable. This is an advantage over other DI-QKD protocols based on the CHSH inequality [23] (which is neither symmetric nor synchronous) as sender versus receiver roles do not need to be negotiated. Additionally, as Alice and Bob select their inputs independently they do not need pre-shared secret bits to decide upon testing versus data rounds.

The mathematical framework needed to prove device-independent security of this protocol was laid out in [20], where four analogues of the Bell/CHSH inequality for synchronous correlations were given. In this work we focus only on one of these, $J_3(p) \geq 0$ (see Equation (3) below). As well, bounds on quantum violations of these were given ($J_3(p) \geq -\frac{1}{8}$), and rigidity of correlations that achieve a maximal violation proven. The two critical analyses needed to complete a proof of security for our DI-QKD protocol are as follows. First, we must prove that if the system is observed to be close to the maximal violation then it is close to the ideal system, which measures a Bell pair. Then, we provide an alternative security assumption that bypasses the causality loophole.

We tackle the first of these through two theorems. For context, Alice and Bob will select their inputs from $X = \{0, 1, 2\}$ and each measure a quantum system that produces a bit output from $Y = \{0, 1\}$. The ideal system, that produces $J_3(p) = -\frac{1}{8}$, involves measuring a Bell pair using three specific projection-valued measures $\{\hat{E}^x_y\}_{y=0,1}$ for $x = 0, 1, 2$ given in Equation (1) below. Any synchronous quantum correlation that achieves $J_3(p) = -\frac{1}{8}$ must have $E_y^x = \hat{E}_y^x \otimes \mathbb{1}$, and hence the measurements have no influence on the larger system. In Section 3 we show that if we take a *synchronous* quantum system that is close to achieving maximal J_3 violation, then it must be close to the ideal system in trace norm.

Unfortunately this introduces a "synchronicity" loophole: rigidity holds among synchronous correlations, but are there asynchronous correlations with $J_3 = -\frac{1}{8}$ that cannot certify maximal entanglement? In Section 4, we close this loophole using recent work on "almost synchronous" correlations [24]. This leads to our complete DI-QKD scheme given as Algorithm 1 below, where in addition to verifying a Bell violation one also bounds the total amount of asynchronicity of the correlation, S, as defined in Equation (7).

In Section 5 we use the Entropy Accumulation Theorem (EAT) [8] to bound the the min-entropy of the outputs given an adversary's side-information. This allows us to derive the key rate of Algorithm 1.

Finally, in Section 6, we pose a new security assumption to close the *causality* or *locality* loophole: the adversary Eve may have unlimited communication and computational power, yet she has imperfect knowledge of Alice and Bob's inputs. Informally, given nonnegative values $\lambda \leq \frac{1}{8}$ and $\mu \leq 1$ there exists a bound ϵ_{max} such that if Eve's uncertainty about Alice and Bob's inputs is greater than ϵ_{max} then there is no device she can create where Alice and Bob's expected Bell violation J_3 and asynchronicity S satisfy $-\frac{1}{8} \leq J_3 \leq -\frac{1}{8} + \lambda$ and $0 \leq S \leq \mu$.

2 Preliminaries

We present some definitions that will be used in the protocol later. Like other device-independent schemes, our protocol is expressed in terms of a nonlocal game, which is characterized by a conditional probability distribution (or correlation) $p(y_A, y_B|x_A, x_B)$ where $x_A, x_B \in X$ and $y_A, y_B \in Y$ are from finite sets X and Y. By a nonlocal game we mean the players Alice and Bob will receive inputs $x_A, x_B \in X$ from a referee and will produce outputs $y_A, y_B \in Y$. These are then adjudicated by the referee against some criterion, synchronicity in our case. Alice and Bob are not allowed to communicate once they receive their inputs, which is characterized by the famous nonsignaling conditions on the correlation [19, 6].

▶ **Definition 1.** *A correlation is* synchronous *if $p(y_A, y_B \mid x, x) = 0$ whenever $x \in X$ and $y_A \neq y_B \in Y$. A correlation is* symmetric *if $p(y_A, y_B \mid x_A, x_B) = p(y_B, y_A \mid x_B, x_A)$.*

Unlike nonlocal games such as the CHSH or Magic Square games, or their generalizations [15, 18, 6, 3, 7], it is straightforward for Alice and Bob to create a perfect winning strategy for synchronicity. Prior to the games they agree on some function $f : X \to Y$, then regardless of how the referee selects $x_A, x_B \in X$, they output $y_A = f(x_A)$ and $y_B = f(x_B)$. Hence the "value" of any synchronous game (Alice's and Bob's expected success probability) is always 1, and so value plays no role in the following.

The analysis of nonlocal games relies on understanding the set of local (or "classical" or "hidden variables") correlations like the one above within the set of quantum correlations. While a general quantum correlation has the form $p(y_A, y_B \mid x_A, x_B) = \mathrm{tr}(\rho(E_{y_A}^{x_A} \otimes F_{y_B}^{x_B}))$ for a density operator ρ and sets of positive operator-valued measures $\{E_y^x\}_{y \in Y}$ and $\{F_y^x\}_{y \in Y}$ on Hilbert spaces $\mathfrak{H}_A$ and $\mathfrak{H}_B$, a synchronous quantum correlation is always a convex combination of so-called "tracial" states [17, 20] of the form $p(y_A, y_B \mid x_A, x_B) = \frac{1}{d}\mathrm{tr}(E_{y_A}^{x_A} E_{y_B}^{x_B})$ where $d = \dim \mathfrak{H}_A$.

For input and output $X = \{0, 1, 2\}$ and $Y = \{0, 1\}$, respectively, there are four Bell inequalities for synchronous hidden variables theories. That is, the synchronous classical correlations (among general nonsignaling synchronous correlations) are characterized by four inequalities $J_0, J_1, J_2, J_3 \geq 0$ where each $J_i = J_i(p)$ is a linear combination of the correlation components $p(y_A, y_B \mid x_A, x_B)$. For this work, we will focus only on one of these as given in Equation (3) below (see also [20]).

Synchronous quantum correlations can violate the inequality $J_3 \geq 0$. However one can show an analogue of Tsirl'son bound, in that any synchronous quantum correlation must have $J_3 \geq -\frac{1}{8}$. This follows from Equation (6) below. Of particular interest are correlations that maximize this quantum violation. Like CHSH or Magic Square games, one can show a rigidity result: there is a unique synchronous quantum correlation with $J_3 = -\frac{1}{8}$, which involves a maximally entangled state shared between Alice and Bob. One can then use principal decompositions, or two projections theory, to convert this into a self-test for certifying a single EPR pair, the basis for device-independence.

We denote the binary entropy function by $h(p) = -p\log(p) - (1-p)\log(1-p)$ for $p \in [0,1]$. The von Neumann entropy of a quantum state ρ is given by $H(\rho) = -\mathrm{tr}(\rho\log(\rho))$. Given two operators ρ_1 and ρ_2, we say $\rho_1 \geq \rho_2$ if $\rho_1 - \rho_2 \geq 0$.

▶ **Definition 2.** *For a bipartite quantum state $\rho_{AB} \in \mathfrak{H}_A \otimes \mathfrak{H}_B$, the min-entropy of A conditioned on B is:*

$$H_{\min}(A \mid B)_{\rho_{AB}} = \max\{s \in \mathbb{R} : \exists \sigma_B \in \mathcal{D}(\mathfrak{H}_B) \textit{ such that } 2^{-s}\mathrm{id}_A \otimes \sigma_B \geq \rho_{AB}\}$$

where $\mathcal{D}(\mathfrak{H}_B)$ is the set of density operators in $\mathfrak{H}_B$.

The ϵ-smooth version of the conditional min-entropy considers states that are ϵ-close to ρ_{AB}. The notion of closeness that is typically used is the purified distance $P(\rho,\sigma) = \sqrt{1 - F(\rho,\sigma)^2}$, where $F(\rho,\sigma)$ is the fidelity between states ρ and σ.

▶ **Definition 3.** *For a bipartite quantum state $\rho_{AB} \in \mathfrak{H}$, the ϵ-smooth min-entropy of A conditioned on B is defined as:*

$$H^{\epsilon}_{\min}(A \mid B)_{\rho_{AB}} = \max_{\substack{\tilde{\rho}_{AB} \in \mathcal{S}(\mathfrak{H}) \\ P(\rho_{AB}, \tilde{\rho}_{AB}) \leq \epsilon}} H_{\min}(A \mid B)_{\tilde{\rho}_{AB}}$$

The quantum ϵ-smooth max-entropy is defined as:

$$H^{\epsilon}_{\max}(A \mid B)_{\rho_{AB}} = \log \inf_{\substack{\tilde{\rho}_{AB} \in \mathcal{S}(\mathfrak{H}) \\ P(\rho_{AB}, \tilde{\rho}_{AB}) \leq \epsilon}} \sup_{\sigma_B} \left|\left|\tilde{\rho}_{AB}^{\frac{1}{2}} \sigma_B^{-\frac{1}{2}}\right|\right|_1^2 .$$

where $\mathcal{S}(\mathfrak{H})$ is the set of sub-normalized states in $\mathfrak{H}$ and $||A||_\alpha = \mathrm{tr}\left(\left(\sqrt{A^\dagger A}\right)^\alpha\right)^{\frac{1}{\alpha}}$.

3 A synchronous DI-QKD protocol

We present a synchronous device-independent quantum key distribution protocol that is symmetric with respect to Alice and Bob, each party performing the same tasks.

Suppose Alice and Bob share an EPR pair. Each draws $x_A, x_B \in X = \{0,1,2\}$ respectively, and measures according to $\{\hat{E}^{x_A}_y\}_{y \in Y}$ and $\{\hat{E}^{x_B}_y\}_{y \in Y}$ to get outputs $y_A, y_B \in Y = \{0,1\}$, where the projection-valued measures $\{\hat{E}^x_y\}_{y \in \{0,1\}}$ for $x \in \{0,1,2\}$ are:

$$\begin{aligned}
&\hat{E}^0_1 = |\phi_0\rangle\langle\phi_0|,\ \hat{E}^0_0 = \mathbb{1} - \hat{E}^0_1, \quad \text{where } |\phi_0\rangle = |1\rangle \\
&\hat{E}^1_1 = |\phi_1\rangle\langle\phi_1|,\ \hat{E}^1_0 = \mathbb{1} - \hat{E}^1_1, \quad \text{where } |\phi_1\rangle = \tfrac{\sqrt{3}}{2}|0\rangle + \tfrac{1}{2}|1\rangle \\
&\hat{E}^2_1 = |\phi_2\rangle\langle\phi_2|,\ \hat{E}^2_0 = \mathbb{1} - \hat{E}^2_1, \quad \text{where } |\phi_2\rangle = \tfrac{\sqrt{3}}{2}|0\rangle - \tfrac{1}{2}|1\rangle
\end{aligned} \tag{1}$$

The likelihood of Alice's and Bob's results are characterized by the correlation [20]

$$p(y_A, y_B \mid x_A, x_B) = \frac{1}{2}\mathrm{tr}(\hat{E}^{x_A}_{y_A}\hat{E}^{x_B}_{y_B}).$$

In particular, this strategy produces a synchronous quantum correlation with correlation matrix:

$$[p(y_A, y_B|x_A, x_B)] = \frac{1}{8}\begin{array}{c|ccccccccc|c} & (0,0) & (0,1) & (0,2) & (1,0) & (1,1) & (1,2) & (2,0) & (2,1) & (2,2) & \\ \hline & 4 & 1 & 1 & 1 & 4 & 1 & 1 & 1 & 4 & (0,0) \\ & 0 & 3 & 3 & 3 & 0 & 3 & 3 & 3 & 0 & (0,1) \\ & 0 & 3 & 3 & 3 & 0 & 3 & 3 & 3 & 0 & (1,0) \\ & 4 & 1 & 1 & 1 & 4 & 1 & 1 & 1 & 4 & (1,1) \end{array} \tag{2}$$

One can verify this correlation yields a maximal violation of the Bell inequality, $J_3 = -\frac{1}{8}$, where

$$\begin{aligned} J_3 \quad = \quad & 1 - \tfrac{1}{4}\big(\, p(0,1 \mid 0,1) + p(1,0 \mid 0,1) + p(0,1 \mid 1,0) + p(1,0 \mid 1,0) \\ & + p(0,1 \mid 0,2) + p(1,0 \mid 0,2) + p(0,1 \mid 2,0) + p(1,0 \mid 2,0) \\ & + p(0,1 \mid 1,2) + p(1,0 \mid 1,2) + p(0,1 \mid 2,1) + p(1,0 \mid 2,1)\,\big). \end{aligned} \tag{3}$$

This correlation is rigid in that any synchronous quantum correlation that achieves $J_3 = -\frac{1}{8}$ must have implemented the strategy above. This follows from our Theorem 4 below. In particular, this maximal violation of J_3 is a self-test of the device to detect interference from adversary: Alice and Bob can certify that their devices hold maximally entangled pairs, and by monogamy of entanglement can establish that Eve doesn't have any information about their inputs.

Our protocol extends the above scenario to n rounds. It is important to note that the observable for our synchronous Bell inequality (3) only involves correlations where Alice and Bob use different inputs. Critically, neither Alice nor Bob must pre-select which rounds will used for testing versus key generation. Upon revealing their choices of bases, testing rounds are given by those where they selected different bases and key generation rounds where they selected the same basis. In particular, they need not have any pre-shared randomness.

Of course no physical device adheres to a theoretical model perfectly, so in practice one still must perform standard information reconciliation and privacy amplification on the results.

Once the n rounds of the protocol are over, Alice and Bob communicate their basis selection over an authenticated classical channel. When they chose different bases (i.e. $x_A \neq x_B$), they exchange their measurement outcomes and use those to compute J_3. If the value of J_3 deviates too much from $-\frac{1}{8}$, they abort. The protocol is synchronous, therefore $y_A = y_B$ whenever $x_A = x_B$ and those can be used as the raw key bits for further standard privacy amplification and information reconciliation.

Our first main result is our technical rigidity statement that synchronous quantum correlations near $J_3 = -\frac{1}{8}$ have the desired security. Informally, after splitting off a space $\mathfrak{L}$ of small relative dimension, the correlation's projections are near (in trace norm) the ideal one, which separates Alice and Bob performing the perfect protocol on $\mathbb{C}^2$, and Eve and all other parties receiving no information having measurement outcomes from $\mathbb{1}_{\mathfrak{K}}$.

▶ **Theorem 4.** *Let $p(y_A, y_B \mid x_A, x_B) = \frac{1}{d}\mathrm{tr}(E^{x_A}_{y_A} E^{x_B}_{y_B})$ be a synchronous quantum correlation with maximally entangled state, where $\{E^x_y\}$ is a projection-valued measure on a d-dimensional Hilbert space $\mathfrak{H}$. Suppose $J_3(p) \leq -\frac{1}{8} + \lambda$. Then on $\mathfrak{H} = \mathfrak{L} \oplus (\mathbb{C}^2 \otimes \mathfrak{K})$ there exists a projection-value measure $\{\tilde{E}^x_y\}$ where (1) $\tilde{E}^x_y = L^x_y + \hat{E}^x_y \otimes \mathbb{1}_{\mathfrak{K}}$, (2) $\frac{\dim \mathfrak{L}}{\dim \mathfrak{H}} \leq 8\lambda$, and (3) $\frac{1}{3}\sum_{x,y} \frac{1}{d}\mathrm{tr}\left(\left(E^x_y - \tilde{E}^x_y\right)^2\right) \leq 8\lambda$. In particular, the expected statistical difference*

$$\frac{1}{3}\sum_{x,y} \left| p(y, y \mid x, x) - \frac{1}{2} \right| \leq \frac{1}{3}\left(\sqrt{8}\sqrt{\lambda} + 32\lambda\right).$$

Proof. We begin by defining the ±1-valued observables $M_x = E^x_0 - E^x_1$, so $M_x^2 = \mathbb{1}$, and following customary notation write

$$a_x = \frac{1}{d}\mathrm{tr}(M_x) \text{ and } c_{x_A x_B} = \frac{1}{d}\mathrm{tr}(M_{x_A} M_{x_B}).$$

Similarly denote $\tilde{M}_x = \tilde{E}^x_0 - \tilde{E}^x_1$. Notice $E^x_0 = \frac{1}{2}(\mathbb{1} + M_x)$ and $E^x_1 = \frac{1}{2}(\mathbb{1} - M_x)$ so

$$\frac{1}{3}\sum_{x,y} \frac{1}{d}\mathrm{tr}\left(\left(E^x_y - \tilde{E}^x_y\right)^2\right) = \frac{1}{6}\sum_{x} \frac{1}{d}\mathrm{tr}\left(\left(M_x - \tilde{M}_x\right)^2\right).$$

Now define $\Delta := M_0 + M_1 + M_2$, and compute

$$\begin{aligned}
\Delta^2 &= M_0^2 + M_1^2 + M_2^2 + M_0M_1 + M_1M_0 + M_0M_2 + M_2M_0 + M_1M_2 + M_2M_1 \\
&= 3\mathbb{1} + M_0M_1 + M_1M_0 + (M_0 + M_1)M_2 + M_2(M_0 + M_1) \qquad (4) \\
&= \mathbb{1} + M_0M_1 + M_1M_0 + (M_0 + M_1 + M_2)M_2 + M_2(M_0 + M_1 + M_2) \\
&= \mathbb{1} + M_0M_1 + M_1M_0 + \Delta M_2 + M_2\Delta \qquad (5)
\end{aligned}$$

We have Δ^2 relates to J_3, and hence we obtain the following bound:

$$\begin{aligned}
\frac{1}{d}\mathrm{tr}(\Delta^2) &= \frac{1}{d}\mathrm{tr}\left(M_0^2 + M_1^2 + M_2^2 + 2M_0M_1 + 2M_0M_2 + 2M_1M_2\right) \\
&= \frac{3}{d}\mathrm{tr}\left(\mathbb{1}\right) + \frac{2}{d}\mathrm{tr}\left(M_0M_1 + M_0M_2 + M_1M_2\right) \\
&= 3 + 2(c_{01} + c_{02} + c_{12}) = 1 + 2(1 + c_{01} + c_{02} + c_{12}) = 1 + 8J_3 \\
&\leq 1 + 8\left(-\frac{1}{8} + \lambda\right) = 8\lambda \qquad (6)
\end{aligned}$$

Using two projections theory [2, 10, 5], we have a decomposition of the Hilbert space $\mathfrak{H}$

$$\mathfrak{H} = \mathfrak{L}_{00} \oplus \mathfrak{L}_{01} \oplus \mathfrak{L}_{10} \oplus \mathfrak{L}_{11} \oplus \bigoplus_{j=1}^{k} \mathfrak{H}_j,$$

where $\dim(\mathfrak{L}_{\alpha\beta}) = l_{\alpha\beta}$ for $\alpha, \beta \in \{0, 1\}$, and $\dim(\mathfrak{H}_j) = 2$, where the projections E^0_0 and E^1_0 take the form:

$$E^0_0 = 0_{l_{00}} \oplus 0_{l_{01}} \oplus \mathbb{1}_{l_{10}} \oplus \mathbb{1}_{l_{11}} \oplus \bigoplus_{j=1}^{k} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$E^1_0 = 0_{l_{00}} \oplus \mathbb{1}_{l_{01}} \oplus 0_{l_{10}} \oplus \mathbb{1}_{l_{11}} \oplus \bigoplus_{j=1}^{k} \begin{pmatrix} \cos^2\theta_j & \sin\theta_j\cos\theta_j \\ \sin\theta_j\cos\theta_j & \sin^2\theta_j \end{pmatrix}.$$

That is, we can express

$$M_0 = -\mathbb{1}_{\mathfrak{L}_{00}} \oplus -\mathbb{1}_{\mathfrak{L}_{01}} \oplus \mathbb{1}_{\mathfrak{L}_{10}} \oplus \mathbb{1}_{\mathfrak{L}_{11}} \oplus \bigoplus_{j=1}^{k} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$M_1 = -\mathbb{1}_{\mathfrak{L}_{00}} \oplus \mathbb{1}_{\mathfrak{L}_{01}} \oplus -\mathbb{1}_{\mathfrak{L}_{10}} \oplus \mathbb{1}_{\mathfrak{L}_{11}} \oplus \bigoplus_{j=1}^{k} \begin{pmatrix} \cos 2\theta_j & \sin 2\theta_j \\ \sin 2\theta_j & -\cos 2\theta_j \end{pmatrix}.$$

Now let us define $\tilde{M}_0, \tilde{M}_1, \tilde{M}_2$ as follows. Note that our ideal projections $\hat{E}_0^1, \hat{E}_1^1$ correspond to angle $\hat{\theta} = \frac{2\pi}{3}$, and without loss of generality we can assume[1] $|\theta_j - \hat{\theta}| \leq \frac{\pi}{6}$.

$$\tilde{M}_0 = M_0 = -\mathbb{1}_{\mathfrak{L}_{00}} \oplus -\mathbb{1}_{\mathfrak{L}_{01}} \oplus \mathbb{1}_{\mathfrak{L}_{10}} \oplus \mathbb{1}_{\mathfrak{L}_{11}} \oplus \bigoplus_{j=1}^{k} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$\tilde{M}_1 = -\mathbb{1}_{\mathfrak{L}_{00}} \oplus \mathbb{1}_{\mathfrak{L}_{01}} \oplus -\mathbb{1}_{\mathfrak{L}_{10}} \oplus \mathbb{1}_{\mathfrak{L}_{11}} \oplus \bigoplus_{j=1}^{k} \begin{pmatrix} \cos 2\hat{\theta} & \sin 2\hat{\theta} \\ \sin 2\hat{\theta} & -\cos 2\hat{\theta} \end{pmatrix},$$

$$\tilde{M}_2 = \mathbb{1}_{\mathfrak{L}_{00}} \oplus \mathbb{1}_{\mathfrak{L}_{01}} \oplus -\mathbb{1}_{\mathfrak{L}_{10}} \oplus -\mathbb{1}_{\mathfrak{L}_{11}} \oplus \bigoplus_{j=1}^{k} \begin{pmatrix} -1-\cos 2\hat{\theta} & -\sin 2\hat{\theta} \\ -\sin 2\hat{\theta} & 1+\cos 2\hat{\theta} \end{pmatrix}.$$

As desired, $\tilde{M}_x = (L_0^x - L_1^x) + \hat{M}_x \otimes \mathbb{1}_{\mathbb{C}^k}$, where the $\{L_y^x\}$ are the projection onto the summands $\mathfrak{L}_{\mu\nu}$.

First we bound the dimension of each $\mathfrak{L}_{\mu\nu}$. Consider (4) for Δ^2. If $|\psi_{01}\rangle \in \mathfrak{L}_{01}$, then

$$\begin{aligned}\langle\psi_{01}|\Delta^2|\psi_{01}\rangle &= \langle\psi_{01}|(3\mathbb{1} + M_0M_1 + M_1M_0 + (M_0+M_1)M_2 + M_2(M_0+M_1)|\psi_{01}\rangle \\ &= 3-1-1+0+0 = 1.\end{aligned}$$

The same equality holds for $|\psi_{10}\rangle \in \mathfrak{L}_{10}$, namely $\langle\psi_{10}|\Delta^2|\psi_{10}\rangle = 1$.

For a vector $|\psi_{00}\rangle$ in $\mathfrak{L}_{00}$ we again use (4) to get $\langle\psi_{00}|\Delta^2|\psi_{00}\rangle = 3+1+1-4\langle\psi_{00}|M_2|\psi_{00}\rangle$. Now from Cauchy-Schwarz, and that $M_2^2 = \mathbb{1}$, we have

$$|\langle\psi_{00}|M_2|\psi_{00}\rangle| \leq |\langle\psi_{00}|\psi_{00}\rangle|^{\frac{1}{2}} |\langle\psi_{00}|M_2^2|\psi_{00}\rangle|^{\frac{1}{2}} = 1$$

and thus $\langle\psi_{00}|\Delta^2|\psi_{00}\rangle \geq 1$. Similarly for $|\psi_{11}\rangle$ in $\mathfrak{L}_{11}$ we have

$$\langle\psi_{11}|\Delta^2|\psi_{11}\rangle = 5 + 4\langle\psi_{11}|M_2|\psi_{11}\rangle \geq 5 - 4|\langle\psi_{11}|M_2|\psi_{11}\rangle| \geq 1.$$

Putting everything together, since $\langle\psi_{\alpha\beta}|\Delta^2|\psi_{\alpha\beta}\rangle \geq 1$ on each $\mathfrak{L}_{\alpha\beta}$, for $\alpha, \beta \in \{0,1\}$, summing over bases of the respective spaces

$$\frac{l}{d} = \frac{1}{d}(l_{00} + l_{01} + l_{10} + l_{11}) \leq \frac{1}{d}\sum_{j=1}^{l}\langle\psi_j|\Delta^2|\psi_j\rangle \leq \frac{1}{d}\mathrm{tr}(\Delta^2) \leq 8\lambda.$$

where the second-to-last inequality follows from Δ^2 being positive semidefinite.

This immediately provides the claimed bound on the statistical difference from uniform. We can explicitly bound the quantities $|a_0|$ and $|a_1|$ as follows:

$$\begin{aligned}|a_0| &= \frac{1}{d}|\mathrm{tr}(M_0)| = \frac{1}{d}|-l_{00} - l_{01} + l_{10} + l_{11}| \leq \frac{l}{d} \leq 8\lambda \\ |a_1| &= \frac{1}{d}|\mathrm{tr}(M_1)| = \frac{1}{d}|-l_{00} + l_{01} - l_{10} + l_{11}| \leq \frac{l}{d} \leq 8\lambda.\end{aligned}$$

[1] Direct examination of (1) reveals that any θ_j is within $\frac{\pi}{6}$ of the image of some E_y^x; the bound we prove is symmetric in x, y we may reorder the labeling in each $\mathfrak{H}_j$ so that θ_j is close to E_0^1 with $\hat{\theta} = \frac{2\pi}{3}$.

Using Cauchy-Schwarz, we bound $|a_2|$. As

$$a_0 + a_1 + a_2 = \frac{1}{d}\mathrm{tr}(\Delta) \leq \left(\frac{1}{d}\mathrm{tr}(\Delta^2)\right)^{\frac{1}{2}} \left(\frac{1}{d}\mathrm{tr}(\mathbb{1}^2)\right)^{\frac{1}{2}} \leq \sqrt{8\lambda},$$

we have $a_2 \leq \sqrt{8\lambda} - a_0 - a_1$ and therefore $|a_2| \leq \sqrt{8\lambda} + |a_0| + |a_1| \leq \sqrt{8}\sqrt{\lambda} + 16\lambda$.

Finally we bound each $\frac{1}{d}\mathrm{tr}\left(\left(M_x - \tilde{M}_x\right)^2\right)$. Note $M_0 - \tilde{M}_0 = 0$ by construction. Then

$$\begin{aligned}\frac{1}{d}\mathrm{tr}\left(\left(M_1 - \tilde{M}_1\right)^2\right) &= \frac{1}{d}\sum_j \mathrm{tr}\left(\begin{pmatrix} \cos 2\theta_j - \cos 2\hat{\theta} & \sin 2\theta_j - \sin 2\hat{\theta} \\ \sin 2\theta_j - \sin 2\hat{\theta} & -\cos 2\theta_j + \cos 2\hat{\theta} \end{pmatrix}^2\right) \\ &= \frac{1}{d}\sum_j (4 - 4\cos(2(\theta_j - \hat{\theta}))) \;=\; \frac{8}{d}\sum_j \sin^2(\theta_j - \hat{\theta})\end{aligned}$$

To bound this, we note that on any $\mathfrak{H}_j$:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} \cos 2\theta_j & \sin 2\theta_j \\ \sin 2\theta_j & -\cos 2\theta_j \end{pmatrix} + \begin{pmatrix} \cos 2\theta_j & \sin 2\theta_j \\ \sin 2\theta_j & -\cos 2\theta_j \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = 2\cos 2\theta_j \cdot \mathbb{1}_{\mathfrak{H}_j}.$$

From this we obtain

$$\left[\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + \begin{pmatrix} \cos 2\theta_j & \sin 2\theta_j \\ \sin 2\theta_j & -\cos 2\theta_j \end{pmatrix}\right]^2 = 4\cos^2\theta_j \mathbb{1}_{\mathfrak{H}_j}.$$

Hence there exists a basis $\{|\psi_0\rangle, |\psi_1\rangle\}$ of $\mathfrak{H}_j$ such that

$$(M_0 + M_1)|\psi_0\rangle = 2\cos\theta_j|\psi_0\rangle \text{ and } (M_0 + M_1)|\psi_1\rangle = -2\cos\theta_j|\psi_1\rangle.$$

Therefore again from (4) we have

$$\begin{aligned}\langle\psi_0|\Delta^2|\psi_0\rangle &= 3 + 2\cos 2\theta_j + 4\cos\theta_j\langle\psi_0|M_2|\psi_0\rangle \\ \langle\psi_1|\Delta^2|\psi_1\rangle &= 3 + 2\cos 2\theta_j - 4\cos\theta_j\langle\psi_1|M_2|\psi_1\rangle.\end{aligned}$$

In particular, $\langle\psi_0|\Delta^2|\psi_0\rangle + \langle\psi_1|\Delta^2|\psi_1\rangle \geq 6 + 4\cos 2\theta_j - 8|\cos\theta_j|$. It is straightforward to show for $\theta \in \left[\frac{2\pi}{3} - \frac{\pi}{6}, \frac{2\pi}{3} + \frac{\pi}{6}\right]$ that $6 + 4\cos 2\theta - 8|\cos\theta| \geq 4\sin^2\left(\theta - \frac{2\pi}{3}\right)$. And hence we obtain the bound

$$\begin{aligned}\frac{1}{d}\mathrm{tr}(\Delta^2) &\geq \frac{1}{d}\sum_j (6 + 4\cos 2\theta_j - 8|\cos\theta_j|) \\ &\geq \frac{1}{d}\sum_j 4\sin^2(\theta_j - \hat{\theta}) \;=\; \frac{1}{2d}\mathrm{tr}\left(\left(M_1 - \tilde{M}_1\right)^2\right).\end{aligned}$$

In particular, $\frac{1}{d}\mathrm{tr}\left(\left(M_1 - \tilde{M}_1\right)^2\right) \leq 16\lambda$.

Finally, note $\tilde{M}_0 + \tilde{M}_1 + \tilde{M}_2 = -\mathbb{1}_{\mathfrak{L}_{00}} \oplus \mathbb{1}_{\mathfrak{L}_{01}} \oplus -\mathbb{1}_{\mathfrak{L}_{10}} \oplus \mathbb{1}_{\mathfrak{L}_{11}}$. By Jensen's inequality

$$\begin{aligned}\frac{1}{d}\mathrm{tr}\left(\left(M_2 - \tilde{M}_2\right)^2\right) &= \frac{1}{d}\mathrm{tr}\left(\left(\Delta - (-\mathbb{1}_{\mathfrak{L}_{00}} \oplus \mathbb{1}_{\mathfrak{L}_{01}} \oplus -\mathbb{1}_{\mathfrak{L}_{10}} \oplus \mathbb{1}_{\mathfrak{L}_{11}}) + (\tilde{M}_1 - M_1)\right)^2\right) \\ &\leq \frac{1}{d}\mathrm{tr}\left(\Delta^2\right) + \frac{1}{d}\mathrm{tr}\left(\mathbb{1}_{\mathfrak{L}}\right) + \frac{1}{d}\mathrm{tr}\left(\left(\tilde{M}_1 - M_1\right)^2\right) \leq 32\lambda.\end{aligned}$$

Therefore, $\frac{1}{3}\sum_{x,y}\frac{1}{d}\mathrm{tr}\left(\left(E^x_y - \tilde{E}^x_y\right)^2\right) \leq 8\lambda$ as desired.

It is straightforward to get a bound on the statistical difference to any synchronous quantum correlation close to $J_3 = -\frac{1}{8}$. Every synchronous quantum correlation is a convex sum of synchronous quantum correlations with maximally entangled states, and so we may write $p = \sum_j c_j p_j$ where p_j is as in the theorem above. Say $J_3(p_j) \leq -\frac{1}{8} + \lambda_j$, and so

$$J_3(p) = \sum_j c_j J_3(p_j) \leq -\frac{1}{8} + \sum_j c_j \lambda_j = -\frac{1}{8} + \lambda$$

where we define $\lambda = \sum_j c_j \lambda_j$. With two uses of Jensen's inequality,

$$\begin{aligned}\frac{1}{3}\sum_{x,y}\left|p(y,y\,|\,x,x) - \frac{1}{2}\right| &\leq \frac{1}{3}\sum_{j,x,y} c_j \left|p_j(y,y\,|\,x,x) - \frac{1}{2}\right| \\ &\leq \sum_j c_j(C\sqrt{\lambda_j} + C'\lambda_j) \leq C\sqrt{\lambda} + C'\lambda.\end{aligned}$$ ◀

Unfortunately, this does not yet produce a fully device-independent protocol as we still suffer from a "synchronicity" loophole. We discuss this loophole and close the loophole in the next section.

4 Measure of asynchronicity

That $J_3 = -\frac{1}{8}$ can be achieved by a unique synchronous quantum correlation, which necessarily can only be realized through a maximally entangled state, provides the device-independent security of the above QKD scheme. However this opens a "synchronicity" security loophole: can a (asynchronous) quantum device simulate $J_3 = -\frac{1}{8}$ without using maximally entangled states (and hence potentially leak information about the derived shared keys)? Fortunately a recent work shows that the same results apply to "almost" synchronous correlations [24]. This allows us to close this synchronicity loophole by also bounding the asynchronicity of the observed correlation.

▶ **Definition 5.** *The* asynchronicity *with respect to a basis choice $x \in X$ and set of measurement outcomes Y is $S_x(p) = \sum_{y_A \neq y_B} p(y_A, y_B\,|\,x, x)$. The* total *(or* expected*) asynchronicity is*

$$S(p) = \frac{1}{|X|}\sum_{x \in X} S_x(p) \tag{7}$$

In [24], this measure is called the "default to synchronicity" and denoted δ_{sync}. While the expected asynchronicity is the average likelihood of an asynchronous result where the inputs are sampled uniformly at random, all results here and in [24], apply to the case where the expectation is computed over inputs sampled with respect to some other fixed distribution. To bound the asynchronicity, we modify the scheme in Section 3 so that for some data rounds where Alice and Bob have selected the same inputs they still reveal their output, stated as Algorithm 1 below.

Here we state the main result [24, Theorem 3.1] in the notation used above. Note that this theorem refers to symmetric (albeit asynchronous) correlations, which is the natural setting as every synchronous quantum correlation is symmetric. This implies a special form for the projections in the correlation, involving the transpose with respect to the natural basis given by the Schmidt-decomposition of the entangled state used in the correlation.

▶ **Theorem 6** (Vidick). *There are universal constants $c, C > 0$ such that the following holds. Let X and Y be finite sets and p a symmetric quantum correlation with input set X, measurement results Y, and asynchronicity $S = S(p)$. Write $p(y_A, y_B \mid x_A, x_B) = \langle\psi|E^{x_A}_{y_A} \otimes (E^{x_B}_{y_B})^T|\psi\rangle$ where $\{E^x_y\}_{y\in Y}$ is a POVM on a finite-dimensional Hilbert space $\mathfrak{H}$ and $|\psi\rangle$ a state on $\mathfrak{H}\otimes\mathfrak{H}$. Let $|\psi\rangle = \sum_{j=1}^r \sqrt{\sigma_j} \sum_{m=1}^{d_j} |\phi^A_{j,m}\rangle \otimes |\phi^B_{j,m}\rangle$ be the Schmidt decomposition, and write $|\psi_j\rangle = \frac{1}{\sqrt{d_j}} \sum_{m=1}^{d_j} |\phi^A_{j,m}\rangle \otimes |\phi^B_{j,m}\rangle$. Then*

1. *$\mathfrak{H} = \bigoplus_{j=1}^r \mathfrak{H}_j$ with $|\psi_j\rangle$ being maximally entangled on $\mathfrak{H}_j \otimes \mathfrak{H}_j$;*
2. *there is a projective measurement $\{E^{j,x}_y\}_{y\in Y}$ on each $\mathfrak{H}_j$ so that*

$$p_j(y_A, y_B \mid x_A, x_B) = \langle\psi_j|E^{j,x_A}_{y_A} \otimes (E^{j,x_B}_{y_B})^T|\psi_j\rangle = \frac{1}{d_j}\mathrm{tr}(E^{j,x_A}_{y_A} E^{j,x_B}_{y_B})$$

is a synchronous quantum correlation and $p \approx \sum_{j=1}^r d_j\sigma_j p_j$ in that:

$$\frac{1}{|X|}\sum_{x\in X}\sum_{y\in Y}\sum_{j=1}^r \frac{1}{d_j}\sum_{m=1}^{d_j} \langle\phi^A_{j,m}|\left(E^x_y - E^{j,x}_y\right)^2|\phi^A_{j,m}\rangle \le CS^c.$$

As indicated in [24, §4.1], this result can be used to transfer rigidity from synchronous to almost synchronous correlations. As $\sum_j d_j\sigma_j = 1$, we also transfer the bound on the statistical difference from uniform to convex sums in this theorem exactly as in the previous section. As for the full correlation we rephrase Lemma 2.10 of [24] in the context of Theorem 6 as follows.

▶ **Corollary 7.** *Let $p(y_A, y_B \mid x_A, x_B) = \langle\psi|E^{x_A}_{y_A} \otimes (E^{x_B}_{y_B})^T|\psi\rangle$ be a quantum correlation with asynchronocity S as in Theorem 6, and let $\bar{p} = \sum_{j=1}^r d_j\sigma_j p_j$ with*

$$\frac{1}{|X|}\sum_{x\in X}\sum_{y\in Y}\sum_{j=1}^r \frac{1}{d_j}\sum_{m=1}^{d_j} \langle\phi^A_{j,m}|\left(E^x_y - E^{j,x}_y\right)^2|\phi^A_{j,m}\rangle = \gamma$$

as given in Theorem 6. Then

$$\frac{1}{|X|^2}\sum_{x_A,x_B,y_A,y_B} |p(y_A, y_B \mid x_A, x_B) - \bar{p}(y_A, y_B \mid x_A, x_B)| \le 3S + 4\sqrt{\gamma}.$$

Note that this bound on the statistical difference directly bounds $J_3(p)$ in terms of the convex sum of the analogous $J_3(p_j)$. Note that J_3, as seen in (3), is an affine function so $J_3(\bar{p}) = \sum_{j=1}^r \sigma_j d_j J_3(p_j)$ using the notation of Theorem 6 above. Then immediately from Corollary 7, $|J_3(p) - J_3(\bar{p})| \le \frac{27}{4}S + 9\sqrt{\gamma}$. In turn from Theorem 6 we have $\gamma \le CS^c$, and so there are different universal constants C', c' so that

$$|J_3(p) - J_3(\bar{p})| \le C'S^{c'}. \tag{8}$$

▶ **Corollary 8.** *Let $p(y_A, y_B \mid x_A, x_B) = \langle\psi|E^{x_A}_{y_A} \otimes (E^{x_B}_{y_B})^T|\psi\rangle$ be a quantum correlation as in Theorem 6 and suppose $J_3(p) = -\frac{1}{8} + \lambda$. Then the Hilbert space decomposes as $\mathfrak{H} = \bigoplus_{j=1}^r \mathfrak{H}_j = \bigoplus_{j=1}^r (\mathfrak{L}_j \oplus (\mathbb{C}^2 \otimes \mathfrak{K}_j))$ where $\frac{\dim\mathfrak{L}_\mathrm{j}}{\dim\mathfrak{H}_\mathrm{j}} \le 8\lambda_j$. On each summand we have projection-valued measures $\{\tilde{E}^{j,x}_y\}$ such that $\tilde{E}^{j,x}_y = L^{j,x}_y + \hat{E}^x_y \otimes \mathbb{1}_{\mathfrak{K}_j}$ and*

$$\frac{1}{3}\sum_{x,y}\sum_{j=1}^r \sigma_j d_j \left(\frac{1}{d_j}\sum_{m=1}^{d_j}\langle\phi^A_{j,m}|(E^x_y - \tilde{E}^{j,x}_y)^2|\phi^A_{j,m}\rangle\right) \le C_1 S^c + C_2\lambda$$

for universal constants c, C_1, C_2.

Proof. Given $\{E_y^x\}$ as above, we obtain projections $\{E_y^{j,x}\}$ defining synchronous correlations p_j from Theorem 6. Write $J_3(p_j) = -\frac{1}{8} + \lambda_j$. From Theorem 4, we obtain the given decomposition of the Hilbert space and projection-valued measures $\{\tilde{E}_y^{j,x}\}$ where

1. $\tilde{E}_y^{j,x} = L_y^{j,x} + \hat{E}_y^x \otimes \mathbb{1}_{\mathfrak{K}_j}$,
2. $\frac{\dim \mathfrak{L}_j}{\dim \mathfrak{H}_j} \leq 8\lambda_j$, and
3. $\frac{1}{3}\sum_{x,y} \frac{1}{d_j} \sum_{m=1}^{d_j} \langle \phi_{j,m}^A | (E_y^{j,x} - \tilde{E}_y^{j,x})^2 | \phi_{j,m}^A \rangle \leq C_2 \lambda_j$.

Then using the notation and (8) above $|J_3(p) - J_3(\bar{p})| = \left|\lambda - \sum_{j=1}^r \sigma_j d_j \lambda_j\right| \leq C' S^{c'}$ and thus

$$\frac{1}{3}\sum_{x,y}\sum_{j=1}^r \sigma_j d_j \left(\frac{1}{d_j} \sum_{m=1}^{d_j} \langle \phi_{j,m}^A | (E_y^{j,x} - \tilde{E}_y^{j,x})^2 | \phi_{j,m}^A \rangle \right) \leq C_2 \sum_{j=1}^r \sigma_j d_j \lambda_j = C_2 \lambda + C_2 C' S^{c'}.$$

On the other hand,

$$\begin{aligned} &\frac{1}{3}\sum_{x,y}\sum_{j=1}^r \sigma_j d_j \left(\frac{1}{d_j} \sum_{m=1}^{d_j} \langle \phi_{j,m}^A | (E_y^{x} - E_y^{j,x})^2 | \phi_{j,m}^A \rangle \right) \\ &\quad \leq \frac{1}{3}\sum_{x,y}\sum_{j=1}^r \left(\frac{1}{d_j} \sum_{m=1}^{d_j} \langle \phi_{j,m}^A | (E_y^{x} - E_y^{j,x})^2 | \phi_{j,m}^A \rangle \right) \leq C'' S^{c''} \end{aligned}$$

directly from Theorem 6. So by Jensen's inequality

$$\begin{aligned} &\frac{1}{3}\sum_{x,y}\sum_{j=1}^r \sigma_j d_j \left(\frac{1}{d_j} \sum_{m=1}^{d_j} \langle \phi_{j,m}^A | (E_y^{x} - \tilde{E}_y^{j,x})^2 | \phi_{j,m}^A \rangle \right) \\ &\quad \leq \frac{2}{3}\sum_{x,y}\sum_{j=1}^r \sigma_j d_j \left(\frac{1}{d_j} \sum_{m=1}^{d_j} \langle \phi_{j,m}^A | (E_y^{x} - E_y^{j,x})^2 | \phi_{j,m}^A \rangle \right) \\ &\qquad + \frac{2}{3}\sum_{x,y}\sum_{j=1}^r \sigma_j d_j \left(\frac{1}{d_j} \sum_{m=1}^{d_j} \langle \phi_{j,m}^A | (E_y^{j,x} - \tilde{E}_y^{j,x})^2 | \phi_{j,m}^A \rangle \right) \\ &\quad \leq 2C_1 S^c + 2C_2 \lambda \end{aligned}$$

for some universal constant C_1. ◀

5 Security and key-rate analysis

Our synchronous fully device-independent quantum key distribution protocol is stated in Algorithm 1. For an honest, but possibly noisy implementation of the protocol, we assume that Alice and Bob perform measurements $E_{y_A}^{x_A^i} \otimes E_{y_B}^{x_B^i}$ on the state ρ_{AB}. We assume a depolarization channel and take ρ_{AB} to be the state $(1-\nu)|\Phi^+\rangle\langle\Phi^+| + \frac{\nu}{4}\mathbb{1}$, where $\nu \in [0,1]$ is the depolarization noise and $|\Phi^+\rangle$ is the EPR pair. Using measurements according to Equation (1), we get $J_3 = -\frac{1}{8} + \frac{3}{8}\nu$, and $S = \frac{\nu}{2}$. A general framework for analyzing device-independent protocols was laid out in [4], which we use to show completeness and soundness of our protocol.

Algorithm 1 Synchronous QKD Protocol.

```
Input:
    $\lambda \in [0, \frac{1}{8})$:  Allowed error in $J_3$ violation
    $\mu \in [0, \mu_0]$:  Allowed error in asynchronicity $S$ with $\mu_0$ being a pre-decided threshold
    $n \in \mathbb{N}$:  Total number of rounds
    $m \in \mathbb{N}$:  Parameter for choosing asynchronicity check rounds. $\kappa := \frac{1}{m}$
    $\gamma \in (0, 1]$:  Expected fraction of test rounds
    $\delta_{est}^{J_3} \in (0, 1)$:  Width of statistical interval for the $J_3$ test
    $\delta_{est}^{S} \in (0, 1)$:  Width of statistical interval for the $S$ test
    EC:  Error Correction protocol
    PA:  Privacy Amplification protocol
For $i \in [n]$:
Alice and Bob draw $x_A^i \leftarrow X$, $x_B^i \leftarrow X$ according to Equation (9)
They produce outputs $y_A^i$ and $y_B^i$ using $\{E_y^{x_A^i}\}$ and $\{E_y^{x_B^i}\}$ respectively
They share their inputs $x_A^i$ and $x_B^i$.
Error Correction: Alice and Bob use error correction protocol EC to obtain
    outputs $\tilde{Y}_A$ and $\tilde{Y}_B$. They abort if the error correction protocol aborts.
Parameter Estimation:
Bob estimates the $J_3$ violation in rounds where $x_A^i \neq x_B^i$, i.e. he sets $R_i = 1$ if
    $\tilde{y}_A^i \neq y_B^i$ else 0. He aborts if $\sum_i R_i < \left[\gamma\left(\frac{3}{4} - \frac{2}{3}\lambda\right) - \delta_{est}^{J_3}\right] \cdot n$
He also estimates the asynchronicity $S$ in rounds where $x_A^i = x_B^i$ and $i \pmod{m} = 0$,
    i.e. he sets $Q_i = 1$ if $\tilde{y}_A^i \neq y_B^i$ else 0 in those rounds. He aborts if
    $\sum_i Q_i < \left[\kappa(1-\gamma)\mu - \delta_{est}^{S}\right] \cdot n$
Privacy Amplification: Alice and Bob use privacy amplification protocol PA to
    create final keys $K_A$ and $K_B$ using $\tilde{y}_A^i$ and $\tilde{y}_B^i$ where $x_A^i = x_B^i$ and $i \pmod{m} \neq 0$.
```

▶ **Lemma 9** (Completeness). *Let ϵ_{EC}^c be the completeness error of the EC protocol, and ϵ_{EC} be the probability that the EC protocol does not abort but Alice and Bob hold different outputs post error correction. Then, Protocol 1 has completeness error $\epsilon_{QKD}^c \leq exp\left(-2n\left((\delta_{est}^S)^2) + (\delta_{est}^{J_3})^2\right)\right) + \epsilon_{EC}^c + \epsilon_{EC}$.*

Proof. The protocol either aborts in the error correction step or the parameter estimation step. The probability of aborting during the J_3 and S tests can be bounded using Hoeffding's inequality as follows:

$$\Pr\left(\sum_j R_j > \left[\gamma\left(\frac{3}{4} - \frac{2}{3}\lambda\right) - \delta_{est}^{J_3}\right] \cdot n \bigwedge \sum_j Q_j > \left[\kappa(1-\gamma)\mu - \delta_{est}^{S}\right] \cdot n\right)$$
$$\leq exp\left(-2n\left((\delta_{est}^S)^2) + (\delta_{est}^{J_3})^2\right)\right).$$

The rest of the proof follows analogously to [4, Lemma 5.2 and Eq. 5.2] ◀

We use the Entropy Accumulation Theorem (EAT) [8], to bound the min-entropy of Alice and Bob's outputs with respect to an adversary Eve's side information. To that effect, we define Ω as the event that Alice and Bob do not abort the protocol in the parameter estimation step. The EAT yields a bound on the min-entropy, given we find an appropriate *min-tradeoff* function.

We state the min-entropy bound in the following theorem.

▶ **Theorem 10.** *Let $\rho_{Y_A Y_B X_A X_B T E}$ be the joint state of Alice, Bob and Eve's system along with the register T for indicating testing versus data rounds, and let Ω be the event that the protocol does not abort during parameter estimation. We write $\rho_{|\Omega}$ for the state of the system conditioned on Ω. Let $\epsilon_{EA}, \epsilon_s \in (0,1)$. Then either*

1. *The protocol aborts with probability greater than $1 - \epsilon_{EA}$, or*
2. *$H_{\min}^{\epsilon_s}(Y_A Y_B | X_A X_B T E)_{\rho_{|\Omega}} > n \cdot \mathsf{OPT}(\epsilon_s, \epsilon_{EA})$, where OPT is defined as follows:*

$$g(p) = \begin{cases} 1 - h\left(3 - 4\frac{p(1)}{\gamma}\right) & \frac{p(1)}{\gamma} \in \left[\frac{2}{3}, \frac{3}{4}\right] \\ 1 & \frac{p(1)}{\gamma} \in \left[\frac{3}{4}, 1\right], \end{cases}$$

$$f_{\min}^{J_3}(p, p_t) = \begin{cases} g(p) & \text{if } p(1) \leq p_t(1) \\ \frac{d}{dp(1)} g(p)\Big|_{p_t} \cdot p(1) + g(p_t) - \frac{d}{dp(1)} g(p)\Big|_{p_t} \cdot p_t(1) & \text{if } p(1) > p_t(1), \end{cases}$$

$$f_{EAT} = n f_{\min}^{J_3}(p, p_t) - \frac{2}{\sqrt{n}} \left(\log 9 + \left\lceil \frac{d}{dp(1)} g(p) \middle| \right\rceil \right) \sqrt{1 - 2\log(\epsilon_s \cdot \epsilon_{EA})},$$

$$\mathsf{OPT}(\epsilon_s, \epsilon_{EA}) = \max_{\frac{2}{3} < \frac{p_t(1)}{\gamma} < \frac{3}{4}} f_{EAT}(p, p_t, \epsilon_s, \epsilon_{EA}).$$

Before we state the proof, we develop some key ideas and prove some lemmas that will be used in the proof. In round $i \in [n]$, Alice and Bob draw from a local biased distribution with $p_0, p_1, p_2 \in [0,1]$:

$$x_i = \begin{cases} i \pmod 3 & \text{with probability } p_0, \\ i+1 \pmod 3 & \text{with probability } p_1, \\ i+2 \pmod 3 & \text{with probability } p_2. \end{cases} \tag{9}$$

Without loss of generality we may assume that the total number of rounds is a multiple of 3, i.e. $n = 3N$ for some N. There are two cases in which they perform a testing round – first for testing the violation of the Bell inequality J_3, and second to test the asynchronicity of the protocol. Let γ be the probability of performing a J_3 test. Thus we have $\gamma = p(x_A \neq x_B)$.

$$\gamma = p(x_A \neq x_B) = \frac{1}{3}\sum_{i=0}^{2} p(x_A^i \neq x_B^i) = 2(p_0 p_1 + p_0 p_2 + p_1 p_2).$$

For the J_3 test we define a random variable R_i as follows:

$$R_i = \begin{cases} 1 & \text{if } y_A^i \neq y_B^i \text{ and } x_A^i \neq x_B^i, \\ 0 & \text{if } y_A^i = y_B^i \text{ and } x_A^i \neq x_B^i, \\ \perp & \text{if } x_A^i = x_B^i. \end{cases}$$

The probability that $R_i = 1$ is given by

$$\begin{aligned} p(R_i = 1) = p(y_A^i \neq y_B^i \wedge x_A^i \neq x_B^i) &= \sum_{i}^{3N} \sum_{\substack{y_A^i \neq y_B^i \\ x_A^i \neq x_B^i}} p(y_A^i, y_B^i \mid x_A^i, x_B^i) \cdot p(x_A^i, x_B^i) \cdot \frac{1}{3N} \\ &= \frac{1}{3}\sum_{i=0}^{2} \sum_{\substack{y_A^i \neq y_B^i \\ x_A^i \neq x_B^i}} p(y_A^i, y_B^i \mid x_A^i, x_B^i) \cdot p(x_A^i, x_B^i) \\ &= \frac{1}{3}(p_0 p_1 + p_0 p_2 + p_1 p_2) \sum_{\substack{y_A \neq y_B \\ x_A \neq x_B}} p(y_A, y_B \mid x_A, x_B) \\ &= \frac{1}{3}(p_0 p_1 + p_0 p_2 + p_1 p_2)(4 - 4J_3) = \gamma\left(\frac{2}{3} - \frac{2}{3}J_3\right). \end{aligned}$$

Similarly, we define a random variable Q_i corresponding to the asyncronicity. We reserve every mth key generation round to perform an asynchronicity check i.e. if $i = 0 \pmod m$ for i such that $x_A^i = x_B^i$. We denote by $\kappa = 1/m$ the fraction of asynchronicity check rounds. We have

$$Q_i = \begin{cases} 1 & \text{if } y_A^i \neq y_B^i \text{ and } x_A^i = x_B^i \text{ and } i = 0 \pmod m, \\ 0 & \text{if } y_A^i = y_B^i \text{ and } x_A^i = x_B^i, \\ \perp & \text{ if } x_A^i \neq x_B^i. \end{cases}$$

The probability that $Q_i = 1$ is given by

$$\begin{aligned} p(Q_i = 1) &= p(y_A^i \neq y_B^i \wedge x_A^i = x_B^i \wedge i = 0 \pmod m) \\ &= \frac{1}{m} \sum_i^{3N} \sum_{x_A^i = x_B^i} \sum_{y_A^i \neq y_B^i} p(y_A^i, y_B^i \mid x_A^i, x_B^i) \cdot p(x_A^i, x_B^i) \cdot \frac{1}{3N} \\ &= \frac{\kappa}{3} \sum_{i=0}^{2} \sum_{\substack{y_A^i \neq y_B^i \\ x_A^i = x_B^i}} p(y_A^i, y_B^i \mid x_A^i, x_B^i) \cdot p(x_A^i, x_B^i) \\ &= \frac{\kappa}{3}(p_0^2 + p_1^2 + p_2^2) \sum_{\substack{y_A \neq y_B \\ x_A = x_B}} p(y_A, y_B \mid x_A, x_B) = \frac{\kappa}{3}(1-\gamma) \cdot 3S = \kappa(1-\gamma)S. \end{aligned}$$

Thus if $p(x_A \neq x_B) = \gamma$, then the probability that we are in a testing round (J_3 or S), i.e. $T_i = 1$ is given by $\gamma + \kappa(1-\gamma)$. We can tune γ arbitrarily by choosing p_0, p_1 and p_2 appropriately.

Before proving Theorem 10, we first show a bound on the mutual information between Alice's output and Eve's system. Following the outline in [1], we assume that Eve provides Alice and Bob a Bell diagonal state with eigenvalues $\lambda_{\Phi^+}, \lambda_{\Phi^-}, \lambda_{\Psi^+}, \lambda_{\Psi^-}$ corresponding to the Bell states

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \qquad & |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \qquad & |\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned}$$

We may write the Bell diagonal state as

$$\rho_\lambda = \begin{pmatrix} \lambda_{\Phi^+} & & & \\ & \lambda_{\Psi^-} & & \\ & & \lambda_{\Phi^-} & \\ & & & \lambda_{\Psi^-} \end{pmatrix} \tag{10}$$

The following lemma provides a bound on the mutual information between Alice's output and Eve's system. This bound is then used in the proof of the theorem in bounding the min-entropy of Alice and Bob's outputs in the protocol conditioned on Eve's side information.

▶ **Lemma 11.** *Let Y_A^i be Alice's output in round $i \in [n]$, and E be Eve's register. If Eve provides Alice and Bob the Bell diagonal state ρ_λ in Equation* (10)*, with eigenvalues ordered as $\lambda_{\Phi^+} \geq \lambda_{\Psi^-}$ and $\lambda_{\Phi^-} \geq \lambda_{\Psi^+}$, we have*

$$\chi(Y_A^i : E) \leq h(\lambda_{\Phi^-}).$$

Proof. For Alice and Bob's measurement operators $E^{x_A}_{y_A}$ and $F^{x_B}_{y_B}$, the probability of getting outputs (y_A, y_B) given inputs (x_A, x_B) and state ρ is given by the Born rule, $p(y_A, y_B \,|\, x_A, x_B) = \operatorname{tr}\left((E^{x_A}_{y_A} \otimes F^{x_B}_{y_B})\,\rho\right)$. For the Bell diagonal state ρ_λ, this probability may be expanded as follows:

$$\begin{aligned}
p(y_A, y_B \,|\, x_A, x_B) &= \operatorname{tr}\left((E^{x_A}_{y_A} \otimes F^{x_B}_{y_B})\rho_\lambda\right)\\
&= \lambda_{\Phi^+}\operatorname{tr}\left((E^{x_A}_{y_A} \otimes F^{x_B}_{y_B})|\Phi^+\rangle\langle\Phi^+|\right) + \lambda_{\Phi^-}\operatorname{tr}\left((E^{x_A}_{y_A} \otimes F^{x_B}_{y_B})|\Phi^-\rangle\langle\Phi^-|\right)\\
&\quad + \lambda_{\Psi^+}\operatorname{tr}\left((E^{x_A}_{y_A} \otimes F^{x_B}_{y_B})|\Psi^+\rangle\langle\Psi^+|\right) + \lambda_{\Psi^-}\operatorname{tr}\left((E^{x_A}_{y_A} \otimes F^{x_B}_{y_B})|\Psi^-\rangle\langle\Psi^-|\right)\\
&= \lambda_{\Phi^+}\operatorname{tr}\left((E^{x_A}_{y_A} \otimes F^{x_B}_{y_B})|\Phi^+\rangle\langle\Phi^+|\right) + \lambda_{\Phi^-}\operatorname{tr}\left((E^{x_A}_{y_A} \otimes ZF^{x_B}_{y_B}Z)|\Phi^+\rangle\langle\Phi^+|\right)\\
&\quad + \lambda_{\Psi^+}\operatorname{tr}\left((E^{x_A}_{y_A} \otimes XF^{x_B}_{y_B}X)|\Phi^+\rangle\langle\Phi^+|\right) + \lambda_{\Psi^-}\operatorname{tr}\left((E^{x_A}_{y_A} \otimes YF^{x_B}_{y_B}Y)|\Phi^+\rangle\langle\Phi^+|\right)\\
&= \frac{\lambda_{\Phi^+}}{2}\operatorname{tr}\left(E^{x_A}_{y_A}\overline{F^{x_A}_{y_A}}\right) + \frac{\lambda_{\Phi^-}}{2}\operatorname{tr}\left(E^{x_A}_{y_A}\overline{ZF^{x_A}_{y_A}Z}\right)\\
&\quad + \frac{\lambda_{\Psi^+}}{2}\operatorname{tr}\left(E^{x_A}_{y_A}\overline{XF^{x_A}_{y_A}X}\right) + \frac{\lambda_{\Psi^-}}{2}\operatorname{tr}\left(E^{x_A}_{y_A}\overline{YF^{x_A}_{y_A}Y}\right)
\end{aligned}$$

Using this probability, we can compute the values of J_3 and S. One can show that choosing $E^{x_A}_{y_A} = \overline{F^{x_B}_{y_B}}$ is the optimal choice for minimizing J_3 and S simultaneously, but we skip the proof here. We define projection operators using variables $\theta_1, \theta_2, \gamma_1$ and γ_2 which we later optimize:

$$\begin{aligned}
E^0_0 &= |\phi_0\rangle\langle\phi_0| \quad \text{with } |\phi_0\rangle = |0\rangle\\
E^1_0 &= |\phi_1\rangle\langle\phi_1| \quad \text{with } |\phi_1\rangle = \cos\theta_1|0\rangle + e^{i\gamma_1}\sin\theta_1|1\rangle\\
E^2_0 &= |\phi_2\rangle\langle\phi_2| \quad \text{with } |\phi_2\rangle = \cos\theta_2|0\rangle + e^{i\gamma_2}\sin\theta_2|1\rangle
\end{aligned}$$

and where the corresponding $E^x_1 = \mathbb{1} - E^x_0$ for $x \in \{0,1,2\}$. Computing the asynchronicity S directly according to Equation (7) we get

$$S = \frac{\lambda_{\Phi^-}}{3}\left[\sin^2(2\theta_1) + \sin^2(2\theta_2)\right] + \frac{\lambda_{\Psi^+}}{3}\left[3 - (\sin^2(2\theta_1) + \sin^2(2\theta_2)\right] + \lambda_{\Psi^-}$$

The λ_{Ψ^-} term doesn't depend on θ_1 and θ_2, so we may take $\lambda_{\Psi^-} = 0$ since we want to minimize S. Further, since $\sin^2(2\theta_1) + \sin^2(2\theta_2) \geq 0$ and $\lambda_{\Phi^-} \geq \lambda_{\Psi^+}$, we may take $\lambda_{\Psi^+} = 0$. Next we define δ_1 and δ_2 to be the deviation in angles from the angles in the optimal strategy defined in Equation (1) (the optimal angles are given by $\theta_1 = \frac{\pi}{3}$ and $\theta_2 = -\frac{\pi}{3}$). Thus the equations we obtain for J_3 and S using $\theta_1 = \frac{\pi}{3} + \delta_1$ and $\theta_2 = -\frac{\pi}{3} + \delta_2$ are:

$$\begin{aligned}
J_3 = -(2\lambda_{\Phi^-} - 1)&\cos\left(\frac{\pi}{3} + \delta_1\right)\cos\left(-\frac{\pi}{3} + \delta_2\right)\sin\left(\frac{\pi}{3} + \delta_1\right)\sin\left(-\frac{\pi}{3} + \delta_2\right)\\
&+ \cos^2\left(\frac{\pi}{3} + \delta_1\right)\cos^2\left(-\frac{\pi}{3} + \delta_2\right)
\end{aligned}$$

Since we want to minimize J_3, we minimize the term independent of the factor λ_{Φ^-}. We call this term c_{J_3} and find that this term is

$$\begin{aligned}
c_{J_3} &= \cos\left(\frac{\pi}{3} + \delta_1\right)\cos\left(-\frac{\pi}{3} + \delta_2\right)\sin\left(\frac{\pi}{3} + \delta_1\right)\sin\left(-\frac{\pi}{3} + \delta_2\right)\\
&\quad + \cos^2\left(\frac{\pi}{3} + \delta_1\right)\cos^2\left(-\frac{\pi}{3} + \delta_2\right)\\
&= \cos\left(\frac{2\pi}{3} + \delta_1 - \delta_2\right)\cos\left(\frac{\pi}{3} + \delta_1\right)\cos\left(\frac{\pi}{3} - \delta_2\right)
\end{aligned}$$

Minimizing c_{J_3} for δ_1 and δ_2 we find that $\delta_1 = \frac{\delta_2}{2}$, and $\delta_2 \in \{0, \frac{2\pi}{3}, \frac{4\pi}{3}\}$. The solutions $\delta_2 = \frac{2\pi}{3}$ and $\delta_2 = \frac{4\pi}{3}$ are equivalent to $\delta_2 = 0$, so we only consider the latter solution. This suggests that in order for Eve to minimize J_3, her strategy must match the ideal strategy developed in Equation (1). Using $\delta_1 = \delta_2 = 0$, we get

$$\begin{aligned} J_3 &= -\frac{1}{8} + \frac{3}{8}\lambda_{\Phi^-} \\ S &= \frac{1}{2}\lambda_{\Phi^-} \end{aligned} \tag{11}$$

From [1, Lemma 5], we have

$$\begin{aligned} \chi(Y_A^i : E) &\leq H([\lambda_{\Phi^+}, \lambda_{\Phi^-}, \lambda_{\Psi^+}, \lambda_{\Psi^-}]) - h(\lambda_{\Phi^+} + \lambda_{\Phi^-}) \\ &= h(\lambda_{\Phi^-}) = \begin{cases} h(\frac{1}{3} + \frac{8}{3}J_3) \\ h(2S) \end{cases} \end{aligned}$$

Where the second to last equality follows because $\lambda_{\Psi^+} = \lambda_{\Psi^-} = 0$, thus $H([\lambda_{\Phi^+}, \lambda_{\Phi^-}]) = h(\lambda_{\Phi^-})$, and $h(\lambda_{\Phi^+} + \lambda_{\Phi^-}) = h(1) = 0$ ◀

Proof of Theorem 10. In similar fashion to [4, Theorem 4.1], we need to find a min-tradeoff function in order to apply the EAT. From Lemma 11, we have $\chi(Y_A^i : E|X_A^i = 0) \leq h\left(\frac{1}{3} + \frac{8}{3}J_3\right)$. Thus

$$H(Y_A^i|X_A^iX_B^iE) \geq 1 - h\left(\frac{1}{3} + \frac{8}{3}J_3\right) \tag{12}$$

Inserting this back into Equation (12), we get

$$H(Y_A^i|X_A^iX_B^iE) \geq 1 - h\left(\frac{1}{3} + \frac{8}{3}\left(1 - \frac{3}{2}\frac{p(R_i = 1)}{\gamma}\right)\right) = 1 - h\left(3 - 4\frac{p(R_i = 1)}{\gamma}\right)$$

For $\frac{p(1)}{\gamma} \in \left[\frac{2}{3}, 1\right]$, let

$$g(p) = \begin{cases} 1 - h\left(3 - 4\frac{p(1)}{\gamma}\right) & \frac{p(1)}{\gamma} \in \left[\frac{2}{3}, \frac{3}{4}\right] \\ 1 & \frac{p(1)}{\gamma} \in \left[\frac{3}{4}, 1\right] \end{cases}$$

We note that we only define $g(p)$ in the regime $\frac{p(1)}{\gamma} \in \left[\frac{2}{3}, 1\right]$ since that range is operationally relevant. The function can be extended to values of $\frac{p(1)}{\gamma} \in \left[0, \frac{2}{3}\right]$ for completeness but is not necessary for the purposes of the proof. The function $g(p)$ has unbounded gradient at $\frac{p(1)}{\gamma} = \frac{3}{4}$, and therefore needs to be modified using the "cutting-and-gluing" trick of [4] in order to define a min-tradeoff function that can be used in the EAT. To that effect, we define two functions l_1 and l_2 over a point p_t that can be later optimized:

$$l_1(p_t) = \left\lceil \frac{d}{dp(1)} g(p)\bigg|_{p_t} \right\rceil, \qquad l_2(p_t) = g(p_t) - l_1(p_t) \cdot p_t(1)$$

and define $f_{\min}^{J_3}$ as follows:

$$f_{\min}^{J_3}(p, p_t) = \begin{cases} g(p) & \text{if } p(1) \leq p_t(1) \\ l_1(p_t) \cdot p(1) + l_2(p_t) & \text{if } p(1) > p_t(1) \end{cases}$$

Applying the EAT with min-tradeoff function $f_{\min}^{J_3}(p, p_t)$ for any p_t such that $\frac{2}{3} < \frac{p_t(1)}{\gamma} < \frac{3}{4}$, and plugging in $\frac{p(1)}{\gamma} = \frac{p(R_i=1)}{\gamma} = \frac{2}{3} - \frac{2}{3}J_3$, we get the bound on the smooth min-entropy $H_{\min}^{\epsilon_s}(Y_AY_B \mid X_AX_BE)_{\rho_{|\Omega}}$ ◀

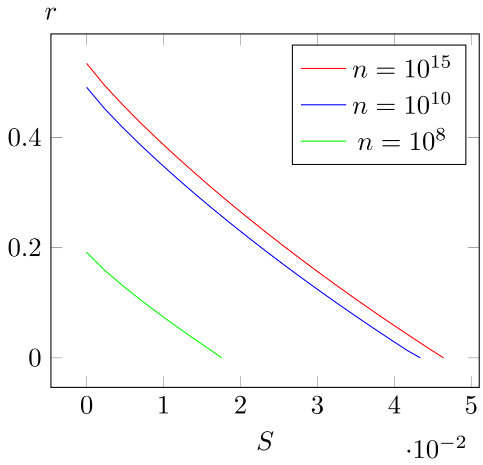

Figure 1 Values of $r = l/n$ against S

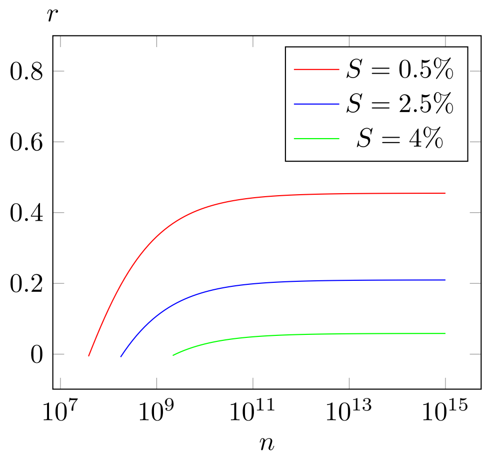

Figure 2 Values of $r = l/n$ against n

The soundness proof for the protocol follows identically to [4, Lemmas 5.3 and 5.4]. The key length l generated at the end of Protocol 1 is derived analogously to [4, Theorem 5.1 and Eq 5.4] which for completeness we state here:

$$\begin{aligned} l = n \cdot \mathsf{OPT}(\epsilon_s/4, \epsilon_{EA} + \epsilon_{EC}) - \mathsf{leak}_{\mathsf{EC}} - 3\log\left(1 - \sqrt{1 - (\epsilon_s/4)^2}\right) \\ - \gamma \cdot n - \sqrt{n} 2 \log 7 \sqrt{1 - 2\log(\epsilon_s/4 \cdot (\epsilon_{EA} + \epsilon_{EC}))} - 2\log(1/\epsilon_{PA}) \end{aligned} \tag{13}$$

where $\mathsf{leak}_{\mathsf{EC}}$ is discussed in detail in [4, §5.5.1 and Eq 5.9].

Based on Theorem 10 and [4, Theorem 5.1], we plot the key rate, defined as $r = \frac{l}{n}$. In Figure 1, we plot the key rate against the asynchronicity (referred to as the bit-error rate in [4]), and in Figure 2 we plot the key-rate against the total number of rounds while keeping asynchronicity constant. For large n, we are able to tolerate asynchronicity of up to 4.6% before the key-rate goes to 0. We use the values $\epsilon_{EC} = 10^{-10}, \epsilon_{EA} = \epsilon^s_{QKD} = 10^{-5}, \epsilon^c_{QKD} = 10^{-2}, p_0 = 0.97, p_1 = p_2 = 0.015$ and $\delta^{J_3}_{est} = 10^{-3}$ to plot the key rate curves in Figures 1 and 2.

6 Causality Loophole

In this section we describe what is called the *causality* or *locality* loophole common to device independent quantum key distribution protocols that use non-local games, and propose a solution to the loophole using a new security assumption.

As seen in Section 4, the bound for the Bell inequality $J_3 \geq -\frac{1}{8}$ is sharp and rigid only among synchronous quantum correlations. There exist more powerful synchronous nonsignaling strategies that violate those bounds. Furthermore, if classical communication is allowed between the parties in the protocol, even greater violations can be achieved. This is the *causality loophole*: unless Alice and Bob are acausally separated, then the statistics for the synchronous Bell inequalities can simply be simulated using classical communication.

In order to resolve the causality loophole in our protocol we pose a new security assumption: instead of limiting Eve's computational power or limiting the communication she can perform, we assume that she has imperfect knowledge of the basis Alice and Bob use in the protocol. We state this more formally:

Let ϵ be Eve's uncertainty about Alice and Bob's inputs. Without loss of generality, we assume that this is symmetric across all basis selections. For $x', x \in \{0,1,2\}$ we have

$$\Pr\{\text{Eve guesses basis } x' \mid \text{Alice (or Bob) selects basis } x\} = \begin{cases} 1-\epsilon & \text{when } x' = x \\ \frac{\epsilon}{2} & \text{when } x' \neq x. \end{cases} \tag{14}$$

In greater generality, we model the basis selection that Alice and Bob use for their inputs as a classical-quantum state on $\mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathfrak{H}_E$, corresponding to Alice, Bob, and Eve respectively. Alice and Bob's states are classical while Eve can have quantum side information which she may use to produce a correlation for a cheating strategy. We denote this state by ρ_{ABE}. For inputs $x_A, x_B \in \{0,1,2\}$ for Alice and Bob respectively, we have $\rho_{ABE} = |x_A\rangle\langle x_A| \otimes |x_B\rangle\langle x_B| \otimes \rho_E^{x_A,x_B}$, where $\rho_E^{x_A,x_B}$ quantifies Eve's side information. Based on (14) above we further decompose

$$\begin{aligned}\rho_E^{x_A,x_B} = \Big((1-\epsilon)^2\sigma_{x_A,x_B} &+ (1-\epsilon)\frac{\epsilon}{2}(\sigma_{x_A,x_B\oplus 1} + \sigma_{x_A,x_B\oplus 2} + \sigma_{x_A\oplus 1,x_B} + \sigma_{x_A\oplus 2,x_B}) \\ &+ \frac{\epsilon^2}{4}(\sigma_{x_A\oplus 1,x_B\oplus 1} + \sigma_{x_A\oplus 1,x_B\oplus 2} + \sigma_{x_A\oplus 2,x_B\oplus 1} + \sigma_{x_A\oplus 2,x_B\oplus 2})\Big),\end{aligned}$$

where we denote $x_A \oplus i := x_A + i \pmod 3$, and similarly for x_B. Writing Eve's guess for Alice's input by z_A and for Bob's input by z_B, the σ_{z_A,z_B} for $z_A, z_B \in \{0,1,2\}$ are densities containing Eve's side information depending on her guess for x_A and x_B respectively. With these, we also allow Eve to have unlimited computational power and communication to produce outputs (y_A, y_B). We denote the resulting conditional probability distribution as $\Pr\{(y_A, y_B \mid z_A, z_B)\}_{\sigma_{z_A,z_B}}$. As this is also a correlation, Eve has her own Bell term which we denote by $\tilde{J}_3$ and her own asynchronicity term which we denote by $\tilde{S}$.

Eve's goal is to program Alice and Bob's devices such that the device outputs pass statistical tests for estimating Bell violation and asynchronicity. The following theorem shows that Eve's uncertainty ϵ is upper-bounded by a function of the allowed errors in Alice and Bob's Bell and asynchronicity terms. If Eve's uncertainty exceeds a certain threshold then there does not exist a distribution $\Pr\{(y_A, y_B \mid z_A, z_B)\}_{\sigma_{z_A,z_B}}$ she can use to provide outputs to Alice and Bob that still pass their Bell and asynchronicity checks. We state the theorem formally as follows.

▶ **Theorem 12.** *Let $0 \leq \lambda < \frac{1}{8}$ be the allowed error in Alice and Bob's J_3 term, and $0 \leq \mu$ be their asynchronicity bound. On Eve's side, let $\tilde{J}_3$ and $\tilde{S}$ be analogous Bell inequality and asynchronicity terms for her correlation. Let ϵ be Eve's uncertainty about Alice and Bob's inputs as given in Equation* (14)*, and δ be such that $0 \leq \delta$. If $\epsilon > \epsilon_{max}^{\delta}$, where*

$$\epsilon_{max}^{\delta} = \frac{2}{3} - \frac{2}{3}\left(\frac{\sqrt{144(\delta-1)\lambda + 64\lambda^2 + 6(36\delta + 8\lambda - 9)\mu - 72\mu^2 - 162\delta + 81}}{6\mu - 18\delta - 8\lambda + 9}\right),$$

then Eve's asynchronicity $\tilde{S} < \delta$.

Proof. For inputs $x_A, x_B \in \{0,1,2\}$, the correlation that Alice and Bob use to compute key bits and self-test their devices is then given by:

$$p(y_A, y_B \mid x_A, x_B) = \tag{15}$$

$$\sum_{z_A,z_B} \Pr\{y_A, y_B \mid z_A, z_B\}_{\sigma_{z_A,z_B}} \cdot \left\{\begin{array}{ll} 1-\epsilon & \text{for } z_A = x_A \\ \frac{\epsilon}{2} & \text{otherwise} \end{array}\right\} \cdot \left\{\begin{array}{ll} 1-\epsilon & \text{for } z_B = x_B \\ \frac{\epsilon}{2} & \text{otherwise} \end{array}\right\}$$

We begin by deriving expressions for the expected values of J_3 and S.

$$\begin{aligned}\langle 1 - J_3\rangle &= \frac{1}{4}\big(p(0,1 \mid 0,1) + p(1,0 \mid 0,1) + p(0,1 \mid 1,0) + p(1,0 \mid 1,0)\\ &\quad + \; p(0,1 \mid 0,2) + p(1,0 \mid 0,2) + p(0,1 \mid 2,0) + p(1,0 \mid 2,0)\\ &\quad + \; p(0,1 \mid 1,2) + p(1,0 \mid 1,2) + p(0,1 \mid 2,1) + p(1,0 \mid 2,1)\big)\\ &= \left(1 - \epsilon + \tfrac{3}{4}\epsilon^2\right)(1 - \tilde{J}_3) + \left(\tfrac{3}{2}\epsilon - \tfrac{9}{8}\epsilon^2\right)\tilde{S} \qquad (16)\end{aligned}$$

A similar computation for S gives us:

$$\begin{aligned}\langle S\rangle &= \frac{1}{3}\big(p(0,1 \mid 0,0) + p(1,0 \mid 0,0) + p(0,1 \mid 1,1)\\ &\quad + p(1,0 \mid 1,1) + p(0,1 \mid 2,2) + p(1,0 \mid 2,2)\big)\\ &= \left(1 - 2\epsilon + \tfrac{3}{2}\epsilon^2\right)\tilde{S} + \left(\tfrac{4}{3}\epsilon - \epsilon^2\right)(1 - \tilde{J}_3) \qquad (17)\end{aligned}$$

Using Equations (16) and (17), we can solve for $\tilde{J}_3$ and $\tilde{S}$ as:

$$\begin{bmatrix} 1 - \tilde{J}_3 \\ \tilde{S} \end{bmatrix} = \begin{bmatrix} 1 - \epsilon + \frac{3}{4}\epsilon^2 & \frac{3}{2}\epsilon - \frac{9}{8}\epsilon^2 \\ \frac{4}{3}\epsilon - \epsilon^2 & 1 - 2\epsilon + \frac{3}{2}\epsilon^2 \end{bmatrix}^{-1} \begin{bmatrix} \frac{9}{8} - \lambda \\ \mu \end{bmatrix}$$

We get solutions:

$$\tilde{J}_3 = \frac{(3\epsilon^2 - 4\epsilon)(3 - 6\mu + 8\lambda) + 16\lambda - 2}{4\,(3\epsilon - 2)^2} \qquad \tilde{S} = \frac{(3\epsilon^2 - 4\epsilon)(6\mu - 8\lambda + 9) + 24\mu}{6\,(3\epsilon - 2)^2}. \qquad (18)$$

Plugging $\tilde{S} = \delta$ in Equation (18), and solving for ϵ gives us:

$$\epsilon^{\delta}_{max} = \frac{2}{3} - \frac{2}{3}\left(\frac{\sqrt{144(\delta - 1)\lambda + 64\lambda^2 + 6(36\delta + 8\lambda - 9)\mu - 72\mu^2 - 162\delta + 81}}{6\mu - 18\delta - 8\lambda + 9}\right) \qquad (19)$$

◀

▶ **Corollary 13.** *For $\epsilon > \epsilon^0_{max}$, there is no correlation Eve can use to produce a cheating strategy against Alice and Bob.*

Proof. Plugging in $\delta = 0$ in Equation (19),

$$\epsilon_{max} := \epsilon^0_{max} = \frac{2}{3} - \frac{2}{3}\left(\frac{\sqrt{64\lambda^2 + 6(8\lambda - 9)\mu - 72\mu^2 - 144\lambda + 81}}{6\mu - 8\lambda + 9}\right).$$

If Eve's uncertainty $\epsilon > \epsilon_{max}$, then $\tilde{S} < 0$, and since no correlation can have negative asynchronicity, no such $\Pr\{(y_A, y_B \mid z_A, z_B)\}_{\sigma_{z_A,z_B}}$ exists. ◀

By the corollary above, we conclude that Eve's uncertainty cannot grow too much before her asynchronicity becomes negative, therefore resulting in an infeasible strategy. Fixing a reasonable threshold for the error allowed in the Bell term, say $\lambda = 0.05$, we plot values of ϵ_{max} against varying values of Alice and Bob's allowed asynchronicity μ in Figure 3. The plot shows that even for allowed asynchronicity $\mu = 5\%$, Eve must have close to perfect certainty $\approx 97\%$ about Alice and Bob's inputs. Thus even with unlimited computational and communication power, when $\epsilon > \epsilon_{max}$, no correlation exists to perfectly simulate statistics that pass Alice and Bob's Bell and asynchronicity checks.

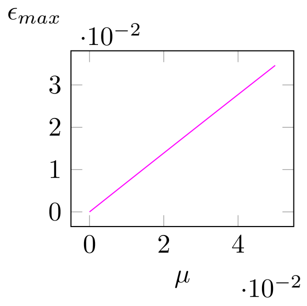

Figure 3 Values of μ vs. ϵ_{max} for which $\tilde{S}$ is non-negative

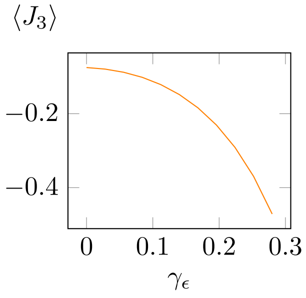

Figure 4 Values of $\langle J_3 \rangle$ vs. γ_ϵ for $\mu = 0.05, \lambda = 0.05$

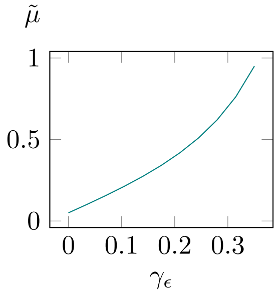

Figure 5 Values of $\langle S \rangle = \tilde{\mu}$ vs. γ_ϵ for $\mu = 0.05, \lambda = 0.05$

We further examine the regime where Eve's uncertainty $\epsilon > \epsilon_{max}$. In this case the best Eve can do in order to provide Alice and Bob an expected asynchronicity value $\langle S \rangle$ close to μ, is to use a synchronous correlation herself, i.e. $\tilde{S} = 0$. Fixing $\tilde{S} = 0$, we plot $\langle J_3 \rangle$ as Eve's uncertainty exceeds ϵ_{max}. Let $\gamma_\epsilon := \epsilon - \epsilon_{max}$ denote how much Eve's uncertainty is above the maximum. Figure 4 shows that even with a lot of uncertainty, Eve can make $\langle J_3 \rangle$ as close to $-\frac{1}{8}$ as she likes. Since Eve is not restricted to quantum strategies, she can in fact violate the $-\frac{1}{8}$ bound. However, providing a $\langle J_3 \rangle$ value smaller than $-\frac{1}{8}$ is not in her best interest since Alice and Bob check if their estimated J_3 is in $[-\frac{1}{8}, -\frac{1}{8} + \lambda]$.

As a result, detecting Eve's interference depends *only* on the asynchronicity check. Since Eve's $\tilde{S} = 0$, she has to provide a value for Alice and Bob's $\langle S \rangle = \tilde{\mu}$ that is strictly larger than their decided error threshold μ. We use Equation (17) to plot the effect of increasing ϵ past ϵ_{max} on $\langle S \rangle = \tilde{\mu}$ for a fixed λ and μ. Figure 5 shows the comparison between γ_ϵ and $\tilde{\mu}$ for $\mu = 0.05$ and $\lambda = 0.05$. In our analysis the choice of 0.05 for both λ and μ is arbitrary, and is made to demonstrate the effect of increasing Eve's uncertainty ϵ on the expected value $\langle S \rangle$. Alice and Bob may pick any reasonable error values for their J_3 and S terms without affecting the following calculations. From Figure 5, we see that $\tilde{\mu}$ increases sharply as γ_ϵ increases, which in turn implies that Alice and Bob's asynchronicity test always fails except with negligible probability. We show this using a straightforward Chernoff argument and bounding the probability that Alice and Bob's output is asynchronous in fewer than a μ fraction of the asynchronicity check rounds. Formally, let's assume Alice and Bob have m asynchronicity check rounds. Let A_i be a $\{0,1\}$ random variable denoting whether their output is asynchronous in round $i \in [m]$. Since Eve provides an asynchronous output with probability $\tilde{\mu}$, we have

$$A_i = \begin{cases} 1 & \text{with probability } \tilde{\mu}, \\ 0 & \text{otherwise.} \end{cases}$$

Let $A_S = \sum_i A_i$. Therefore $\langle A_S \rangle = \sum_i \langle A_i \rangle = m\tilde{\mu}$. Using a Chernoff bound we get

$$\Pr(A_S \le m\mu) \le \exp\left(-\frac{(\tilde{\mu} - \mu)^2 k}{2\tilde{\mu}}\right).$$

Alice and Bob can thus make this probability arbitrarily small by picking an appropriate value m for the number of asynchronicity check rounds they perform.

References

1 Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23):230501, 2007.

2 Werner Oskar Amrein and Kalyan B Sinha. On pairs of projections in a Hilbert space. *Linear algebra and its applications*, 208:425–435, 1994.

3 Alex Arkhipov. Extending and characterizing quantum magic games. *arXiv preprint arXiv:1209.3819*, 2012.

4 Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick. Simple and tight device-independent security proofs. *SIAM Journal on Computing*, 48(1):181–225, 2019.

5 Albrecht Böttcher and Ilya M Spitkovsky. A gentle guide to the basics of two projections theory. *Linear Algebra and its Applications*, 432(6):1412–1459, 2010.

6 Richard Cleve, Peter Høyer, Benjamin Toner, and John Watrous. Consequences and limits of nonlocal strategies. In *Computational Complexity, 2004. Proceedings. 19th IEEE Annual Conference on*, pages 236–249. IEEE, 2004.

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

8 Frederic Dupuis, Omar Fawzi, and Renato Renner. Entropy accumulation. *Communications in Mathematical Physics*, 379(3):867–913, 2020.

9 Marissa Giustina, Marijn AM Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, et al. Significant-loophole-free test of bell's theorem with entangled photons. *Physical review letters*, 115(25):250401, 2015.

10 Paul R Halmos. Two subspaces. *Transactions of the American Mathematical Society*, 144:381–389, 1969.

11 Bas Hensen, Hannes Bernien, Anaïs E Dréau, Andreas Reiserer, Norbert Kalb, Machiel S Blok, Just Ruitenberg, Raymond FL Vermeulen, Raymond N Schouten, Carlos Abellán, et al. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015.

12 Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP* = RE. *arXiv preprint arXiv:2001.04383*, 2020.

13 Se-Jin Kim, Vern Paulsen, and Christopher Schafhauser. A synchronous game for binary constraint systems. *Journal of Mathematical Physics*, 59(3):032201, 2018.

14 Laura Mancinska and David Roberson. Graph homomorphisms for quantum players. In *9th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2014)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2014.

15 N David Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical review letters*, 65(27):3373, 1990.

16 Carl A Miller and Yaoyun Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *Journal of the ACM (JACM)*, 63(4):1–63, 2016.

17 Vern I Paulsen, Simone Severini, Daniel Stahlke, Ivan G Todorov, and Andreas Winter. Estimating quantum chromatic numbers. *Journal of Functional Analysis*, 270(6):2188–2222, 2016.

18 Asher Peres. Incompatible results of quantum measurements. *Physics Letters A*, 151(3-4):107–108, 1990.

19 Sandu Popescu and Daniel Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24(3):379–385, 1994.

20 Nishant Rodrigues and Brad Lackey. Nonlocal games, synchronous correlations, and Bell inequalities. *arXiv preprint arXiv:1707.06200v4*, 2020.

21 Lynden K Shalm, Evan Meyer-Scott, Bradley G Christensen, Peter Bierhorst, Michael A Wayne, Martin J Stevens, Thomas Gerrits, Scott Glancy, Deny R Hamel, Michael S Allman, et al. Strong loophole-free test of local realism. *Physical review letters*, 115(25):250402, 2015.

22 Ben F Toner and Dave Bacon. Communication cost of simulating Bell correlations. *Physical Review Letters*, 91(18):187904, 2003.

23 Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Physical Review Letters*, 113(14):Art–No, 2014.

24 Thomas Vidick. Almost synchronous quantum correlations. *arXiv preprint arXiv:2103.02468*, 2021.