Security proof for Round Robin Differential Phase Shift QKD

Daan Leermakers and Boris Škorić
TU Eindhoven
d.leermakers.1@tue.nl, b.skoric@tue.nl

We give the first information-theoretic security proof of the 'Round Robin Differential Phase Shift' Quantum Key Distribution scheme. Our proof consists of the following steps. We construct an EPR variant of the scheme. We identify Eve's optimal way of coupling an ancilla to an EPR qudit pair under the constraint that the bit error rate between Alice and Bob should not exceed a value β. We determine, as a function of β, which POVM measurement on the ancilla Eve has to perform in order to learn as much as possible about Alice's bit.
It turns out that Eve's potential knowledge is much smaller than suggested in existing security analyses.

1 Introduction

1.1 Quantum Key Distribution and the RRDPS scheme

Quantum-physical information processing is different from classical information processing in several remarkable ways. Performing a measurement on an unknown quantum state typically destroys information; It is impossible to clone an unknown state by unitary evolution [1]; Quantum entanglement is a form of correlation between subsystems that does not exist in classical physics. Numerous ways have been devised to exploit these quantum properties for security purposes [2]. By far the most popular and well studied type of protocol is Quantum Key Distribution (QKD). QKD was first proposed in a famous paper by Bennett and Brassard in 1984 [3]. Given that Alice and Bob have a way to authenticate classical messages to each other (typically a short key), and that there is a quantum channel from Alice to Bob, QKD allows them to create a random key of arbitrary length about which Eve knows practically nothing. BB84 works with two conjugate bases in a two-dimensional Hilbert space. Many QKD variants have since been described in the literature [4, 5, 6, 7, 8, 9], using e.g. different sets of qubit states, EPR pairs, qudits instead of qubits, or continuous variables. Furthermore, various proof techniques have been developed [10, 11, 12, 13].
In 2014, Sasaki, Yamamoto and Koashi introduced *Round-Robin Differential Phase-Shift* (RRDPS) [14], a QKD scheme based on d-dimenional qudits. It has the advantage that it is very noise resilient while being easy to implement using photon pulse trains and interference measurements. One of the interesting aspects of RRDPS is that it is possible to omit the monitoring of signal disturbance. Even at high disturbance, Eve can obtain little information $I_{\rm AE}$ about Alice and Bob's secret. The value of $I_{\rm AE}$ determines how much privacy amplification is needed. As a result of this, the maximum possible QKD rate (the number of actual key bits conveyed per quantum state) is $1-h(\beta)-I_{\rm AE}$, where h is the binary entropy function and β the bit error rate.[1]

1.2 The security of RRDPS

The security of RRDPS has been discussed in a number of papers [14, 16, 17, 18]. However, the existing analyses are either incomplete, not tight, or do not have the mathematical rigour customary in cryptography. In the original RRDPS paper it is claimed that

$$I_{\rm AE} \leq h(\frac{1}{d-1}) \tag{1}$$

(Eq. 5 in [14] with photon number set to 1). The security analysis in [14] relies on the fact that Eve cannot distinguish between (a) the real protocol and (b) a fake protocol that produces the

[1] Monitoring of signal disturbance induces a small penalty on the QKD rate. However, the number of qubits that needs to be discarded is only logarithmic in the length of the derived key [15] and hence we will ignore it.

same statistical distribution of classical messages while Bob learns very little. There are two issues with this analysis. First, it was not really proven that the existence of the fake protocol puts an upper bound on Eve's knowledge. Second, even if the argument is valid, it is not known how tight the bound is.
Ref. [16] follows [14] and does a more accurate computation of phase error rate, tightening the $1/(d-1)$ in (1) to $1/d$. In [17] Sasaki and Koashi add β-dependence to their analysis and claim a bound

$$I_{\rm AE} \leq h(\frac{2\beta}{d-2}) \qquad \text{for } \beta \leq \frac{1}{2}\cdot\frac{d-2}{d-1} \tag{2}$$

and $I_{\rm AE} \leq h(\frac{1}{d-1})$ for $\beta \in [\frac{1}{2}\cdot\frac{d-2}{d-1}, \frac{1}{2}]$. The analysis in [18] considers only intercept-resend attacks, and hence puts a *lower bound* on Eve's potential knowledge, $I_{\rm AE} \geq 1 - h(\frac{1}{2}+\frac{1}{d}) = \mathcal{O}(1/d^2)$.[2]

1.3 Contributions and outline

In this paper we prove the security of RRDPS against the strongest possible adversary. We adopt a proof technique inspired by [11], [13] and [10]. For qubit-based QKR schemes it has been shown [19] that it suffices to consider attacks on individual qubits, as opposed to more complicated attacks on multiple qubits. The same reasoning applies to qudits.
We consider the case where Alice and Bob *do monitor the channel*, i.e. they are able to choose the amount of privacy amplification as a function of the observed bit error rate.

- We determine the optimal attack against an individual qudit, as a function of the bit error rate β. We do this as follows. We construct an EPR variant of RRDPS.[3] We identify Eve's optimal way of coupling an ancilla to an EPR qudit pair under the constraint that the bit error rate between Alice and Bob does not exceed β. (After meddling with the EPR pair Eve has the purification of the Alice-Bob mixed state.) We determine Eve's optimal POVM measurement on the ancilla given the information available to her.
- We show that Eve's optimal attack on the EPR pair can be written as an attack on Bob's qudit only.
- It turns out that the amount of information that Eve can obtain about Alice's secret bit is a rather complicated function of β. For $\beta \in [0, \beta_{\rm sat}]$, with $\beta_{\rm sat} = \frac{1}{4}\cdot\frac{d-2}{d-1}$, the leakage is an increasing function of β. For $\beta > \beta_{\rm sat}$ it 'saturates', i.e. remains constant. In terms of min-entropy, the leakage is $\log(1+\frac{1}{\sqrt{d-1}}\frac{\sqrt{\beta}}{\beta_{\rm sat}}\sqrt{2\beta_{\rm sat}-\beta})$ below the saturation point and $\log(1+\frac{1}{\sqrt{d-1}})$ above. In terms of Shannon entropy, the leakage is $1-h[\frac{1}{2}+\frac{1}{2\sqrt{d-1}}\frac{\sqrt{\beta}}{\beta_{\rm sat}}\sqrt{2\beta_{\rm sat}-\beta}]$ below the saturation point, and $1-h[\frac{1}{2}+\frac{1}{2\sqrt{d-1}}]$ above.
- Our (Shannon) leakage result is significantly smaller than the upper bound (2). Hence the actual performance of RRDPS is a lot better than previously thought.

In Section 2 we introduce notation and briefly summarise extraction of classical information from (mixed) quantum states, the RRDPS scheme, and the attacker model. In Section 3 we introduce the EPR version of RRDPS. It is completely equivalent to the original scheme security-wise. In Section 4 we impose the constraint that Eve's actions must not cause a bit error rate higher than β, and determine which mixed states of the Alice-Bob system are still allowed. There are only two scalar degrees of freedom left, which we denote as μ and V. In Section 5 we do the purification of the Alice-Bob mixed state, thus obtaining an expression for the state of Eve's ancilla. Although the ancilla space has dimension d^2, we show that only a four-dimensional subspace is relevant for the analysis. In Section 6 we derive the optimal POVM on the ancilla, at given μ, V and then maximise the min-entropy leakage over μ, V. In Section 7 we compute the Shannon entropy leakage. Section 8 compares our results to previous bounds.

[2] Ref. [18] gives a min-entropy of $-\log(\frac{1}{2}+\frac{1}{d})$, which translates to Shannon entropy $h(\frac{1}{2}+\frac{1}{d})$.
[3] This is similar to the Shor-Preskill technique [11]. Security of the EPR version implies security of the original protocol.

2 Preliminaries

2.1 Notation and terminology

Classical Random Variables (RVs) are denoted with capital letters, and their realisations with lowercase letters. The probability that a RV X takes value x is written as $\Pr[X = x]$. The expectation with respect to RV X is denoted as $\mathbb{E}_x f(x) = \sum_{x\in\mathcal{X}} \Pr[X = x] f(x)$. The constrained sum $\sum_{t,t':t\neq t'}$ is abbreviated as $\sum_{[tt']}$ and $\mathbb{E}_{u,v:u\neq v}$ as $\mathbb{E}_{[uv]}$. The Shannon entropy of X is written as $\mathsf{H}(X)$. Sets are denoted in calligraphic font. The notation 'log' stands for the logarithm with base 2. The min-entropy of $X \in \mathcal{X}$ is $\mathsf{H}_{\min}(X) = -\log \max_{x\in\mathcal{X}} \Pr[X = x]$, and the conditional min-entropy is $\mathsf{H}_{\min}(X|Y) = -\log \mathbb{E}_y \max_{x\in\mathcal{X}} \Pr[X = x|Y = y]$. The notation h stands for the binary entropy function $h(p) = p\log\frac{1}{p} + (1-p)\log\frac{1}{1-p}$. Bitwise XOR of binary strings is written as '$\oplus$'. The Kronecker delta is denoted as δ_{ab}. For quantum states we use Dirac notation. The notation 'tr' stands for trace. The Hermitian conjugate of an operator A is written as $A^\dagger$. When A is a complicated expression, we sometimes write $(A + \text{h.c.})$ instead of $A + A^\dagger$. The complex conjugate of z is denoted as z^*. We use the Positive Operator Valued Measure (POVM) formalism. A POVM $\mathcal{M}$ consists of positive semidefinite operators, $\mathcal{M} = (M_x)_{x\in\mathcal{X}}$, $M_x \geq 0$, and satisfies the condition $\sum_x M_x = \mathbb{1}$. The trace norm of A is $\|A\|_1 = \text{tr}\sqrt{A^\dagger A}$. The trace distance between matrices ρ and σ is denoted as $\frac{1}{2}\|\rho-\sigma\|_1$.

2.2 (Min-)entropy of a classical variable given a quantum state

The notation $\mathcal{M}(\rho)$ stands for the classical RV resulting when $\mathcal{M}$ is applied to mixed state ρ. Consider a bipartite system 'AB' where the 'A' part is classical, i.e. the state is of the form $\rho^{\text{AB}} = \mathbb{E}_{x\in\mathcal{X}}|x\rangle\langle x| \otimes \rho_x$ with the $|x\rangle$ forming an orthonormal basis. The min-entropy of the classical RV X given part 'B' of the system is [20]

$$\mathsf{H}_{\min}(X|\rho_X) = -\log \max_{\mathcal{M}} \mathbb{E}_{x\in\mathcal{X}} \text{tr}\,[M_x\rho_x]. \tag{3}$$

Here $\mathcal{M} = (M_x)_{x\in\mathcal{X}}$ denotes a POVM. Let $\Lambda \stackrel{\text{def}}{=} \sum_x \rho_x M_x$. If a POVM can be found that satisfies the condition[4] [21]

$$\forall_{x\in\mathcal{X}}:\ \Lambda - \rho_x \geq 0, \tag{4}$$

then there can be no better POVM for guessing X (but equally good POVMs may exist).
For states that also depend on a classical RV $Y \in \mathcal{Y}$, the min-entropy of X given the quantum state and Y is

$$\mathsf{H}_{\min}(X|Y,\rho_X(Y)) = -\log \mathbb{E}_{y\in\mathcal{Y}} \max_{\mathcal{M}} \mathbb{E}_{x\in\mathcal{X}} \text{tr}\,[M_x\rho_x(y)]. \tag{5}$$

A simpler expression is obtained when X is a binary variable. Let $X \in \{0,1\}$.
Then

$$X \sim (p_0,p_1):\quad \mathsf{H}_{\min}(X|Y,\rho_X(Y)) = -\log\left(\frac{1}{2} + \frac{1}{2}\mathbb{E}_y \text{tr}\left\|p_0\rho_0(y) - p_1\rho_1(y)\right\|_1\right). \tag{6}$$

This generalizes in a straightforward manner for states that depend on multiple classical RVs. The Shannon entropy of a classical variable given a quantum state is given by

$$\mathsf{H}(X|\rho_X) = \min_{\mathcal{M}} \mathsf{H}(X|\mathcal{M}(\rho_X)). \tag{7}$$

In contrast to the min-entropy case, there is no simple test analogous to (4) which tells you whether a local minimum in (7) is a global minimum.

[4]Ref. [21] specifies a second condition, namely $\Lambda^\dagger = \Lambda$. However, the hermiticity of Λ already follows from the condition (4).

2.3 The RRDPS scheme in a nutshell

The dimension of the qudit space is d. The basis states[5] are denoted as $|t\rangle$, with time indices $t \in \{0, \ldots, d-1\}$. Whenever we use notation "$t_1 + t_2$" it should be understood that the addition of time indices is modulo d. The RRDPS scheme consists of the following steps.

1. Alice generates a random bitstring $a \in \{0,1\}^d$. She prepares the single-photon state

$$|\mu_a\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{d}} \sum_{t=0}^{d-1} (-1)^{a_t} |t\rangle \tag{8}$$

   and sends it to Bob.

2. Bob chooses a random integer $r \in \{1, \ldots, d-1\}$. Bob performs a POVM measurement $\mathcal{M}^{(r)}$ described by a set of $2d$ operators $(M_{ks}^{(r)})_{k\in\{0,\ldots,d-1\}, s\in\{0,1\}}$,

$$M_{ks}^{(r)} = \frac{1}{2} |\Psi_{ks}^{(r)}\rangle\langle\Psi_{ks}^{(r)}| \quad ; \quad |\Psi_{ks}^{(r)}\rangle = \frac{|k\rangle + (-1)^s |k+r\rangle}{\sqrt{2}}. \tag{9}$$

   The result of the measurement $\mathcal{M}^{(r)}$ on $|\mu_a\rangle$ is an random integer $k \in \{0, \ldots, d-1\}$ and a bit $s = a_k \oplus a_{k+r}$.[6]

3. Bob announces k and r over a public but authenticated channel. Alice computes $s = a_k \oplus a_{k+r}$. Alice and Bob now have a shared secret bit s.

This procedure is repeated multiple times.
To detect eavesdropping, Alice and Bob can compare a small randomly selected fraction of their secret bits. If this comparison is not performed, Alice and Bob have to assume that Eve learns as much as when causing bit error rate $\beta = \frac{1}{2}$. This mode of operation (without monitoring) was proposed in the original RRDPS paper [14].
Finally, on the remaining bits Alice and Bob carry out the standard procedures of information reconciliation and privacy amplification.
The security of RRDPS is intuitively understood as follows. A measurement in a d-dimensional space cannot extract more than $\log d$ bits of information. The state $|\mu_a\rangle$, however, contains $d-1$ pieces of information, which is a lot more than $\log d$. Eve can learn only a fraction of the phase information embedded in the qudit. Furthermore, what information she has is of limited use, because she cannot force Bob to select specific phases. (i) She cannot force Bob to choose a specific r value. (ii) Even if she feeds Bob a state of the form $|\Psi_{\ell u}^{(r)}\rangle$, where r accidentally equals Bob's r, then there is a $\frac{1}{2}$ probability that Bob's measurement $\mathcal{M}^{(r)}$ yields $k \neq \ell$ *with random* s.

2.4 Attacker model; channel monitoring

There is a quantum channel from Alice to Bob. There is an authenticated but non-confidential classical channel between Alice and Bob. We allow Eve to attack quantum states in any way allowed by the laws of quantum physics, e.g. using unbounded quantum memory, entanglement, lossless operations, arbitrary POVMs, arbitrary unitary operators etc. All photon losses and bit errors observed by Alice and Bob are assumed to be caused by Eve. Eve cannot influence the random choices of Alice and Bob, nor the state of their (measurement) devices. There are no side channels. This is the standard attacker model for quantum-cryptographic schemes.
We consider the following way of channel monitoring. Alice and Bob test the bit error rate *for each value of* k *separately*, demanding that for each $k \in \{0, \ldots, d-1\}$ the bit error rate does not exceed β. Since Eve has no control over r, a and Bob's bit s, this implies that for all a, r, s, k the

[5] The physical implementation [14] is a *pulse train*: a photon is split into d coherent pieces which are released at different, equally spaced, points in time.

[6] The phase $(-1)^{a_k \oplus a_{k+r}}$ is the phase of the field oscillation in the $(k+r)$'th pulse relative to the k'th. The measurement $\mathcal{M}^{(r)}$ is an interference measurement where one path is delayed by r time units.

bit error rate does not exceed β. The number of qudits required to perform d tests is of order $d \log n$, where n is the length of the final key [15]. We will assume that n is chosen sufficiently large to ensure $d \log n \ll n$. In Section 6 we will see that the leakage becomes constant when β exceeds a saturation point $\beta_{\rm sat}$. If Alice and Bob are willing to tolerate such a noise level, then channel monitoring is no longer necessary; they just assume that the maximum possible leakage occurs.

3 EPR version of the protocol

We follow the standard Shor-Preskill technique [11] and re-formulate the protocol using EPR pairs. This will make it easier and more intuitive to describe the most general attack Eve can perform. Proving the security of the EPR version of the protocol guarantees the security of the original protocol.

E1 Alice prepares a maximally entangled two-qudit state

$$|\alpha_0\rangle \stackrel{\rm def}{=} \frac{1}{\sqrt{d}} \sum_{t=0}^{d-1} |tt\rangle. \tag{10}$$

She sends the second qudit to Bob.

E2 Eve does something with the Bob's qudit. Then Bob receives the qudit.

E3 Alice performs a POVM $\mathcal{Q} = (Q_a)_{a \in \{0,1\}^d}$ on her own qudit, where

$$Q_a = \frac{d}{2^d} |\mu_a\rangle\langle\mu_a|. \tag{11}$$

This results in a measured string a.

E4 Bob picks a random integer $r \in \{1, \ldots, d-1\}$ and performs the POVM measurement $\mathcal{M}^{(r)}$ on his qudit. The result of the measurement is an integer $k \in \{0, \ldots, d-1\}$ and a bit s.

E5 Bob announces r and k. Alice computes $s' = a_k \oplus a_{k+r}$.

Lemma 3.1 *The hermitian matrices Q_a as defined in (11) form a POVM, i.e.* $\sum_{a \in \{0,1\}^d} Q_a = \mathbb{1}$.

<u>*Proof:*</u> $\sum_a |\mu_a\rangle\langle\mu_a| = \sum_a \frac{1}{d} \sum_{t,t'=0}^{d-1} (-1)^{a_{t'}+a_t} |t\rangle\langle t'| = \frac{1}{d} \sum_{t,t'=0}^{d-1} |t\rangle\langle t'| \sum_a (-1)^{a_{t'}+a_t}$.
Using $\sum_a (-1)^{a_{t'}+a_t} = 2^d \delta_{tt'}$ we get $\sum_a |\mu_a\rangle\langle\mu_a| = \frac{2^d}{d} \sum_t |t\rangle\langle t| = \frac{2^d}{d}\mathbb{1}$. □

It is not important whether $\mathcal{Q}$ is practical or not; it is a theoretical construct which allows us to build an EPR version of the protocol equivalent to the original protocol. In the initial calculation, we allow Eve to attack the qudit that is sent to Bob as well as the qudit that is kept by Alice. We will show that the most general attack Eve can perform without being detected can also be achieved by attacking Bob's qudit only. We don't overestimate nor do we underestimate Eve's possible attack. Note that Alice and Bob's measurements can be carried out in the opposite order.

4 Imposing the noise constraint

Let $\rho^{\rm AB}$ denote the pure EPR state of Alice and Bob. The channel monitoring restricts the ways in which Eve can alter the state to some mixed state $\tilde{\rho}^{\rm AB}$ without being detected. We will determine the most general allowed $\tilde{\rho}^{\rm AB}$ that is compatible with bit error rate *exactly* β for all values of (a, k, r, s). Such $\tilde{\rho}^{\rm AB}$ corresponds to the strongest possible noise that goes undetected.

After Eve's actions in step E2, Alice and Bob have a bipartite mixed state $\tilde{\rho}^{\rm AB}$ that can be represented in its most general form as

$$\tilde{\rho}^{\rm AB} = \sum_{t,t',\tau,\tau' \in \{0,\ldots,d-1\}} \rho^{tt'}_{\tau\tau'} |t,t'\rangle\langle\tau,\tau'|, \tag{12}$$

with $\rho^{\tau\tau'}_{tt'} = (\rho^{tt'}_{\tau\tau'})^*$ and $\sum_{tt'} \rho^{tt'}_{tt'} = 1$. We introduce the notation $P_{aks|r} = \Pr[A = a, K = k, S = s|R = r]$.

Lemma 4.1 *Let Alice and Bob's bipartite state be given by (12) and let them perform the measurements $\mathcal{Q}$ and $\mathcal{M}^{(r)}$ respectively. The joint probability of the outcomes a, k, s is given by*

$$P_{aks|r} = \frac{1}{4 \cdot 2^d} \sum_{t\tau} (-1)^{a_t + a_\tau} [\rho^{tk}_{\tau k} + \rho^{t,k+r}_{\tau,k+r} + (-1)^s (\rho^{tk}_{\tau,k+r} + \rho^{t,k+r}_{\tau k})]. \tag{13}$$

<u>*Proof:*</u> $P_{aks|r} = {\rm tr}\, (Q_a \otimes M^{(r)}_{ks}) \tilde{\rho}^{\rm AB}$
$= {\rm tr}\, (\frac{1}{2^d} \sum_{\ell\ell'} (-1)^{a_\ell + a_{\ell'}} |\ell\rangle\langle\ell'| \otimes \frac{1}{2} \frac{|k\rangle + (-1)^s |k+r\rangle}{\sqrt{2}} \frac{\langle k| + (-1)^s \langle k+r|}{\sqrt{2}}) \sum_{tt'\tau\tau'} \rho^{tt'}_{\tau\tau'} |t\rangle\langle\tau| \otimes |t'\rangle\langle\tau'|$
$= \frac{1}{2^d 4} \sum_{tt'\tau\tau'} \rho^{tt'}_{\tau\tau'} (-1)^{a_t + a_\tau} [\delta_{t'k} + (-1)^s \delta_{t',k+r}][\delta_{\tau' k} + (-1)^s \delta_{\tau',k+r}]$
$= \frac{1}{2^d 4} \sum_{t\tau} (-1)^{a_t + a_\tau} [\rho^{tk}_{\tau k} + \rho^{t,k+r}_{\tau,k+r} + (-1)^s \rho^{tk}_{\tau,k+r} + (-1)^s \rho^{t,k+r}_{\tau k}]$. □
We impose the constraint that a and k are independent uniform RVs, and furthermore that the event $s \neq s'$ occurs with probability β for all combinations (a, r, k).

Theorem 4.2 *The constraint $\forall_{a,k,s,r} : P_{aks|r} = \frac{1}{2^d d} [\delta_{s,a_k \oplus a_{k+r}} (1 - \beta) + (1 - \delta_{s,a_k \oplus a_{k+r}}) \beta]$ can only be satisfied by a density function of the form*

$$\tilde{\rho}^{\rm AB} = (1 - 2\beta - V) |\alpha_0\rangle\langle\alpha_0| + V \frac{1}{d} \sum_{tt'} |tt'\rangle\langle t't| + (2\beta - \mu) \frac{\mathbb{1}}{d^2} + \mu \frac{1}{d} \sum_t |tt\rangle\langle tt| \tag{14}$$

with $\mu, V \in \mathbb{R}$. Written componentwise,

$$\rho^{tt'}_{\tau\tau'} = \frac{1 - 2\beta - V}{d} \delta_{t't} \delta_{\tau'\tau} + \frac{V}{d} \delta_{\tau t'} \delta_{\tau' t} + \frac{2\beta - \mu}{d^2} \delta_{\tau t} \delta_{\tau' t'} + \frac{\mu}{d} \delta_{t' t} \delta_{\tau t} \delta_{\tau' t}. \tag{15}$$

<u>*Proof:*</u> In expression (13) we distinguish two cases. (i) In the terms without s-dependence we have to make sure that the factor $(-1)^{a_t + a_\tau}$ vanishes. This requires setting $\tau = t$, i.e. $\rho^{tt'}_{\tau\tau'} = \alpha \delta_{\tau t}$, where α is allowed to depend on t; however, α cannot depend on t' and τ' (other than via $\delta_{t'\tau'}$) since then $P_{aks|r}$ would depend on k and $k + r$. (ii) In the terms containing $(-1)^s$ we have to make sure that $(-1)^{a_t + a_\tau} = (-1)^{a_k + a_{k+r}}$. This requires setting $\rho^{tt'}_{\tau\tau'} \propto \delta_{tt'} \delta_{\tau\tau'}$ or $\rho^{tt'}_{\tau\tau'} \propto \delta_{t\tau'} \delta_{\tau t'}$, where the proportionality constant can not depend on t or τ other than via $\delta_{t\tau}$.
Combining these two cases we get the general expression

$$\rho^{tt'}_{\tau\tau'} \quad = \quad f_t \delta_{t\tau} \delta_{t'\tau'} (1 - \delta_{tt'}) + c \delta_{tt'} \delta_{\tau\tau'} (1 - \delta_{t\tau}) + e \delta_{t\tau'} \delta_{\tau t'} (1 - \delta_{t\tau}) + g \delta_{tt'} \delta_{t\tau} \delta_{t\tau'} \tag{16}$$

with $f_t, c, e, g \in \mathbb{R}$ and $gd + (d - 1) \sum_t f_t = 1$. (The latter in order to ensure that the trace equals 1.) Substitution into (13) yields

$$P_{aks|r} = \frac{1}{4 \cdot 2^d} [2 \sum_t f_t - f_k - f_{k+r} + 2g + 2(c + e)(-1)^{s + a_k + a_{k+r}}]. \tag{17}$$

In order to remove the dependence on k and $k+r$ we have to set $f_t = f$, i.e. constant. Furthermore we have to set $c + e = (1 - 2\beta)/d$ in order to satisfy the noise constraint. Finally we reparametrise our constants as $\mu = 2\beta - d^2 f$, $V = de$. □
Theorem 4.2 shows that (at fixed β) there are only two degrees of freedom, μ and V, in Eve's manipulation of the EPR pair.

5 Purification

According to the attacker model we have to assume that Eve has the purification of the state $\tilde\rho^{\rm AB}$. The purification contains all information that exists outside the AB system.

5.1 The purified state and its properties

We introduce the following notation,

$$|\alpha_j\rangle \stackrel{\rm def}{=} \frac{1}{\sqrt{d}}\sum_t e^{i\frac{2\pi}{d}jt}|tt\rangle, \qquad j\in\{0,\ldots,d-1\} \tag{18}$$

$$|D^\pm_{tt'}\rangle \stackrel{\rm def}{=} \frac{|tt'\rangle\pm|t't\rangle}{\sqrt2} \qquad t<t'. \tag{19}$$

Lemma 5.1 *The operator $\tilde\rho^{\rm AB}$ given in (14) has the following orthonormal eigensystem,*

$$\begin{array}{lll} |\alpha_0\rangle & \textit{with eigenvalue } \lambda_0 \stackrel{\rm def}{=} \frac{2\beta-\mu}{d^2}+\frac{\mu+V}{d}+1-2\beta-V \\ |\alpha_j\rangle \quad j\in\{1,\ldots,d-1\} & \textit{with eigenvalue } \lambda_1 \stackrel{\rm def}{=} \frac{2\beta-\mu}{d^2}+\frac{\mu+V}{d}. \\ |D^\pm_{tt'}\rangle \quad (t<t') & \textit{with eigenvalue } \lambda_\pm \stackrel{\rm def}{=} \frac{2\beta-\mu}{d^2}\pm\frac{V}{d} \end{array} \tag{20}$$

<u>*Proof:*</u> The term proportional to $\mathbb{1}$ in (14) yields a contribution $(2\beta-\mu)/d^2$ to each eigenvalue. First we look at $|\alpha_j\rangle$. We have $\langle\alpha_0|\alpha_j\rangle=\delta_{j0}$. Furthermore $\langle t't|\alpha_j\rangle=\delta_{t't}e^{i\frac{2\pi}{d}jt}/\sqrt{d}$, which gives $(\sum_{tt'}|tt'\rangle\langle t't|)|\alpha_j\rangle=|\alpha_j\rangle$. Similarly we have $(\sum_t|tt\rangle\langle tt|)|\alpha_j\rangle=|\alpha_j\rangle$. Next we look at $|D^\pm_{tt'}\rangle$. We have $\langle\alpha_0|D^\pm_{tt'}\rangle=0$ and $\langle uu|D^\pm_{tt'}\rangle=0$. Hence the $(1-2\beta-V)$-term and the μ-term in (14) yield zero when acting on $|D^\pm_{tt'}\rangle$. Furthermore $\sum_{uu'}|uu'\rangle\langle u'u|D^+_{tt'}\rangle=\sum_{uu'}|uu'\rangle\frac{\delta_{ut}\delta_{u't'}+\delta_{ut'}\delta_{u't}}{\sqrt2}$ $=|D^+_{tt'}\rangle$. Similarly, $\sum_{uu'}|uu'\rangle\langle u'u|D^-_{tt'}\rangle=\sum_{uu'}|uu'\rangle\frac{\delta_{ut}\delta_{u't'}-\delta_{ut'}\delta_{u't}}{\sqrt2}{\rm sgn}(u-u')=-|D^-_{tt'}\rangle$. □

In diagonalised form the $\tilde\rho^{\rm AB}$ is given by

$$\tilde\rho^{\rm AB}=\lambda_0|\alpha_0\rangle\langle\alpha_0|+\lambda_1\sum_{j=1}^{d-1}|\alpha_j\rangle\langle\alpha_j|+\lambda_+\sum_{tt':t<t'}|D^+_{tt'}\rangle\langle D^+_{tt'}|+\lambda_-\sum_{tt':t<t'}|D^-_{tt'}\rangle\langle D^-_{tt'}|. \tag{21}$$

The purification is

$$\begin{aligned}|\Psi^{\rm ABE}\rangle &= \sqrt{\lambda_0}|\alpha_0\rangle\otimes|E_0\rangle+\sqrt{\lambda_1}\sum_{j=1}^{d-1}|\alpha_j\rangle\otimes|E_j\rangle \\ &\quad +\sqrt{\lambda_+}\sum_{tt':t<t'}|D^+_{tt'}\rangle\otimes|E^+_{tt'}\rangle+\sqrt{\lambda_-}\sum_{tt':t<t'}|D^-_{tt'}\rangle\otimes|E^-_{tt'}\rangle,\end{aligned} \tag{22}$$

where we have introduced an orthonormal basis $|E_j\rangle$, $|E^\pm_{tt'}\rangle$ in Eve's Hilbert space.
In Theorem 5.2 below we show that Eve does not have to touch Alice's state. Hence the attacks that we are describing here can also be carried out in the original (non-EPR) protocol, where Eve gets access only to the state sent to Bob.

Theorem 5.2 *The operation that maps the pure EPR state to $|\Psi^{\rm ABE}\rangle$ (22) can be represented as a unitary operation on Bob's subsystem and Eve's ancilla.*

<u>*Proof:*</u> Let Eve's ancilla have initial state $|E_0\rangle$. The transition from the pure EPR state to (22) can be written as the following mapping,

$$U\Big(|t\rangle_{\rm B}\otimes|E_0\rangle_{\rm E}\Big)=|\Omega_t\rangle, \tag{23}$$

where $|\Omega_t\rangle$ is a state in the BE system defined as

$$\begin{aligned}|\Omega_t\rangle &\stackrel{\text{def}}{=} \sqrt{\lambda_0}|t\rangle|E_0\rangle + \sqrt{\lambda_1}|t\rangle\sum_{j=1}^{d-1} e^{i\frac{2\pi}{d}jt}|E_j\rangle + \sqrt{\frac{d\lambda_+}{2}}\sum_{t':t'\neq t}|t'\rangle|E^+_{(tt')}\rangle \\ &\quad + \sqrt{\frac{d\lambda_-}{2}}\sum_{t':t'\neq t}|t'\rangle|E^-_{(tt')}\rangle\text{sgn}(t'-t). \end{aligned} \tag{24}$$

The notation (tt') indicates ordering of t and t' such that the smallest index occurs first. It holds that $\langle\Omega_t|\Omega_\tau\rangle = \delta_{t\tau}$. Eqs. (23,24) show that the attack can be represented as an operation that does not touch Alice's subsystem. Next we have to prove that the mapping is unitary. The fact that $\langle\Omega_t|\Omega_\tau\rangle = \delta_{t\tau}$ shows that orthogonality in Bob's space is correctly preserved. In order to demonstrate full preservation of orthogonality we have to define the action of the operator U on states of the form $|t\rangle_{\rm B}\otimes|\varepsilon\rangle_{\rm E}$, where $|\varepsilon\rangle$ is one of Eve's basis vectors orthogonal to $|E_0\rangle$, in such a way that the resulting states are mutually orthogonal and orthogonal to all $|\Omega_t\rangle$, $t\in\{0,\ldots,d-1\}$. The dimension of the BE space is d^3 and allows us to make such a choice of $d(d^2-1)$ vectors. □

Theorem 5.3 *Let Alice send the state $|\mu_a\rangle$ to Bob. Let Eve apply the unitary operation U (specified in the proof of Theorem 5.2) to this state and her ancilla. The result can be written as*

$$U\Big(|\mu_a\rangle\otimes|E_0\rangle\Big) = \frac{1}{\sqrt{d}}\sum_{t=0}^{d-1}(-1)^{a_t}|t\rangle\otimes|A^a_t\rangle, \tag{25}$$

$$|A^a_t\rangle \stackrel{\text{def}}{=} \sqrt{\lambda_0}|E_0\rangle+\sqrt{\lambda_1}\sum_{j=1}^{d-1}e^{i\frac{2\pi}{d}jt}|E_j\rangle+\sqrt{\frac{d}{2}}\sum_{t':t'\neq t}(-1)^{a_t+a_{t'}}\Big[\sqrt{\lambda_+}|E^+_{(tt')}\rangle + \sqrt{\lambda_-}\text{sgn}(t'-t)|E^-_{(tt')}\rangle\Big]. \tag{26}$$

The states $|A^a_t\rangle$ are normalised and satisfy $\forall_{t\tau:\tau\neq t}\ \langle A^a_\tau|A^a_t\rangle = (1-2\beta)$.

<u>*Proof:*</u> We start from $U(|\mu_a\rangle|E_0\rangle) = (1/\sqrt{d})\sum_t(-1)^{a_t}|\Omega_t\rangle$ and we substitute (24). Re-labeling of summation variables yields (25,26). The norm $\langle A^a_t|A^a_t\rangle$ equals $\lambda_0+(d-1)\lambda_1+\frac{d(d-1)}{2}\lambda_++\frac{d(d-1)}{2}\lambda_-$, which equals 1 since this is also equal to the trace of $\tilde\rho^{\rm AB}$. For $\tau\neq t$ the inner product $\langle A^a_\tau|A^a_t\rangle$ yields

$$\lambda_0+\lambda_1\sum_{j=1}^{d-1}e^{i\frac{2\pi}{d}j(t-\tau)}+\frac{d}{2}\sum_{t'\neq t}\sum_{\tau'\neq\tau}(-1)^{a_t+a_{t'}+a_\tau+a_{\tau'}}\delta_{t'\tau}\delta_{\tau' t}[\lambda_++\lambda_-\text{sgn}(t'-t)\text{sgn}(\tau'-\tau)]. \tag{27}$$

We use $\sum_{j=1}^{d-1}e^{i\frac{2\pi}{d}j(t-\tau)} = d\delta_{\tau t}-1=-1$. Furthermore the Kronecker deltas in (27) set the phase $(-1)^{\cdots}$ to 1 and $\text{sgn}(t'-t)\text{sgn}(\tau'-\tau) = \text{sgn}(\tau-t)\text{sgn}(t-\tau)=-1$. Finally we use $\lambda_0-\lambda_1 = 1-2\beta-V$ and $\lambda_+-\lambda_- = 2V/d$. □

Theorem 5.3 reveals an intuitive picture. In the noiseless case ($\beta=0$) it holds that $\forall_t\ |A^a_t\rangle = |E_0\rangle$, i.e. Eve does nothing, resulting in the factorised state $|\mu_a\rangle|E_0\rangle$. In the case of extreme noise ($\beta=\frac{1}{2}$) we have $\langle A^a_t|A^a_\tau\rangle=\delta_{t\tau}$, which corresponds to a maximally entangled state between Bob and Eve.

Corollary 5.4 *The pure state (25) in Bob and Eve's space gives rise to the following mixed state $\rho^{\rm B}_a$ in Bob's subsystem,*

$$\rho^{\rm B}_a = (1-2\beta)|\mu_a\rangle\langle\mu_a| + 2\beta\frac{\mathbb{1}}{d}. \tag{28}$$

<u>*Proof:*</u> Follows directly from (25) by tracing out Eve's space and using the inner product $\langle A^a_\tau|A^a_t\rangle = (1-2\beta)$ for $\tau\neq t$. □

From Bob's point of view, what he receives is a mixture of the $|\mu_a\rangle$ state and the fully mixed state. The interpolation between these two is linear in β. Note that the parameters μ, V are not visible in $\rho^{\rm B}_a$.

5.2 Eve's state

Eve waits for Alice and Bob to make their measurements and reveal k and r. She then performs a measurement on her ancilla. The measurement is allowed to depend on k and r.

Lemma 5.5 *After Alice has measured $a \in \{0,1\}^d$ and Bob has measured $k \in \{0,\ldots,d-1\}$, $s \in \{0,1\}$, Eve's state is given by*

$$\sigma_{as}^{rk} = \mathrm{tr}_{\mathrm{AB}}\Big[|\Psi^{\mathrm{ABE}}\rangle\langle\Psi^{\mathrm{ABE}}|\frac{Q_a \otimes M_{ks}^{(r)} \otimes \mathbb{1}}{P_{aks|r}}\Big] \tag{29}$$

with $P_{aks|r}$ as defined in Theorem 4.2.

Proof: The POVM elements Q_a and $M_{ks}^{(r)}$ are proportional to projection operators. Hence the tripartite ABE pure state after the measurement is proportional to $(Q_a \otimes M_{ks}^{(r)} \otimes \mathbb{1})|\Psi^{\mathrm{ABE}}\rangle$. It is easily verified that the normalisation in (29) is correct: taking the trace in E-space yields $\mathrm{tr}_{\mathrm{AB}}\mathrm{tr}_{\mathrm{E}}|\Psi^{\mathrm{ABE}}\rangle\langle\Psi^{\mathrm{ABE}}|Q_a \otimes M_{ks}^{(r)} \otimes \mathbb{1} = \mathrm{tr}_{\mathrm{AB}}\, \tilde{\rho}^{\mathrm{AB}} Q_a \otimes M_{ks}^{(r)} = P_{aks|r}$. □

Lemma 5.6 *It holds that*

$$\frac{d}{2^d} \sum_{\substack{a_0\cdots a_{d-1} \\ \text{without } a_k, a_{k+r}}} |\mu_a\rangle\langle\mu_a| = \frac{1}{4}\mathbb{1} + \frac{1}{4}(-1)^{a_k + a_{k+r}}\Big(|k\rangle\langle k+r| + |k+r\rangle\langle k|\Big) \tag{30}$$

$$= M_{k,a_k \oplus a_{k+r}}^{(r)} + \frac{1}{4} \sum_{t: t\neq k, k+r} |t\rangle\langle t|. \tag{31}$$

Proof: We have $|\mu_a\rangle\langle\mu_a| = \frac{1}{d}\mathbb{1} + \frac{1}{d}\sum_{[t\tau]} |t\rangle\langle\tau|(-1)^{a_t + a_\tau}$. Summation of the $\frac{1}{d}\mathbb{1}$ term is trivial and yields $2^{d-2} \cdot \frac{1}{d}\mathbb{1}$. In the summation of the factor $(-1)^{a_t + a_\tau}$ in the second term, any summation $\sum_{a_t}(-1)^{a_t}$ yields zero. The only nonzero contribution arises when $t = k, \tau = k+r$ or $t = k+r, \tau = k$; the a-summation then yields a factor 2^{d-2}. □

Lemma 5.7 *It holds that*

$$\mathbb{E}_{a: a_k \oplus a_{k+r} = s'} |\mu_a\rangle\langle\mu_a| = \frac{\mathbb{1}}{d} + (-1)^{s'} \frac{|k\rangle\langle k+r| + |k+r\rangle\langle k|}{d}. \tag{32}$$

Proof: We have $\mathbb{E}_{a: a_k \oplus a_{k+r} = s'} |\mu_a\rangle\langle\mu_a| = 2^{-(d-1)} \sum_{a_k} \sum_{a_{k+r}} \delta_{a_k \oplus a_{k+r}, s'} \sum_{a \text{ without } a_k, a_{k+r}} |\mu_a\rangle\langle\mu_a|$. For the rightmost summation we use Lemma 5.6. Performing the $\sum_{a_k}$ and $\sum_{a_{k+r}}$ summations yields (32). □

Eve's task is to guess Alice's bit $s' = a_k \oplus a_{k+r}$ from the mixed state σ_{as}^{rk}, where Eve does not know a and s. We define

$$\sigma_{s'}^{rk} = \mathbb{E}_{s, a: a_k \oplus a_{k+r} = s'}[\sigma_{as}^{rk}]. \tag{33}$$

Eve's ability to distinguish between the cases $s' = 0$ and $s' = 1$ depends on the distance between σ_0^{rk} and σ_1^{rk} (see Section 2.2).

Theorem 5.8 *It holds that*

$$\sigma_0^{rk} - \sigma_1^{rk} = d\, \mathrm{tr}_{\mathrm{AB}} |\Psi^{\mathrm{ABE}}\rangle\langle\Psi^{\mathrm{ABE}}| \Big\{ |kk\rangle\langle k+r, k| + |k, k+r\rangle\langle k+r, k+r| + \text{h.c.} \Big\} \otimes \mathbb{1}. \tag{34}$$

Proof: We have

$$\sigma_{s'}^{rk} = \mathrm{tr}_{\mathrm{AB}} |\Psi^{\mathrm{ABE}}\rangle\langle\Psi^{\mathrm{ABE}}| \mathbb{E}_{a|s'rk} Q_a \otimes \mathbb{E}_{s|s'} \frac{M_{ks}^{(r)}}{P_{aks|r}} \otimes \mathbb{1}$$

$$= d2^d\, \mathrm{tr}_{\mathrm{AB}} |\Psi^{\mathrm{ABE}}\rangle\langle\Psi^{\mathrm{ABE}}| [\mathbb{E}_{a|s'rk} Q_a] \otimes [\sum_s M_{ks}^{(r)}] \otimes \mathbb{1}. \tag{35}$$

In the last line we used that $P_{aks|r} = \Pr[s|s']/(d2^d)$. We have $\sum_s M_{ks}^{(r)} = \frac{1}{2}|k\rangle\langle k| + \frac{1}{2}|k+r\rangle\langle k+r|$. We apply Lemma 5.7 to evaluate the expectation over a. Taking the difference between σ_0^{rk} and σ_1^{rk}, the term $\mathbb{1}/d$ in (32) vanishes. □

Theorem 5.9 *There exists a set of orthonormal states $|A\rangle, |B\rangle, |C\rangle, |D\rangle$ in Eve's Hilbert space such that $\sigma_0^{rk} - \sigma_1^{rk}$ can be written as*

$$\sigma_0^{rk} - \sigma_1^{rk} = \sqrt{d}\sqrt{\lambda_+}\sqrt{2\lambda_0 + (d-2)\lambda_1}(|A\rangle\langle C| + |C\rangle\langle A|) - d\sqrt{\lambda_-\lambda_1}(|B\rangle\langle D| + |D\rangle\langle B|). \tag{36}$$

Proof: Let $\ell_1 = \min(k, k+r \mod d)$ and $\ell_2 = \max(k, k+r \mod d)$. We introduce shorthand notation for the following (un-normalised) vectors in Eve's Hilbert space:
$|w\rangle \stackrel{\text{def}}{=} \langle kk|\Psi^{\text{ABE}}\rangle = \sqrt{\lambda_0/d}|E_0\rangle + \sqrt{\lambda_1/d}\sum_{j=1}^{d-1}(e^{i\frac{2\pi}{d}})^{jk}|E_j\rangle$,
$|x\rangle \stackrel{\text{def}}{=} \langle k+r, k+r|\Psi^{\text{ABE}}\rangle = \sqrt{\lambda_0/d}|E_0\rangle + \sqrt{\lambda_1/d}\sum_{j=1}^{d-1}(e^{i\frac{2\pi}{d}})^{j(k+r)}|E_j\rangle$,
$|y\rangle \stackrel{\text{def}}{=} \langle k, k+r|\Psi^{\text{ABE}}\rangle = \sqrt{\lambda_+/2}|E^+_{\ell_1\ell_2}\rangle + \text{sgn}([k+r \bmod d] - k)\sqrt{\lambda_-/2}|E^-_{\ell_1\ell_2}\rangle$,
$|z\rangle \stackrel{\text{def}}{=} \langle k+r, k|\Psi^{\text{ABE}}\rangle = \sqrt{\lambda_+/2}|E^+_{\ell_1\ell_2}\rangle - \text{sgn}([k+r \bmod d] - k)\sqrt{\lambda_-/2}|E^-_{\ell_1\ell_2}\rangle$.
We have the following norms and inner products,
$\langle w|y\rangle = \langle w|z\rangle = \langle x|y\rangle = \langle x|z\rangle = 0$.
$\langle w|w\rangle = \langle x|x\rangle = \frac{\lambda_0}{d} + (d-1)\frac{\lambda_1}{d}$.
$\langle y|y\rangle = \langle z|z\rangle = (\lambda_+ + \lambda_-)/2$.
$\langle w|x\rangle = \frac{\lambda_0}{d} + \frac{\lambda_1}{d}\sum_{j=1}^{d-1}(e^{i2\pi/d})^{jr} = (\lambda_0 - \lambda_1)/d$.
$\langle y|z\rangle = (\lambda_+ - \lambda_-)/2$.
We define $\cos 2\alpha = \frac{\langle w|x\rangle}{\langle w|w\rangle} = 1 - \frac{d\lambda_1}{\lambda_0+(d-1)\lambda_1}$ and $\cos 2\varphi = \frac{\langle y|z\rangle}{\langle y|y\rangle} = 1 - \frac{2\lambda_-}{\lambda_+ + \lambda_-}$.
From (34) it follows that

$$\frac{\sigma_0^{rk} - \sigma_1^{rk}}{d} = |z\rangle\langle w| + |w\rangle\langle z| + |x\rangle\langle y| + |y\rangle\langle x|. \tag{37}$$

We write

$$|w\rangle = \sqrt{\langle w|w\rangle}\big(\cos\alpha|A\rangle + \sin\alpha|B\rangle\big) \quad ; \quad |x\rangle = \sqrt{\langle w|w\rangle}\big(\cos\alpha|A\rangle - \sin\alpha|B\rangle\big) \tag{38}$$

$$|y\rangle = \sqrt{\langle y|y\rangle}\big(\cos\varphi|C\rangle + \sin\varphi|D\rangle\big) \quad ; \quad |z\rangle = \sqrt{\langle y|y\rangle}\big(\cos\varphi|C\rangle - \sin\varphi|D\rangle\big) \tag{39}$$

where $|A\rangle, |B\rangle, |C\rangle, |D\rangle$ are orthonormal. Substitution into (37) and using
$\cos x = \sqrt{\frac{1}{2} + \frac{1}{2}\cos(2x)}$ and $\sin x = \sqrt{\frac{1}{2} - \frac{1}{2}\cos(2x)}$ yields (36). □
Theorem 5.9 directly allows us to compute the leakage.

6 Min-entropy

When the number of qudits (n) is small, the relevant quantity to determine how much Eve can learn about the established key is the min-entropy leakage. At very large n the Shannon-entropy leakage (mutual information) is the relevant quantity. The min-entropy leakage is always greater or equal to the Shannon-entropy leakage.
In Sections 4 and 5 we have fixed everything except Eve's attack parameters μ, V. We will now compute the min-entropy leakage as a function of μ, V using (6) and then optimise the parameters so as to maximise the leakage. Eq. (6) with $p_0 = \frac{1}{2}$, $p_1 = \frac{1}{2}$ tells us that the relevant quantity is $\|\sigma_0^{rk} - \sigma_1^{rk}\|_1$. For notational convenience we define the value β_{sat},

$$\beta_{\text{sat}} \stackrel{\text{def}}{=} \frac{1}{4}\cdot\frac{d-2}{d-1}. \tag{40}$$

Lemma 6.1 *For all r and k, the choice for μ and V that maximizes the trace distance $\frac{1}{2}\left\|\sigma_0^{rk} - \sigma_1^{rk}\right\|_1$ is*

$$\beta < \beta_{\text{sat}}: \qquad \mu = -\tfrac{4}{d-2}\beta \qquad V = \frac{2}{d-2}\beta \tag{41}$$

$$\beta \geq \beta_{\text{sat}}: \qquad \mu = 2\beta - \tfrac{d}{2(d-1)} \qquad V = \frac{1-2\beta}{d} \tag{42}$$

which gives

$$\frac{1}{2}\left\|\sigma_0^{rk}-\sigma_1^{rk}\right\|_1 = \begin{cases} \frac{1}{\sqrt{d-1}}\frac{\sqrt{\beta}}{\beta_{\rm sat}}\sqrt{2\beta_{\rm sat}-\beta} & \textit{for} \quad \beta<\beta_{\rm sat} \\ \frac{1}{\sqrt{d-1}} & \textit{for} \quad \beta\geq\beta_{\rm sat}. \end{cases} \tag{43}$$

<u>*Proof:*</u> From Theorem 5.9 it is easy to see that

$$\frac{1}{2}\left\|\sigma_0^{rk}-\sigma_1^{rk}\right\|_1 = d\sqrt{\lambda_-\lambda_1}+\sqrt{d}\sqrt{\lambda_+}\sqrt{2\lambda_0+(d-2)\lambda_1}. \tag{44}$$

Using the normalisation constraint $\lambda_0+(d-1)\lambda_1+\frac{d(d-1)}{2}(\lambda_++\lambda_-)=1$ and rewriting λ_1 as $\lambda_1=\lambda_++\frac{2\beta}{d}-\frac{d(\lambda_++\lambda_-)}{2}$ using the definitions in Lemma 5.1, we can rewrite the trace distance in terms of λ_+ and λ_-:

$$\frac{1}{2}\left\|\sigma_0^{rk}-\sigma_1^{rk}\right\|_1 = \sqrt{d\lambda_-}\sqrt{d\lambda_++2\beta-\frac{d^2}{2}(\lambda_++\lambda_-)}+\sqrt{d\lambda_+}\sqrt{d\lambda_-+2(1-\beta)-\frac{d^2}{2}(\lambda_++\lambda_-)}. \tag{45}$$

In the Appendix we derive the λ_+, λ_- that maximize (45) while keeping all eigenvalues non-negative,

$$\lambda_+ = \frac{4\beta}{d(d-2)} \qquad \lambda_-=0 \qquad \text{for } \beta<\beta_{\rm sat} \tag{46}$$

$$\lambda_+ = \frac{4\beta_{\rm sat}}{d(d-2)}-\frac{2(\beta-\beta_{\rm sat})}{d^2} \qquad \lambda_-=\frac{2(\beta-\beta_{\rm sat})}{d^2} \qquad \text{for } \beta\geq\beta_{\rm sat}. \tag{47}$$

The corresponding values for μ and V are given in (41,42). □

Fig. 1 shows the optimal λ_+ and λ_- together with the constraints on the λ parameters. The lower dot in the figure corresponds to $\beta=\frac{1}{2}$. As β decreases the optimum moves towards the top corner of the triangle. At $\beta\leq\beta_{\rm sat}$ the optimum is the top corner, with $\lambda_-=0$ and $\lambda_1=0$.

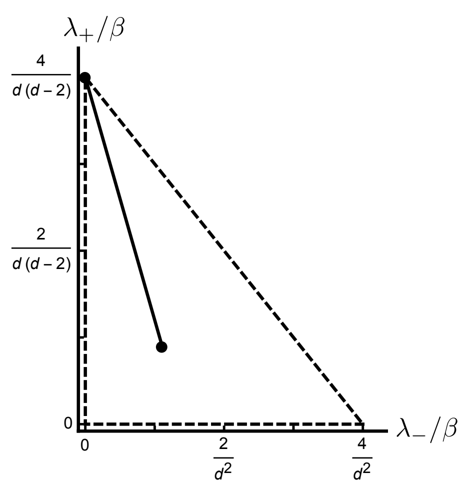

Figure 1: *Optimal choice of λ_+ and λ_-. The dashed triangle represents the region for which the eigenvalues λ_+,λ_- and λ_1 are non-negative. Black points indicate the choices at $\beta=\frac{1}{2}$ (lower point) and $\beta\leq\beta_{\rm sat}$ (higher point). Not shown in this plot is the $\lambda_0\geq 0$ constraint which cuts off the upper left corner of the triangle for $\beta>2\beta_{\rm sat}$.*

Knowing the optimal values for μ and V, we finally compute the leakage.

Theorem 6.2 *The min-entropy of the bit S' given R,K and the state $\sigma_{S'}^{RK}$ is*

$$\beta<\beta_{\rm sat}: \qquad \mathsf{H}_{\rm min}(S'|RK\sigma_{S'}^{RK}) = -\log\left(\frac{1}{2}+\frac{1}{2\sqrt{d-1}}\frac{\sqrt{\beta}}{\beta_{\rm sat}}\sqrt{2\beta_{\rm sat}-\beta}\right). \tag{48}$$

$$\beta\geq\beta_{\rm sat}: \qquad \mathsf{H}_{\rm min}(S'|RK\sigma_{S'}^{RK}) = -\log\left(\frac{1}{2}+\frac{1}{2\sqrt{d-1}}\right). \tag{49}$$

Proof: Eq. (6) with X uniform, $X \to S'$, $Y \to (R,K)$ becomes

$$\begin{aligned} \mathsf{H}_{\min}(S'|RK\sigma_{s'}^{RK}) &= -\log\left(\frac{1}{2}+\frac{1}{2}\mathbb{E}_{rk}\left\|\frac{1}{2}\sigma_0^{rk}-\frac{1}{2}\sigma_1^{rk}\right\|_1\right) \\ &= -\log\left(\frac{1}{2}+\frac{1}{4}\left\|\sigma_0^{rk}-\sigma_1^{rk}\right\|_1\right) \qquad (r,k \text{ arbitrary}). \end{aligned} \tag{50}$$

In the last step we omitted the expectation over r and k since the trace distance does not depend on r,k. Substitution of (43) into (50) gives the end result. □

Corollary 6.3 *Eve's optimal POVM $\mathcal{T}^{rk} = (T_0^{rk}, T_1^{rk})$ for maximising the min-entropy leakage is given by*

$$T_0^{rk} = \frac{1}{2}\Big(\mathbb{1} + |A\rangle\langle C| + |C\rangle\langle A| - |B\rangle\langle D| - |D\rangle\langle B|\Big) \quad ; \quad T_1^{rk} = \mathbb{1} - T_0^{rk}. \tag{51}$$

Proof: The trace distance in Lemma 6.1 is the sum of the positive eigenvalues of $\sigma_0^{rk} - \sigma_1^{rk}$. In the space spanned by $|A\rangle, |B\rangle, |C\rangle, |D\rangle$, the optimal T_0 consists of the projection onto the space spanned by the eigenvectors corresponding to the positive eigenvalues. These eigenvectors are $|v_1\rangle = \frac{|A\rangle+|C\rangle}{\sqrt{2}}$ and $|v_2\rangle = \frac{|D\rangle-|B\rangle}{\sqrt{2}}$. The matrix that projects onto them is $|v_1\rangle\langle v_1| + |v_2\rangle\langle v_2| = \frac{1}{2}|A\rangle\langle A| + \frac{1}{2}|B\rangle\langle B| + \frac{1}{2}|C\rangle\langle C| + \frac{1}{2}|D\rangle\langle D| + |A\rangle\langle C| + |C\rangle\langle A| - |B\rangle\langle D| - |D\rangle\langle B|$. In order to satisfy the constraint $T_0 + T_1 = \mathbb{1}$ and symmetry, half the identity matrix in the remaining $d^2 - 4$ dimensions has to be added to T_0. We mention, without showing it, that (51) satisfies the test (4). □

As expected, the min-entropy loss decreases as the dimension of the Hilbert space grows. We see that the entropy loss saturates at $\beta = \beta_{\text{sat}}$; hence RRDPS is secure up to arbitrarily high noise levels. Fig. 2 shows the min-entropy leakage as a function of β.

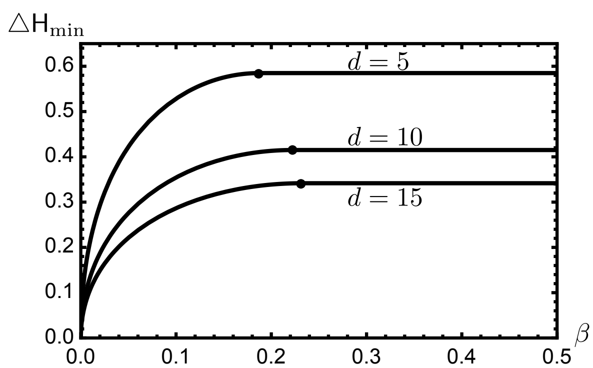

Figure 2: *Min-entropy leakage as a function of the bit error rate for $d = 5$, $d = 10$ and $d = 15$. A dot indicates the saturation point β_{sat}.*

7 Shannon Entropy

When the number of qudits (n) is very large, not the min-entropy but the Shannon-entropy is the relevant quantity to consider. We wish to determine the Shannon-entropy of $S' = A_K \oplus A_{K+R}$ given R,K and the quantum state σ_{AS}^{RK} (but for unknown A and S).

Lemma 7.1 *Let $X \in \mathcal{X}$ be a uniformly distributed random variable. Let $Y \in \mathcal{Y}$ be a random variable. Let ρ_{xy} be a quantum state coupled to the classical x, y. The Shannon entropy of X given ρ_{XY} (for unknown X and Y) is given by*

$$\mathsf{H}(X|\rho_{XY}) = \min_{POVM\ \mathcal{M}=(M_m)_{m\in\mathcal{X}}} \mathbb{E}_{x\in\mathcal{X}} \mathsf{H}(\{\operatorname{tr} M_m \mathbb{E}_{y|x}\rho_{xy}\}_{m\in\mathcal{X}}). \tag{52}$$

Proof: We have $\mathsf{H}(X|\rho_{XY}) = \min_{\mathcal{M}} \mathsf{H}(X|Z)$, where Z is the outcome of the POVM measurement $\mathcal{M}$. Z is a classical random variable that depends on X and Y. We can write $\mathsf{H}(X|Z) = \mathsf{H}(X) - \mathsf{H}(Z) + \mathsf{H}(Z|X)$. Since X is uniform, and Z is an estimator for X, the Z is uniform as well. Thus we have $\mathsf{H}(X) - \mathsf{H}(Z) = 0$, which yields $\mathsf{H}(X|\rho_{XY}) = \min_{\mathcal{M}} \mathsf{H}(Z|X) = \min_{\mathcal{M}} \mathbb{E}_x \mathsf{H}(Z|X = x)$. The probability $\Pr[z|x]$ is given by $\Pr[z|x] = \mathbb{E}_{y|x} \Pr[z|xy] = \mathbb{E}_{y|x} \mathrm{tr}\, M_z \rho_{xy}$. □

Corollary 7.2

$$\mathsf{H}(S'|RK\sigma_{AS}^{RK}) = \mathbb{E}_{rk} \min_{\mathcal{G}^{rk}=(G_0^{rk},G_1^{rk})} \mathbb{E}_{s'} h(\mathrm{tr}\, G_m^{rk}\sigma_{s'}^{rk}) \qquad \textit{with } m \in \{0,1\} \textit{ arbitrary.} \tag{53}$$

Proof: Application of Lemma 7.1 yields

$$\begin{aligned} \mathsf{H}(S'|RK\sigma_{AS}^{RK}) &= \mathbb{E}_{rk} \min_{\mathcal{G}^{rk}=(G_0^{rk},G_1^{rk})} \mathbb{E}_{s'} H(\{\mathrm{tr}\, G_m^{rk} \mathbb{E}_{as|s'} \sigma_{as}^{rk}\}_{m\in\{0,1\}}) \\ &= \mathbb{E}_{rk} \min_{\mathcal{G}^{rk}=(G_0^{rk},G_1^{rk})} \mathbb{E}_{s'} H(\{\mathrm{tr}\, G_m^{rk} \sigma_{s'}^{rk}\}_{m\in\{0,1\}}) \end{aligned} \tag{54}$$

where in the last step we used the definition of $\sigma_{s'}^{rk}$. Finally, the Shannon entropy of a binary variable is given by the binary entropy function h, where $h(1-p) = h(p)$. □
From Corollary 7.2 we see that the POVM $\mathcal{T}^{rk}$ associated with the min-entropy also optimizes the Shannon entropy: maximising the guessing probability $\mathrm{tr}\, G_{s'}^{rk}\sigma_{s'}^{rk}$ also minimises the Shannon entropy.

Theorem 7.3 *The Shannon entropy of the bit S' given the state σ_{AS}^{RK}, R and K is:*

$$\beta < \beta_{\rm sat}: \qquad \mathsf{H}(S'|RK\sigma_{AS}^{RK}) = h\left(\frac{1}{2} + \frac{1}{2\sqrt{d-1}} \frac{\sqrt{\beta}}{\beta_{\rm sat}} \sqrt{2\beta_{\rm sat} - \beta}\right). \tag{55}$$

$$\beta \geq \beta_{\rm sat}: \qquad \mathsf{H}(S'|RK\sigma_{AS}^{RK}) = h\left(\frac{1}{2} + \frac{1}{2\sqrt{d-1}}\right). \tag{56}$$

Proof: The min-entropy result (48,49) can be written as $\mathsf{H}_{\rm min}(S'|RK\sigma_{S'}^{RK}) = -\log \mathrm{tr}\, T_{s'}^{rk}\sigma_{s'}^{rk}$, so we already have an expression for $\mathrm{tr}\, T_{s'}^{rk}\sigma_{s'}^{rk}$. Substitution of $\mathcal{T}^{rk}$ for $\mathcal{G}^{rk}$ in (53) yields the result. □
Since the optimal POVM for min- and Shannon entropy are the same, saturation occurs at the same point ($\beta = \beta_{\rm sat}$). Fig 3 shows the Shannon entropy leakage (mutual information) $I_{\rm AE} = 1 - \mathsf{H}(S'|RK\sigma_{AS}^{RK})$ as a function of β.

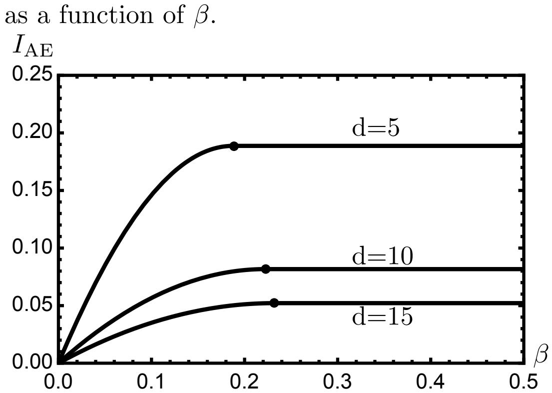

Figure 3: *Shannon entropy leakage as a function of β for $d = 5$, $d = 10$ and $d = 15$. A dot indicates the saturation point $\beta_{\rm sat}$.*

8 Discussion

8.1 Comparison with previous analyses

Figs. 4 and 5 illustrate the gap between our results and previous bounds on the leakage. It is clear that RRDPS performs much better than previously thought. Note too that the saturation point

$\beta_{\rm sat} = \frac{1}{4} \cdot \frac{d-2}{d-1}$ occurs at half the value given in (2) [17]. At $\beta \geq 0.25 - \mathcal{O}(\frac{1}{d})$ there is no reason to monitor the channel, other than to determine which error-correcting code should be used.

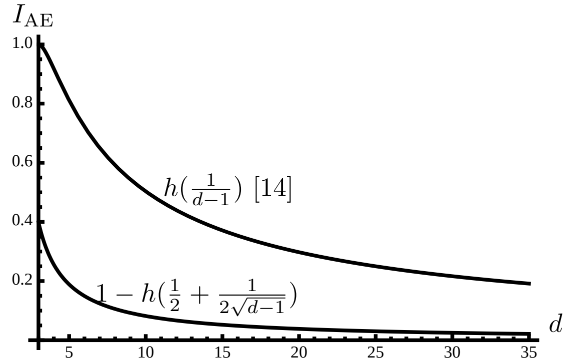

Figure 4: *Saturated Shannon leakage as a function of d. Comparison of [14] and our result (Theorem 7.3).*

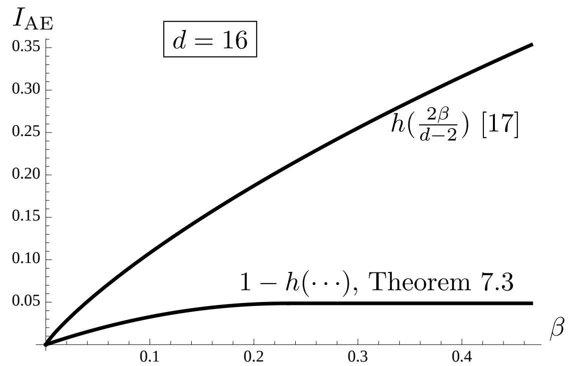

Figure 5: *Shannon leakage as a function of β, for $d = 16$. Comparison of [17] and our result (Theorem 7.3).*

8.2 Remarks

We find the symmetry argument in [14] difficult to understand. Our analysis, in contrast, follows the well established steps of purification of the noisy Alice-Bob EPR state, followed by an optimal POVM performed by Eve.
The $\tilde{\rho}^{\rm AB}$ mixed state allowed by the noise constraint has two degrees of freedom, μ and V. While this is more than the zero degrees of freedom in the case of qubit-based QKD [12], it is still a small number, given the dimension d^2 of the Hilbert space.
Eve's attack has an interesting structure. Eve entangles her ancilla with Bob's qudit. Bob's measurement affects Eve's state. When Bob reveals r, k, Eve knows which 4-dimensional subspace is relevant. However, the basis state $|k\rangle$ in Bob's qudit is coupled to $|A_k^a\rangle$ in Eve's space, which is spanned by $d-1$ different basis vectors $|E^+_{(kt')}\rangle$ (Eq. 26 with $\lambda_1 = 0$, $\lambda_- = 0$), each carrying different phase information $a_k \oplus a_{t'}$. Only one out of $d-1$ carries the information she needs, and she cannot select which one to read out. Her problem is aggravated by the fact that the $|A_t^a\rangle$ vectors are not orthogonal (except at $\beta = \frac{1}{2}$). Note that this entanglement-based attack is far more powerful than the intercept-resend attack studied in [18].

Acknowledgements

We thank Serge Fehr for useful discussions. Part of this research was funded by NWO (CHIST-ERA project ID_IOT).

Appendix: Optimization

Here we prove that (46,47) maximizes (45). We first show that (45) is concave and obtain the optimum for $\beta \geq \beta_{\rm sat}$. Then we take into account the constraints on the eigenvalues and derive the optimum for $\beta < \beta_{\rm sat}$.

Unconstrained optimization

For notational convenience we define

$$w_1 = \sqrt{d\lambda_+ + 2\beta - \frac{d^2}{2}(\lambda_+ + \lambda_-)}, \quad w_2 = \sqrt{d\lambda_- + 2(1-\beta) - \frac{d^2}{2}(\lambda_+ + \lambda_-)}. \tag{57}$$

This allows us to formulate everything in terms of λ_+ and λ_-. Eq. (45) becomes

$$\frac{1}{2}\left\|\sigma_0^{rk} - \sigma_1^{rk}\right\|_1 = \sqrt{d\lambda_-}w_1 + \sqrt{d\lambda_+}w_2. \tag{58}$$

Next we compute the derivatives,

$$\frac{\partial}{\partial\lambda_+}\left\|\sigma_0^{rk} - \sigma_1^{rk}\right\|_1 = -\frac{d^2}{2}\frac{\sqrt{\lambda_+}}{w_2} + \frac{w_2}{\sqrt{\lambda_+}} + (d - \frac{d^2}{2})\frac{\sqrt{\lambda_-}}{w_1} \tag{59}$$

$$\frac{\partial}{\partial\lambda_-}\left\|\sigma_0^{rk} - \sigma_1^{rk}\right\|_1 = -\frac{d^2}{2}\frac{\sqrt{\lambda_-}}{w_1} + \frac{w_1}{\sqrt{\lambda_-}} + (d - \frac{d^2}{2})\frac{\sqrt{\lambda_+}}{w_2}. \tag{60}$$

Setting both these derivatives to zero yields a stationary point of the function. Setting $w_1\sqrt{\lambda_+}\frac{\partial}{\partial\lambda_+}\left\|\sigma_0^{rk} - \sigma_1^{rk}\right\|_1 - w_2\sqrt{\lambda_-}\frac{\partial}{\partial\lambda_-}\left\|\sigma_0^{rk} - \sigma_1^{rk}\right\|_1$ to zero gives $\lambda_+ w_1^2 - \lambda_- w_2^2 = 0$, which describes a hyperbola

$$(\tfrac{1}{2}d^2 - d)(\lambda_-^2 - \lambda_+^2) + 2\beta\lambda_+ - 2(1-\beta)\lambda_- = 0. \tag{61}$$

Next, the equations $\sqrt{\lambda_+}w_1 w_2\frac{\partial}{\partial\lambda_+}\left\|\sigma_0^{rk} - \sigma_1^{rk}\right\|_1 = 0$ and $\sqrt{\lambda_-}w_1 w_2\frac{\partial}{\partial\lambda_-}\left\|\sigma_0^{rk} - \sigma_1^{rk}\right\|_1 = 0$ can both easily be written in the form $\frac{w_2}{w_1} = \textit{expression}$. Equating these two expressions gives us another hyperbola,

$$\left(d^2\lambda_+ + \frac{d^2}{2}\lambda_- - d\lambda_- - 2(1-\beta)\right)\left(d^2\lambda_- + \frac{d^2}{2}\lambda_+ - d\lambda_+ - 2\beta\right) - \lambda_-\lambda_+(d - \frac{d^2}{2}) = 0. \tag{62}$$

The stationary point lies at the crossing of these two hyperbolas. There are four crossing points,

$$\lambda_+ = 0 \quad ; \quad \lambda_- = \frac{4(1-\beta)}{d(d-2)} \tag{63}$$

$$\lambda_+ = \frac{4\beta}{d(d-2)} \quad ; \quad \lambda_- = 0 \tag{64}$$

$$\lambda_+ = \frac{1}{2d(d-1)} + \frac{1-2\beta}{d^2} \quad ; \quad \lambda_- = \frac{1}{2d(d-1)} - \frac{1-2\beta}{d^2} \tag{65}$$

$$\lambda_+ = \frac{2 + d(1-2\beta)}{2d^2} \quad ; \quad \lambda_- = \frac{2 - d(1-2\beta)}{2d^2}. \tag{66}$$

In the steps above, we have multiplied our derivatives by λ_+, λ_-, w_1 and w_2; this has introduced spurious zeros that now need to be removed. From (59,60) it is easily seen that $\lambda_+ = 0$ and $\lambda_- = 0$ are never stationary points since the derivatives diverge near these values. Furthermore, we find that substitution of (66) into the derivatives does not yield two zeros. Expression (65) is the only stationary point. As the function value lies higher there than in other points, we conclude that $\left\|\sigma_0^{rk} - \sigma_1^{rk}\right\|_1$ is concave.

Constrained optimization

The optimization problem is constrained by the fact that the λ eigenvalues are non-negative. For $\beta \geq \beta_{\rm sat}$ the stationary point satisfies the constraints and hence is the optimal choice for $\beta \geq \beta_{\rm sat}$. For $\beta < \beta_{\rm sat}$ the stationary point has $\lambda_- < 0$, i.e. it lies outside the allowed region. Because of the concavity the highest function value which satisfies the constraints occurs at $\lambda_0 = 0$, $\lambda_1 = 0$, $\lambda_+ = 0$ or $\lambda_- = 0$. It is easily seen that $\lambda_0 \geq 0$ implies $\lambda_+ \leq \frac{1}{d-1} - \frac{2\beta}{d}$ and $\lambda_1 \geq 0$ implies $\lambda_+ \leq \frac{4\beta}{d(d-2)} - \frac{d}{d-2}\lambda_-$ and $\lambda_- \leq \frac{4\beta}{d^2} - \frac{d-2}{d}\lambda_+$. In the range $\beta < \beta_{\rm sat}$ it holds that $\frac{4\beta}{d(d-2)} > \frac{1}{d-1} - \frac{2\beta}{d}$; hence the λ_0-constraint is irrelevant in this region. We get $\lambda_1 = 0$ when $\lambda_+ = \frac{4\beta}{d(d-2)} - \frac{d}{d-2}\lambda_-$. Substitution gives $\frac{1}{2}\left|\left|\sigma_0^{rk} - \sigma_1^{rk}\right|\right|_1 = \frac{\sqrt{2}}{d-2}\sqrt{2(1-\beta) + d(1-2\beta + d\,(1-2\beta(d-1)\lambda_-))\,(d^2\lambda_- - 4\beta)}$ which has its maximum at $\lambda_- = 0$ for non-negative values of λ_-. So either $\lambda_- = 0$ or $\lambda_+ = 0$. This leaves two options for the maximum at low β,

$$\lambda_+ = 0 \quad ; \quad \lambda_- = \frac{4\beta}{d^2} \quad \Rightarrow \quad \frac{1}{2}\left\|\sigma_0^{rk} - \sigma_1^{rk}\right\|_1 = 0. \tag{67}$$

$$\lambda_- = 0 \quad ; \quad \lambda_+ = \frac{4\beta}{d(d-2)} \quad \Rightarrow \quad \frac{1}{2}\left\|\sigma_0^{rk} - \sigma_1^{rk}\right\|_1 = 2\sqrt{2}\frac{\sqrt{\beta(d-2) - 2\beta^2(d-1)}}{d-2}. \tag{68}$$

Clearly (68) is the larger of the two and therefore the optimal choice. □

References

[1] W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[2] A. Broadbent and C. Schaffner. Quantum cryptography beyond quantum key distribution. *Des. Codes Cryptogr.*, 78:351–382, 2016.

[3] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[4] A.K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661 – 663, 1991.

[5] C.H. Bennett. Quantum cryptography using any two nonorthogonal states. *Pys. Rev. Lett.*, 68(21):3121–3124, 1992.

[6] T.C. Ralph. Continuous variable quantum cryptography. *Phys. Rev. A*, 61:010303, 1999.

[7] M. Hillery. Quantum cryptography with squeezed states. *Phys. Rev. A*, 61:022309, 2000.

[8] D. Gottesman and J. Preskill. Secure quantum key distribution using squeezed states. *Phys. Rev. A*, 63:022309, 2001.

[9] K. Inoue, E. Waks, and Y. Yamamoto. Differential phase shift quantum key distribution. *Phys. Rev. Lett.*, 89(3):037902,1–3, 2002.

[10] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81(14):3018–3021, 1998.

[11] P. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys.Rev.Lett.*, 85:441, 2000.

[12] R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys.Rev.A*, 72:012332, 2005.

[13] B. Kraus, N. Gisin, and R. Renner. Lower and upper bounds on the secret key rate for quantum key distribution protocols using one-way classical communication. *Phys.Rev.Lett.*, 95:080501, 2005.

[14] T. Sasaki, Y. Yamamoto, and M. Koashi. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature*, 509:475–478, May 2014.

[15] Hoi-Kwong Lo. Efficient quantum key distribution scheme and a proof of its unconditional security. *Journal of Cryptology*, 2005.

[16] Z. Zhang, X. Yuan, Z. Cao, and X. Ma. Round-robin differential-phase-shift quantum key distribution. `http://arxiv.org/abs/1505.02481v1`, 2015.

[17] T. Sasaki and M. Koashi. A security proof of the round-robin differential phase shift quantum key distribution protocol based on the signal disturbance. `https://arxiv.org/abs/1701.08509`, 2017.

[18] B. Škorić. A short note on the security of Round-Robin Differential Phase-Shift QKD, 2017.

[19] R. Renner. Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, 3:645–649, 2007.

[20] R. König, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Trans.Inf.Th.*, 55(9):4337–4347, 2009.

[21] A.S. Holevo. Statistical decision theory for quantum systems. *Journal of multivariate analysis*, 3:337–394, 1973.