Security of a High Dimensional Two-Way Quantum Key Distribution Protocol

Walter O. Krawec

Two-way quantum key distribution (QKD) protocols utilize bi-directional quantum communication to establish a shared secret key. Due to the increased attack surface, security analyses remain challenging. Here a high-dimensional variant of the Ping Pong protocol is investigated and an information theoretic security analysis in the finite-key setting is performed. The main contribution in this work is to show a new proof methodology for two-way quantum key distribution protocols based on the quantum sampling framework of Bouman and Fehr introduced in 2010 and also sampling-based entropic uncertainty relations introduced by the authors in 2019. The Ping Pong protocol is only investigated here, but these methods may be broadly applicable to other QKD protocols, especially those relying on two-way channels. Along the way, some fascinating benefits to high-dimensional quantum states applied to two-way quantum communication are also showed.

1. Introduction

Quantum key distribution (QKD) allows two parties to establish a shared secret key, secured against computationally unbounded adversaries. This is in contrast to classical key distribution where computational assumptions are always required for security. Typically, QKD protocols utilize a one-way quantum channel, allowing Alice to send quantum resources to Bob. However, two-way quantum channels, allowing for bi-directional quantum communication between Alice and Bob, are also a possibility and have several exciting benefits, at least in theory, over one-way protocols. For instance, deterministic key distribution is possible along with secure direct communication[1-4] and protocols with devices restrictions, such as the so-called “semi-quantum” model of cryptography[5-9] (note that not all two-way QKD protocols contain all these advantages—we are simply discussing some of the advantages this communication model can provide). Experimental implementations of such protocols are also possible.[10-13] They are also interesting in their own way as they show how alternative methods, such as super dense coding (SDC)[14] can be used for QKD (as in the Ping Pong protocol[1] or its extension described in ref. [2]). Certain fiber implementations also may benefit from two-way quantum communication as polarization drift can be compensated for in the return channel.[15,16]

Naturally, there are also disadvantages to such two-way systems, in particular when considering photon loss over fiber (as a signal must now travel twice as long) or side-channel attacks against devices. Furthermore, the two-way channel introduces a second opportunity for Eve to attack each quantum signal making security analyses very difficult in general. Thus, from a practical perspective, two-way QKD may not always be ideal when compared to standard BB84. Despite this, the study of two-way QKD protocols is still of importance for a variety of reasons: first, they can exhibit, as mentioned, several advantages over one-way protocols (at least in theory) and, second, and in our opinion more importantly, their study may lead to breakthroughs in other fields of quantum cryptography and quantum information science (e.g., in new proof techniques, protocol design methods, or countermeasures to noisy channels). See[17-19] for general surveys of QKD, both theory and practice.

QKD protocols relying on a two-way channel are arguably not as well understood as their one-way counterparts, especially in the practical finite-key setting. One of the most powerful methods of proving QKD security is to reduce a protocol to an equivalent entanglement based version and then utilize entropic uncertainty.[20-25] However, these methods typically cannot be applied directly to two-way protocols due to the ability for an adversary to interact twice with a quantum signal (with the second attack perhaps depending on the first attack and the receiving party’s actions). Typical reduction based proofs to entanglement based protocols simply do not work for the most part.

Rather interestingly, in ref. [16] a method for reducing certain types of two-way protocols to equivalent entanglement based versions was shown (thus allowing for the use of entropic uncertainty to derive key-rates and prove security). However, that result only applied to protocols which held a certain symmetry property which not all do. In such a protocol, Eve would prepare a tripartite state, sending part to Alice, part to Bob, and keeping part for herself, concluding the quantum communication stage of the protocol. However, this symmetry property, needed for results in ref. [16] to be applicable, does not always hold, especially for protocols where users are restricted in some way (e.g., they have measurement/preparation limitations as with the protocol we consider in this work). Thus, it is important to develop alternative techniques to handle such scenarios.

W. O. Krawec
Department of Computer Science and Engineering
University of Connecticut
Storrs, CT 06269, USA
E-mail: walter.krawec@uconn.edu; walter.krawec@gmail.com

The ORCID identification number(s) for the author(s) of this article can be found under https://doi.org/10.1002/qute.202200024
DOI: 10.1002/qute.202200024
In this paper, we analyze a two-way protocol based on the Ping Pong protocol introduced in ref. [1]. At a high level, this protocol involves Alice creating a Bell pair \( |\psi\rangle = \frac{1}{\sqrt{2}}((00) + (11)) \) and sending one particle to Bob while keeping the other private. Bob will then encode his key-bit on the qubit by either performing an identity operator (if his key-bit is zero) or a phase flip \( \sigma_z \) (if his key-bit is one). On return, Alice will measure in the Bell basis to determine the key-bit. Obviously if this were the entirety of the protocol it would be completely insecure; thus Alice and Bob must perform suitable checks by measuring in alternative bases to guarantee security. Interestingly, an extended version of this, using the full super-dense-coding (SDC) protocol was discussed in ref. [2].

In this work, we consider a high-dimensional variant of the Ping Pong protocol introduced in ref. [26]. However, we consider a restricted version of this protocol. The protocol we consider in this work is more similar to the original Ping Pong protocol in that it does not fully utilize all possible SDC encodings however, in doing so, it also significantly simplifies the measurement capabilities needed by users (especially as the dimension increases). This makes it potentially easier to implement in practice, and also introduces some interesting theoretical problems and insights. For instance, we show later that the noise tolerance of the Ping Pong protocol and the more complicated SDC protocol in ref. [2] are identical in the qubit case. The noise tolerance of both also matches that of BB84 in the qubit case. However as the dimension increases, high-dimensional BB84 (HD-BB84) always outperforms the two-way protocol we analyze here (in stark contrast to the qubit case).

Since the protocol we analyze does not contain the necessary symmetry property for results in ref. [16] to be applied, we are also forced to use alternative methods to prove security. We develop an alternative approach, based on the framework of quantum sampling by Bouman and Fehr [28] and our recent proof methods for sampling based entropic uncertainty [29] to compute the quantum min entropy needed to evaluate finite key-rates. We also consider the case of imperfect measurement devices and lossy channels. Our proof of security may be highly beneficial to other QKD protocols. To our knowledge, we are the first to derive a rigorous finite key analysis for this high-dimensional two-way protocol (the qubit case was analyzed in ref. [30]). Note that our proof also covers the qubit case, thus giving an alternative proof of security for the original qubit-based Ping Pong protocol.

We make several contributions in this work. Perhaps most importantly, we develop a proof of security in the finite-key setting for general attacks, in both the ideal device scenario and the non-ideal device scenario (including lossy channels and imperfect detectors). Our main results are described in Theorems 2 and 3. In particular, we prove that the secret key size of the protocol may be bounded by

\[
\ell = n \left( \log_2 d - \frac{H_d(Q + \delta)}{\log_2 2} \right) - 1 \text{eak}_{\text{EC}} - 2 \log \frac{1}{\epsilon}
\]  

(1)

where \( n \) is the number of signals sent that are not used for testing; \( d \) is the dimension of a single round’s signal state; \( 1 \text{eak}_{\text{EC}} \) is the amount of information leaked during error correction; and \( Q + \delta \) is a function of the observed noise in the channel along with finite sampling imprecision.

Our proof method may be applicable to other QKD protocols (both one way and two-way) where standard tools cannot be directly applied, thus giving new mathematical tools for other researchers to utilize when proving other protocols secure. Finally, we perform a rigorous analysis of our resulting key-rates for various dimensions, showing some fascinating properties of the protocol as the dimension of the quantum signal increases. High-dimensional quantum states have been shown to be very beneficial to various QKD protocols [27,31–41] (see [42] for a recent survey on high-dimensional quantum communication); we show in this work more evidence that they can also benefit two-way protocols in the finite key setting (though not to the same extent as in one-way protocols as our evaluations show). Though the protocol we analyze does not outperform BB84 in the evaluation settings we consider (which is not surprising), the development of new mathematical tools to prove QKD protocols secure, and the study of alternative protocols in general, is still an important task.

2. Notation and Definitions

We begin by introducing some notation and preliminary concepts which we will use throughout this paper. We use \( A_i \) to denote an alphabet of \( d \) characters which has a distinguished 0 character. Without loss of generality, we simply assume \( A_i = \{0, 1, \ldots, d - 1\} \). Given a word \( q \in A_i^n \) and a subset \( t \subset \{1, \ldots, n\} \), we write \( q_t \) to mean the substring of \( q \) indexed by \( t \), namely: \( q_t = q_{t_1} q_{t_2} \cdots q_{t_r} \). We write \( q_\sim \) to mean the substring indexed by the complement of \( t \). We use \( H_\delta \) to denote a \( d \)-dimensional Hilbert space.

We use \( w(q) \) to mean the relative Hamming weight of \( q \) defined to be: \( w(q) = \frac{|\{|1 \leq i \leq n; q_i = 0\}|}{|\{i \leq n\}|} \). Given \( x, y \in A_i^n \), we use \( \Delta(x, y) \) to be the Hamming distance between words \( x \) and \( y \), namely \( \Delta(x, y) = |\{i \leq n; x_i \neq y_i\}| \). Finally, let \( \delta \geq 0 \), then, given two real numbers \( x, y \), we write

\[
x \sim y \iff |x - y| \leq \delta.
\]  

(2)

Given a density operator \( \rho_{AB} \) acting on some Hilbert space \( \mathcal{H}_k \otimes \mathcal{H}_k \), we write \( \rho_{AB} \) to mean the state resulting from tracing out the A system, namely \( \rho_{AB} = \text{tr}_A \rho_{AB} \), similarly for the other system. The conditional quantum min entropy [43] is defined to be

\[
H_{\infty}(A|B)_\rho = \sup_{\sigma_A} \{ \lambda \in \mathbb{R} : 2^{-\lambda} I_k \otimes \sigma_A - \rho_{AB} \geq 0 \}
\]  

(3)

where \( X \geq 0 \) implies \( X \) is positive semi-definite. When the B system is trivial, it is not difficult to see that

\[
H_{\infty}(A)_\rho = -\log_2 \max\{ \lambda : \lambda \text{ is an eigenvalue of } \rho_A \}
\]  

(4)

The smooth conditional min entropy is defined to be [43]  

\[
H_{\infty}^*(A|B)_\rho = \sup_{\sigma_A \in \mathcal{B}_k} H_{\infty}(A|B)_\sigma
\]  

(5)

where \( \mathcal{B}_k \) is the set of \( k \)-qubit states and \( ||X|| \) is the trace distance of operator \( X \).

Quantum min entropy is a highly useful quantity to measure in quantum cryptography as it is directly related to the number of uniform independent random bits that may be extracted
Lemma 1. Let \( \omega \) we proved in ref. [44]; here we generalize the result to a broader range of applications:

where the probability is over the random variable \( X \). Note that the \( \tau \) system may be trivial if not needed; however it may be used to represent, for instance, additional seed randomness needed by \( F \).

Proof. Since CPTP maps do not increase trace distance, we have

Thus, to determine the final size of the secret key following the process, consisting of hashing the classical \( A \) register using a universal hash function with output size \( t \) bits resulting in final entropic uncertainty relations [29,44]. We review the terminology and concepts from ref. [28] in this section, making some generalizations.

Fix an alphabet \( \mathcal{A}_d \) and a number \( N > 1 \). We define a classical sampling strategy as a triple \((P_t,g,r)\) where \( P_t \) is a probability distribution over all subsets of \( \{1,\ldots,N\} \) and \( g,r : \mathcal{A}_d^N \rightarrow \mathbb{R} \). The function \( g \) is a "guessing function" while the function \( r \) is a "target function." At a high-level, a sampling strategy chooses a random subset \( t \), observes a portion of some word \( q \in \mathcal{A}_d^t \) indexed by \( t \) (that is, observes \( q_t \)), and, using this observation, tries to guess at the value of the target function evaluated on the unobserved portion \( q_{t^c} \).

Later, we will prove security of the protocol under investigation by considering an "ideal" state that is \( \epsilon \) close to a real state, on average over a separate, classical, subsystem. The following lemma will allow us to argue about the entropy in the real state assuming one can bound the entropy of the ideal state under all possible classical outcomes. This lemma is a generalization of something we proved in ref. [44]; here we generalize the result to a broader range of applications:

Lemma 1. Let \( \rho, \sigma, \) and \( \tau \) be three quantum states such that \( \frac{1}{\epsilon} \| \rho - \sigma \| \leq \epsilon \). Let \( F \) be a CPTP map such that

Then, it holds that

\[
\Pr\left( H_{\infty}^{2/3}(A|E)_{\rho^{[t]}} \geq H_{\infty}(A|E)_{\rho^{[t]}} \right) \geq 1 - 2\epsilon^{1/3}
\]
More formally, given some word \( q \in \mathcal{A}_d^N \), the strategy consists of the following process: first, sample a subset \( t \) according to \( P_t \). Next, given the observation \( q \), i.e., given the actual value of \( q \) on subset \( t \), evaluate \( g(q) \) to produce a "guess" as to the value of \( r(q) \). The guess (using only the observed portion) should be close to the actual target evaluation (of the unobserved portion) with high probability. In particular, for a good sampling strategy, it should be that, with high probability over the subset choice, one has \( g(q) \sim \varepsilon \), \( r(q) \). As an example, one may take \( g(x) = r(x) = w(x) \). In this case, the sampling strategy attempts to guess at the relative Hamming weight in the unobserved portion of some string and the guess is simply the relative Hamming weight of the observed portion.

To define the error probability of a sampling strategy, first fix \( \delta > 0 \) and some subset \( t \). Then we define the set of "good" words in \( \mathcal{A}_d^N \) to be

\[
\mathcal{G}_{\varepsilon, \delta} = \{ q \in \mathcal{A}_d^N : r(i) \sim \varepsilon g(i) \}
\]

(17)

Notice that this set consists of all words in the alphabet such that the guess function, given some observed portion of the word, produces a \( \delta \)-close guess at the target function in the unobserved portion for the fixed subset \( t \). Namely, this set consists of all words for which the sampling strategy is guaranteed to work assuming the given subset \( t \) was actually chosen. The error probability of the given classical sampling strategy, then, is defined to be

\[
\varepsilon^\delta_{\varepsilon} = \max_{q \in \mathcal{A}_d^N} \Pr (q \notin \mathcal{G}_{\varepsilon, \delta})
\]

(18)

where the probability is over all subsets \( t \) chosen according to \( P_t \). The "cl" superscript is used to indicate that this is the failure probability of a "classical" sampling strategy. It is easy to see that, given a word \( q \in \mathcal{A}_d^N \), the probability that the sampling strategy fails to produce a \( \delta \)-close guess at the target value for this particular word is at most \( \varepsilon^\delta_{\varepsilon} \).

As an example, one very natural sampling strategy was already hinted at. Let \( g(x) = r(x) = w(x) \), the relative Hamming weight of \( x \). Let \( P_t \) be the uniform distribution over all subset of size \( m \) for some fixed \( m \). Then, in this case the set of good words is simply

\[
\mathcal{G}_{\varepsilon, \delta} = \{ q \in \mathcal{A}_d^N : w(i) \sim \varepsilon w(i) \}
\]

(19)

that is, the set of all words where the relative Hamming weight in the observed portion is \( \delta \)-close to the weight in the unobserved portion. A simple expression for \( \varepsilon^\delta_{\varepsilon} \), as a function of \( \delta, N, \) and \( m \) was found in ref. [28].

Quantum Sampling: To translate these notions into a quantum sampling strategy, fix an orthonormal basis \( \{ |0 \rangle, \ldots, |d-1 \rangle \} \) of the \( d \)-dimensional Hilbert space \( \mathcal{H}_d \). This basis may be arbitrary. Now, consider some quantum state \( |\psi \rangle \in \mathcal{H}_d^N \otimes \mathcal{H}_E \) living in some \( d^N \) dimensional Hilbert space (namely living in a Hilbert space consisting of \( N \)-tensor copies of a \( d \)-dimensional space) and potentially entangled with some environment system \( E \) (which, later, when we consider cryptographic applications, will actually be an adversarial system). The strategy will choose a random subset \( t \) according to \( P_t \) and measure those \( d \)-dimensional systems indexed by \( t \) in the given basis. This produces a classical outcome \( q_t \in \mathcal{A}_d^N \) along with a post-measured quantum state

\[
|\psi^t \rangle \in \mathcal{H}_d^N \otimes \mathcal{H}_E.
\]

The question, then, is what can we say about the structure of this post-measured state? The main result from ref. [28] shows that this post-measured state behaves with high-probability like a superposition of states that are \( \delta \)-close in target-value to the observed \( q_t \) (with respect to the given guess function, namely \( g(q_t) \)). This is all, of course, with respect to the given arbitrary basis. The probability this fails is directly related to the failure probability of the classical strategy.

To formalize this, consider \( \text{span}(\mathcal{G}_{\varepsilon, \delta}) \) defined to be

\[
\text{span}(\mathcal{G}_{\varepsilon, \delta}) = \text{span}\{ |q \rangle : q \in \mathcal{G}_{\varepsilon, \delta} \}
\]

(20)

where \( |q \rangle = |q_1 \rangle \otimes \cdots \otimes |q_N \rangle \) (again, where each \( |q_i \rangle \) is with respect to the given, but arbitrary, orthonormal basis). Similar to how \( \mathcal{G}_{\varepsilon, \delta} \) represents the set of classical "good" words, a state \( |\phi \rangle \) living in the above spanning set will be called an ideal quantum state. It is one where sampling in the given basis is guaranteed to produce a collapsed state that acts in a well behaved and understood manner, if using fixed subset \( t \). In particular, given \( |\phi \rangle \in \text{span}(\mathcal{G}_{\varepsilon, \delta}) \otimes \mathcal{H}_E \) (where the \( E \) system may be arbitrarily entangled with the \( A \) portion), if the \( A \) portion, indexed by fixed subset \( t \), is measured in the given basis resulting in outcome \( x \), then it is guaranteed that the unmeasured portion of the state collapses to a superposition of the form

\[
|\phi(x) \rangle = \sum_{i \in \mathcal{J}_x} \alpha_i |i \rangle \otimes |E_i \rangle
\]

(21)

where \( \mathcal{J}_x \) is a collection of ideal states \( |\phi_i \rangle \), indexed over all subsets \( t \) with \( P_t(t) > 0 \), such that

1) Each ideal state lives in the spanning set of good classical words, namely \( |\phi_i \rangle \in \text{span}(\mathcal{G}_{\varepsilon, \delta}) \otimes \mathcal{H}_E \).

2) On average over all ideal states, the resulting system is \( \sqrt{\varepsilon^\delta_{\varepsilon}} \) close to the given input state, namely

\[
\frac{1}{2} \left| \left| \sum_i P_t(t) |t \rangle \otimes (|\psi_i \rangle \langle \psi_i^t | \otimes |\phi_i \rangle \langle \phi_i |) - |\phi \rangle \langle \phi | \right| \right| \leq \varepsilon^\delta_{\varepsilon}
\]

(22)

Note that the above theorem is a slight rewording of the result in ref. [28]. For a proof that this version follows from results in ref. [28], see our work in [45]. Ultimately, the above theorem says that, given some quantum state \( |\psi \rangle \) (perhaps produced by some cryptographic protocol), instead of having to analyze \( |\psi \rangle \) directly, we may instead define "ideal states." These ideal states behave nicely when sampling is performed and, furthermore, their post-measured state may be described with high detail allowing one to better analyze, say, the min entropy of the resulting state. In general, once the ideal state is analyzed, one may then promote the analysis to the full case using a probabilistic argument (such as in Lemma 1).
To use Theorem 1, one must first define a sampling strategy which, thus, defines a set $G_{\delta}$. From this, if one knows the error probability of the classical sampling strategy, Theorem 1 may be used to “promote” the strategy to a quantum one acting on superposition states.

In our protocol analysis, we will require the following natural two-party sampling strategy. Given a word $(x, y) \in A_N^y \times A_N^x$, with $N = n + m$, a subset $t \subseteq \{1, \ldots, N\}$ of size $m$ is chosen uniformly at random. We are then given observation $(x_t, y_t)$. The target function is the Hamming distance of $x_t$ and $y_t$, namely: $d(x_t, y_t) = \Delta_{1}(x_t, y_t)$. The guess function is the Hamming distance of the observed strings, namely: $g(x_t, y_t) = \Delta_{1}(x_t, y_t)$. In particular, this strategy observes the $t$ portion of both $x$ and $y$ and guesses that the Hamming distance in the unobserved portion is $\delta$-close to the Hamming distance of the observed strings. Note that the set of good words for this strategy, therefore, is:

$$G_{\delta} = \{(x, y) \in A_N^y \times A_N^x : \Delta_{1}(x_t, y_t) \sim \Delta_{1}(x_t, y_t)\}$$

The following Lemma was proven in ref. [45]:

**Lemma 2** (From ref. [45]). Given the above sampling strategy with $m \leq n$ and $\delta > 0$, then

$$\epsilon_{\delta} \leq 2 \exp\left(-\delta^2 m(n + m)\right) m + n + 2$$

The above sampling strategy is highly useful in a two-party scenario. Alice and Bob will each hold a portion of some quantum register and will measure their respective systems in some “test” basis. The above sampling strategy, when combined with Theorem 1, allows us to say something meaningful about the post-measured state with respect to the Hamming distance of Alice and Bob’s results (also with respect to the chosen “test” basis).

**3. Protocol**

We consider a variant of the high-dimensional version of the Ping Pong protocol[26] which, as discussed in the introduction, utilizes a two-way quantum channel. We assume the dimension of a single signal state is $d \geq 2$ (when $d = 2$ we recover the original Ping Pong protocol). At a high level, the protocol involves Alice preparing a high-dimensional entangled state and sending one portion to Bob while keeping the other portion private. Bob encodes his key choice into his received particle using a simplified version of the super-dense-coding (SDC) protocol.[14] The state returns to Alice who performs a measurement to extract Bob’s key choice. Of course suitable tests must be done by both parties to ensure protection against adversaries.

The protocol is described in detail below.

**3.1. Quantum Communication Stage**

Repeat the following until a sufficiently large raw key is established:

1) Alice prepares an entangled state of the form

$$|\psi_0\rangle = \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} |a, a\rangle_{AT}$$

She keeps the $A$ register private and sends the $T$ register to Bob (note that both the $A$ and $T$ registers are each $d$-dimensional). We use “$T$” to mean the “transit” register.

2) Bob, on receipt of the signal, will choose randomly whether this round will be a Test Round (with probability $p_T$) or a Key Round (with probability $p_K = 1 - p_T$)

- **Test Round**: Bob will measure his signal in the computational $Z = \{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ basis and send his measurement result to Alice over the public authenticated channel. In this case, Alice knows Bob chose this round to be a Test Round and so she, too, will measure her $A$ register in the $Z$ basis comparing the result to Bob’s outcome. Note that in the absence of noise, these two measurement outcomes should be correlated; any discrepancy will be considered noise and will be later factored into our security analysis and key-rate derivation.

- **Key Round**: In this case, Bob will choose a random key digit $k \in A_d$ for this round and encode his choice onto the received signal in the $T$ register. This encoding is done using the unitary operator

$$U_k = \sum_{a=0}^{d-1} \exp(2\pi i k a/d) |a\rangle\langle a|$$

Bob then returns the signal (the $T$ register) to Alice.

3) Alice, on receipt of the signal from Bob, will measure both her original $A$ register, and the returned $T$ register, using POVM $\Lambda = \{\Lambda_0, \ldots, \Lambda_{d-1}\}$ where

$$\Lambda_k = \sum_a \left( \sum_j \exp(2\pi i k j/d) |j + a\rangle\langle j + a| \right)$$

and where $P(z) = z^d$. Notice that, in the event of no noise, if Bob chose to encode a particular $k \in A_d$, then Alice will observe POVM element $\Lambda_k$ with probability one.

4) The above process repeats $N$ times, for $N$ sufficiently large. Each round that is not a Test Round will contribute log $d$ bits to the users’ raw keys.

**3.2. Classical Post-Processing Stage**

Alice and Bob will run a standard error correction protocol and privacy amplification protocol to establish their final secret key of size $\ell$-bits. Later, we compute a bound on $\ell$ based on the observed noise in the quantum channel.

It is not difficult to see that the above protocol is correct as it is based on a simplified version of the high-dimensional SDC protocol.[14] Note that, the main operational difference between our protocol and that of ref. [26] is that Bob has fewer encoding options with our protocol—this decreases the overall efficiency of the protocol compared to the original, but also decreases user’s complexity (interestingly, if Bob were to have more encoding options, he would also have to do more test measurements, besides $Z$, to ensure the fidelity of the state sent from Alice). Thus, though we limit the transmission rate below what is theoretically possible by creating this $d^2$ state, we also only require Bob to measure in the $Z$ basis as opposed to a number of bases scaling with
the dimension of the system as required in the original protocol. Depending on the physical encoding system used (e.g., time bin encoding\(^{[46]}\) which is a useful encoding method for high-dimensional quantum cryptography\(^{[47-49]}\)), this can greatly simplify Bob’s device requirements. It also simplifies Alice’s device as she must only measure in two bases.

To analyze the security of this protocol in the finite key setting, we will actually consider a slightly modified version where we allow Eve to prepare the initial signal state. In particular, Eve will prepare a quantum state \(|\psi\rangle_{AT}\) where the A and T registers each live in a Hilbert space of dimension \(d^n\), where \(d\) is the dimension of a single round’s signal state and \(N\) is the total number of rounds used in the protocol (a parameter that may be optimized by the users Alice and Bob). Note that we make no assumptions on this state other than the dimension of the A and T portions. The A register is given to Alice and the T register is given to Bob. Ideally, the state prepared should be \(N\) copies of Equation (25), unentangled with Eve’s ancilla. However, we allow Eve to have the capability of general coherent attacks and she may prepare any arbitrary quantum state for all \(N\) rounds initially.

Alice and Bob next choose a random subset \(t\) of size \(m \leq N/2\) where \(m\) is another parameter that users may optimize over (these will be the test rounds). This process may be done by having Bob choosing the subset and sending it to Alice over the authenticated channel; or if \(m\) is small enough, it may be produced using a small pre-shared secret key. We assume the former option but our proof works in the second scenario simply by subtracting \(\log_2 \binom{N}{m}\) bits from our final derived secret key \(\epsilon\). On this test subset, Alice and Bob measure their signals in the Z basis recording the result as \(q_a\) and \(q_b\). Both parties send their measurement outcomes to each other over the authenticated channel allowing them to compute \(\Delta_{at}(q_a, q_b)\). Note that, if Eve were honest and prepared the state \(|\psi_{\text{ATE}}\rangle\otimes|0\rangle_E\), it should be that \(\Delta_{at}(q_a, q_b) = 0\). Any \(\Delta_{at}(q_a, q_b) > 0\) will be considered noise and will be factored into our key-rate equation. If the noise is too high, parties will abort.

After this test, Bob will choose a random key \(K = k_1 \ldots k_n \in A^n\) where \(n = N - m\). He then applies the unitary operator \(U_K = U_{k_1} \otimes \cdots \otimes U_{k_n}\) to the remaining, unmeasured, portion of his signal received from Eve. After this, he sends his quantum state to Alice who will subsequently measure each state using POVM \(A\) producing her raw-key \(\tilde{K}\) which, in the noiseless case, should match exactly Bob’s key encoding of \(K\). Parties then run error correction and privacy amplification as before. It is not difficult to see that security of this protocol, where Eve prepares the initial state, will imply security of the desired protocol where Alice prepares the state. Note that this is not a full entanglement based protocol as it still involves two-way quantum communication and Eve still has two opportunities to attack. Nonetheless, we will show a method to prove general security in this scenario. See Figure 1 for a diagram depicting the two scenarios. The partial entanglement based protocol is summarized below:

**Quantum communication stage:**

1) Eve prepares an arbitrary initial state \(|\psi\rangle_{ATE}\) where the A and T registers are of dimension \(d^n\) each for a user-specified \(N\). Here, \(N\) is the number of rounds used. She sends the A register to Alice, the T register to Bob, and keeps the E register private.

2) Alice and Bob will choose a random subset \(t \subset \{1, 2, \ldots, N\}\) of size \(|t| = m < N/2\) uniformly at random from all subsets of size \(m\). This choice is made is discussed in the text. The subset \(t\) will be used to index those \(d\)-dimensional subsystems of their registers that will be used as Test Rounds.

3) Alice and Bob will measure their subsystems indexed by \(t\) in the computational Z basis resulting in outcomes \(q_a \in A^n_t\) (for Alice) and \(q_b \in A^n_{\bar{t}}\) (for Bob). Ideally, it should hold that \(q_a = q_b\).

4) For the remaining \(n = N - m\) subsystems not indexed by \(t\), Bob will choose a random key string \(K = k_{1n} \ldots k_{nn} \in A^n\), and encode his key choice into his remaining, unmeasured, system. This is done by applying unitary operator

\[
U_K = U_{k_1} \otimes \cdots \otimes U_{k_n}
\]

5) Alice, on receipt of the signal from Bob, will measure both her A register (given to her initially by Eve), and the returned T register from Bob, using POVM \(A = \{A_0, \ldots, A_{d^n-1}\}\) as in the original protocol leading to her guess of Bob’s key encoding choice. Namely, she will measure each of the \(n\) registers individually in this POVM.

**Classical post-processing stage:** Alice and Bob will run a standard error correction protocol and privacy amplification protocol to establish their final secret key of size \(\epsilon\)-bits.

### 4. Security Analysis

We now analyze the security of the partial entanglement based protocol in the finite key setting. In particular, we compute a bound on \(\epsilon\), the number of secret key bits that may be distilled from the partial-entanglement based protocol. This serves as a
lower-bound on the number of secret key bits that may be distilled from the actual prepare-and-measure protocol. Before we state our main theorem, we will require one technical lemma stated below. This lemma and its proof is similar to a result in ref. [43] however the statement is different and does not immediately follow from that prior work. Thus it is worth stating and proving here

**Lemma 3.** Consider the quantum state $\sigma_{KTE}$

$$\sigma = \sum_{k \in S^1_{A_J}} \frac{1}{d^1} |k\rangle\langle k|_K \otimes P \left( \sum_{b \in J} |\beta_b\rangle \exp(i \cdot f(b,k)) |b\rangle_T \otimes |E_b\rangle_E \right)$$  (29)

where $\beta_b \in \mathbb{C}$ satisfying $\sum_b |\beta_b|^2 = 1$; $f(b,k)$ is some arbitrary real-valued function of $b$ and $k$; and where $J \subseteq A_J^n$. Above, the states in the $E$ system are arbitrary but normalized and the dimension of the $K$ and $T$ registers are $d^1$ each. Then it holds that

$$H_{\omega}(K|E)_\sigma \geq n \log_2 d - \log_2 |J|$$  (30)

**Proof.** Given $\sigma$, we define the following mixed state

$$\chi = \sum_{k \in S^1_{A_J}} \frac{1}{d^1} |k\rangle\langle k|_K \otimes \sum_{b \in J} |\beta_b|^2 |b\rangle_T \otimes |E_b\rangle_E$$  (31)

First, note that $H_{\omega}(K|TE)_\chi = n \log_2 d$ since the $K$ and $T$ registers are separable. We now claim that $H_{\omega}(K|E)_\sigma = H_{\omega}(K|TE)_\chi - \log_2 |J|$. To prove our claim, we will use a proof technique from ref. [43] used to bound the min entropy of a superposition state.

Consider an arbitrary vector $|\zeta\rangle \in H_K \otimes H_{TE}$. We may write $|\zeta\rangle = \sum_b |\gamma_b\rangle |b\rangle_T$. Then

$$\langle \zeta | \chi \rangle^2 = \sum_b |\gamma_b|^2 \sum_{b \in J} |\beta_b|^2 \langle \psi_b | b, E_{b,\nu} \rangle^2$$  (32)

and

$$\langle \zeta | \sigma | \zeta \rangle = \sum_b |\gamma_b|^2 \sum_{b, b' \in J} \beta_b \beta_{b'}^* \exp(i f(b,k) - f(b',k)) \langle \psi_b | b, E_{b,\nu} \rangle \langle \psi_{b'} | b', E_{b',\nu} \rangle$$

$$\times \langle \psi_{b'} | b', E_{b',\nu} \rangle = \sum_b |\gamma_b|^2 \sum_{b \in J} |\beta_b|^2 \exp(i \cdot f(b,k)) \langle \psi_{b} | b, E_{b,\nu} \rangle^2$$  (33)

From the Cauchy–Schwarz inequality, it holds that

$$\langle \zeta | \chi \rangle^2 \geq \sum_b |\gamma_b|^2 \frac{1}{|J|} \sum_{b \in J} |\beta_b|^2 \exp(i \cdot f(b,k)) \langle \psi_{b} | b, E_{b,\nu} \rangle$$

$$\geq \frac{1}{|J|} \langle \zeta | \sigma | \zeta \rangle$$  (34)

Since $|\zeta\rangle$ was arbitrary, it follows that $|J| \geq \sigma$ as desired. Thus, it holds that

$$H_{\omega}(K|E)_\sigma \geq H_{\omega}(K|TE)_\sigma \geq n \log_2 d - \log_2 |J|$$  (35)

completing the proof.

With the above proven, we are ready to state and prove our main theorem involving the security of the protocol.

**Theorem 2.** Let $\epsilon > 0$, $d$, $m$, $n \in \mathbb{N}$ with $d \geq 2$ and $m < n$ be given. Consider a particular run of the protocol resulting in test outcome $q_{\lambda}$ and $q_{\delta}$. Then, except with probability $\epsilon_{\text{fail}} = 2\epsilon^{1/3}$ (where the probability is over the test subset chosen and the measurement outcomes $q_{\lambda}$ and $q_{\delta}$), the two-way QKD protocol produces a secret key of size $\epsilon$-bits that is $\epsilon_{\text{sec}} = 9\epsilon + 4\epsilon^{1/3}$ close to an ideal secret key (as defined in Equation (6)) with

$$\epsilon = n \left( \log_2 d - \frac{H_{\sigma}(q_{\lambda}, q_{\delta}) + \delta}{\log_2 d} \right) - 1 \epsilon_{\text{sec}} = 2 \log_2 1 - \epsilon$$  (36)

where $\epsilon_{\text{sec}}$ is the amount of information leaked during error correction and where

$$\delta = \sqrt{\frac{(m + n + 2) \log 2(2\epsilon^2)}{m(m + n)}}$$  (37)

**Proof.** We actually prove security of the partial entanglement-based protocol from which security of the actual prepare-and-measure protocol will follow. First, note that the sampling method used in the protocol is exactly the strategy discussed in Section 2.1 and analyzed in Lemma 2. Using this, we have $G_{\text{sec}}$ as defined in Equation (23).

Let $\gamma > 0$ be given and let $N = n + m$. Here, $N$ is the number of signals sent while $m$ is the subset size chosen for testing. Note that, from Lemma 2, this implies $\gamma^2 = \epsilon$.

Let $|\psi\rangle_{ATE}$ be the initial state $\text{Eve}$ prepares with the $A$ and $T$ registers each consisting of $N$ copies of a $d$-dimensional Hilbert space. From Theorem 1, using the sampling strategy discussed in Section 2.1, we know that there exist ideal states $|\psi\rangle$, such that $|\psi\rangle \in \text{span}(G_{\text{sec}}) \otimes H_K$ and, furthermore

$$\left\| \frac{1}{T} \sum_t |t\rangle \otimes |\psi\rangle - \frac{1}{T} \sum_t |t\rangle \otimes |\psi\rangle \langle \psi\rangle \right\| \leq \sqrt{\epsilon^2} = \epsilon$$  (38)

Above, we are defining the quantum ideal set span$(G_{\text{sec}})$ with respect to the computational basis $\{|0\rangle, \ldots, |d - 1\rangle\}$. We will first analyze the ideal state $\sigma = \frac{1}{T} \sum_t |t\rangle \otimes |\psi\rangle \langle \psi\rangle$ and later promote this analysis to the real state $|\psi\rangle\langle \psi|$ actually produced by the adversary.

4.1. Analyzing the Ideal State: Initial System

Consider $\sigma$; choosing a subset for sampling is equivalent to measuring the first register causing the state to collapse to a particular ideal state $|\psi\rangle\langle \psi|$. At this point, Alice and Bob measure their systems, indexed by $i$ in the $Z$ basis resulting in outcome $q_{\lambda}$ and $q_{\delta}$ respectively (these are $m$-character strings in some $d$-letter alphabet). Since $|\psi\rangle \in \text{span}(G_{\text{sec}}) \otimes H_K$, it is clear that, conditioning on measurement outcome $q_{\lambda}$, $q_{\delta}$, the state collapses to one of the form

$$|\psi\rangle(q_{\lambda}, q_{\delta}) = |\mu\rangle = \sum_{a,b \in Z_{(n,m)}} a_{a,b} |a, b\rangle_{AB} \otimes |\tilde{E}_{a,b}\rangle$$  (39)
where
\[ f(q_A, q_B) = \{(a, b) \in A_d^n \times A_d^n : \Delta_1(a, b) = \Delta_1(q_A, q_B)\} \]  
(40)

We may rewrite the above in the equivalent form

\[ |\mu\rangle = \sum_{a \in A_d^n} \sum_{b \in A_d^n} \alpha_{ab} |a\rangle \otimes |b\rangle |E_{a,b}\rangle \]  
(41)

with

\[ J(q_A, q_B : a) = \{ b \in A_d^n : \Delta_1(a, b) = \Delta_1(q_A, q_B)\} \]  
(42)

Note that some of the \(a\)'s and \(b\)'s appearing above may be zero.

### 4.2. Analyzing the Ideal State: Bob's Encoding

From this post measurement state, Bob will encode his key choice. He chooses a random key \( K = k_1 \cdots k_n \in A_d^n \) and applies \( U_K \) to his portion of the quantum state \( |\mu\rangle \). Let \(|\mu^K\rangle = I_a \otimes U_K \otimes I_b |\mu\rangle \). Then it is not difficult to see that:

\[ |\mu^K\rangle = \sum_{a \in A_d^n} \sum_{b \in A_d^n} \alpha_{ab} |a\rangle \otimes \beta_{ab} \exp(2\pi i b \cdot K/d) |b\rangle |E_{a,b}\rangle \]  
(43)

where \( b \cdot K = b_1 k_1 + \cdots + b_n k_n \). This entire process of \( B \) choosing \( K \) and encoding his choice onto \( |\mu\rangle \) may be described by the density operator

\[ \sum_{K \in A_d^n} \frac{1}{d^n} |K\rangle \langle K| \otimes |\mu^K\rangle \langle \mu^K|_{\text{TE}} \]  
(44)

At this point, Bob sends the T register to Alice, keeping, of course, the \( K \) register private. Eve intercepts this return signal and is allowed to probe all \( n \) of the returning qubits simultaneously with an attack which also may depend on her initial ancilla (see Figure 1). After this probe, Eve must forward an \( n \)-qubit register to Alice for her to complete the protocol. Eve’s goal is to gain information on the \( K \) register held privately by Bob. In particular, we need a bound on the min entropy \( H_{\infty}(K|E') \) of the quantum state following this probe and the forwarding of the \( n \) qubits to Alice. However, we will actually compute a bound on \( H_{\infty}(K|TE) \) before this probe and before Eve forwards an \( n \)-qubit register to Alice; from this data processing inequality, it is clear that this will serve as a lower bound for our desired \( H_{\infty}(K|E') \), namely \( H_{\infty}(K|E') \geq H_{\infty}(K|TE) \).

### 4.3. Analyzing the Ideal State: Entropy Bound

Consider \( \sigma' \) as defined above. Tracing out the \( A \) register yields

\[ \sigma'_{\text{TE}} = \sum_{s \in A_d^n} |s|^2 \times \frac{1}{d^n} |K\rangle \langle K| \otimes \prod_{b \in J(q_A, q_B : a)} \beta_{ab} \exp(2\pi i b \cdot K/d) |b\rangle |E_{a,b}\rangle \]  
(45)

From Equation (8), we have \( H_{\infty}(K|TE) \geq \min_a H_{\infty}(K|TE)_{\mu^{aE}} \). We claim that for any \( a \), it holds that

\[ H_{\infty}(K|TE)_{\mu^{aE}} \geq n \left( \log_2 d - \frac{H_{\Delta_1}(q_A, q_B) + \delta}{\log_2 2} \right) \]  
(46)

To give some intuition behind this claim, imagine the ideal case where there is absolutely no noise (thus \( b = a \) always) and no finite sampling imprecision (i.e., \( \delta = 0 \)). In this case \(|J(q_A, q_B : a)| = 1 \) which implies that \( \sigma'_{\text{TE}} \) is of the form

\[ \sigma'_{\text{TE}} = \sum_{a \in A_d^n} \frac{1}{d^n} |K\rangle \langle K| \otimes \exp(2\pi i a \cdot K/d) |a\rangle \langle a| \otimes |E_{a,a}\rangle \langle E_{a,a}| \]  
(47)

From this, it is obvious that \( H_{\infty}(K|TE) = n \log_2 d \) since the TE system is independent of the \( K \) register. Of course, this ideal case is impossible to achieve (even without noise, it would still hold that \( \delta = 0 \) in a finite key setting). However, if the noise is “small enough” then the set \(|J(q_A, q_B : a)| = 1 \) which implies that \( \sigma'_{\text{TE}} \) is of the form

\[ \sigma'_{\text{TE}} = \sum_{a \in A_d^n} \frac{1}{d^n} |K\rangle \langle K| \otimes \exp(2\pi i a \cdot K/d) |a\rangle \langle a| \otimes |E_{a,a}\rangle \langle E_{a,a}| \]  
(48)

This completes the proof.

Note that, to estimate \( 1 e_{\text{EC}} \), parties would sample their raw key error rate. This is purely a classical problem at that point and \( 1 e_{\text{EC}} \) is a quantity that may be observed directly. Later, when we evaluate, we will simulate a reasonable value for \( 1 e_{\text{EC}} \) based on the channel noise observed in the forward and reverse channel. Though since that is a purely classical process we do not elaborate further on this how is done here. Interestingly, later, when we
consider imperfect devices, the noise in both channels (forward and reverse) will be needed to bound the quantum min entropy and so will warrant further discussion later.

4.5. Evaluation

We now evaluate this protocol and compare also to high-dimensional BB84. To make a fair comparison, we will compare to two parallel copies of BB84 as was done in ref. [16] (though, there, only qubit systems were discussed); namely, we will assume that Alice and Bob are able to run two parallel “sessions” of BB84 using the two-way quantum channel thus effectively doubling the key-rate in that case. To perform a numerical comparison, we will model both channels (the “forward” channel connecting Alice to Bob and the “reverse” channel connecting Bob to Alice) as depolarization channels. Note that this assumption is not required for our security proof which works for any channel (the users must simply determine \( \Delta_i(q_a, q_b) \) and then evaluate Equation (49)). Instead, we use this assumption only to evaluate and also to compare with prior work (which often assumes depolarization channels when evaluating key-rates). A depolarization channel acting on a \( d \)-dimensional system \( \rho \) acts as follows: \( \mathcal{E} : \rho \mapsto (1 - Q) \rho + Q/dI \), where \( I \) is the \( d \)-dimensional identity operator.

We will actually consider two specific cases for the two-way quantum channel typically considered when evaluating two-way QKD protocols, namely dependent and independent channels. In the independent case, each channel is modeled as two independent depolarization channels. For the dependent case, the noise in the reverse channel may depend on the forward channel. This may arise, for instance, in certain fiber implementations, where sending a photon back along the same channel it traveled originally will “undue” some of the noise picked up in the first channel.\(^{13,16} \)

For the independent case, we may easily compute the expected error in the measurement string \( q_a \) and \( q_b \). If the initial state prepared were \( |\psi_0\rangle \) then, following the first depolarization channel, it will evolve to

\[
|\psi_0\rangle \langle \psi_0 | \mapsto (1 - Q)|\psi_0\rangle \langle \psi_0 | + \frac{Q}{d} I = \rho
\]

from which we compute \( \Delta_i(q_a, q_b) = \frac{Q}{d^2} (d^2 - d) = Q (1 - \frac{1}{d}) \). The remaining, unmeasured portions, have the key encoded into them and returned to Alice. This return operation is modeled as a second depolarization channel. If \( \rho^k \) is the result of Bob encoding key-digit \( k \) onto \( \rho \), then the state after this second depolarization channel is easily found to be in the independent case

\[
\rho_{\text{ind}}^k = (1 - Q^2)|\psi^k\rangle \langle \psi^k | + \frac{1 - (1 - Q^2)}{d^2} I
\]

where \( |\psi^k\rangle = I_a \otimes U_1|\psi_0\rangle \). In the dependent case, we take the return state to be

\[
\rho_{\text{dep}}^k = (1 - Q)|\psi^k\rangle \langle \psi^k | + \frac{Q}{d^2} I
\]

Note that, in the independent case, the noise in the reverse channel is independent of the noise in the forward channel; whereas in the dependent case, this is not true. Such scenarios can arise, as mentioned, in various fiber implementations.

Alice will then measure the two systems using POVM \( \Lambda \) leading to her guess of Bob’s encoding. Any errors here will result in leakage due to error correction which we account for by setting \( 1 + \text{err}_{\text{qc}} = 1.2H(A|B) \) and where \( H(A|B) \) may be easily computed using the computed state \( \rho^k \) above. In particular, let \( \text{Pr}(A = i | B = k)_{\text{ind}} \) be the conditional probability that, assuming Bob encoded key digit \( k \), that Alice decodes a key digit of \( i \) (in particular her \( A_i \) element clicked) in the independent channel case. From \( \rho_{\text{ind}}^k \), this is easily found to be

\[
\text{Pr}(A = i | B = k)_{\text{ind}} = \left\{ \begin{array}{ll} (1 - Q)^2 + \frac{1 - (1 - Q^2)}{d} & \text{if } k = i \\ \frac{1 - (1 - Q^2)}{d} & \text{if } k \neq i \end{array} \right. \quad (53)
\]

A similar expression may be found for the dependent case

\[
\text{Pr}(A = i | B = k)_{\text{dep}} = \left\{ \begin{array}{ll} (1 - Q) + \frac{Q}{d} & \text{if } k = i \\ \frac{Q}{d} & \text{if } k \neq i \end{array} \right. \quad (54)
\]

Of course \( \text{Pr}(B = k) = 1/d \) (in both dependent and independent cases). Consider, first, the independent case. Let \( x = (1 - Q)^2 + \frac{1 - (1 - Q^2)}{d} \) and \( y = 1 - \frac{1 - (1 - Q^2)}{d} \). Of course \( x + (d - 1)y = 1 \). Simple algebra then shows that for the independent case we have

\[
H(A|B) = H(AB) - H(B) = -\frac{1}{d} \sum_i \left( x \log \frac{x}{d} + \sum_j y \log \frac{1}{d} y \right) - \log d
\]

or\( (x + (d - 1)y) \log d - x \log x - (d - 1)y \log y - \log d
\]

\[
= -x \log x - (d - 1)y \log y.
\]

An identical expression, though changing \( x = 1 - Q + Q/d \) and \( y = Q/d \) may be found for the dependent case. This allows us to compute \( 1 + \text{err}_{\text{qc}} \) and thus evaluate \( \epsilon \) in Equation (49).

The key-rate of the protocol, for dimension \( d = 2, 4 \), and 8 is shown in Figure 2 for the dependent and independent cases. We set \( \epsilon = 10^{-36} \) thus giving both a failure probability, and an \( \epsilon \)-secret key, on the order of \( 10^{-12} \). We note that, as the dimension increases, the key rate also increases. Interestingly, this is not simply due to the fact that, as the dimension increases, the number of possible raw key digits from one signal state increases. If this were the case, running multiple parallel copies of lower dimensions would yield the same result. However, this is clearly not the case as shown in Figure 3 where we compare two parallel executions of the protocol running with \( d = 2 \) to a single execution of the protocol running with \( d = 4 \). We also note that, for higher dimensions, the number of signals needed to first achieve a positive key-rate decreases as the dimension increases. This work thus shows even more advantages to high-dimensional quantum states that cannot be achieved by simple, naive, parallel executions of a lower-dimensional protocol.

In Figure 4, we compare the key-rate of this two-way protocol to running two independent copies of (high-dimensional) BB84. For evaluating the high-dimensional BB84 key-rate we use results from ref. [50]. Interestingly, the key-rate of BB84 in the
Figure 2. Evaluating the key-rate of our protocol under a depolarization channel. Top: Assuming the forward and reverse channels are independent (thus ultimately creating additional noise in the reverse channel); Bottom: Assuming the forward and reverse channel noise is dependent. We note that as the dimension increases, the key-rate also increases and the number of signals needed before a positive key rate can be attained decreases. In both graphs, we take $Q = 10\%$.

Figure 3. Comparing the key-rate of this protocol setting $d = 4$ to two independent copies of running the protocol set at $d = 2$. Note that two copies of a 2D protocol cannot outperform the 4D version in both key-rate and also the point at which the key-rate becomes positive. Here, we have $Q = 10\%$.

qubit-case is exactly twice that of the two-way protocol (thus the advantage is only in the parallel executions of BB84 and not in the protocol itself in this ideal device scenario), yet for higher dimensions, the key-rate of BB84 is more than twice the rate of the two-way protocol analyzed here (implying BB84 as a protocol has an advantage over this two-way protocol in higher dimensions). Finally, we evaluate the key-rate of the protocol as a function of the raw key error when the number of signals is large ($N = 10^{20}$) and compare to BB84 in Figure 5. Here, the raw-key error is defined to be the probability that Alice and Bob’s key digits disagree. We note that the noise tolerance when $d = 2$ and dependent channels is identical to that of standard qubit BB84.
Comparing the key-rate of this protocol under a dependent channel assumption with two independent copies of BB84. Here, we have $d = 4$ and $Q = 10\%$. We note that, for the $d = 2$ case, the key-rate of one copy of BB84 converges to the key-rate of this two-way protocol in the dependent case. For higher dimensions, however, BB84 outperforms the two-way protocol. The graph of the independent channel case is similar, but with, as expected due to its increased noise levels, a more drastic difference between the two protocols.

Figure 4. Comparing the key-rate of this protocol under a dependent channel assumption with two independent copies of BB84. Here, we have $d = 4$ and $Q = 10\%$. We note that, for the $d = 2$ case, the key-rate of one copy of BB84 converges to the key-rate of this two-way protocol in the dependent case. For higher dimensions, however, BB84 outperforms the two-way protocol. The graph of the independent channel case is similar, but with, as expected due to its increased noise levels, a more drastic difference between the two protocols.

Figure 5. Evaluating the noise tolerance of the protocol in terms of raw key error rates (namely the probability that Alice and Bob’s key digits disagree) in the dependent case. Also comparing to HD-BB84. We note that, when $d = 2$ the noise tolerance of both protocols agree and tends toward 11\% (it is slightly lower here, due to our imperfect error correction factor of $1.2H(A|B)$; if the 1.2 is replaced with 1, both protocols achieve a noise tolerance of 11\%). For $d > 2$, BB84 outperforms.

These similarities to BB84 were discovered also in ref. [16] for the qubit case but for a more complicated two-way protocol involving four encoding operations (at the qubit level). Rather surprisingly, our work here shows that these additional encoding operations do not help the noise tolerance of this protocol in the qubit case. However, also interestingly, this similarity between BB84 and the two-way protocol here no longer holds for $d > 2$. In higher dimensions, BB84 always outperforms the two-way protocol.

Figure 5. Evaluating the noise tolerance of the protocol in terms of raw key error rates (namely the probability that Alice and Bob’s key digits disagree) in the dependent case. Also comparing to HD-BB84. We note that, when $d = 2$ the noise tolerance of both protocols agree and tends toward 11\% (it is slightly lower here, due to our imperfect error correction factor of $1.2H(A|B)$; if the 1.2 is replaced with 1, both protocols achieve a noise tolerance of 11\%). For $d > 2$, BB84 outperforms.

5. Imperfect Measurements

We now consider the case where Alice and Bob’s measurement devices are not ideal. In particular, their measurements may have inefficiencies leading to missed detections. Furthermore, we add the possibility of vacuum events (e.g., photon loss). In this case, the protocol is identical as before, except that, now, if Alice detects a vacuum when attempting to decode Bob’s key choice (either a real vacuum or a detector miss due to a low efficiency), she will signal to Bob to discard that particular round’s key digit. The detection of vacuums by Bob and Alice in the check stage will be recorded and used in estimating Eve’s uncertainty. Our contribution in this section is to derive a finite key expression for this two-way protocol under such conditions and to show how our proof method, applied in the previous section for the ideal device scenario, can be readily adapted to more complicated circumstances such as this. Finally, our method does not require
characterization of the device efficiency, thus leading to a (admittedly very) partial form of device independence on the measurement devices. This is in contrast to our work in ref. [45] for HD-BBB4 where only vacuum pulses were analyzed but detectors were perfect and fully characterized; here we tackle the more difficult problem where devices are also inefficient.

Now, Bob’s measurement may be described by the POVM $Z = \{Z_0, \ldots, Z_{d-1}, Z_{\text{vac}}\}$ where

$$Z_j = \eta[j] |j\rangle \langle j|$$

$$Z_{\text{vac}} = I - \sum_j Z_j$$

where $\eta \in [0,1]$ represents the detector’s efficiency (with $\eta = 1$ meaning perfect devices). Alice’s measurements are similarly altered from the previous version of the protocol.

We also increase the dimension of the underlying Hilbert space to $d+1$ and use $|\text{vac}\rangle$ to represent the vacuum state which satisfies $\langle \text{vac}|j\rangle = 0$ for all $j$. Note that $Z_{\text{vac}}$ will click if Eve sends a vacuum pulse (or if there is loss), however it may also click if one of the detectors which ideally would have clicked (if $\eta = 1$) missed the signal. Importantly, users cannot tell the difference between a vacuum state and a missed detection. A similar POVM may be defined for Alice (who also needs one for the key decoding measurement). Interestingly, our analysis does not require actual knowledge of $\eta$. Finally, we note that Bob’s key encoding operator leaves the vacuum state alone so that $U_0 |\text{vac}\rangle = |\text{vac}\rangle$.

To analyze this scenario, we define an extended Hamming distance function $\tilde{\Delta}_n(x, y)$ for strings $x, y \in \{0, 1, \ldots, d-1\}$.

This function will count the number of errors in the strings $x$ and $y$ while also accounting for this new additional vacuum case (denoted by the symbol “$\text{vac}$”). This function is defined as follows

$$\tilde{\Delta}_n(x, y) = \frac{1}{n} \sum_j g(x_j, y_j)$$

where:

$$g(x_j, y_j) = \begin{cases} 1 & \text{if } x_j \neq y_j, \text{ or } x_j = \text{vac}, \text{ or } y_j = \text{vac} \\ 0 & \text{otherwise} \end{cases}$$

Clearly this function $\tilde{\Delta}_n(x, y)$ is counting the number of errors in the $x$ and $y$ strings while also treating any vacuum symbol in either $x$ or $y$ as an error. For example, if $x = 0, 0, 1, 3, \text{vac}, 1, \text{vac}$ and $y = 0, 0, 2, 3, 1, 1, \text{vac}$, then $\tilde{\Delta}_n(x, y) = \frac{5}{7}$ (since the last digit, even though both are “$\text{vac}$,” counts as an error with this function) while $\Delta_n(x, y) = \frac{4}{7}$. Note that $\tilde{\Delta}_n(x, y) \geq \Delta_n(x, y)$.

Before stating and proving our main theorem, we will require the following technical lemma. This lemma provides information on the structure of the ideal state after measuring with these non-ideal POVMs.

**Lemma 4.** Let $Z$ be the POVM described in the text and $t$ some subset of $\{1, 2, \ldots, N\}$. Then consider the ideal state:

$$|\phi^t\rangle_{ABE} \in \text{span}(a, b)_{AB} : a, b \in A_{d+1}^n \text{ and }$$

$$\Delta_t(a, b) \sim \Delta_t(a, b) \otimes H_E.$$
vacuum state, users are certain of the underlying symbol measured; otherwise there is uncertainty and the symbol might have been any of the $d + 1$ characters. From this uncertainty, then, the set $J$ denotes the potential basis states that are $\delta$-close to what might have been observed if devices were ideal. Note that, if $\eta = 1$ and if there is no vacuum state, it holds that $V(q_{\alpha}, q_{\beta}) = \{(q_{\alpha}, q_{\beta})\}$ and so the state above is equivalent to the ideal case in Equation (39) as expected.

With this, we are ready to state and prove our main theorem for this section below. As with the proof of Theorem 2, we analyze the ideal states from Theorem 1 first, though our analysis is more involved in this case as we will need to consider the second attack operator this time. Note that, previously, we could ignore the second attack operator to Eve’s advantage (we computed Eve’s uncertainty before this second probe and before sending additional qubits to Alice - her second probe and transmission would only increase her uncertainty and so by ignoring this, we got a worst-case lower-bound on the key rate). Now, however, the second probe can introduce loss and, furthermore, Alice will discard all rounds where she did not detect a signal. Thus, the final raw key will be conditional, based on the observations of vacuum and, so, we can no longer ignore the second attack in this instance. Eve’s second attack can directly influence the final key beyond simply creating additional errors that are taken into account using the $\text{Leak}_{EC}$ term. See Figure 1.

**Theorem 3.** Let $\epsilon > 0$, $d, m, n \in \mathbb{N}$ with $d \geq 2$ and $m < n$ be given. Consider a particular run of the protocol resulting in test outcome $q_{\alpha}$ and $q_{\beta}$. These are strings in the set $\{0, 1, \ldots, d − 1, \text{vac}\}^{m} \cong \mathcal{A}_{d}^{m}$ where we assume the $d + 1$th character is the vacuum symbol. Also, let $\nu$ be the number of vacuum events that Alice detects in her key-round measurement. Then, except with probability $\epsilon_{\text{fail}} = 2e^{-1/(2\nu)}$ (where the probability is over the test subset chosen, the measurement outcomes $q_{\alpha}$ and $q_{\beta}$, and the number of vacuum events in Alice’s key-round measurements $\nu$), the two-way QKD protocol with imperfect measurements produces a secret key of size $\epsilon$-bits that is $\epsilon_{\text{leak}} = 9\epsilon + 4e^{1/(2\nu)}$ close to an ideal secret key (as defined in Equation (6)) with:

$$\epsilon = (n − \nu) \log_{2}d − \frac{n \log_{2}d}{\nu} + \frac{\delta}{\nu} = \text{Leak}_{EC} − 2\log_{2}d$$

where $\text{Leak}_{EC}$ is the amount of information leaked during error correction and where

$$\delta = \sqrt{\left(\frac{m + n + 2}{m(m + n)}\right) \ln(2/\epsilon^{2})}$$

This proves the scenario, we will again use Theorem 1 as before. Let $|\psi\rangle_{\text{Alice}}$ be the state produced by the source (Eve in our case), where the Alice and Bob systems consist of $N$ tensor copies of a $d + 1$ dimensional Hilbert space spanned by $\{|0\rangle, \ldots, |d − 1\rangle, |\text{vac}\rangle\}$. As we are using the same classical sampling strategy as before, by Theorem 1, there exist ideal states such that

$$|\phi\rangle \in \text{span}(\{|a, b\rangle : \Delta_{d+1}(a, b) \sim \Delta_{d+1}(a_{\text{first}}, b_{\text{last}})\} \otimes \mathcal{H}_{E})$$

where the average over all subsets is $\epsilon$-close in trace distance to the real state (we use the same $\epsilon$ as in Equation (66)). Note that, above, the strings $a$ and $b$ are in a $d + 1$ character alphabet in order to accommodate the additional vacuum state.

5.1. Ideal State Analysis: Initial State Description

Consider a particular run of the protocol on the ideal state $\sigma = \sum_{t, q_{\alpha}, q_{\beta}} |t, q_{\alpha}, q_{\beta}\rangle \langle t, q_{\alpha}, q_{\beta}|$. Let $I$ be the chosen subset and $q_{\alpha}, q_{\beta} \in \{0, 1, \ldots, d − 1, \text{vac}\}^{m}$ be the observed outcome for Alice and Bob using POVM $Z$. Note that, unlike before, we are not making an ideal basis measurement (in the basis $\{|0\rangle, \ldots, |d − 1\rangle, |\text{vac}\rangle\}$) and, so, observing a particular $q_{\alpha}$ and $q_{\beta}$ does not immediately translate to direct information on $a_{\text{Alice}}$ and $b_{\text{Bob}}$ in Equation (67). That is, unlike our earlier analysis where parties knew that $a_{\text{Alice}} = q_{\alpha}$ and $b_{\text{Bob}} = q_{\beta}$ due to them making an ideal basis measurement, the value of $a_{\text{Alice}}$ and $b_{\text{Bob}}$ cannot be directly observed; instead we must use our observation to obtain suitable constraints on what they might be. Thus, our challenge now is to use this observation to determine a “worst case” condition on the structure of the collapsed ideal state. In particular, whenever a “vacuum” is observed, Alice or Bob cannot be certain if it is due to an actual vacuum or a detector inefficiency. Thus, they must assume the worst that it could have been any of the $d + 1$ symbols. Therefore, vacuum observations lead to a significant amount of uncertainty in the final collapsed state of the ideal superposition.

More formally, consider the post-measured state after measuring $|\phi\rangle$ and observing this $q_{\alpha}, q_{\beta}$. From Lemma 4, it holds that the post-measurement state of the unmeasured photon must be of the form

$$\sigma(t, q_{\alpha}, q_{\beta}) = \sum_{\tilde{a}, \tilde{b}} p(\tilde{a}, \tilde{b} | q_{\alpha}, q_{\beta}) P(\tilde{a}, \tilde{b} | a_{\text{Alice}}, b_{\text{Bob}})$$

defined formally in Equation (60).

5.2. Ideal State Analysis: Bob’s Encoding

At this point, Bob encodes his key choice, leading to the state

$$\frac{1}{d^{m}} \sum_{k \in \mathcal{A}_{d}^{m}} |k\rangle \langle k| \otimes \left(\sum_{\tilde{a}, \tilde{b}} P(\tilde{a}, \tilde{b} | q_{\alpha}, q_{\beta}) \sum_{a, b} \exp(2\pi i (b \cdot k/d)|a, b\rangle \langle a, b| \tilde{E}_{\tilde{a}, \tilde{b}, q_{\alpha}, q_{\beta}} \right)$$

where $\tilde{E}_{\tilde{a}, \tilde{b}, q_{\alpha}, q_{\beta}}$ is a $d + 1$ dimensional Hilbert space spanned by $\{|0\rangle, \ldots, |d − 1\rangle, |\text{vac}\rangle\}$.
where
\[
J(q_{\Lambda}, \tilde{q}_{\Lambda} : a) = \{ b \in A_d^{n+1} : \Delta_k(a, b) \sim \Delta_k(q_{\Lambda}, \tilde{q}_{\Lambda}) \}
\]  
(70)

Note that, for the key encoding, we assume that it leaves the vacuum state untouched. In particular, for \(x \in \{0, \ldots, d-1\}\) and \(y \in \{0, \ldots, d-1\}\), we have
\[
U_\gamma|x\rangle = \exp(2\pi i xy/d)|x\rangle
\]  
while:
\[
U_\gamma|\text{vac}\rangle = |\text{vac}\rangle
\]  
(72)

Thus, in Equation (69), by \(b \cdot k\), for some \(b \in A_d^{n+1}\), we mean \(b \cdot k\) where \(b \in A_d^n\) is the same as word \(b\) but with every vacuum symbol replaced with a zero.

### 5.3. Ideal State Analysis: Eve’s Second Attack

At this point, the T system returns to Eve’s control. As mentioned earlier, however, it is not sufficient to compute Eve’s uncertainty holding the transit register at this point. This is due to the fact that Eve’s reverse attack is allowed to create vacuum events which will later be discarded by Alice. Thus, in a way, Eve has some control over which key bits in the \(K\) register are to be used and this must be taken into account. Before, in the ideal device case considered earlier, all key bits were used regardless of Alice’s measurement—the only effect Eve had at that point would be to increase the error rate, thus causing additional information leakage due to error correction (which is taken into account in the \(H_{akk}(v)\) term of our key-rate evaluation). Here, E’s second attack can potentially increase her information by discarding rounds strategically.

We will model Eve’s reverse attack as a unitary operation, \(U_R\), acting on all \(n\) qudits and her previous ancilla state simultaneously. Without loss of generality, the action of this operation may be written
\[
U_R|b, E_{a,b,\tilde{q},\tilde{q}_B}\rangle = \sum_{c \in A_d^{n+1}} |c\rangle|F_{a,b,c,\tilde{q},\tilde{q}_B}\rangle
\]  
(73)

where we assume the \(d + 1\)th character in \(A_d^{n+1}\) represents the vacuum state. After applying this attack operation, the state becomes
\[
\tau = \frac{1}{K} \sum_k |k\rangle \langle k| \otimes \sum_{\tilde{q}, \tilde{q}_B} p(\tilde{q}, \tilde{q}_B) \left( \sum_{a,c} \alpha_{a,b,c,\tilde{q},\tilde{q}_B}\right)_{AT} \otimes \prod_{b \in \{q_{\Lambda}, \tilde{q}_{\Lambda}\}} \beta_{a,b,\tilde{q},\tilde{q}_B} \exp(2\pi ib \cdot k/d)|F_{a,b,c,\tilde{q},\tilde{q}_B}\rangle
\]  
(74)

\[\Lambda_{\text{vac}} = I - \sum_k \Lambda_k\]
(76)

Note that, for Alice, a vacuum outcome results from either a missed detection (based on \(\eta\)) or if either or both of the A or T registers contain a vacuum state. After this measurement, Alice receives some outcome \(\bar{a} \in \{0, 1, \ldots, d-1\}\) and reports all indices where she received a vacuum state (as those will be discarded). Let \(m(\bar{a}) = m_1, \ldots, m_k\), where \(m_i\) is 1 only if the \(i\)th index of \(\bar{a}\) is a vacuum (\(m_i = 0\) otherwise). That is \(m(\bar{a})\) is the classical bit string message that Alice sends to Bob marking all rounds where she received a vacuum. Since this is a message sent on the public channel, we record it in a separate register. For any particular \(m(\bar{a})\), Bob will discard the corresponding bits of his key register. Let \(v(\bar{a})\) be the number of vacuum events in \(\bar{a}\). Thus, the state now becomes
\[
\sum_{\bar{a}} p_v(\bar{a})|\bar{a}\rangle \langle \bar{a}| \otimes r_{v(\bar{a})}
\]  
(77)

where the state \(r_{v(\bar{a})}\) is found to be (after tracing out both the A and T registers, along with the discarded key digit systems)
\[
\frac{1}{d^{v(\bar{a})}} \sum_{k \in A_d^{n+1}} |k\rangle (k) \otimes \sum_{a,b,c} [\alpha_{a,b,c,\tilde{q},\tilde{q}_B}]_{AT}^* \sum_{\{b\}} \beta_{a,b,\tilde{q},\tilde{q}_B} \exp(2\pi ib \cdot f(k, k_m, m(\bar{a}))/d)|F_{a,b,c,\tilde{q},\tilde{q}_B}\rangle
\]  
(78)

where, above, \(f\) is a function that correctly reconstructs \(k\) using \(k_m\) and \(k\), by placing the “keep” key digits \(k_j\) in the correct location relative to the “reject” digits \(k_j\); clearly this depends only on \(m(\bar{a})\).

### 5.5. Ideal State Analysis: Entropy Bound

At this point, we bound the min entropy conditioning on a particular \(t, \bar{a}, q_{\Lambda}, q_{\tilde{a}}\) outcome. We use a similar analysis method as in Section 4 to bound the min entropy (especially the use of Lemma 3). In particular, we find
\[
H_{\text{min}}(K|E) \geq (n - v(\bar{a})) \log_2 d - \max_{a \in \{q_{\Lambda}, \tilde{q}_{\Lambda}\}} \frac{n H(\Delta_k(q_{\Lambda}, \tilde{q}_{\Lambda}) + \delta)}{\log_2 d + 1}
\]
(79)

where the last inequality can be shown using the same analysis method as earlier on bounding the size of the set \(J(q_{\Lambda}, \tilde{q}_{\Lambda} : a)\).

We therefore need only to find the maximum Hamming distance of all \(q_{\Lambda}, \tilde{q}_{\Lambda} \in V(q_{\Lambda}, q_{\tilde{a}})\), given the observed \(q_{\Lambda}\) and \(q_{\tilde{a}}\). However, it is not difficult to see by the definition of \(V(q_{\Lambda}, q_{\tilde{a}})\) (Equation (61)) that this is maximized whenever we set index \(j\) of \(q_{\Lambda}\) and \(\tilde{q}_{\Lambda}\) to be different symbols every time either \(q_{\Lambda}\) or \(q_{\tilde{a}}\) is a
vacuum in index $j$. Said differently, whenever a symbol in $q_A$ is a non-vacuum, the corresponding symbol in A’s element of an entry in $V(q_A, q_B)$ must be that symbol; otherwise if it is a vacuum, the symbol can be anything, similarly for Bob. This gives an upper-bound on the size of the superposition set based only on observed parameters, thus giving a worst-case bound on the min entropy. The min-entropy can only be higher in reality (thus, the key-rate can only be better than what we derive here). We can then conclude that

$$H_{\infty}(K|E) \geq (n - \nu(\bar{a})) \log_2 d - \frac{nH_{d+1}(\bar{\Delta}_d(q_A, q_B) + \delta)}{\log_{d+1} 2} \quad (80)$$

5.6. Real State Analysis

Of course, this is only the ideal state analysis. However, by using Lemma 1, we may promote this to the real-state analysis. Let $\varepsilon_A = 9\varepsilon + 4e^{1/3}$, then, except with a failure probability of $e_{\text{fail}} = 2e^{1/3}$, the final secret key size is

$$\varepsilon = (n - \nu(\bar{a})) \log_2 d - \frac{nH_{d+1}(\bar{\Delta}_d(q_A, q_B) + \delta)}{\log_{d+1} 2} - \text{1leak}_{\text{EC}} - 2\log \frac{1}{\varepsilon} \quad (81)$$

Note that the above analysis did not take into account the actual value of $\eta$; instead any vacuum event was analyzed in a way that gave full advantage to the adversary. If $\eta$ is actually known, tighter bounds may be derived potentially. One may use a more complex sampling strategy which takes into account the number of vacuum counts, instead of treating all vacuums as errors. However, our analysis above does not require Alice and Bob to know the actual value of $\eta$ thus giving a (very partial) form of device independence in the measurement devices, though at the potential cost of decreased key-rate as parties must assume the worst always.

5.7. Evaluation

We evaluate as in the ideal case considered earlier, assuming a depolarization channel (both dependent and independent). To compute the expected observation $\bar{\Delta}_d(q_A, q_B)$, we have

$$\bar{\Delta}_d(q_A, q_B) = \frac{1}{m}(\nu(\text{vacuum symbols in } q_A, q_B)$$

$$+ \nu(\text{number of errors in remaining symbols})) \quad (82)$$

We assume for evaluation purposes the probability of a vacuum event is $\mu$ (this can be due to loss, detector inefficiencies, or both). Then, assuming a depolarization channel with parameter $Q$ (see Section 4.1), we have that

$$\bar{\Delta}_d(q_A, q_B) = \mu + (1 - \mu)Q \left(1 - \frac{1}{d}\right) \quad (83)$$

We also require an expected value for $\nu(\bar{a})$, the number of vacuum events in Alice’s second measurement. For this, we evaluate the simple case where a loss can occur either in the first channel, or, if not in the first channel, then in the second. Thus

$$\frac{1}{n} \nu(\bar{a}) = \mu + (1 - \mu)\mu \quad (84)$$

Of course, this is only for our evaluation purposes; our security proof works for any observed value of $\nu(\bar{a})$. Finally, for $\text{1leak}_{\text{EC}}$, we use the same analysis as in Section 4.1 to compute the error correction leakage. This gives us everything needed to evaluate our bound.

We evaluate the key-rate of the protocol for different values of $\mu$ (the probability of a vacuum click) in Figure 6. We observe that this protocol is highly sensitive to vacuum events, though as the dimension increases, the protocol can withstand this better. Whether this is a consequence of the protocol, or our security proof in this section not being tight, is an open question. Though we do suspect it is more a consequence of the protocol being highly sensitive to noise. Indeed, it has already been discovered that the qubit Ping Pong protocol is highly sensitive to loss by devising specific attacks\cite{51-53} (with the attack in ref. \cite{52} breaking security with only 25% loss). Our bound shows a loss tolerance much lower than this 25%, however we are also analyzing general attacks—our security analysis covers prior attacks but also new, undiscovered ones. Thus, it may in fact be the case
that this protocol is this highly sensitive to noise in the finite key setting and other countermeasures may be necessary. None the less, we have demonstrated a positive key rate is possible under general attacks with loss and that the dimension of the underlying signal can benefit key-rates under lossy channels.

6. Closing Remarks

In this paper, we considered the high-dimensional Ping Pong protocol introduced in ref. [26]. In particular, we considered a variant of the protocol placing fewer device requirements on users (thus making it potentially easier to implement in practice while also creating some interesting theoretical problems). Importantly, we derived an information theoretic security proof in the finite key setting. Our methods may be broadly applicable to other QKD protocols which are not immediately reducible to full-entanglement based versions (making standard tools difficult, or impossible, to use). For example, our proof approach may be applied to two-way protocols that do not exhibit the necessary symmetry requirements needed to use results in ref. [16] for reducing to entanglement-based versions, thus creating opportunities to analyze protocols where standard tools cannot be immediately applied. We also showed how our methods can be used to analyze imperfect detectors and lossy channels. Finally, we performed a rigorous evaluation of the protocol’s performance in a variety of dimensions and scenarios. Our work provides additional evidence, beyond that already known as mentioned in the introduction, that high-dimensional quantum states may benefit, at least in theory, quantum communication, including in the two-way case.

Several interesting problems remain open. Our proof does not require an exact characterization of the efficiency of the detectors, leading to a pessimistic key-rate bound under loss. Whether this is a consequence of our proof method in this scenario, or that the protocol itself has low loss tolerance (due in part to its two-way channel), is an open question. Also, adapting our proof to work with stronger forms of device independence could be interesting. One potential way forward there may be to consider measurement devices that are not characterized, except for their overlap (as was done in [16] for two-way qubit based protocols obeying certain symmetry properties).

Acknowledgements

The author would like to thank the anonymous reviewers and the editors for their comments which have greatly improved the quality of this manuscript. The author would like to acknowledge support from NSF grant number 2006126.

Conflict of Interest

The author declares no conflict of interest.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Keywords

quantum cryptography, quantum information theory, quantum key distribution

Received: March 6, 2022
Revised: June 6, 2022
Published online: August 7, 2022

[1] K. Boström, T. Felbinger, Phys. Rev. Lett. 2002, 89, 187902.
[2] Q.-y. Cai, B.-w. Li, Phys. Rev. A 2004, 69, 054301.
[3] M. Lucamarini, S. Mancini, Phys. Rev. Lett. 2005, 94, 140501.
[4] F.-G. Deng, G. L. Long, Phys. Rev. A 2004, 69, 052319.
[5] M. Boyer, D. Kenigsberg, T. Mor, Phys. Rev. Lett. 2007, 99, 140501.
[6] M. Boyer, R. Gelles, D. Kenigsberg, T. Mor, Phys. Rev. A 2009, 79, 032341.
[7] X. Zou, D. Qiu, L. Li, L. Wu, L. Li, Phys. Rev. A 2009, 79, 052312.
[8] X. Zou, D. Qiu, Sci. China: Phys., Mech. Astron. 2014, 57, 1696.
[9] H. Iqbal, W. O. Krawec, Quantum Inf. Process. 2020, 19, 97.
[10] A. Cerè, M. Lucamarini, G. Di Giuseppe, P. Tombesi, Phys. Rev. Lett. 2006, 96, 200501.
[11] R. Kumar, M. Lucamarini, G. Di Giuseppe, R. Natali, G. Mancini, P. Tombesi, Phys. Rev. A 2008, 77, 022304.
[12] F. Massa, P. Yadav, A. Moqanaki, W. O. Krawec, P. Mateus, N. Paunković, A. Souto, P. Walther, arXiv:1908.01780, 2019.
[13] P. Gurevich, M. Orenstein, T. Mor, Ph. D. Thesis, 2013.
[14] C. H. Bennett, S. J. Wiesner, Phys. Rev. Lett. 1992, 69, 2881.
[15] M. Lucamarini, S. Mancini, Theor. Comput. Sci. 2014, 560, 46.
[16] N. J. Beaudry, M. Lucamarini, S. Mancini, R. Renner, Phys. Rev. A 2013, 88, 062302.
[17] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, P. Wallden, Adv. Opt. Photonics 2020, 12, 1012.
[18] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Du ̈sek, N. Lütkenhaus, M. Peev, Rev. Mod. Phys. 2009, 81, 1301.
[19] O. Amer, V. Garg, W. O. Krawec, IEEE Aerosp. Electron. Syst. Mag. 2021, 36, 30.
[20] H. Maassen, J. B. Uffink, Phys. Rev. Lett. 1988, 60, 1103.
[21] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, R. Renner, Nat. Phys. 2010, 6, 659.
[22] P. J. Coles, M. Berta, M. Tomamichel, S. Wehner, Rev. Mod. Phys. 2017, 89, 015002.
[23] I. Białynicki-Birula, L. Rudnicki, in Statistical Complexity (Ed: K. Sen), Vol. 1–34, Springer, Dordrecht 2011.
[24] S. Wehner, A. Winter, New J. Phys. 2010, 12, 025009.
[25] M. Tomamichel, A. Leverrier, Quantum 2017, 1, 14.
[26] C. Wang, F.-G. Deng, Y.-S. Li, X.-S. Liu, G. L. Long, Phys. Rev. A 2005, 71, 044305.
[27] H. Bechmann-Pasquinucci, W. Tittel, Phys. Rev. A 2000, 61, 062308.
[28] N. J. Bouman, S. Fehr, in Advances in Cryptology - CRYPTO 2010 (Ed: T. Rabin), Lecture Notes in Computer Science, Vol. 6223, Springer, Berlin, Heidelberg 2010, pp. 724–741.
[29] W. O. Krawec, Quantum Inf. Process. 2019, 18, 12.
[30] J. S. Shaarvi, S. Mancini, Entropy 2015, 17, 2723.
[31] H. F. Chau, IEEE Trans. Inf. Theory 2005, 51, 1451.
[32] L. Sheridan, V. Scarani, Phys. Rev. A 2010, 82, 030301.
[33] T. Sasaki, Y. Yamamoto, M. Koashi, Nature 2014, 509, 475.
[34] H. Chau, Phys. Rev. A 2015, 92, 062324.
[35] C. Vlachou, W. Krawec, P. Mateus, N. Paunković, A. Souto, Quantum Inf. Process. 2018, 17, 11.
[36] N. J. Cerf, M. Bourennane, A. Karlsson, N. Gisin, Phys. Rev. Lett. 2002, 88, 127902.
[37] G. M. Nikolopoulos, G. Alber, Phys. Rev. A 2005, 72, 032320.
[38] H. Iqbal, W. O. Krawec, *IEEE Trans. Quantum Eng.* 2020, 1, 4100917.
[39] G. M. Nikolopoulos, K. S. Ranade, G. Alber, *Phys. Rev. A* 2006, 73, 032325.
[40] Z.-Q. Yin, S. Wang, W. Chen, Y.-G. Han, R. Wang, G.-C. Guo, Z.-F. Han, *Nat. Commun.* 2018, 9, 457.
[41] M. Doda, M. Huber, G. Murta, M. Pivoluska, M. Plesch, C. Vlachou, *Phys. Rev. Appl.* 2021, 15, 034003.
[42] D. Cozzolino, B. Da Lio, D. Bacco, L. K. Oxenløwe, *Adv. Quantum Technol.* 2019, 2, 1900038.
[43] R. Renner, *Int. J. Quantum Inf.* 2008, 6, 1.
[44] W. O. Krawec, in 2020 IEEE Int. Symp. on Information Theory (ISIT), IEEE, Piscataway, NJ 2020, pp. 1978–1983.
[45] K. Yao, W. O. Krawec, J. Zhu, *IEEE Trans. Inf. Theory* 2022, pp. 1–1.
[46] W. Boucher, T. Debuisschert, *Phys. Rev. A* 2005, 72, 062325.
[47] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, H. Zbinden, *Appl. Phys. Lett.* 2018, 112, 171108.
[48] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, D. J. Gauthier, *Sci. Adv.* 2017, 3, e1701491.
[49] T. Brougham, S. M. Barnett, K. T. McCusker, P. G. Kwiat, D. J. Gauthier, *J. Phys. B: At., Mol. Opt. Phys.* 2013, 46, 104010.
[50] K. Brádler, M. Mirhosseini, R. Fickler, A. Broadbent, R. Boyd, *New J. Phys.* 2016, 18, 073030.
[51] A. Wójcik, *Phys. Rev. Lett.* 2003, 90, 157901.
[52] Z. Zhang, Z. Man, Y. Li, *Phys. Lett. A* 2004, 333, 46.
[53] K. Boström, T. Felbinger, *Phys. Lett. A* 2008, 372, 3953.