Noname manuscript No.
(will be inserted by the editor)

Analysis of a High-Dimensional Extended B92 Protocol

Hasan Iqbal* · Walter O. Krawec

Received: date / Accepted: date

Abstract Quantum key distribution (QKD) allows two parties to establish a shared secret key that is secure against all-powerful adversaries. One such protocol named B92 is quite appealing due to its simplicity but is highly sensitive to channel noise. In this work, we investigate a high-dimensional variant of an extended version of the B92 protocol and show that it can distill a key over high noise channels. The protocol we consider requires that Alice send only three high-dimensional states and Bob only perform partial measurements. We perform an information-theoretic security analysis of our protocol and compare its key rate to that of a high-dimensional BB84 protocol over depolarization and amplitude damping channels.

Keywords Quantum Key Distribution · Quantum Information

1 Introduction

The need for perfect security necessitated the development of cryptographic systems where there are no computational constraints on the capabilities of the adversary. Quantum key distribution (QKD) is one such system that is extensively studied and is increasingly maturing to the point of real-world adoption. In QKD, using quantum mechanical properties of communication resources, two parties Alice (A) and Bob (B), following a specified set of steps, generate a shared secret that is secure from an all-powerful adversary Eve (E).

Since the first QKD protocol by Bennett and Brassard in 1984 (BB84) [1], there have been numerous advances in both theoretical and practical aspects [2–4]. However, because generating, maintaining, and manipulating quantum

* Email: `hasan.iqbal@uconn.edu`

Department of Computer Science and Engineering
University of Connecticut
Storrs, CT 06269 USA

resources are exceptionally hard with current technologies, people have strived to create conceptually simpler protocols that also require less quantum resources. For instance, BB84 itself uses four quantum states and two measurement bases. In 1992, Bennett proposed an even simpler QKD protocol called B92, that uses only two non-orthogonal states and measurement bases [5].

The unconditional security of this protocol has been investigated by several authors [6, 7] with continually improving results (for instance, in [7], a noise tolerance of 6.5% is reported). However, B92 is very noise sensitive compared to other protocols like BB84 as was already noted in the original paper [5]. Lucamarini et al. [8], proposed an extended version of B92 (Ext-B92) which added two additional non-informative states to better bound Eve's information gain. Depending on the user-defined choice for key encoding states, the noise tolerance of that protocol can approach 11% in the asymptotic scenario [8], similar to BB84, and at least 7% in the finite key scenario [9].

These protocols mentioned above use qubits (dimension two systems) as the communication resource between Alice and Bob. However, higher dimensional quantum systems (see [10] for a brief survey) have been shown to have several advantages and interesting properties over qubit-based protocols. Some protocols have been shown to withstand a high channel noise level as the dimension of the system increases [11–14]. Others exhibit interesting theoretical properties such as the so-called "Round Robin" protocol which can bound Eve's information based only on the dimension of the system and not necessarily through observing channel noise [15]. In addition to several theoretical results that prove the unconditional security of HD-QKD protocols, the actual technology to implement high-dimensional systems is also becoming more mature with recent high-dimensional protocols proving to be feasible to implement [16–20]. Thus, it is worth studying protocols that are highly susceptible to noise, like B92 based variants (in our case the extended B92), to see if HD-systems give an advantage.

In this work, we propose a high-dimensional variant of the Ext-B92 protocol of [8]. Keeping in mind that certain high-dimensional states are difficult to create or distinguish, we make sure in our protocol to limit the required state preparations and measurement operations required. In particular, Alice need only be able to send three high dimensional states while Bob need only be able to perform a computational basis measurement (distinguishing any computational state $\{|0\rangle, |1\rangle, \cdots, |D-1\rangle\}$) or be able to perform a partial basis measurement in an alternative basis - this partial measurement need only distinguish a particular superposition state defined in the protocol and need not be capable of distinguishing all D possible states. As far as we are aware, this is a novel high-dimensional QKD protocol.

Despite these limitations on Alice and Bob's capabilities, we show that these higher dimensional states do help improve noise tolerance in this protocol as the dimension of the system increases which agrees with recent research on high-dimensional BB84. We perform an information-theoretic security analysis and show that it can maintain a positive key rate while withstanding noise levels of 5.35% for qubits (dimension 2) to 15.5% for dimension 2^{14} in a depolarizing channel. Thus, we show that higher dimensions can aid in depolarization noise tolerance for a B92 style encoding scheme with (partial) extended test cases in the form of a third basis state being transmitted for testing the channel. Moreover, we consider an amplitude damping channel and show that choosing the distinguished superposition state carefully in a high-dimensional QKD protocol is of significant importance as different choices lead to different noise tolerances.

We make several contributions in this work. First, we describe and analyze a high-dimensional version of the Ext-B92 protocol originally introduced for qubits [8]. We perform an information theoretic security analysis against collective attacks (a powerful class of attacks against QKD protocols) to derive its key rate in the asymptotic scenario for arbitrary dimensions and channel parameters. Our methods here may have a broader impact in other QKD protocol security analyses, especially for high-dimensional systems with only partial basis measurements or state preparations as with our protocol here. Finally, we evaluate our resulting key rate and compare it with a high-dimensional version of the BB84 protocol, showing how the choice of states to send can greatly affect the key rate depending on the channel.

2 Notation

For a quantum system A we will use ρ_A to denote its density operator. Its von Neumann entropy will be denoted by $S(A) = S(\rho_A)$ and is defined by $-\operatorname{tr}(\rho_A \log \rho_A)$. Given a bipartite quantum state ρ_{AE} shared by two systems A and E, we will denote the conditional von Neumann entropy of A given access to E, by $S(A|E)_\rho$. We will often forgo writing the subscript ρ when the context is clear. This conditional entropy is defined as $S(AE) - S(E)$. The Shannon entropy of A will be denoted by $H(A)$ and the conditional Shannon entropy of two systems A and B, will be denoted by $H(A|B)$. The binary entropy function will also be represented by $H(p)$ where $H(p) = -p\log(p) - (1-p)\log(1-p)$ for $p \in [0,1]$. All logarithms presented in this work are base 2. For an arbitrary quantum state $|\psi\rangle$, we use $P(|\psi\rangle)$ to denote its projector $|\psi\rangle\langle\psi|$. Finally, given a vector $|x\rangle$ and a numerical value such as $\frac{1}{2}$ we sometimes write $\left|\frac{1}{2}x\right\rangle$ to mean $\frac{1}{2}|x\rangle$.

Later, to compute the lower bound of the conditional von Neumann entropy of a classical-quantum state ρ_{AE}, we make use of the following theorem:

Theorem 1 *(From [21]): Let $\mathcal{H}_A \otimes \mathcal{H}_E$ be a finite dimensional Hilbert space. Consider the following density operator.*

$$\rho_{AE} = \frac{1}{N}\left(|0\rangle\langle 0|_A \otimes \sum_{i=1}^{\tau} \left|e_i^0\right\rangle\left\langle e_i^0\right| + |1\rangle\langle 1|_A \otimes \sum_{i=1}^{\tau} \left|e_i^1\right\rangle\left\langle e_i^1\right| \right),$$

where $N > 0$ is a normalization term, $\tau < \infty$, and each $\left|e_i^j\right\rangle \in \mathcal{H}_E$ (these are not necessarily normalized, nor orthogonal, states; also it might be that

$\left|e_i^j\right\rangle \equiv 0$ *for some* i *and* j*). Let* $n_i^j = \left\langle e_i^j \middle| e_i^j \right\rangle \geq 0$*. Then:*

$$S(A|E)_\rho \geq \sum_{i=1}^{\tau} \left(\frac{n_i^0 + n_i^1}{N}\right) \cdot S_i,$$

where:

$$S_i = \begin{cases} h\left(\frac{n_i^0}{n_i^0+n_i^1}\right) - h(\lambda_i) & \textit{if } n_i^0 > 0 \textit{ and } n_i^1 > 0, \\ 0 & \textit{otherwise.} \end{cases}$$

and:

$$\lambda_i = \frac{1}{2} + \frac{\sqrt{(n_i^0 - n_i^1)^2 + 4\,\mathrm{Re}^2 \left\langle e_i^0 | e_i^1 \right\rangle}}{2(n_i^0 + n_i^1)}.$$

As an interesting observation, we can see that the bound in Theorem 1 is non-negative. While not proven in [21], this is easy to show. In particular, we show that each S_i term is non-negative. First assume $n_i^0 \geq n_i^1$ (the other case is similar). Then $n_i^0 - n_i^1 \leq \sqrt{(n_i^0 - n_i^1)^2 + 4x}$, where $x = \mathrm{Re}^2 \left\langle e_i^0 | e_i^1 \right\rangle$ is a non-negative value. This of course implies that $2n_i^0 \leq n_i^0 + n_i^1 + \sqrt{(n_i^0 - n_i^1)^2 + 4x}$ which further implies that $\frac{n_i^0}{n_i^0+n_i^1} \leq \lambda_i$. Since $n_i^0 \geq n_i^1$, we have $\frac{n_i^0}{n_i^0+n_i^1} \geq \frac{1}{2}$. Thus, it holds that each $S_i \geq 0$ since the entropy function is a decreasing function on the interval $[1/2, 1]$. The case when $n_i^0 < n_i^1$ is similar.

3 The Protocol

The protocol we propose here is a high-dimensional variant of the Ext-B92 protocol originally described in [8]. In that protocol, two non-orthogonal states, similar to B92, are used for key encoding while two additional states are used for quantum tomography (these four states together come from two distinct bases). In the higher dimensional case we analyze here, we will use two non-orthogonal states for key encoding; for error testing, we adopt a simplification from [9] (done there for the qubit case) and not require users to be able to control two complete bases. More specifically, in our high-dimensional extended B92, Alice sends $|i\rangle$ and $|\phi\rangle = \frac{1}{\sqrt{2}}(|i\rangle + |j\rangle)$ to encode classical key bits of 0 and 1 respectively, where $|i\rangle, |j\rangle$ are fixed and chosen from the D-dimensional computational basis states $\{|0\rangle, ..., |D-1\rangle\}$. We ask that Alice send only $|j\rangle$ as the additional uninformative state. Thus, Alice need only be able to prepare and send three distinct quantum states. On Bob's part, we require his ability to measure in two POVMs. These are $Z = \{|0\rangle\langle 0|, ..., |D-1\rangle\langle D-1|\}$ (the complete computational basis) and $X = \{|\phi\rangle\langle\phi|, \mathbb{I} - |\phi\rangle\langle\phi|\}$ where of course, the identity operator $\mathbb{I}$ is understood to be D-dimensional. Hence, Bob would be able to detect any computational basis state but would only need to detect $|\phi\rangle$. Our protocol, which we call here HD-Ext-B92, in detail appears in Protocol 1.

Protocol 1 High-dimensional Extended B92 (HD-Ext-B92)

Public Parameters: The dimension of a signal state $D \geq 2$ and the choice of distinct $i, j \in \{0, 1, \cdots, D-1\}$ are arbitrary, but are fixed at the start of the protocol and known to all parties (including the adversary).

Quantum Communication Stage: The quantum communication stage of the protocol will repeat the following until a sufficiently large raw-key has been distilled:

1. Alice chooses randomly whether this round will be a "key-round", where a raw key bit will attempt to be established, or a "test" round, which will be used for error testing later. If this is a key-round, she will choose a random key bit and if this is 0, she will prepare and send the state $|i\rangle$; otherwise, she sends the state $|\phi\rangle$. If this is a test round, she will prepare $|i\rangle$, $|j\rangle$, or $|\phi\rangle$ choosing uniformly at random.
2. Bob measures in either the Z basis or using POVM X. In a key-round, if he uses Z and observes any outcome other than $|i\rangle$, then he sets his bit to be 1. Otherwise, if he uses POVM X and observes $\mathbb{I} - |\phi\rangle\langle\phi|$, then he sets his bit to be 0. All other results are considered inconclusive.
3. Alice informs Bob over the authenticated channel whether this was a test round or a key-round. If this is a key-round, Bob also tells Alice if his result was inconclusive (in which case both parties discard the iteration). On test-rounds, both parties disclose their choices and measurement outcomes to determine the error rate in the channel. In particular, they will observe those statistics enumerated in Table 1. Note that we will not discard mismatched basis events; i.e., events where Alice and Bob use different bases. Indeed, such events can greatly improve key generation rates [22–26] and so we use this technique here.

Classical Communication Stage: Alice and Bob will next run an error correction protocol and a privacy amplification protocol resulting in a secret key of size ℓ bits (possibly $\ell = 0$ if it is determined that Eve has too much information, to be discussed later in this paper, and so parties abort the protocol).

Table 1 Definition of Alice and Bob's directly observable parameters ($|b\rangle \in \{|0\rangle, ..., |D-1\rangle\}$)

Parameter	Description of Probability Value
p_{ib}	Bob observes $|b\rangle$ if Alice sends $|i\rangle$ and he chooses the Z basis
p_{jb}	Bob observes $|b\rangle$ if Alice sends $|j\rangle$ and he chooses the Z basis
$p_{\phi b}$	Bob observes $|b\rangle$ if Alice sends $|\phi\rangle$ and he chooses the Z basis
$p_{i\phi}$	Bob observes $|\phi\rangle$ if Alice sends $|i\rangle$ and he chooses the POVM X
$p_{j\phi}$	Bob observes $|\phi\rangle$ if Alice sends $|j\rangle$ and he chooses the POVM X
$p_{\phi\phi}$	Bob observes $|\phi\rangle$ if Alice sends $|\phi\rangle$ and he chooses the POVM X

4 Security Analysis

In the quantum communication stage of our protocol, Alice and Bob use the quantum channel to establish a raw-key. Because Eve has total control over this channel, she may attack the traveling signals arbitrarily while only respecting the laws of physics. In this paper, we consider collective attacks whereby Eve attacks each round of the protocol independently and identically, but may delay her measurements until the end of the protocol. These are a powerful class of attack which often imply security of general coherent attacks [27, 28], though we leave a complete proof of whether this applies to our protocol as future work.

The goal of our analysis is to obtain a lower bound on the conditional von Neumann entropy $S(A|E)$, which represents how much entropy is left in Alice's register A, given Eve's (quantum) memory E. Then, we will find how much this quantity differs from the conditional Shannon entropy $H(A|B)$, which represents how much entropy is left in Alice's register given Bob's memory B. These two terms will ultimately let us calculate our quantity of interest from this protocol, which is, the key rate r (namely, the number of secret key bits, denoted ℓ over the size of the produced raw key denoted M). To compute the key rate we use the Devetak Winter key rate [29,30], which states the key rate r in the asymptotic setting is:

$$r = \lim_{M\to\infty} \frac{\ell}{M} = \inf[S(A|E) - H(A|B)], \tag{1}$$

where the infimum is over all collective attacks performed by Eve that fall within the range of observed noise statistics (in our case, those statistics shown in Table 1). Note that the above entropy functions are computed over a single key-round. However $S(A|E)$ is not straightforward to calculate, unlike $H(A|B)$, because it involves Eve's quantum memory on which we only have partial information. Nevertheless, we can obtain a lower bound on $S(A|E)$ which will be the main goal of our security analysis.

We begin by modeling the state of the joint quantum system held between Alice, Bob, and Eve at the end of one key-round of the protocol. That is, to compute Equation 1, we need the von Neumann entropy of the resulting density operator conditioned on a key bit being distilled and so we must model the joint quantum state, conditioning on the event that Alice and Bob establish a key bit.

At the beginning of the protocol, Alice decides on her classical bit and sends her qudit accordingly to Bob. If she wants to send classical bit 0, she sends a $|i\rangle$ and if she wants to send 1, she sends a $|\phi\rangle$. So when she sends the qudits, her own classical register, denoted by A and the transit register, denoted by T (used to model the traveling qudit), is in the following state:

$$\rho_{AT}^{(0)} = \frac{1}{2} |0\rangle\langle 0|_A \otimes |i\rangle\langle i|_T + \frac{1}{2} |1\rangle\langle 1|_A \otimes |\phi\rangle\langle\phi|_T .$$

Eve attacks this traveling qudit with a unitary attack operator U, which acts on Hilbert space $\mathcal{H}_T \otimes \mathcal{H}_E$. Here, $\mathcal{H}_E$ models Eve's memory space. We assume that, at the start of every iteration, Eve's private ancilla is initialized to some default pure state $|\chi\rangle_E$ of Eve's choice, independent of Alice and Bob's registers (this is before Alice sends anything). Note that, this is to Eve's advantage in a collective attack scenario (as holding a mixed state, or an unknown initial state, can only increase her uncertainty). Note that we make no assumptions on this state (including its dimension), other than Eve knows exactly what it is. In this case, whenever a quantum signal $|\psi\rangle_T$ is sent from Alice, the joint state is simply $|\psi\rangle_T \otimes |\chi\rangle_E$. From this, we can describe U's action on basis states as follows:

$$U\left|a\right\rangle_T \otimes \left|\chi\right\rangle_E = \sum_{b=0}^{D-1} \left|b, e_b^a\right\rangle_{TE},$$

where D is the dimension of each qudit and each $\left|e_b^a\right\rangle$ is an arbitrary state in Eve's ancilla. Because U is unitary, we note that the following must hold: $\sum_{b=0}^{D-1} \left\langle e_b^i \middle| e_b^i \right\rangle = 1$. Additionally, by linearity of U we have:

$$\begin{aligned} U\left|\phi\right\rangle_T \otimes \left|\chi\right\rangle_E &= U\frac{1}{\sqrt{2}}\left(\left|i\right\rangle_T + \left|j\right\rangle_T\right) \otimes \left|\chi\right\rangle_E \\ &= \frac{1}{\sqrt{2}}\sum_{b=0}^{D-1} \left|b\right\rangle_T \otimes \left(\left|e_b^i\right\rangle_E + \left|e_b^j\right\rangle_E\right) \\ &= \frac{1}{\sqrt{2}}\sum_{b=0}^{D-1} \left|b\right\rangle_T \otimes \left|f_b\right\rangle_E, \end{aligned} \tag{2}$$

where, $\left|f_b\right\rangle_E := \left|e_b^i\right\rangle_E + \left|e_b^j\right\rangle_E$. So the result of Eve's attack on $\rho_{AT}^{(0)}$ is the following:

$$\begin{aligned} \rho_{ATE}^{(1)} &= \frac{1}{2}\left|0\middle\rangle\middle\langle 0\right|_A \otimes U\left(\left|i\middle\rangle\middle\langle i\right|_T \otimes \left|\chi\middle\rangle\middle\langle\chi\right|_E\right)U^\dagger + \frac{1}{2}\left|1\middle\rangle\middle\langle 1\right|_A \otimes U\left(\left|\phi\middle\rangle\middle\langle\phi\right|_T \otimes \left|\chi\middle\rangle\middle\langle\chi\right|_E\right)U^\dagger \\ &= \frac{1}{2}\left|0\middle\rangle\middle\langle 0\right|_A \otimes P\left(\sum_{b=0}^{D-1}\left|b, e_b^i\right\rangle_{TE}\right) + \frac{1}{2}\left|1\middle\rangle\middle\langle 1\right|_A \otimes P\left(\frac{1}{\sqrt{2}}\sum_{b=0}^{D-1}\left|b\right\rangle_T \otimes \left|f_b\right\rangle_E\right), \end{aligned}$$

where, recall, $P(|z\rangle) = |z\rangle\langle z|$ is the projection operator. Henceforth, we will forgo writing the subscript for a register when the context is clear. Now, after the qudit arrives at Bob's lab, he measures the transit register T in either POVM Z or X with equal probability. Let's consider the case when he uses X and gets the outcome $\mathbb{I} - |\phi\rangle\langle\phi|$ (we are conditioning on a successful key-round for this analysis). This is the case when Bob sets his key-bit to 0, because in a noiseless scenario, this outcome could only be obtained when Alice would have sent an $|i\rangle$. Let's define the measurement operator in this case as $M_0 = \mathbb{I}_A \otimes (\mathbb{I} - |\phi\rangle\langle\phi|) \otimes \mathbb{I}_E$. Then the un-normalized post-measurement state, conditioned on him observing M_0 (again, we are only interested, for the moment, in a successful key distillation round) is:

$$
\begin{aligned}
\rho^X_{ATE} &= M_0 \cdot \rho^{(1)}_{ATE} \cdot M_0^\dagger \\
&= \frac{1}{2} |0\rangle\langle 0| \otimes P\Big(((\mathbb{I} - |\phi\rangle\langle\phi|) \otimes \mathbb{I}) \sum_b \left|b, e^i_b\right\rangle \Big) \\
&+ \frac{1}{2} |1\rangle\langle 1| \otimes P\Big(\frac{1}{\sqrt{2}} ((\mathbb{I} - |\phi\rangle\langle\phi|) \otimes \mathbb{I}) \sum_b |b\rangle \otimes |f_b\rangle \Big) \\
&= \frac{1}{2} |0\rangle\langle 0| \otimes P\Big(\sum_b \left|b, e^i_b\right\rangle - \frac{1}{2}(\left|i, e^i_i\right\rangle + \left|i, e^i_j\right\rangle + \left|j, e^i_i\right\rangle + \left|j, e^i_j\right\rangle) \Big) \\
&+ \frac{1}{2} |1\rangle\langle 1| \otimes P\Big(\frac{1}{\sqrt{2}} (\sum_b |b, f_b\rangle - \frac{1}{2}(|i, f_i\rangle + |i, f_j\rangle + |j, f_i\rangle + |j, f_j\rangle)) \Big) \\
&= \frac{1}{2} |0\rangle\langle 0| \otimes P\Big(\sum_{b \neq i, b \neq j} \left|b, e^i_b\right\rangle + \frac{1}{2}(|i\rangle \otimes (\left|e^i_i\right\rangle - \left|e^i_j\right\rangle)) \\
&\qquad\qquad\qquad - \frac{1}{2}(|j\rangle \otimes (\left|e^i_i\right\rangle - \left|e^i_j\right\rangle)) \Big) \\
&+ \frac{1}{2} |1\rangle\langle 1| \otimes P\Big(\frac{1}{\sqrt{2}} (\sum_{b \neq i, b \neq j} |b, f_b\rangle + \frac{1}{2}(|i\rangle \otimes (|f_i\rangle - |f_j\rangle)) \\
&\qquad\qquad\qquad - \frac{1}{2}(|j\rangle \otimes (|f_i\rangle - |f_j\rangle))) \Big) \\
&= \frac{1}{2} |0\rangle\langle 0| \otimes P\Big(\sum_{b \neq i, b \neq j} \left|b, e^i_b\right\rangle + \frac{1}{2} |i, g\rangle - \frac{1}{2} |j, g\rangle \Big) \\
&+ \frac{1}{2} |1\rangle\langle 1| \otimes P\Big(\frac{1}{\sqrt{2}} (\sum_{b \neq i, b \neq j} |b, f_b\rangle + \frac{1}{2} |i, h\rangle - \frac{1}{2} |j, h\rangle) \Big), \qquad (3)
\end{aligned}
$$

where in the last equality, we have defined $|g\rangle = \left|e^i_i\right\rangle - \left|e^i_j\right\rangle$ and $|h\rangle = |f_i\rangle - |f_j\rangle$. Now that Bob has his X basis measurement result at his hand, we can trace out the transit register T and add Bob's register B to hold his measurement result. Then the resulting state is:

$$
\begin{aligned}
\rho^X_{AEB} = &\frac{1}{2} |0\rangle\langle 0|_A \otimes \Big(\sum_{b \neq i, b \neq j} \left|e^i_b\right\rangle\left\langle e^i_b\right| + \frac{1}{2} |g\rangle\langle g| \Big) \otimes |0\rangle\langle 0|_B \\
&+ \frac{1}{2} |1\rangle\langle 1|_A \otimes \frac{1}{2} \Big(\sum_{b \neq i, b \neq j} |f_b\rangle\langle f_b| + \frac{1}{2} |h\rangle\langle h| \Big) \otimes |0\rangle\langle 0|_B \, .
\end{aligned}
$$

Similarly, if he uses POVM Z and gets outcome $\mathbb{I} - |i\rangle\langle i|$, he can be certain in a noiseless scenario that Alice has sent a $|\phi\rangle$. With the measurement operator $M_1 := \mathbb{I}_A \otimes (\mathbb{I} - |i\rangle\langle i|) \otimes \mathbb{I}_E$, in this case we get the following un-normalized post-measurement state:

$$\begin{aligned}
\rho^Z_{ATE} &= M_1 \cdot \rho^{(1)}_{ATE} \cdot M_1^\dagger \\
&= \frac{1}{2} \lvert 0 \rangle\langle 0 \rvert \otimes P\Big((\mathbb{I} - \lvert i \rangle\langle i \rvert) \sum_b \lvert b, e^i_b \rangle \Big) \\
&+ \frac{1}{2} \lvert 1 \rangle\langle 1 \rvert \otimes P\Big(\frac{1}{\sqrt{2}} (\mathbb{I} - \lvert i \rangle\langle i \rvert) \sum_b \lvert b, f_b \rangle \Big) \\
&= \frac{1}{2} \lvert 0 \rangle\langle 0 \rvert \otimes P\Big(\sum_{b \neq i} \lvert b, e^i_b \rangle \Big) + \frac{1}{2} \lvert 1 \rangle\langle 1 \rvert \otimes P\Big(\frac{1}{\sqrt{2}} \sum_{b \neq i} \lvert b \rangle \otimes \lvert f_b \rangle \Big).
\end{aligned}$$

Following a similar procedure as before, we trace out the transit register T and add Bob's register holding his measurement result. The resulting density operator is:

$$\rho^Z_{AEB} = \frac{1}{2} \lvert 0 \rangle\langle 0 \rvert_A \otimes \sum_{b \neq i} \lvert e^i_b \rangle\langle e^i_b \rvert \otimes \lvert 1 \rangle\langle 1 \rvert_B + \frac{1}{2} \lvert 1 \rangle\langle 1 \rvert_A \otimes \frac{1}{2} \sum_{b \neq i} \lvert f_b \rangle\langle f_b \rvert \otimes \lvert 1 \rangle\langle 1 \rvert_B .$$

Then the total (still non-normalized) density operator that represents a key-bit generation round, is the following:

$$\begin{aligned}
\rho_{AEB} &= \rho^X_{AEB} + \rho^Z_{AEB} \\
&= \frac{1}{2} \lvert 0 \rangle\langle 0 \rvert_A \otimes \Big(\sum_{b \neq i, b \neq j} \lvert e^i_b \rangle\langle e^i_b \rvert + \frac{1}{2} \lvert g \rangle\langle g \rvert \Big) \otimes \lvert 0 \rangle\langle 0 \rvert_B \\
&+ \frac{1}{2} \lvert 1 \rangle\langle 1 \rvert_A \otimes \frac{1}{2} \Big(\sum_{b \neq i, b \neq j} \lvert f_b \rangle\langle f_b \rvert + \frac{1}{2} \lvert h \rangle\langle h \rvert \Big) \otimes \lvert 0 \rangle\langle 0 \rvert_B \\
&+ \frac{1}{2} \lvert 0 \rangle\langle 0 \rvert_A \otimes \sum_{b \neq i} \lvert e^i_b \rangle\langle e^i_b \rvert \otimes \lvert 1 \rangle\langle 1 \rvert_B + \frac{1}{2} \lvert 1 \rangle\langle 1 \rvert_A \otimes \frac{1}{2} \sum_{b \neq i} \lvert f_b \rangle\langle f_b \rvert \otimes \lvert 1 \rangle\langle 1 \rvert_B \\
&= \frac{1}{2} \lvert 0 \rangle\langle 0 \rvert_A \otimes \Big((\sum_{b \neq i, b \neq j} \lvert e^i_b \rangle\langle e^i_b \rvert + \frac{1}{2} \lvert g \rangle\langle g \rvert) \otimes \lvert 0 \rangle\langle 0 \rvert_B \\
&\qquad\qquad + \sum_{b \neq i} \lvert e^i_b \rangle\langle e^i_b \rvert \otimes \lvert 1 \rangle\langle 1 \rvert_B \Big) \\
&+ \frac{1}{2} \lvert 1 \rangle\langle 1 \rvert_A \otimes \Big(\frac{1}{2} (\sum_{b \neq i, b \neq j} \lvert f_b \rangle\langle f_b \rvert + \frac{1}{2} \lvert h \rangle\langle h \rvert) \otimes \lvert 0 \rangle\langle 0 \rvert_B \\
&\qquad\qquad + \frac{1}{2} \sum_{b \neq i} \lvert f_b \rangle\langle f_b \rvert \otimes \lvert 1 \rangle\langle 1 \rvert_B \Big).
\end{aligned} \tag{4}$$

Keeping in mind that, our ultimate goal is to bound Eve's entropy about Alice's register, i.e. $S(A|E)$, in the case where Alice and Bob shares a key-bit, we trace out Bob's register too, keeping only the registers of Alice and Eve.

Thus, we calculate the final required density operator as:

$$
\begin{aligned}
N \cdot \rho_{AE} &= \frac{1}{2} |0\rangle\langle 0|_A \otimes \Big(\sum_{b\neq i, b\neq j} |e_b^i\rangle\langle e_b^i| + \frac{1}{2} |g\rangle\langle g| + \sum_{b\neq i} |e_b^i\rangle\langle e_b^i| \Big) \\
&+ \frac{1}{2} |1\rangle\langle 1|_A \otimes \Big(\frac{1}{2} \sum_{b\neq i, b\neq j} |f_b\rangle\langle f_b| + \frac{1}{4} |h\rangle\langle h| + \frac{1}{2} \sum_{b\neq i} |f_b\rangle\langle f_b| \Big) \\
&= |0\rangle\langle 0|_A \otimes \Big(\frac{1}{2} \sum_{b\neq i, b\neq j} |e_b^i\rangle\langle e_b^i| + \frac{1}{4} |g\rangle\langle g| + \frac{1}{2} \sum_{b\neq i, b\neq j} |e_b^i\rangle\langle e_b^i| + \frac{1}{2} |e_j^i\rangle\langle e_j^i| \Big) \\
&+ |1\rangle\langle 1|_A \otimes \Big(\frac{1}{4} \sum_{b\neq i, b\neq j} |f_b\rangle\langle f_b| + \frac{1}{8} |h\rangle\langle h| + \frac{1}{4} \sum_{b\neq i, b\neq j} |f_b\rangle\langle f_b| + \frac{1}{4} |f_j\rangle\langle f_j| \Big) \\
&= |0\rangle\langle 0| \otimes \Big(\sum_{b\neq i, b\neq j} |e_b^i\rangle\langle e_b^i| + \frac{1}{2} |e_j^i\rangle\langle e_j^i| + \frac{1}{4} |g\rangle\langle g| \Big) \\
&+ |1\rangle\langle 1| \otimes \Big(\frac{1}{2} \sum_{b\neq i, b\neq j} |f_b\rangle\langle f_b| + \frac{1}{4} |f_j\rangle\langle f_j| + \frac{1}{8} |h\rangle\langle h| \Big), \qquad (5)
\end{aligned}
$$

where the normalization term N can be calculated as:

$$
N = \sum_{b\neq i, b\neq j} \langle e_b^i | e_b^i \rangle + \frac{1}{2} \langle e_j^i | e_j^i \rangle + \frac{1}{4} \langle g|g\rangle + \frac{1}{2} \sum_{b\neq i, b\neq j} \langle f_b | f_b \rangle + \frac{1}{4} \langle f_j | f_j \rangle + \frac{1}{8} \langle h|h\rangle \qquad (6)
$$

Now, using Theorem 1, we may compute the conditional entropy as:

$$
S(A|E) \geq \sum_{b\neq i, b\neq j} \left(\frac{n_b^0 + n_b^1}{N} \right) s_b + \left(\frac{n_i^0 + n_i^1}{N} \right) s_i + (\frac{n_j^0 + n_j^1}{N}) s_j, \qquad (7)
$$

where:

$$
\begin{aligned}
n_b^0 &:= \langle e_b^i | e_b^i \rangle, \qquad n_b^1 := \frac{1}{2} \langle f_b | f_b \rangle, \text{ for all } b \neq i, j \\
n_i^0 &:= \frac{1}{2} \langle e_j^i | e_j^i \rangle, \qquad n_i^1 := \frac{1}{8} \langle h|h \rangle, \\
n_j^0 &:= \frac{1}{4} \langle g|g \rangle, \qquad n_j^1 := \frac{1}{4} \langle f_j | f_j \rangle.
\end{aligned}
$$

and:

$$s_b = H_2\left(\frac{n_b^0}{n_b^0+n_b^1}\right) - H_2\left(\frac{1}{2} + \frac{\sqrt{(n_b^0-n_b^1)^2 + 4\times \mathrm{Re}^2\left\langle e_b^i\middle|\frac{1}{\sqrt{2}}f_b\right\rangle}}{2(n_b^0+n_b^1)}\right)$$

$$s_i = H_2\left(\frac{n_i^0}{n_i^0+n_i^1}\right) - H_2\left(\frac{1}{2} + \frac{\sqrt{(n_i^0-n_i^1)^2 + 4\times \mathrm{Re}^2\left\langle \frac{1}{2}e_j^i\middle|\frac{1}{2\sqrt{2}}h\right\rangle}}{2(n_i^0+n_i^1)}\right)$$

$$s_j = H_2\left(\frac{n_j^0}{n_j^0+n_j^1}\right) - H_2\left(\frac{1}{2} + \frac{\sqrt{(n_j^0-n_j^1)^2 + 4\times \mathrm{Re}^2\left\langle \frac{1}{2}g\middle|\frac{1}{2}f_j\right\rangle}}{2(n_j^0+n_j^1)}\right).$$

Thus, to find a lower bound on $S(A|E)$ (thus giving us a lower bound on the protocol's key rate), we must determine bounds for the inner-products appearing in the above expressions. Of course, these inner products are functions of Eve's quantum ancilla. We show how to determine suitable bounds on these systems based only on parameters that are directly observable in our protocol during test rounds (see Table 1).

4.1 Parameter Estimation

To calculate the conditional entropy of ρ_{AE}, we need to estimate all the inner products appearing in equation (6). This can be done by connecting these inner products with observable noise statistics that arise from test rounds of Alice and Bob's quantum communication. Let us see the statistics that can be observed directly in a test round. For example, in a round where Alice sends an $|i\rangle$ or a $|j\rangle$, Eve attacks with U, and Bob measures in Z; the probability that Bob gets a particular outcome $|b\rangle\langle b|$ in Z can be used to estimate partial Z basis channel noise. In the following, by p_{ib} and p_{jb}, we denote the probability that, given that Alice prepares $|i\rangle$ or $|j\rangle$ and Bob measures the transit register in basis Z then the outcome is $|b\rangle\langle b|$ for a particular $b \in \{0, ..., D-1\}$. (See also Table 1.)

$$p_{ib} = \langle i|\, U^\dagger(|b\rangle\langle b| \otimes \mathbb{I})U\, |i\rangle = \left\langle e_b^i\middle|e_b^i\right\rangle \tag{8}$$

$$p_{jb} = \langle j|\, U^\dagger(|b\rangle\langle b| \otimes \mathbb{I})U\, |j\rangle = \left\langle e_b^j\middle|e_b^j\right\rangle \tag{9}$$

thus giving us $\{n_b^0\}$ as needed in the entropy equation. Now, we trace the evolution of the quantum system when Alice prepares $|i\rangle$ and Bob measures in POVM X. For example, we can not observe the inner product $\left\langle e_i^i\middle|e_j^i\right\rangle$ directly. But we consider the probability that Alice sends an $|i\rangle$, Eve attacks with U, and Bob measures in X to find a $|\phi\rangle$, denoted as $p_{i\phi}$:

$$\begin{aligned}
p_{i\phi} &= \langle i|\, U^\dagger(|\phi\rangle\langle\phi| \otimes \mathbb{I})U\, |i\rangle \\
&= \sum_{b,c} \langle b|\, |\phi\rangle\langle\phi|\, |c\rangle \left\langle e_b^i \middle| e_c^i \right\rangle \\
&= \frac{1}{2}\sum_{b,c} \langle b|\, (|i\rangle\langle i| + |i\rangle\langle j| + |j\rangle\langle i| + |j\rangle\langle j|)\, |c\rangle \left\langle e_b^i \middle| e_c^i \right\rangle \\
&= \frac{1}{2}(\left\langle e_i^i \middle| e_i^i \right\rangle + \left\langle e_i^i \middle| e_j^i \right\rangle + \left\langle e_j^i \middle| e_i^i \right\rangle + \left\langle e_j^i \middle| e_j^i \right\rangle) \\
&= \frac{1}{2}(p_{ii} + 2\,\mathrm{Re}\left\langle e_i^i \middle| e_j^i \right\rangle + p_{ij}),
\end{aligned} \tag{10}$$

where, we have used equation (8) for p_{ii}, p_{ij} and an elementary property of complex inner products. Notice that, even though we could not observe $\left\langle e_i^i \middle| e_j^i \right\rangle$, equation (10) will imply:

$$2\,\mathrm{Re}\left\langle e_i^i \middle| e_j^i \right\rangle = 2p_{i\phi} - p_{ii} - p_{ij}. \tag{11}$$

Using this estimation of $\mathrm{Re}\left\langle e_i^i \middle| e_j^i \right\rangle$, we can now estimate the inner product $\langle g|g\rangle$, which appears in the normalizer N in equation (6). This is:

$$\begin{aligned}
\langle g|g\rangle &= (\left\langle e_i^i \right| - \left\langle e_j^i \right|)(\left| e_i^i \right\rangle - \left| e_j^i \right\rangle) \\
&= \left\langle e_i^i \middle| e_i^i \right\rangle - \left\langle e_i^i \middle| e_j^i \right\rangle - \left\langle e_j^i \middle| e_i^i \right\rangle + \left\langle e_j^i \middle| e_j^i \right\rangle \\
&= p_{ii} - 2\,\mathrm{Re}\left\langle e_i^i \middle| e_j^i \right\rangle + p_{ij} \\
&= 2p_{ii} + 2p_{ij} - 2p_{i\phi}.
\end{aligned} \tag{12}$$

Now let's focus on calculating $\langle f_b|f_b\rangle$. Remembering that $|f_b\rangle = \left| e_b^i \right\rangle + \left| e_b^j \right\rangle$ (See equation (2)), we can easily derive the following:

$$\begin{aligned}
\langle f_b|f_b\rangle &= (\left\langle e_b^i \right| + \left\langle e_b^j \right|)(\left| e_b^i \right\rangle + \left| e_b^j \right\rangle) \\
&= \left\langle e_b^i \middle| e_b^i \right\rangle + \left\langle e_b^i \middle| e_b^j \right\rangle + \left\langle e_b^j \middle| e_b^i \right\rangle + \left\langle e_b^j \middle| e_b^j \right\rangle \\
&= p_{ib} + 2\,\mathrm{Re}\left\langle e_b^i \middle| e_b^j \right\rangle + p_{jb},
\end{aligned} \tag{13}$$

where we have used equation (8) and (9) for p_{ib}, p_{jb}. Now if we look closely at equation (2), we see that $\langle f_b|f_b\rangle$ is actually directly observable. Because it is the probability that Alice sends a $|\phi\rangle$, Eve attacks with U, and conditioned on the case that Bob measures in Z, gets an outcome $|b\rangle$. We denote it by $p_{\phi b}$

and see that:

$$\begin{aligned} p_{\phi b} &= \langle\phi| U^\dagger (|b\rangle\langle b| \otimes \mathbb{I}) U |\phi\rangle \\ &= \Big(\frac{1}{\sqrt{2}} \sum_{c=0}^{D-1} \langle c| \otimes \langle f_c| \Big)(|b\rangle\langle b| \otimes \mathbb{I}) \Big(\frac{1}{\sqrt{2}} \sum_{d=0}^{D-1} |d\rangle \otimes |f_d\rangle \Big) \\ &= \frac{1}{2} \sum_{c,d=0}^{D-1} \langle c| \, |b\rangle\langle b| \, |d\rangle \langle f_c|f_d\rangle \\ &= \frac{1}{2} \langle f_b|f_b\rangle , \end{aligned} \tag{14}$$

and consequently, $\langle f_b|f_b\rangle = 2p_{\phi b}$. So, from equations (13) and (14) we infer the following:

$$2\,\mathrm{Re}\left\langle e_b^i \middle| e_b^j \right\rangle = 2p_{\phi b} - p_{ib} - p_{jb}. \tag{15}$$

Notice that equation (13) and consequently (15), holds for all $b = 0, ..., D-1$. So we immediately get $\langle f_j|f_j\rangle$ for normalizer N. Now let's calculate the last inner product in N which is $\langle h|h\rangle$. First let's discover the constituent inner products for $\langle h|h\rangle$. Then we will connect each of those to Alice and Bob's observables.

$$\begin{aligned} \langle h|h\rangle &= (\langle f_i| - \langle f_j|)(|f_i\rangle - |f_j\rangle) \\ &= \langle f_i|f_i\rangle - \langle f_i|f_j\rangle - \langle f_j|f_i\rangle + \langle f_j|f_j\rangle \\ &= \langle f_i|f_i\rangle - 2\,\mathrm{Re}\,\langle f_i|f_j\rangle + \langle f_j|f_j\rangle . \end{aligned} \tag{16}$$

Now, let us take advantage of another directly observable quantity. Which is the probability that Bob would measure a $|\phi\rangle$ in the X basis if Alice indeed sent a $|\phi\rangle$. We denote it as $p_{\phi\phi}$ and see that:

$$\begin{aligned} p_{\phi\phi} &= \langle\phi| U^\dagger (|\phi\rangle\langle\phi| \otimes \mathbb{I}) U |\phi\rangle \\ &= \frac{1}{\sqrt{2}} \Big(\sum_b \langle b, f_b| \Big) \big(|\phi\rangle\langle\phi| \otimes \mathbb{I}\big) \frac{1}{\sqrt{2}} \Big(\sum_c |c, f_c\rangle \Big) \\ &= \frac{1}{4} \Big(\sum_{b,c} \big(\langle b| \, |i\rangle\langle i| \, |c\rangle \otimes \langle f_b|f_c\rangle + \langle b| \, |i\rangle\langle j| \, |c\rangle \otimes \langle f_b|f_c\rangle \\ &+ \langle b| \, |j\rangle\langle i| \, |c\rangle \otimes \langle f_b|f_c\rangle + \langle b| \, |j\rangle\langle j| \, |c\rangle \otimes \langle f_b|f_c\rangle \big) \Big) \\ &= \frac{1}{4} (\langle f_i|f_i\rangle + \langle f_i|f_j\rangle + \langle f_j|f_i\rangle + \langle f_j|f_j\rangle) \\ &= \frac{1}{4} (\langle f_i|f_i\rangle + 2\,\mathrm{Re}\,\langle f_i|f_j\rangle + \langle f_j|f_j\rangle) \\ &= \frac{1}{2} (p_{\phi i} + \mathrm{Re}\,\langle f_i|f_j\rangle + p_{\phi j}). \end{aligned} \tag{17}$$

Equation (17) implies that:

$$\mathrm{Re}\,\langle f_i|f_j\rangle = 2p_{\phi\phi} - p_{\phi i} - p_{\phi j}. \tag{18}$$

Along with the fact that $\langle f_i|f_i\rangle = 2p_{\phi i}$ and $\langle f_j|f_j\rangle = 2p_{\phi j}$ from equation (14), we can say from equation (16) and (18) that:

$$\langle h|h\rangle = 4(p_{\phi i} + p_{\phi j} - p_{\phi\phi}).$$

This concludes the estimation of inner products appearing in the normalizer N of ρ_{AE} in (6). We need to estimate the real parts of three more classes of inner products to calculate each of the λ-terms appearing in Theorem 1. These are $\{\mathrm{Re}\left\langle e_b^i\middle|\frac{1}{\sqrt{2}}f_b\right\rangle\}_b, \mathrm{Re}\left\langle\frac{1}{2}g\middle|\frac{1}{2}f_j\right\rangle, \mathrm{Re}\left\langle\frac{1}{2}e_j^i\middle|\frac{1}{2\sqrt{2}}h\right\rangle$. In the following we connect these inner products to observable statistics. Let's focus on the first one:

$$\begin{aligned}\mathrm{Re}\left\langle e_b^i\middle|\frac{1}{\sqrt{2}}f_b\right\rangle &= \frac{1}{\sqrt{2}}\,\mathrm{Re}((\langle e_b^i|)(|e_b^i\rangle + \left|e_b^j\right\rangle))\\ &= \frac{1}{\sqrt{2}}\,\mathrm{Re}(\langle e_b^i|e_b^i\rangle + \left\langle e_b^i\middle|e_b^j\right\rangle)\\ &= \frac{1}{\sqrt{2}}(p_{ib} + p_{\phi b} - \frac{p_{ib}}{2} - \frac{p_{jb}}{2}),\end{aligned} \tag{19}$$

where we have used the definition of $|f_b\rangle$ in the first equality and have used equation (8) and (15) to insert the value of $\mathrm{Re}\,\langle e_b^i|e_b^i\rangle, \mathrm{Re}\left\langle e_b^i\middle|e_b^j\right\rangle$. Now let's focus on the second inner product $\mathrm{Re}\left\langle\frac{1}{2}g\middle|\frac{1}{2}f_j\right\rangle$:

$$\begin{aligned}\mathrm{Re}\left\langle\frac{1}{2}g\middle|\frac{1}{2}f_j\right\rangle &= \frac{1}{4}\,\mathrm{Re}((\langle e_i^i| - \langle e_j^i|)(|e_j^i\rangle + \left|e_j^j\right\rangle))\\ &= \frac{1}{4}\,\mathrm{Re}(\langle e_i^i|e_j^i\rangle + \left\langle e_i^i\middle|e_j^j\right\rangle - \langle e_j^i|e_j^i\rangle - \left\langle e_j^i\middle|e_j^j\right\rangle)\\ &= \frac{1}{4}(p_{i\phi} - \frac{p_{ii}}{2} + \mathrm{Re}\left\langle e_i^i\middle|e_j^j\right\rangle - p_{ij} - p_{\phi j} + \frac{p_{jj}}{2}).\end{aligned} \tag{20}$$

The value of $\mathrm{Re}\,\langle e_i^i|e_j^i\rangle$ and $\mathrm{Re}\left\langle e_j^i\middle|e_j^j\right\rangle$ is found in (11) and (15) respectively. Furthermore, $\langle e_j^i|e_j^i\rangle$ is simply p_{ij} because of equation (8). Noticeably, the term $\left\langle e_i^i\middle|e_j^j\right\rangle$ is not observable. We will deal with this a bit later. Now we move on to the last of the necessary inner products for the theorem, $\mathrm{Re}\left\langle\frac{1}{2}e_j^i\middle|\frac{1}{2\sqrt{2}}h\right\rangle$.

$$\begin{aligned}\frac{1}{2}\times\frac{1}{2\sqrt{2}}\,\mathrm{Re}\,\langle e_j^i|h\rangle &= \frac{1}{4}\,\mathrm{Re}\,\langle e_j^i|\,(|f_i\rangle - |f_j\rangle)\\ &= \frac{1}{4}\,\mathrm{Re}\,\langle e_j^i|\,(|e_i^i\rangle + \left|e_i^j\right\rangle - |e_j^i\rangle - \left|e_j^j\right\rangle)\\ &= \frac{1}{4}\,\mathrm{Re}(\langle e_j^i|e_i^i\rangle + \left\langle e_j^i\middle|e_i^j\right\rangle - \langle e_j^i|e_j^i\rangle - \left\langle e_j^i\middle|e_j^j\right\rangle)\\ &= \frac{1}{4}\left(p_{i\phi} - \frac{p_{ii}}{2} + \mathrm{Re}\left\langle e_j^i\middle|e_i^j\right\rangle - p_{ij} - p_{\phi j} + \frac{p_{jj}}{2}\right),\end{aligned} \tag{21}$$

where the unknown terms $\mathrm{Re}\,\langle e_j^i|e_i^i\rangle = \mathrm{Re}\,\langle e_i^i|e_j^i\rangle, \mathrm{Re}\left\langle e_j^i\middle|e_j^j\right\rangle$ can be found in equations (11) and (15) respectively. In equation (21), we are again faced with a term $\mathrm{Re}\left\langle e^i_j \middle| e^j_i \right\rangle$ for which we do not have a direct observation. Now we deal with this term and the other unobservable term from equation (20), which is $\mathrm{Re}\left\langle e^i_i \middle| e^j_j \right\rangle$. Although it is not hard to see, we need to take several steps to find an equation that relates these two inner products. Consider $\langle f_i | f_j \rangle$ which we may expand as:

$$2\,\mathrm{Re}\,\langle f_i | f_j \rangle = 2\,\mathrm{Re}(\langle e^i_i | e^i_j \rangle + \left\langle e^i_i \middle| e^j_j \right\rangle + \left\langle e^j_i \middle| e^i_j \right\rangle + \left\langle e^j_i \middle| e^j_j \right\rangle) \tag{22}$$

First let's deal with the unobservable term $\left\langle e^j_i \middle| e^j_j \right\rangle$. It is easy to see that, the probability of Alice sending a $|j\rangle$, Eve attacking with U and Bob measures in X to find a $|\phi\rangle$, denoted by $p_{j\phi}$ is:

$$\begin{aligned} p_{j\phi} &= \langle j|\, U^\dagger (|\phi\rangle\langle\phi| \otimes \mathbb{I}) U \,|j\rangle \\ &= \sum_{b,c} \langle b|\, |\phi\rangle\langle\phi|\, |c\rangle \left\langle e^j_b \middle| e^j_c \right\rangle \\ &= \frac{1}{2} \sum_{b,c} \langle b|\, (|i\rangle\langle i| + |i\rangle\langle j| + |j\rangle\langle i| + |j\rangle\langle j|)\, |c\rangle \left\langle e^j_b \middle| e^j_c \right\rangle \\ &= \frac{1}{2} (\left\langle e^j_i \middle| e^j_i \right\rangle + \left\langle e^j_i \middle| e^j_j \right\rangle + \left\langle e^j_j \middle| e^j_i \right\rangle + \left\langle e^j_j \middle| e^j_j \right\rangle) \\ &= \frac{1}{2} (p_{ji} + 2\,\mathrm{Re} \left\langle e^j_i \middle| e^j_j \right\rangle + p_{jj}). \end{aligned} \tag{23}$$

From equation (23), it is clear that:

$$2\,\mathrm{Re} \left\langle e^j_i \middle| e^j_j \right\rangle = 2p_{j\phi} - p_{ji} - p_{jj}. \tag{24}$$

The value of one of the other three unobservable terms appearing in equation (22), i.e., $\langle e^i_i | e^i_j \rangle$ can be found in equation (11). However, $\mathrm{Re}\left\langle e^i_i \middle| e^j_j \right\rangle, \mathrm{Re}\left\langle e^j_i \middle| e^i_j \right\rangle)$ are unobservable at this point. With the help of equations (11) and (24), we can rewrite equation (22) as:

$$2\,\mathrm{Re}\,\langle f_i | f_j \rangle = 2p_{i\phi} - p_{ii} - p_{ij} + 2\,\mathrm{Re}(\left\langle e^i_i \middle| e^j_j \right\rangle + \left\langle e^j_i \middle| e^i_j \right\rangle) + 2p_{j\phi} - p_{ji} - p_{jj}, \tag{25}$$

We further notice from equation (18),

$$2\,\mathrm{Re}\,\langle f_i | f_j \rangle = 4p_{\phi\phi} - 2p_{\phi i} - 2p_{\phi j}. \tag{26}$$

Then, we equate the previous two equations (25), (26) to ultimately find:

$$\begin{aligned}
4p_{\phi\phi} - 2p_{\phi i} - 2p_{\phi j} &= 2p_{i\phi} - p_{ii} - p_{ij} + 2\,\mathrm{Re}(\left\langle e_i^i \middle| e_j^j \right\rangle + \left\langle e_i^j \middle| e_j^i \right\rangle) \\
&\quad + 2p_{j\phi} - p_{ji} - p_{jj} \\
\implies 2\,\mathrm{Re}(\left\langle e_i^i \middle| e_j^j \right\rangle + \left\langle e_i^j \middle| e_j^i \right\rangle) &= 4p_{\phi\phi} - 2p_{\phi i} - 2p_{\phi j} - 2p_{i\phi} + p_{ii} + p_{ij} \\
&\quad - 2p_{j\phi} + p_{ji} + p_{jj} \\
\implies \mathrm{Re}(\left\langle e_i^i \middle| e_j^j \right\rangle + \left\langle e_i^j \middle| e_j^i \right\rangle) &= 2p_{\phi\phi} - p_{\phi i} - p_{\phi j} - p_{i\phi} + \frac{p_{ii}}{2} + \frac{p_{ij}}{2} \\
&\quad - p_{j\phi} + \frac{p_{ji}}{2} + \frac{p_{jj}}{2} := K.
\end{aligned} \tag{27}$$

Where we define the right-hand side of equation (27) to be K, the value of which may be computed by Alice and Bob based only on observed statistics of the quantum channel. Now we have all the pieces necessary to compute the conditional entropy $S(A|E)$ according to Theorem 1.

We minimize $S(A|E)$ given by Equation (7) over one of the two unobservable values stated on the left side of equation (27). More specifically, based on equation (27), we can say that, $\mathrm{Re}\left\langle e_i^i \middle| e_j^j \right\rangle = K - \mathrm{Re}\left\langle e_i^j \middle| e_j^i \right\rangle$ and then optimize over $\mathrm{Re}\left\langle e_i^j \middle| e_j^i \right\rangle$. Note that we minimize over these unobservable quantities as we must assume that Eve choose the attack strategy that gives her the most information. However, her attack must be constrained by the above analysis. The independent unobservable inner-product $\mathrm{Re}\left\langle e_i^j \middle| e_j^i \right\rangle$ is further restricted by Cauchy-Schwarz in that $-\mathrm{Re}\left(\left\langle e_i^j \middle| e_i^j \right\rangle \langle e_j^i | e_j^i \rangle\right) \leq Re\left\langle e_j^i \middle| e_i^j \right\rangle \leq \mathrm{Re}\left(\left\langle e_i^j \middle| e_i^j \right\rangle \langle e_j^i | e_j^i \rangle\right)$, which in terms of observable probabilities from equations (8) and (9), can be seen to be $-\sqrt{p_{ij} \cdot p_{ji}} \leq Re\left\langle e_j^i \middle| e_i^j \right\rangle \leq \sqrt{p_{ij} \cdot p_{ji}}$. A method for computing the minimization of $S(A|E)$ and subsequently, the key rate, is presented in algorithm (2). Note that to perform the minimization we discretized the continuous search interval of the one free parameter into points of distance ϵ. For small enough ϵ, this algorithm will approach the actual minimum to an arbitrary level of accuracy set by the user (note that von Neumann entropy is a continuous function [31–33]). Finally, we also confirmed these results by performing the minimization using Mathematica's `NMinimize` command.

With the bound on $S(A|E)$ calculated, we can focus on the Shannon entropy of Alice's register given Bob's register, i.e. $H(A|B)$. However, this is easy to compute as it is based entirely on Alice and Bob's probability distribution on their raw key bits. In particular, let p_{ab} be the probability that Alice's raw key bit is "a" and Bob's raw key bit is "b" conditioned on them not rejecting the iteration. This is clearly something that Alice and Bob can estimate by classical sampling and, so, may directly compute $H(A|B)$. To actually evaluate

Algorithm 2 An algorithm for calculating the key rate

```
**Input:** All observable parameters: $p_{ib}, p_{jb}, p_{i\phi}, p_{j\phi}, p_{\phi b}, p_{\phi\phi}$ $\forall b \in \{0, 1, ..., D-1\}$
**Output:** Key rate given observed parameters.
**Algorithm:**
Compute $N$ (From equation (6))
Compute $p_{00}, p_{01}, p_{10}, p_{11}$ (From equations (28), (29), (30), (31) respectively)
Compute $K$ (From Equation (27))
$v_1 \leftarrow -\sqrt{p_{ij} \cdot p_{ji}}$ (Here, $v_1$ represents $Re\left\langle e_j^i \middle| e_i^j \right\rangle$)
$minSAE \leftarrow \infty$
**while** $v_1 \leq \sqrt{p_{ij} \cdot p_{ji}}$ **do**
    $v_2 \leftarrow K - v_1$ (Here, $v_2$ represents $Re\left\langle e_i^i \middle| e_j^j \right\rangle$)
    Compute $p_1, p_2, p_3$ (From equations (19), (20), (21) respectively using $v_1$ and $v_2$)
    $tmpSAE \leftarrow S(A|E)$ (From equation (7) using $p_1, p_2, p_3$)
    **if** $tmpSAE < minSAE$ **then**
        $minSAE \leftarrow tmpSAE$
    **end if**
    $v_1 \leftarrow v_1 + \epsilon$ (For small $\epsilon$)
**end while**
**return** $minSAE - [H(p_{00}, p_{01}, p_{10}, p_{11}) - H(p_{00} + p_{10})]$
```

our bound, we will require numerical values for these under simulated channels. For this, we can use ρ_{AEB} from Equation (4) and our earlier analysis to derive the following:

$$p_{00} = \frac{1}{2N}\Big(\sum_{b\neq i, b\neq j} \langle e_b^i | e_b^i \rangle + \frac{1}{2}\langle g|g\rangle\Big) = \frac{1}{2N}\left(1 - p_{i\phi}\right), \tag{28}$$

$$p_{01} = \frac{1}{2N}\sum_{b\neq i} |e_b^i\rangle\langle e_b^i| = \frac{1}{2N}\left(1 - p_{ii}\right), \tag{29}$$

$$p_{10} = \frac{1}{2N}\Big(\frac{1}{2}\sum_{b\neq i, b\neq j} |f_b\rangle\langle f_b| + \frac{1}{4}|h\rangle\langle h|\Big) = \frac{1}{2N}\left(1 - p_{\phi\phi}\right), \tag{30}$$

$$p_{11} = \frac{1}{4N}\sum_{b\neq i} |f_b\rangle\langle f_b| = \frac{1}{2N}\left(1 - p_{\phi i}\right). \tag{31}$$

Importantly, the values p_{ab} may be directly observed by Alice and Bob. The above expressions are what Alice and Bob should expect these values to be (and so they may actually estimate them using these expressions and probability values, already required by the rest of our proof, instead of sacrificing additional key material for sampling to learn p_{ab} directly). Taken together, we may now easily compute a lower-bound on the min-entropy $S(A|E)$ and also directly compute $H(A|B)$ thus giving us a lower-bound on the key rate of this protocol.

4.2 Comment on General Attacks

The above assumed collective attacks which is a standard assumption in the majority of QKD security proofs. Often, security against such attacks may be promoted to security against general coherent attacks through post-selection methods [28] or de Finetti techniques [27]. We strongly suspect the same holds for our protocol. To prove this rigorously, however, an equivalent entanglement based version of the prepare and measure protocol must be derived and security against general attacks there must be proven to imply security against general attacks for the prepare and measure protocol. We attempted to apply standard techniques for qubit-style B92 protocols for this (see, for instance, [6, 34, 30]), however the higher dimensional system does complicate the proof of the entanglement reduction. Thus, though we suspect these standard tools can be applied to promote our security analysis to general attacks, we leave this investigation, and a rigorous proof, as interesting future work. However our analysis in the previous sections for collective attacks should be immediately applicable to that case. We further comment that our results in the previous sections are also applicable if one wished to perform a finite key analysis using methods in [35] for which collective attacks are commonly assumed.

4.3 Evaluation

Note that the above security analysis and bound of $S(A|E)$ and $H(A|B)$, would hold for an arbitrary quantum channel; one need only observe those values listed in Table 1 in order to minimize $S(A|E)$ as described in the previous section. As examples, and to compare with other protocols, we will evaluate our protocol in two different channels, commonly used in QKD protocol evaluation. These are the depolarizing channel and the amplitude damping channel. First, let's consider the depolarization channel. Given a density operator σ acting on a Hilbert space of dimension D, the depolarization channel with parameter Q, denoted here as $\mathcal{E}_Q$ acts as follows:

$$\mathcal{E}_Q(\sigma) = \left(1 - \frac{D}{D-1}Q\right)\sigma + \frac{Q}{D-1}I. \tag{32}$$

To calculate the key rate of our protocol, we calculate the required observable statistics assuming the adversary uses this channel (in particular, the statistics indexed in Table 1). These are easily found to be:

$$\begin{aligned} p_{ii} = p_{jj} = p_{\phi\phi} &= 1 - Q \\ p_{ib} = p_{jb} = p_{\phi b} &= \frac{Q}{D-1} \\ p_{i\phi} = p_{j\phi} = p_{\phi i} = p_{\phi j} &= \frac{1}{2}\Big(1 - \frac{DQ}{D-1}\Big) + \frac{Q}{D-1}. \end{aligned}$$

This is sufficient to evaluate the key rate of our protocol as shown in Figure 1. Note that, as with other high-dimensional QKD protocols, as the dimension of the system increases, the tolerance to depolarization noise also increases. In our numerical evaluations, the noise tolerance approaches 15.5% as the dimension increases thus showing that, as with other high-dimensional

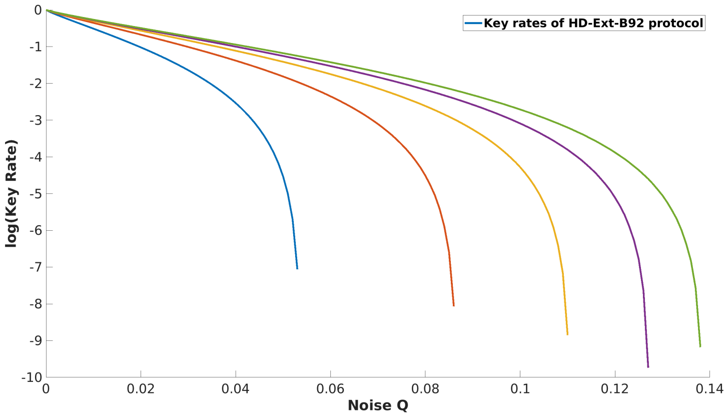

Fig. 1 The key rate of the HD-Ext-B92 protocol for various dimensions D assuming a depolarization channel. Here the dimension increases from left-to-right from $D = 2^1$ to $D = 2^5$ in powers of two. We observe numerically, as the dimension continues to increase, the noise tolerance for this channel tends towards 15.5%.

QKD protocols, the extended-B92 style scheme can also benefit from higher dimensional systems, at least against this particular channel type.

We also compare with the HD-BB84 protocol [36] which we now state for completeness. Similar to the qubit case, the qudit based HD-BB84 uses two bases, namely, the computational basis $Z = \{|0\rangle, |1\rangle, ..., |D-1\rangle\}$ and another basis denoted by X where $X = \{|x_0\rangle, |x_1\rangle, ..., |x_f\rangle\}$. We assume the two bases are mutually unbiased. Alice sends basis states from these two bases and Bob measures in X or Z. If both parties chose the Z basis, the result is used for their raw key; otherwise, if both parties choose the X basis, they use this to measure the noise in the quantum channel. The unconditional security of this protocol has been proven [37,38]. An entropic uncertainty relation presented in [39] can be used to easily derive the following asymptotic key rate r for HD-BB84 assuming a depolarization channel with a noise parameter Q. The final equation reads:

$$r = \log D - 2(H_2(Q) + Q\log(D-1)),$$

The result of this comparison is presented in Figure 2. As expected, BB84 outperforms our protocol. However, this is not surprising as BB84 at the qubit level also outperforms the B92 and Extended B92 protocol. Furthermore, our high-dimensional protocol is not even utilizing two complete bases as HD-BB84 does; instead, we are using a weak version where Alice need only send three states and Bob need only perform partial measurements in the second basis. Note also that we did not choose an optimal basis choice and, indeed, alternative encoding selections for the X state may lead to higher key rates for our HD-Ext-B92 protocol as demonstrated at least for the qubit case [8, 21].

Another channel of interest is the amplitude damping channel. Our primary curiosity of analyzing our protocol in this channel stems from the fact that

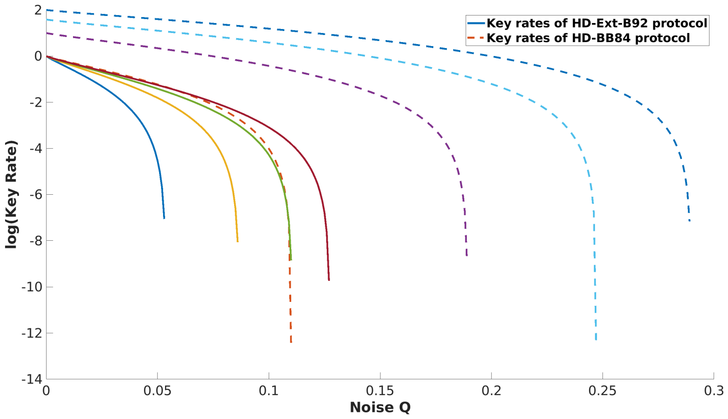

Fig. 2 key rate comparison between our HD-Ext-B92 protocol (solid lines) and the HD-BB84 protocol (dashed lines). Here the dimension for each protocol line individually increases left-to-right from $D = 2^1$ up to $D = 2^4$. Note that for $D = 2^1$, HD-BB84 has a noise tolerance of 11% (as expected since, in that case, it is standard BB84) while the HD-Ext-B92 protocol does not attain that level of noise tolerance until $D = 2^3$. See text for further discussion.

we suspected that in some channels, the choice of public parameters i, j may not be trivial. This channel confirmed our suspicion on which we elaborate a bit later. Amplitude damping channel is used in physics to model energy dissipation and in quantum information, it can be used to model low-noise scenarios [40]. It has seen usage in QKD context in [41,23], for teleportation in [42] and for error correcting codes in [43]. This channel can be described its Kraus operators:

$$E_0 = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \sqrt{1-p} & 0 & \cdots & 0 \\ 0 & 0 & \sqrt{1-p} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \sqrt{1-p} \end{pmatrix} \tag{33}$$

and:

$$E_1 = \begin{pmatrix} 0 & \sqrt{p} & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}, \cdots, E_{D-1} = \begin{pmatrix} 0 & 0 & 0 & \cdots & \sqrt{p} \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{34}$$

As before, we can compute those observable parameters in Table 1 under this channel and then use our analysis in the previous section to derive a lower-bound on the key rate of our protocol. We can see that the key rate of our protocol can vary significantly with the choice of basis states, in particular the distinguished $|i\rangle$ and $|j\rangle$ as shown in Table 2. Since these are set by the users, they may choose basis states based on the channel properties to maximize the key rate.

Table 2 Key rates for high-dimensional extended B92 protocol with $D = 4$ and different choices of $|i\rangle$ and $|j\rangle$ under an amplitude damping channel with parameter $p = .08$.

$\|\phi\rangle = \frac{1}{\sqrt{2}}(\|i\rangle + \|j\rangle)$	key rate
$\|i\rangle = \|0\rangle, \|j\rangle = \|1\rangle$	.85
$\|i\rangle = \|0\rangle, \|j\rangle = \|2\rangle$	.85
$\|i\rangle = \|1\rangle, \|j\rangle = \|2\rangle$	.29
$\|i\rangle = \|1\rangle, \|j\rangle = \|3\rangle$	.29

5 Closing Remarks

In this work, we have presented the usage of high-dimensional quantum systems as communication resources between Alice and Bob in the extended B92 protocol, originally introduced in [8] for qubits. When extending that protocol to higher dimensions we took care to attempt to minimize the quantum resources used by parties. In particular, our protocol only requires Alice to send three different states while Bob need only perform partial measurements.

We performed an information theoretic security analysis against collective attacks and evaluated under two different channels, the depolarization channel and the amplitude damping channel. We showed that, as with other high-dimensional protocols, under a depolarization channel the noise tolerance tends to increase with the dimension of the system. For the HD-Ext-B92 protocol, this tolerance eventually converges to 15.5% (as observed by our numerical computations). Under an amplitude damping channel, we showed how the choice of basis states used can greatly affect the key rate of the overall protocol.

Perhaps the biggest open question at the moment is to determine the effects of alternative superposition states on the protocol. We only considered a state of the form $\frac{1}{\sqrt{2}}|i\rangle + \frac{1}{\sqrt{2}}|j\rangle$. One obvious candidate to consider would be the effect of having Alice send an equal superposition state. Unfortunately, the security analysis of such a protocol proved to be highly difficult, especially when using the technique of mismatched measurements (as we used here). The analysis might be simplified by having Alice send complete basis states instead of only a small subset of basis states in which case alternative proof methods may be applied. We leave this interesting question as future work. We also only performed an asymptotic key rate analysis - performing a finite key analysis, taking into account also, perhaps, less ideal measurement devices, would also be interesting to consider.

Acknowledgements HI and WOK would like to acknowledge support from NSF grant number 2006126.

References

1. Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175. New York, 1984.

2. Stefano Pirandola, Ulrik L Andersen, Leonardo Banchi, Mario Berta, Darius Bunandar, Roger Colbeck, Dirk Englund, Tobias Gehring, Cosmo Lupo, Carlo Ottaviani, et al. Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4):1012–1236, 2020.
3. Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009.
4. Akshata Shenoy-Hejamadi, Anirban Pathak, and Srikanth Radhakrishna. Quantum cryptography: Key distribution and beyond. *Quanta*, 6(1):1–47, 2017.
5. Charles H Bennett. Quantum cryptography using any two nonorthogonal states. *Physical review letters*, 68(21):3121, 1992.
6. Kiyoshi Tamaki, Masato Koashi, and Nobuyuki Imoto. Unconditionally secure key distribution based on two nonorthogonal states. *Physical review letters*, 90(16):167904, 2003.
7. Ryutaroh Matsumoto. Improved asymptotic key rate of the b92 protocol. In *2013 IEEE International Symposium on Information Theory*, pages 351–353. IEEE, 2013.
8. Marco Lucamarini, Giovanni Di Giuseppe, and Kiyoshi Tamaki. Robust unconditionally secure quantum key distribution with two nonorthogonal and uninformative states. *Physical Review A*, 80(3):032327, 2009.
9. Omar Amer and Walter O Krawec. Finite key analysis of the extended b92 protocol. In *2020 IEEE International Symposium on Information Theory (ISIT)*, pages 1944–1948. IEEE, 2020.
10. Daniele Cozzolino, Beatrice Da Lio, Davide Bacco, and Leif Katsuo Oxenløwe. High-dimensional quantum communication: Benefits, progress, and future challenges. *Advanced Quantum Technologies*, 2(12):1900038, 2019.
11. Helle Bechmann-Pasquinucci and Wolfgang Tittel. Quantum cryptography using larger alphabets. *Physical Review A*, 61(6):062308, 2000.
12. Hoi Fung Chau. Unconditionally secure key distribution in higher dimensions by depolarization. *IEEE Transactions on Information Theory*, 51(4):1451–1468, 2005.
13. Lana Sheridan and Valerio Scarani. Security proof for quantum key distribution using qudit systems. *Physical Review A*, 82(3):030301, 2010.
14. Chrysoula Vlachou, Walter Krawec, Paulo Mateus, Nikola Paunković, and André Souto. Quantum key distribution with quantum walks. *Quantum Information Processing*, 17(11):1–37, 2018.
15. Toshihiko Sasaki, Yoshihisa Yamamoto, and Masato Koashi. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature*, 509(7501):475–478, 2014.
16. Fumin Wang, Pei Zeng, Jiapeng Zhao, Boris Braverman, Yiyu Zhou, Mohammad Mirhosseini, Xiaoli Wang, Hong Gao, Fuli Li, Robert W Boyd, et al. High-dimensional quantum key distribution based on mutually partially unbiased bases. *Physical Review A*, 101(3):032340, 2020.
17. Nurul T Islam, Charles Ci Wen Lim, Clinton Cahall, Jungsang Kim, and Daniel J Gauthier. Provably secure and high-rate quantum key distribution with time-bin qudits. *Science advances*, 3(11):e1701491, 2017.
18. Jacob Mower, Zheshen Zhang, Pierre Desjardins, Catherine Lee, Jeffrey H Shapiro, and Dirk Englund. High-dimensional quantum key distribution using dispersive optics. *Physical Review A*, 87(6):062322, 2013.
19. Beatrice Da Lio, Daniele Cozzolino, Nicola Biagi, Yunhong Ding, Karsten Rottwitt, Alessandro Zavatta, Davide Bacco, and Leif K Oxenløwe. Path-encoded high-dimensional quantum communication over a 2 km multicore fiber. *arXiv preprint arXiv:2103.05992*, 2021.
20. Catherine Lee, Darius Bunandar, Zheshen Zhang, Gregory R Steinbrecher, P Ben Dixon, Franco NC Wong, Jeffrey H Shapiro, Scott A Hamilton, and Dirk Englund. Large-alphabet encoding for higher-rate quantum key distribution. *Optics express*, 27(13):17539–17549, 2019.
21. Walter O. Krawec. Quantum key distribution with mismatched measurements over arbitrary channels. *Quantum Information and Computation*, 17(3 and 4):209–241, 2017.

22. Stephen M Barnett, Bruno Huttner, and Simon JD Phoenix. Eavesdropping strategies and rejected-data protocols in quantum cryptography. *Journal of Modern Optics*, 40(12):2501–2513, 1993.
23. Shun Watanabe, Ryutaroh Matsumoto, and Tomohiko Uyematsu. Tomography increases key rates of quantum-key-distribution protocols. *Physical Review A*, 78(4):042316, 2008.
24. Ryutaroh Matsumoto and Shun Watanabe. Key rate available from mismatched measurements in the bb84 protocol and the uncertainty principle. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 91(10):2870–2873, 2008.
25. Walter O Krawec. Asymptotic analysis of a three state quantum cryptographic protocol. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 2489–2493. IEEE, 2016.
26. Kiyoshi Tamaki, Marcos Curty, Go Kato, Hoi-Kwong Lo, and Koji Azuma. Loss-tolerant quantum cryptography with imperfect sources. *Physical Review A*, 90(5):052314, 2014.
27. Robert König and Renato Renner. A de finetti representation for finite symmetric quantum states. *Journal of Mathematical physics*, 46(12):122108, 2005.
28. Matthias Christandl, Robert König, and Renato Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Physical review letters*, 102(2):020504, 2009.
29. Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science*, 461(2053):207–235, 2005.
30. Renato Renner, Nicolas Gisin, and Barbara Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Physical Review A*, 72(1):012332, 2005.
31. Mark Fannes. A continuity property of the entropy density for spin lattice systems. *Communications in Mathematical Physics*, 31(4):291–294, 1973.
32. Koenraad MR Audenaert. A sharp continuity estimate for the von neumann entropy. *Journal of Physics A: Mathematical and Theoretical*, 40(28):8127, 2007.
33. Andreas Winter. Tight uniform continuity bounds for quantum entropies: conditional entropy, relative entropy distance and energy constraints. *Communications in Mathematical Physics*, 347(1):291–313, 2016.
34. Kiyoshi Tamaki and Norbert Lütkenhaus. Unconditional security of the bennett 1992 quantum key-distribution protocol over a lossy and noisy channel. *Physical Review A*, 69(3):032316, 2004.
35. Valerio Scarani and Renato Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Physical review letters*, 100(20):200501, 2008.
36. Nicolas J Cerf, Mohamed Bourennane, Anders Karlsson, and Nicolas Gisin. Security of quantum key distribution using d-level systems. *Physical review letters*, 88(12):127902, 2002.
37. Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000.
38. Masato Koashi. Simple security proof of quantum key distribution based on complementarity. *New Journal of Physics*, 11(4):045018, 2009.
39. Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M Renes, and Renato Renner. The uncertainty principle in the presence of quantum memory. *Nature Physics*, 6(9):659–662, 2010.
40. Jason L Pereira and Stefano Pirandola. Bounds on amplitude-damping-channel discrimination. *Physical Review A*, 103(2):022610, 2021.
41. Yongtao Zhan and Hoi-Kwong Lo. Tomography-based quantum key distribution. *arXiv preprint arXiv:2008.11628*, 2020.
42. Alejandro Fonseca. High-dimensional quantum teleportation under noisy environments. *Physical Review A*, 100(6):062311, 2019.
43. Markus Grassl, Linghang Kong, Zhaohui Wei, Zhang-Qi Yin, and Bei Zeng. Quantum error-correcting codes for qudit amplitude damping. *IEEE Transactions on Information Theory*, 64(6):4674–4685, 2018.