New Security Proof of a Restricted High-Dimensional QKD Protocol

Hasan Iqbal
School of Computing
University of Connecticut, Storrs CT, USA
Email: hasan.iqbal@uconn.edu

Walter O. Krawec
School of Computing
University of Connecticut, Storrs CT, USA

***Abstract*—High-dimensional states (HD) are promising for quantum key distribution (QKD) due to their noise tolerance and efficiency. However, creating, and measuring, HD states is technologically challenging, thus making it important to study HD-QKD protocols where Alice and Bob are restricted in their quantum capabilities. In this paper, we revisit an HD-QKD protocol, introduced in (PRA 97 (4):042348), which does not require Alice and Bob to be capable of sending and measuring in full mutually unbiased bases. The previous proof of security for this protocol has relied on numerical methods. In this work, we provide a new proof of security, enabling the key-rate evaluation beyond previous work. Furthermore, our new proof produces better results for certain channel and dimension scenarios than prior work.**

For the full version of this paper, please see ([1]).

I. Introduction

Quantum key distribution (QKD) offers provable unconditional security of a shared secret key between two parties Alice and Bob, against an adversary Eve, whose capabilities are only limited by the laws of nature [2], [3]. QKD protocols have crucial real-life significance, such as ensuring the continuance of security in the upcoming era of quantum computation and networking [4]–[6].

However, implementing QKD systems is hard, due to the inherent difficulties of working with quantum resources [7]. Thus, minimizing resource usage is an important area of research [8]–[11]. Along this line is the so-called "3-state-BB84" protocol [12] where Alice can only send one $\mathcal{X}$ basis state. This protocol was extended by Tamaki et al. in [13] where they examined the case when Alice's state preparation source is extremely noisy and she ends up sending only one of the $\mathcal{X}$ basis states.

Nurul et. al., [14] extended Tamaki et al.'s [13] work for high dimensional states (dimension greater than two). We denote this variant of the 3-State-BB84 protocol as "HD-3-State-BB84" protocol. As opposed to the two-dimensional or qubit based cases, high dimensional or qudit based QKD systems [15] often exhibit higher theoretical noise tolerance in security analysis [16]–[21], and there are remarkable advancements in actual implementations recently [22]–[25]. Of course, proving the security of a QKD protocol against the most general form of attack, otherwise known as the coherent attacks, remains one of the challenging aspects of any QKD system. The authors in [14] have used a numerical optimization-based method, to upper bound the phase-error rate of the HD-3-State-BB84, which is used in previous works in different contexts [26]–[28]. However, due to the prohibitive computational complexity of SDP-based numerical optimization in this case for $D > 10$, analyzing noise tolerance in this method [14] becomes computationally difficult. So, one may look for analytical results for arbitrary dimensions that avoid computational complexities.

We make several contributions in this work. First, we revisit this HD-3-State-BB84 protocol [14], and derive a new, information theoretic, security analysis for it. Unlike prior work, our method is analytical and can be used to analyze the key rate of the protocol for any dimension. Previous work, relying on numerical optimization methods, could only realistically be evaluated for relatively small dimensions. Furthermore, we also consider a simpler version of the protocol where Bob only needs to be able to distinguish a single high-dimensional superposition state, making his measurement apparatus significantly simpler to implement practically. Finally, we evaluate our resulting key-rate bounds on a depolarization channel and amplitude damping channel, comparing when possible to prior work. Importantly, unlike prior work, which showed a decreasing trend in the noise tolerance of the protocol as the dimension increased, we show an increasing trend in noise tolerance as the dimension increases. Thus, in this work, we prove that high-dimensional states can indeed benefit this restricted three-state style protocol - *a previously open question*. Along the way, we also derive a new continuity bound for certain types of cq-states which may hold independent interest.

Preliminaries: A density operator ρ describing a quantum state is a Hermitian, positive semi-definite operator with unit trace. In this work, subscripts of a density operator ρ, such as in ρ_{ABE}, means that it is a quantum system shared among parties Alice, Bob, and Eve. We may drop these subscripts if the context is clear. We use $H(A)_\rho$ to denote the von Neumann entropy of ρ_A. The trace norm of density operator ρ is defined as $\|\rho\|_1 := \mathrm{Tr}(\sqrt{\rho\rho^\dagger})$. The trace distance between two density operators ρ and σ is defined as $\frac{1}{2}\|\rho-\sigma\|_1$. We denote the binary entropy function as $h(x) = -x\log x-(1-x)\log(1-x)$, where the logarithm is of base 2, which is also true for all logarithms used in this work. The Shannon entropy of a probability distribution $\vec{p}$ with n outcomes, is denoted in the usual way as: $H(\vec{p}) = -\sum_{i=1}^{n} p_i \log p_i$. The conditional

entropy of a bipartite quantum system ρ_{BE}, denoted by $H(B|E)_\rho$ is defined as $H(B|E)_\rho = H(BE)_\rho - H(E)_\rho$. We use notation $\mathcal{Z} = \{|0\rangle, |1\rangle, ..., |D-1\rangle\}$ to denote the D-dimensional computational basis and use $\mathcal{X}$ to denote the Fourier basis ; i.e., $\mathcal{X} = \{|x_0\rangle, \cdots, |x_{D-1}\rangle\}$ where $|x_a\rangle = \mathcal{F}|a\rangle = \frac{1}{\sqrt{D}} \sum_{b=0}^{D-1} \exp\left(\frac{-\pi i a b}{D}\right) |b\rangle$ where $\mathcal{F}$ is the Fourier transform operator.

To measure the performance of a QKD protocol, we often calculate its key rate K using the Devetak and Winter key rate expression [29], [30] which states that, under a collective attack scenario, for a tripartite density operator $\rho_{A^Z B^Z E}$ where random variables A^Z, B^Z are the classical results of measuring quantum memories A and B in the $\mathcal{Z}$ basis:

$$K = \inf[H(B^Z|E) - H(B^Z|A^Z)], \tag{1}$$

where the infimum is taken over all possible collective attacks by Eve which agree with the observed channel statistics. Furthermore, we also make use of the following *entropic uncertainty relation* obtained by Berta et al [31]:

$$H(A^Z|E) + H(A^X) \geq \log_2 D \tag{2}$$

In [32], an alternative entropic uncertainty relation was shown where, given ρ_{AE}, if a measurement in either the Z basis, or a restricted POVM measurement of the form $\{|x_0\rangle\langle x_0|, I - |x_0\rangle\langle x_0|\}$ is performed, then it holds that:

$$H(A^Z|E) + \frac{H_D(Q_X)}{\log_D 2} \geq \log_2 D, \tag{3}$$

where $H_D(x)$ is the D-ary entropy function:

$$H_D(x) = x\log_D(D-1) - x\log_D(x) - (1-x)\log_D(1-x) \tag{4}$$

and Q_X is the probability of receiving outcome $I - |x_0\rangle\langle x_0|$ if measuring in POVM $\{|x_0\rangle\langle x_0|, I - |x_0\rangle\langle x_0|\}$.

II. The Protocol

The protocol is a high-dimensional variant of the three-state BB84 protocol, introduced in [14]. While that paper considered a larger class of protocol, here we consider the "simplest" version. We also consider two versions of the protocol: `MODE=FULL` and `MODE=PARTIAL`. There are two D-dimensional bases $\mathcal{Z}$ and $\mathcal{X}$ as defined previously and one distinguished $\mathcal{X}$ basis state we denote simply $|x_0\rangle$ (though it may be any of the $\mathcal{X}$ basis states so long as the choice is public knowledge). Alice can send any $\mathcal{Z}$ basis state or the distinguished $|x_0\rangle$ state; Bob can perform (1) a full $\mathcal{Z}$ basis measurement or (2) he can measure in the full $\mathcal{X}$ basis (if `MODE=FULL`) or he can only distinguish $|x_0\rangle$ from any of the other $|x_i\rangle$, $i > 0$ (if `MODE=PARTIAL`). That is, he is always able to measure in the full $\mathcal{Z}$ basis, but he does not need to be able to perform a full $\mathcal{X}$ basis measurement if `MODE=PARTIAL`. A partial-entanglement-based version of the protocol is described below; the equivalent prepare-and-measure version can be found in the full paper ([1]).

Protocol: HD-3-State-BB84

Public Parameters: The dimension of the Hilbert space $D \geq 2$ and the bases $\mathcal{Z}$ and $\mathcal{X}$ as well as Alice's choice of the single $\mathcal{X}$ basis state $|x_0\rangle$. Also the protocol `MODE`, namely `MODE=FULL` or `MODE=PARTIAL`.

Quantum Communication Stage: The quantum communication stage of the protocol repeats the following:

(1) Alice chooses randomly whether this round is a Key Round or a Test Round. If it is a Key Round, she prepares an entangled state $|\psi\rangle_{AT} \coloneqq \frac{1}{\sqrt{D}} \sum_{a=0}^{D-1} |a,a\rangle_{AT}$ and sends the T register to Bob through the communication channel. Otherwise, in a Test Round, she sends $|x_0\rangle_T$ (unentangled with her system).

(2) Bob chooses randomly to measure in the $\mathcal{Z}$ basis or the $\mathcal{X}$ basis. If the latter, and if `MODE=FULL`, he measures in the full X basis; otherwise, if `MODE=PARTIAL`, he actually measures using the two outcome POVM $\{|x_0\rangle\langle x_0|, I - |x_0\rangle\langle x_0|\}$.

(3) Alice and Bob inform each other of their basis choice but not measurement or preparation choices. If this is a Key Round and Bob uses the $\mathcal{Z}$ basis, then Alice measures her own register also in the $\mathcal{Z}$ basis, in which case, this round can contribute towards the raw key. Otherwise, if this is a Test Round and Bob uses the $\mathcal{X}$ basis, then this round can contribute towards estimating Eve's disturbance.

Classical Communication Stage: Alice and Bob proceed with error correction and privacy amplification to obtain a secret key if the protocol was not aborted.

III. Security Analysis

The ultimate goal of our security analysis is to obtain a lower bound on the achievable key rate using equation (1). However, in equation (1), the entropy involving Eve's quantum memory E and Bob's classical random variable B^Z, denoted as $H(B^Z|E)$, is not straightforward to calculate. Our goal in this section is to calculate a lower bound on this quantity. Note that $H(B^Z|A^Z)$ is easily computed by Alice and Bob, as this only involves their $\mathcal{Z}$ basis measurement results. We proceed with our security analysis assuming collective attacks. We only consider ideal single qubit, lossless channels in this work and leave defense against practical attacks [7], [33], [34] as interesting future work.

The method that we are using to analyze the security of this protocol is based on the works in [35], [36]. We prove the security in three steps.

First step - Calculate density operators for states that Alice sends and Bob measures in the $\mathcal{Z}$ basis:

We first calculate the density operators for states where Alice sends a $\mathcal{Z}$ basis state and all parties measure in the $\mathcal{Z}$ basis (denoted $\rho_{A^Z B^Z E}$ which is used for a Key Round) and also an operator for when Alice sends the distinguished $\mathcal{X}$ state (denoted σ_{BE} which is used for Bob's testing). Since we are assuming collective attacks, we can model Eve's attack as a unitary operator U which acts on basis states as follows:

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

From this, we may derive the desired states below. For full details, see the full paper ([1]).

$$\rho_{A^z B^z E} = \frac{1}{D}\sum_{a,b} |a\rangle\langle a|_A \otimes |b\rangle\langle b|_B \otimes |e_b^a\rangle\langle e_b^a|_E . \quad (5)$$

$$\sigma_{BE} = P\left(\frac{1}{\sqrt{D}}\sum_b |b\rangle_B \otimes \sum_a |e_b^a\rangle_E\right). \quad (6)$$

With these two density operators σ_{BE} and $\rho_{A^z B^z E}$, where $\rho_{B^z E}$ is needed to generate key bits and σ_{BE} is used to test the fidelity of the channel, we can proceed to our next step.

Second Step - Calculate a lower bound on the key rate: We will bound the needed $H(B|E)_\rho$ by instead bounding $H(B|E)_\sigma$ and using a continuity bound:

Theorem 1. *The key rate of protocol* (II) *when* `MODE=FULL` *is lower bounded by:*

$$K \geq \log_2 D - \Delta - H(B^X)_\sigma - leak_{EC}, \quad (7)$$

and, when `MODE=PARTIAL`*, is lower bounded by:*

$$K \geq \log_2 D - \Delta - \frac{H_d(B^X)_\sigma}{\log_D 2} - leak_{EC}. \quad (8)$$

where $\Delta = |H(B^Z|E)_\rho - H(B^Z|E)_\sigma|$ (note that the σ state is after Bob measures Eq. 6 in the $\mathcal{Z}$ basis). Additionally, $leak_{EC}$ is the information leaked during error correction [30]. Here, B^X is the random variable that represents Bob's $\mathcal{X}$ basis measurement outcomes, when Alice sends $|x_0\rangle$. For `MODE=FULL`, B^X takes on D possible values since B can perform a full $\mathcal{X}$ basis measurement, while for `MODE=PARTIAL`, B^X takes only two values.

Proof. In the case when Alice sends a single $\mathcal{X}$ basis state which, after Bob's measurement, results in the density operator σ_{BE}, we know that by Equation 2, we have for `MODE=FULL`:

$$H(B^Z|E)_\sigma + H(B^X|A)_\sigma \geq \log(D)$$
$$\implies H(B^Z|E)_\sigma \geq \log(D) - H(B^X)_\sigma \quad (9)$$

where $H(B^X)_\sigma$ is easily estimated using the observed error rate in the Test Round case. Then combining equation (9) with the definition of Δ as mentioned before, and remembering that $leak_{EC} = H(B^Z|A^Z)$ asymptotically, if they use an optimal error correction reconciliation protocol [30], Devetak-Winter's key rate equation from [29] finishes the proof for `MODE=FULL`. For `MODE=PARTIAL`, the same arguments can be used, but with Equation 3, thus completing the proof. □

To calculate the key rate, one must bound Δ. The following lemma proven in [36] for an alternative protocol, helps with this as we shortly see:

Lemma 1. *(Adopted from [36]) Assuming Alice and Bob only use mutually unbiased bases for state encoding, it is to Eve's advantage to send an initial state satisfying the following orthogonality constraint:* $\langle e_b^a|e_b^{a'}\rangle = p(b|a)$ *if* $a = a'$ *and* $\langle e_b^a|e_b^{a'}\rangle = 0$ *if* $a \neq a'$*, where,* $p(b|a) = \langle e_b^a|e_b^a\rangle$ *denotes the probability of Bob's* $\mathcal{Z}$ *basis measurement outcome being a specific* $|b\rangle \in \mathcal{Z}$ *given that Alice sent a state* $|a\rangle \in \mathcal{Z}$*.*

Thus, we reduced the problem to computing Δ, the trace distance between $\rho_{B^z E}$ and $\sigma_{B^z E}$. First, we show an analytical expression for Δ assuming symmetric channels. Later, we will show how one may bound Δ for arbitrary channels.

Third Step - Bounding Δ: To bound Δ we take advantage of the continuity of von Neumann entropy; namely that Δ can be upper-bounded as a function of the trace distance between ρ and σ. In particular, [37] bounds the absolute difference of conditional entropies of two bipartite cq-states, in this case, $\rho_{B^z E}$ and $\sigma_{B^z E}$, as a function of their trace distance. We have,

$$\Delta = |H(B^Z|E)_\rho - H(B^Z|E)_\sigma| \leq \epsilon \log|B^Z| + (1+\epsilon)h\left(\frac{\epsilon}{1+\epsilon}\right), \quad (10)$$

where $\epsilon \geq \frac{1}{2}\|\sigma_{B^z E} - \rho_{B^z E}\|_1$ and $|B^Z|$ is the size of the set of outcomes from Bob's $\mathcal{Z}$ basis measurement, in our case, which is simply D.

For symmetric channels, we may use methods developed in [36] to express ϵ as a function of only the noise in the channel and the dimension of each system D. This equation applies to channels where for every $b \neq a$, it holds that $p(b|a) = q/(D-1)$ while for every $b = a$, it holds that $p(b|a) = 1-q$. Depolarization channels are one instance of such a channel. See the full paper for further discussion ([1]). Under these assumptions, it can be found that [1], [36]:

$$\epsilon \leq \frac{1}{2D}\sum_{b=0}^{D-1}\left((D-2)\left|-\frac{q}{D-1}\right| + \left|\lambda^+\right| + \left|\lambda^-\right|\right). \quad (11)$$

for

$$\lambda^\pm = \frac{1}{2}\left((D-2)\beta \pm \sqrt{\beta}\sqrt{(D-1)(4\alpha-4\beta)+\beta D^2}\right).$$

With this value of ϵ calculated, we can easily get Δ as a function of only noise parameter q and dimension D.

In the general case, when the channel is not symmetric, one can find the eigenvalues numerically, for the given channel following an algorithm such as the one presented below:

1) Set a variable $td = 0$
2) For each $b = 0, 1, \cdots D-1$ Do:
   a) Set M to be a zero-matrix of size $D \times D$.
   b) For each $a, a' = 0, 1, \cdots, D-1$ with $a \neq a'$ Do:
      i) $M = M + \sqrt{p(b|a)p(b|a')}\,|a\rangle\langle a'|$
   c) Compute the eigenvalues $\{\lambda_1, \cdots\}$ of M
   d) $td = td + \sum_i |\lambda_i|$
3) Return the Trace Distance: $td/(2D)$.

In general, we found that our algorithm runs significantly faster than the numerical optimization approach used in prior work [14]. Indeed, for the amplitude damping channel, evaluated below, the difference in running time on a standard desktop computer was an order of magnitude faster for our approach (taking seconds as opposed to hours).

Key Rate calculation: To calculate the key rate using Equation 1, we need expressions for two more terms, namely, $H(B^X)$ and the number of classical bits revealed during error correction, $leak_{EC} = H(B^Z|A^Z)$. Both of these are observable parameters, however, and are easily derived using

observed statistics. Later, for evaluation purposes, we will simulate their expected values under a depolarization channel and amplitude damping channel.

A. Improved Continuity Bound

Note that the key rate equation derived above applies to arbitrary dimensions. In a specific case for symmetric channels when $D = 2$ and $0 \leq q \leq .1464$, we can obtain a slightly improved key rate using a new continuity bound we derive below:

Lemma 2. *Assuming $D = 2$, a symmetric channel, and that $\mathcal{Z}$ and $\mathcal{X}$ are mutually unbiased, it then holds that:*

$$\left|H(B^Z|E)_\rho - H(B^Z|E)_\sigma\right| \leq h(1 - q - \sqrt{q(1-q)}).$$

Proof. See the full paper for a proof of this continuity bound ([1]). □

We show later in our evaluations, that this produces a strictly better result than other continuity bounds for dimension two and symmetric attacks.

B. General Attacks

While the above analyzed collective attacks, the security analysis may be promoted straightforwardly to general attacks. First, observe that the protocol may be reduced to an equivalent entanglement-based version in the following way. First, Eve prepares an arbitrary state $|\psi\rangle_{ABE}$ which we may write without loss of generality as: $|\psi\rangle_{ABE} = \frac{1}{\sqrt{D}} \sum_{a,b} |a, b, e_b^a\rangle$.

Note that, if we assume Alice observes $|a\rangle$ with probability $1/D$ (which may be enforced), this then implies $\sum_{b=0}^{D-1} \langle e_b^a | e_b^a \rangle = 1$ (which we assumed in the previous section). Now, on a Key Round, Alice and Bob will measure as normal. On a Test Round, Alice can measure in the X basis and reject the signal if she does not observe $|x_0\rangle$. It is not difficult to see that, conditioning on Alice observing $|x_0\rangle$, this will disentangle her system with Bob and Eve's in the same manner as if she had initially sent $|x_0\rangle$. Thus security there implies security of the entanglement-based version and vice versa. Finally, de Finetti style arguments [38] may be used to promote security to general attacks, thus concluding the proof.

IV. Evaluation

In the following, we evaluate our key rate bound in equation (7) in a depolarizing channel and compare it with prior work in [14]. Then we further evaluate our protocol in the amplitude damping channel.

Depolarizing Channel: Because prior work methods are computationally intensive to replicate, we only present the comparison with our analysis for key rates for up to $D = 8$. For the depolarization channel, our results and comparisons are presented in figure (1) by evaluating our key rate from equation (7).

In figure (1), it can be seen that the noise tolerance determined using the previous method in [14] actually goes down

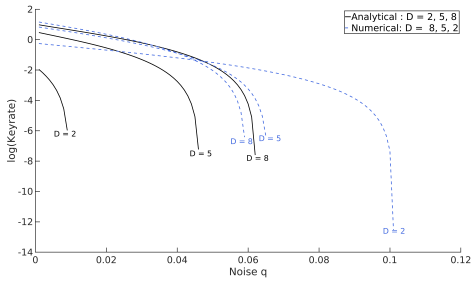

Fig. 1: Comparison of our analysis and the numerical method from [14]. Notice the decreasing trend of key rates in the numerical approach(dotted lines), and the opposite in our case (solid lines). Here we evaluate our protocol in the `MODE=FULL` case, which is the analogous case of [14].

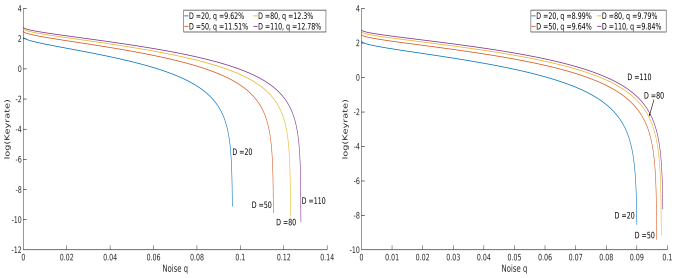

Fig. 2: (a) Noise tolerance of HD-3-State-BB84 in `MODE=FULL` from dimension 10 to 110 in our analysis. (b) Noise tolerance of HD-3-State-BB84 in `MODE=PARTIAL` from dimension 10 to 100.

with increasing dimensions when only one monitoring basis is used. For example, it is 7.45% for $D = 3$ and 7.28% for $D = 6$. As indicated in their work, this may be attributed to the quick rise of the optimal phase error rate produced by the optimization algorithm with increasing dimensions. For example, the phase error rate is 27.68% for $D = 3$ and 45.04% for $D = 6$. This effect is more pronounced when one compares the result in the case of $D = 2$, where their analysis performs best in terms of noise tolerances compared

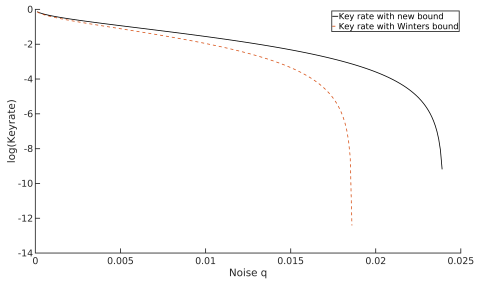

Fig. 3: Comparison of the noise tolerances of HD-3-State-BB84 in dimension 2 and in `MODE=FULL`, considering our lemma 2 and Winter's bound [37] for conditional quantum entropies.

to dimensions $D > 2$. In contrast to their result, in figure (1), we see that our analysis produces better noise tolerances as dimensions increase, as one may expect based on other HD-QKD protocols. As an example, in our analysis, the noise tolerance is 3.541% for $D = 3$ and 6.169% for $D = 6$. In dimension $D = 9$, we see that our noise tolerance is 7.482% compared to 6.63% in prior work [14]. This leads us to suspect that in even higher dimensions $D > 9$, shown in Figure 2, our analysis would continue to produce better noise tolerances.

Thus, while our result under-performs prior work for small dimensions, it greatly outperforms prior work once the dimension increases and also proves for the first time that HD states do, in fact, benefit this HD-three-state protocol (prior work could not confirm this as discussed).

In figure (2), we show the evaluation of protocol (II) in both `MODE=FULL` and `MODE=PARTIAL` for the depolarizing channel. Comparing these two modes, we notice that the performance of `MODE=PARTIAL` is still competitive with `MODE=FULL`. For example, in dimension $D = 20$, we see a noise tolerance of 9.62% in `MODE=FULL` and 8.99% in `MODE=PARTIAL`. It is also interesting to notice that this difference gets slightly more pronounced in even higher dimensions ($D = 110$ for example) between these two modes. It can be said from these graphs that our analysis clearly demonstrates the advantage of using high-dimensional resources as well as the feasibility of obtaining competitive performance even when one uses much fewer quantum resources. Finally, in figure (3), we show the comparison between our new continuity bound (Lemma 2) for Δ and Winter's bound [37] in the restricted case of $D = 2$, by evaluating the key rate equation (7). We see that the noise tolerance increases from 1.85% to 2.39% demonstrating its utility. Notably, this improvement holds for both modes of our protocol, and we only show this for `MODE=FULL`.

Amplitude Damping Channel: We further evaluate our analysis in another widely used noise model, namely, the amplitude damping channel [39]. This channel can be described by the following Kraus operators:

$$E_0 = |0\rangle\langle 0| + \sum_{a=1}^{D-1} \sqrt{1-p}\,|a\rangle\langle a|\,, E_i \quad = \sum_{a=1}^{D-1} \sqrt{p}\,|0\rangle\langle a|\,.$$

We present the evaluation of our analysis for this channel in figure (4). Interestingly, when we consider the `MODE=PARTIAL` for our protocol in this channel, where Bob needs much less resources to implement his measurement apparatus, the noise tolerance is higher than the `MODE=FULL` for dimension 10. However, for $D = 15$, `MODE=FULL` does outperform `MODE=PARTIAL`. From these observations in this channel, We draw similar conclusions as in the depolarizing channel. That is, high-dimensional resources do offer better performance for protocol (II).

V. Closing Remarks

In this work, we have presented a security proof of the HD-3-State-BB84 protocol and showed that, for high enough dimension, our work provides higher noise tolerances in the case when only one monitoring basis is used as compared to prior state of the art work. The key advantage of our analysis is that it avoids computational limitations and provides an analytical expression for key rates in arbitrary dimensions. Our method also clearly demonstrates that indeed, using higher dimensional systems leads to an increment in noise tolerances even when Alice is limited in her ability to send the monitoring basis states. This conclusion could not be made in [14] for this three state protocol.

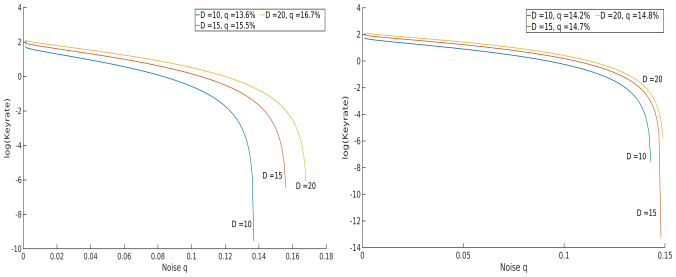

Fig. 4: Key rates for HD-3-state-BB84 protocol in `MODE=FULL` when the amplitude damping channel is used. We consider dimensions $D = 10, 15, 20$ here. Key rates for HD-3-state-BB84-2 protocol, where the two-outcome POVM EU relation is used, in the amplitude damping channel for dimensions D = 10, 15, 20.

Many interesting future problems remain. Extending our methods to the case where Alice sends more than one $\mathcal{X}$ basis state would be useful. Another interesting line of investigation would be to analyze more practical channels, including lossy channels. We leave this analysis as interesting, and important, future work. However, we feel our proof methods may be suitable to tackle lossy conditions, and additional testing states, with suitable extensions.

We have also presented a new continuity bound in Lemma (2) for conditional quantum entropies in this work, for certain types of cq-states. We have shown that, although limited in scope at this point, this new bound provides a noticeable advantage in noise tolerance in our analytical method, compared to Winter's continuity bound [37] (though, we stress, only for a certain type of state and dimension as our lemma is more restricted than Winter's bound, the latter of which can be applied to any state) and provides further support to Wilde's conjecture [40]. Perhaps more importantly, the technique we have used to prove our bound may find use in proving the conjecture itself, or some weaker version of it in arbitrary dimensions, as currently there are no known techniques to prove it.

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

References

[1] Hasan Iqbal and Walter O. Krawec, "New security proof of a restricted high-dimensional qkd protocol," *arXiv preprint arXiv:2307.09560*, 2023.

[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*, vol. 12, no. 4, pp. 1012–1236, 2020.

[3] Omar Amer, Vaibhav Garg, and Walter O Krawec, "An introduction to practical quantum key distribution," *IEEE Aerospace and Electronic Systems Magazine*, vol. 36, no. 3, pp. 30–55, 2021.

[4] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al., "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019.

[5] Andreas Poppe, Momtchil Peev, and Oliver Maurhart, "Outline of the secoqc quantum-key-distribution network in vienna," *International Journal of Quantum Information*, vol. 6, no. 02, pp. 209–218, 2008.

[6] Domenico Ribezzo, Mujtaba Zahidy, Ilaria Vagniluca, Nicola Biagi, Saverio Francesconi, Tommaso Occhipinti, Leif K Oxenløwe, Martin Lončarić, Ivan Cvitić, Mario Stipčević, et al., "Deploying an inter-european quantum network," *arXiv preprint arXiv:2203.11359*, 2022.

[7] Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan, "Practical challenges in quantum key distribution," *npj Quantum Information*, vol. 2, no. 1, pp. 1–12, 2016.

[8] Charles H Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical review letters*, vol. 68, no. 21, pp. 3121, 1992.

[9] Charles H Bennett, Gilles Brassard, and N David Mermin, "Quantum cryptography without bell's theorem," *Physical review letters*, vol. 68, no. 5, pp. 557, 1992.

[10] Michel Boyer, Dan Kenigsberg, and Tal Mor, "Quantum key distribution with classical bob," in *2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07)*. IEEE, 2007, pp. 10–10.

[11] Xiangfu Zou, Daowen Qiu, Lvzhou Li, Lihua Wu, and Lvjun Li, "Semiquantum-key distribution using less than four quantum states," *Physical Review A*, vol. 79, no. 5, pp. 052312, 2009.

[12] Chi-Hang Fred Fung and Hoi-Kwong Lo, "Security proof of a three-state quantum-key-distribution protocol without rotational symmetry," *Physical Review A*, vol. 74, no. 4, pp. 042342, 2006.

[13] Kiyoshi Tamaki, Marcos Curty, Go Kato, Hoi-Kwong Lo, and Koji Azuma, "Loss-tolerant quantum cryptography with imperfect sources," *Physical Review A*, vol. 90, no. 5, pp. 052314, 2014.

[14] Nurul T Islam, Charles Ci Wen Lim, Clinton Cahall, Jungsang Kim, and Daniel J Gauthier, "Securing quantum key distribution systems using fewer states," *Physical Review A*, vol. 97, no. 4, pp. 042347, 2018.

[15] Daniele Cozzolino, Beatrice Da Lio, Davide Bacco, and Leif Katsuo Oxenløwe, "High-dimensional quantum communication: Benefits, progress, and future challenges," *Advanced Quantum Technologies*, vol. 2, no. 12, pp. 1900038, 2019.

[16] Nicolas J Cerf, Mohamed Bourennane, Anders Karlsson, and Nicolas Gisin, "Security of quantum key distribution using d-level systems," *Physical review letters*, vol. 88, no. 12, pp. 127902, 2002.

[17] Antonio Acin, Nicolas Gisin, and Valerio Scarani, "Security bounds in quantum cryptography using d-level systems," *arXiv preprint quant-ph/0303009*, 2003.

[18] Lana Sheridan and Valerio Scarani, "Security proof for quantum key distribution using qudit systems," *Physical Review A*, vol. 82, no. 3, pp. 030301, 2010.

[19] Chrysoula Vlachou, Walter Krawec, Paulo Mateus, Nikola Paunković, and André Souto, "Quantum key distribution with quantum walks," *Quantum Information Processing*, vol. 17, no. 11, pp. 1–37, 2018.

[20] Hasan Iqbal and Walter O Krawec, "Analysis of a high-dimensional extended b92 protocol," *Quantum Information Processing*, vol. 20, no. 10, pp. 1–22, 2021.

[21] Keegan Yao, Walter O Krawec, and Jiadong Zhu, "Quantum sampling for finite key rates in high dimensional quantum cryptography," *IEEE Transactions on Information Theory*, 2022.

[22] 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*, vol. 3, no. 11, pp. e1701491, 2017.

[23] 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*, vol. 27, no. 13, pp. 17539–17549, 2019.

[24] Ilaria Vagniluca, Beatrice Da Lio, Davide Rusca, Daniele Cozzolino, Yunhong Ding, Hugo Zbinden, Alessandro Zavatta, Leif K Oxenløwe, and Davide Bacco, "Efficient time-bin encoding for practical high-dimensional quantum key distribution," *Physical Review Applied*, vol. 14, no. 1, pp. 014051, 2020.

[25] 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.

[26] Darius Bunandar, Luke CG Govia, Hari Krovi, and Dirk Englund, "Numerical finite-key analysis of quantum key distribution," *npj Quantum Information*, vol. 6, no. 1, pp. 1–12, 2020.

[27] Adam Winick, Norbert Lütkenhaus, and Patrick J Coles, "Reliable numerical key rates for quantum key distribution," *Quantum*, vol. 2, pp. 77, 2018.

[28] Ian George, Jie Lin, and Norbert Lütkenhaus, "Numerical calculations of the finite key rate for general quantum key distribution protocols," *Physical Review Research*, vol. 3, no. 1, pp. 013274, 2021.

[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*, vol. 461, no. 2053, pp. 207–235, 2005.

[30] Renato Renner, Nicolas Gisin, and Barbara Kraus, "Information-theoretic security proof for quantum-key-distribution protocols," *Physical Review A*, vol. 72, no. 1, pp. 012332, 2005.

[31] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M Renes, and Renato Renner, "The uncertainty principle in the presence of quantum memory," *Nature Physics*, vol. 6, no. 9, pp. 659–662, 2010.

[32] Walter O Krawec, "A new high-dimensional quantum entropic uncertainty relation with applications," in *2020 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2020, pp. 1978–1983.

[33] Anqi Huang, Stefanie Barz, Erika Andersson, and Vadim Makarov, "Implementation vulnerabilities in general quantum cryptography," *New Journal of Physics*, vol. 20, no. 10, pp. 103016, 2018.

[34] Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, no. 8, pp. 595–604, 2014.

[35] Walter O Krawec, "Key-rate bound of a semi-quantum protocol using an entropic uncertainty relation," in *2018 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2018, pp. 2669–2673.

[36] Hasan Iqbal and Walter O Krawec, "High-dimensional semiquantum cryptography," *IEEE Transactions on Quantum Engineering*, vol. 1, pp. 1–17, 2020.

[37] Andreas Winter, "Tight uniform continuity bounds for quantum entropies: conditional entropy, relative entropy distance and energy constraints," *Communications in Mathematical Physics*, vol. 347, no. 1, pp. 291–313, 2016.

[38] Robert Konig and Renato Renner, "A de finetti representation for finite symmetric quantum states," *Journal of Mathematical physics*, vol. 46, no. 12, pp. 122108, 2005.

[39] Alejandro Fonseca, "High-dimensional quantum teleportation under noisy environments," *Physical Review A*, vol. 100, no. 6, pp. 062311, 2019.

[40] Mark M Wilde, "Optimal uniform continuity bound for conditional entropy of classical–quantum states," *Quantum Information Processing*, vol. 19, no. 2, pp. 1–9, 2020.