High-Dimensional Quantum Conference Key Agreement

Omar Amer
Future Lab for Applied Research and Engineering
JPMorgan Chase Bank, N.A
New York, NY 10017 USA

Walter O. Krawec
Computer Science & Engineering Department
University of Connecticut
Storrs, CT 06269
Email: walter.krawec@uconn.edu

***Abstract*—Quantum Conference Key Agreement (QCKA) protocols are designed to allow multiple parties to agree on a shared secret key, secure against computationally unbounded adversaries. In this paper, we consider a high-dimensional QCKA protocol and prove its information theoretic security against arbitrary, general, attacks in the finite-key scenario. Our proof technique may be useful for other high-dimensional multi-party quantum cryptographic protocols. Finally, we evaluate the protocol in a variety of settings, showing that high-dimensional states can greatly benefit QCKA protocols.**

I. Introduction

Quantum key distribution (QKD) allows for the establishment of a shared secret key between two parties, Alice and Bob, secure against computationally unbounded adversaries (whom we refer to as Eve). Progress in these protocols has rapidly advanced, leading to both a rich theory along with practical commercial systems [1], [2], [3]. Quantum conference key agreement (QCKA) protocols are designed to allow multiple parties to establish a common, shared, secret key secure against computationally unbounded adversaries. Starting from early work in this field [4], [5], QCKA protocols have advanced substantially with new protocols and security proofs [6], [7], [8]; it is also experimentally feasible [9]. Interestingly, it has been shown that there are some scenarios where such multiparty protocols hold an advantage over the naive use of multiple two-party protocols run in parallel [5]. For a recent survey on quantum conference key agreement protocols and the state of the art in security proofs, the reader is referred to [10].

High-dimensional quantum cryptography has been shown to exhibit numerous advantages over qubit-based protocols, especially in two-party QKD [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22]. Encouraged by this, it is worth investigating whether high-dimensional states can benefit QCKA. To our knowledge, only one high-dimensional QCKA protocol exists which was introduced in [23], however no rigorous finite key security analysis exists for it (instead, [23] developed layered QKD protocols and was not concerned with the explicit finite-key analysis of this particular QCKA protocol - in fact, our analysis done in this paper may be useful in proving security of those other protocols introduced in [23], though we leave that as interesting future work).

In this work, we consider a high-dimensional QCKA protocol and prove its security against arbitrary, general attacks in the finite key setting. The protocol we analyze is an extension of the qubit-based protocol from [24] to higher dimensions and also a specific instance of a protocol introduced in [23]. For the security proof, we utilize the quantum sampling framework introduced by Bouman and Fehr in [25], along with proof techniques we developed in [26] to derive sampling-based entropic uncertainty relations. Our proof, though using these two frameworks as a foundation, introduces several new methods which may also be useful when analyzing other quantum cryptographic protocols, both those involving two users and those for multi-users, especially in higher dimensions.

Finally, we evaluate the performance of this protocol in a variety of scenarios, showing some very interesting behavior and shedding new light on the benefits of high-dimensional quantum states. In particular, we show that, as the dimension of the quantum signal increases, the noise tolerance also increases. Interestingly, the key-rate also increases beyond what would be possible by simply running multiple, lower-dimensional, protocols in parallel. This shows that high-dimensional states can greatly benefit QCKA protocols. Our contributions in this work are not only in developing a security proof for a high dimensional QCKA protocol, but also in showing even more benefits to high-dimensional quantum states when applied to quantum cryptography. Our methods may also spur future research in this area, as our proof techniques may be highly adaptable to other scenarios.

A. Notation and Definitions

We begin with some notation and definitions that we will use in this work. Let $d \in \mathbb{N}$, then we write $\mathcal{A}_d$ to be a d-character alphabet with a distinguished 0 element. Given a word $q \in \mathcal{A}_d^n$, and a subset $t \subset \{1, \cdots, n\}$, we write q_t to mean the substring of q indexed by t; we use q_{-t} to mean the substring of q indexed by the complement of t. We write $w(q)$ to be the relative Hamming weight of q, namely $w(q) = \frac{|\{i : q_i \neq 0\}|}{n}$ - that is the number of characters in q that are not zero, divided by the length of q. Given two words x, y in this alphabet, we write xy to mean the concatenation of x and y. Finally, given a, b, numbers between 0 and $d-1$, we write $a +_d b$ to mean the addition of a and b modulo d.

We use $\mathcal{H}_d$ to mean a Hilbert space of dimension d. The standard computational basis will be denoted $Z = \{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$. If we are refering to an alternative

basis we will write the basis label as a superscript. One important basis we will use is the Fourier basis consisting of elements $\mathcal{F} = \{|0\rangle^{\mathcal{F}}, \cdots, |d-1\rangle^{\mathcal{F}}\}$, where: $|j\rangle^{\mathcal{F}} = \frac{1}{\sqrt{d}} \sum_k \exp(2\pi ijk/d) |k\rangle$. If given a word $q \in \mathcal{A}_d^n$, we write $|q\rangle$ to mean $|q_1\rangle \otimes \cdots \otimes |q_n\rangle$. Similarly, we write $|q\rangle^{\mathcal{F}}$ to mean $|q_1\rangle^{\mathcal{F}} \otimes \cdots \otimes |q_n\rangle^{\mathcal{F}}$. Note that if there is no superscript, then $|q\rangle$ is assumed to be the computational Z basis. Finally, given pure state $|\psi\rangle$, we write $[\psi]$ to mean $|\psi\rangle\langle\psi|$.

A density operator is a positive semi-definite Hermitian operator of unit trace acting on some Hilbert space. If ρ_{AE} acts on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_E$, then we write ρ_A to mean the operator resulting from tracing out the E system, namely $\rho_A = tr_E \rho_{AE}$. Similarly for other, or multiple, systems.

The Shannon entropy of a random variable X is denoted $H(X)$. The d-ary entropy function is denoted $H_d(x)$, for $x \in [0,1]$, and is defined to be:

$$H_d(x) = x \log_d(d-1) - x \log_d x - (1-x) \log_d(1-x).$$

Note that when $d = 2$ this is simply the binary Shannon entropy. Given density operator ρ_{AE}, the conditional *quantum min entropy* is defined to be [27]: $H_\infty(A|E)_\rho = \sup_{\sigma_E} \max\{\lambda \in \mathbb{R} \ : \ 2^{-\lambda} I_A \otimes \sigma_E - \rho_{AE} \geq 0\}$, where the supremum is over all density operators acting on the E system. If $\rho = [\psi]$ is a pure state, then we often write $H_\infty(A|E)_\psi$. Given ρ_{AE}, we write $H_\infty(A_Z|E)_\rho$ to mean the min entropy of the resulting state following a measurement of the A register in the Z basis.

There are many important properties of quantum min entropy we will use. In particular, if the E system is trivial or independent of the A system, then $H_\infty(A)_\rho = -\log_2 \max \lambda$, where the maximum is over all eigenvalues λ of ρ_A. Given a state $\rho_{AEC} = \sum_{c=0}^M p_c \rho_{AE}^{(c)} \otimes [\mathbf{c}]$ (i.e., the C register is classical), then:

$$H_\infty(A|EC)_\rho \geq \min_c H_\infty(A|E)_{\rho^{(c)}}. \tag{1}$$

An important result proven in [25], based on a lemma in [27], is the following which allows one to compute the min entropy of a superposition state based on the min entropy of a suitable mixture state:

Lemma 1. (From [25]): Let Z and X be two orthonormal bases of $\mathcal{H}_d$. Then for any pure state $|\psi\rangle_{AE} = \sum_{i \in J} \alpha_i |i\rangle^X \otimes |E_i\rangle$, with $J \subset \mathcal{A}_d^N$, it holds that: $H_\infty(A_Z|E)_\psi \geq H_\infty(A_Z|E)_\rho - \log_2 |J|$, where $\rho_{AE} = \sum_{i \in J} |\alpha_i|^2 [\mathbf{i}]^X \otimes [\mathbf{E_i}]$, and where the entropies above are computed on the state following a Z basis measurement.

Quantum min-entropy is a vital resource in QKD security used to measure the amount of uniform independent randomness that may be extracted from a classical-quantum state. In particular, let σ_{KE} be the resulting state after using privacy amplification on a state ρ_{AE}, then it was shown in [27] that:

$$\left|\left|\sigma_{KE} - I/2^\ell \otimes \sigma_E\right|\right| \leq 2^{-\frac{1}{2}(H_\infty(A|E)_\rho - \ell)}. \tag{2}$$

In our security proof, we will utilize a quantum sampling framework originally introduced in 2010 by Bouman and Fehr [25] and used by us recently to prove novel sampling-based entropic uncertainty relations [26], [28] and proofs of security for high-dimensional BB84 [29]. We review some of the terminology and results from [25] here; for more information on these results, the reader is referred to that original reference.

Fix $d \geq 2$ and $N \geq 1$. A *classical sampling strategy* is a tuple (P_T, f, g) where P_T is a distribution over all subsets of $\{1, \cdots, N\}$ and $f, g : \mathcal{A}_d^* \to \mathbb{R}$. Given $q \in \mathcal{A}_d^N$, the strategy will first choose t according to P_T; it will then observe q_t and evaluate $f(q_t)$. This evaluation should be a "guess" as to the value of some target function, g, evaluated on the *unobserved* portion. Namely, for a good sampling strategy, with high probability over the choice of subset t, it should hold that $f(q_t)$ is δ-close to $g(q_{-t})$ for given $\delta > 0$.

More formally, fix a subset t with $P_T(t) > 0$. We define the set of "good" words $\mathcal{G}_t$ to be:

$$\mathcal{G}_t = \{q \in \mathcal{A}_d^N \ : \ |f(q_t) - g(q_{-t})| \leq \delta\} \tag{3}$$

Note that, given $q \in \mathcal{G}_t$, if subset t were to be chosen by the sampling strategy, it is guaranteed that the strategy will succeed (the guess will be δ-close to the target value). The *error probability* of the sampling strategy, then, is: $\epsilon^{cl} = \max_{q \in \mathcal{A}_d^N} Pr\left(q \notin \mathcal{G}_t\right)$, where the probability is over all subsets chosen according to P_T. One sampling strategy we will need later is summarized in the following lemma:

Lemma 2. (From [25]): Let $\delta > 0$ and $m \leq N/2$. Define P_T to be the uniform distribution over all subsets of $\{1, \cdots, N\}$ of size m. Define $f(x) = g(x) = w(x)$. Then: $\epsilon^{cl} \leq 2 \exp\left(\frac{-\delta^2 m N}{N+2}\right)$.

These definitions may be promoted to the quantum case. Fixing a sampling strategy and a d-dimensional basis $\mathcal{B}$, we define $\text{span}(\mathcal{G}_t) = \text{span}(|q\rangle^{\mathcal{B}} \ : \ q \in \mathcal{G}_t)$. The main result from [25] may then be stated as follows:

Theorem 1. (From [25] though reworded for our application in this work): Let (P_T, f, g) be a classical sampling strategy with error probability ϵ^{cl} for a given $\delta > 0$ and let $|\psi\rangle_{AE}$ be a quantum state where the A register lives in a Hilbert space of dimension d^N. Then, there exist ideal states $|\phi^t\rangle \in \text{span}(\mathcal{G}_t) \otimes \mathcal{H}_E$ (with respect to some given, fixed, d-dimensional basis $\mathcal{B}$) such that: $\frac{1}{2} \left|\left|\sum_t P_T(t) [\mathbf{t}] \otimes \left([\psi] - \left[\phi^{\mathbf{t}}\right]\right)\right|\right| \leq \sqrt{\epsilon_{cl}}$, where the above summation is over all subsets $t \subset \{1, \cdots, N\}$.

Note that the above is a slight rewording of the main result from [25]. For a proof that Theorem 1 follows from the main result in [25], the reader is referred to [29].

II. Protocol

The protocol we consider is a high-dimensional variant of the QCKA agreement protocol originally introduced and analyzed in [24]. It is also a specific instance of a protocol introduced for a layered QKD system in [23] (though without a complete proof of security). We assume there are p Bob's and one Alice all of whom wish to agree on a shared secret group key. The protocol begins by having Alice prepare the following high-dimensional GHZ state: $|\psi_0\rangle =$

$\frac{1}{\sqrt{d}}\sum_{a=0}^{d-1}|a,\cdots,a\rangle_{AB_1\cdots,B_p}$. Above, d is the dimension of a single system ($d=2$ in the protocol analyzed in [24]). The B_i system is sent to the i'th Bob while Alice retains the A register. Randomly, Alice and the p Bob's will measure their registers in the Fourier basis $\mathcal{F}$ resulting in outcome $q_{AB_1\cdots B_p}\in\mathcal{A}_d^{p+1}$. If there is no noise in the channel, it should hold that whenever parties measure in the $\mathcal{F}$ basis, the results should sum to 0 modulo d, namely: $q_A +_d q_{B_1} +_d \cdots +_d q_{B_p} = 0$; any non-zero sum will be considered noise and factored into our key-rate analysis. Otherwise, if Alice and the p Bob's choose not to measure in the Fourier basis, they will measure in the computational basis, the result of which will be used to add $\log_2 d$ bits to their raw key. Note that the choice of whether to measure in the Fourier basis or the computational Z basis may be made randomly by all parties (discarding events when choices are not consistent) or by using a pre-shared secret key (as was done in [24]). The above process is repeated for a freshly prepared and sent $|\psi_0\rangle$ until a raw key of sufficient length has been established. Following the establishment of the raw key, Alice and the p Bob's will run a pair-wise error correction protocol followed by a standard privacy amplification protocol.

III. Security Proof

To prove security of our protocol, we analyze the security of an equivalent entanglement based version where Eve prepares a quantum signal and sends it to all parties (as opposed to Alice preparing and sending a signal). We also use as a foundation, a proof methodology we introduced in [26], though making several modifications for the multi-party protocol being analyzed here. Our proof of security, at a high level, proceeds in three steps; note that, due to space constraints, we have removed several details; for complete details on the proof, please see the full version of this paper [30].

Entanglement Based Protocol - Let $|\psi\rangle\in\mathcal{H}_A\otimes\mathcal{H}_{B_1}\otimes\cdots\otimes\mathcal{H}_{B_p}\otimes\mathcal{H}_E$ be the state Eve prepares where each $\mathcal{H}_A\cong\mathcal{H}_{B_i}\cong\mathcal{H}_d^{\otimes N}$. Here N is the user-specified number of rounds used by the protocol and is a parameter users may optimize. Ideally $|\psi\rangle=|\psi_0\rangle^{\otimes N}$. At this point, the users choose a random subset $t\subset\{1,2,\cdots,N\}$ of size $m<N/2$ for sampling. This can be done by having Alice choose the subset and sending it to the Bob's (the option we assume here) or by using a small pre-shared key (the option used in [24]). Each party will measure their respective d dimensional signals, indexed by t, in the d-dimensional Fourier basis, $\mathcal{F}$, resulting in outcome $q=q_Aq_{B_1}\cdots q_{B_p}\in\mathcal{A}_d^{m(p+1)}$. Here, each $q_A,q_{B_1},\cdots,q_{B_p}$ is an m character string which we may enumerate as $q_A=q_A^1\cdots q_A^m$ and $q_{B_i}=q_{B_i}^1\cdots q_{B_i}^m$.

Let $s_i(q)=q_A^i+_d q_{B_1}^i+_d\cdots+_d q_{B_p}^i$. That is, s_i is the sum, modulo the dimension d, of all user measurement outcomes for signal i. Also, define $s(q)=s_1(q)\cdots s_m(q)\in\mathcal{A}_d^m$. If the source E were honest, it should be that $w(s(q))=0$ since this will be the case in the event Eve prepared copies of $\frac{1}{\sqrt{d}}\sum_{a=0}^{d-1}|a,a,\cdots,a\rangle_{AB_1\cdots B_p}$ as discussed earlier.

Step 1: Classical Sample Strategy Analysis - We now wish to use Theorem 1 to analyze the security of this protocol. To do so, we require a suitable classical sampling strategy which corresponds to the sampling done by the actual protocol, and a bound on its error probability. Consider the following classical sampling strategy: given a word $q=q^0q^1q^2\cdots q^p\in\mathcal{A}_d^{(p+1)\cdot N}$ (i.e., each $q^j\in\mathcal{A}_d^N$), then first choose a subset $t\subset\{1,\cdots,N\}$ of size $m\leq N/2$ and observe $q_t=q_t^0q_t^1q_t^2\cdots q_t^p$ (namely, one observes the t portion of each of the $p+1$ strings). From this, compute $f(q_t)=w(s(q_t))$ to estimate the value of $g(q_{-t})=w(s(q_{-t}))$. Putting this into the notation introduced earlier, we have the set of "good" words (see Equation 3) as: $\mathcal{G}_t=\{q\in\mathcal{A}_d^{(p+1)\cdot N}\ :\ |w(s(q_t))-w(s(q_{-t}))|\leq\delta\}$. This is exactly the sampling strategy we wish to use in our QCKA protocol. Users will observe a value based on their measurement in the Fourier basis, in particular, they observe the number of outcomes that do not sum to 0 modulo d. We wish to argue that the remaining, unmeasured portion, satisfies a similar restriction in the $\mathcal{F}$ basis, thus placing a constraint on the form of the state Eve prepared, needed to compute the min entropy later. In order to use Theorem 1, needed to construct suitable ideal quantum states, we require a bound on the error probability of this classical sampling strategy. In particular, we require: $\epsilon^{cl}=\max_{q\in\mathcal{A}_d^{(p+1)N}}Pr\left(q\notin\mathcal{G}_t\right)$. We show in the full version of the paper [30] that $\epsilon^{cl}\leq 2\exp\left(\frac{-\delta^2mN}{N+2}\right)$.

Step 2: Ideal State Analysis - We now return to the security analysis of our protocol. Let $\epsilon>0$ be given (it will, as we discuss later, determine the security level of the secret key). From Theorem 1, using the above sampling strategy with respect to the Fourier basis, there exists an ideal state of the form $\frac{1}{T}\sum_t[\mathbf{t}]\otimes\left[\phi^{\mathbf{t}}\right]$ where $T=\binom{N}{m}$ and: $|\phi^t\rangle\in\text{span}\{|q\rangle^{\mathcal{F}}\ :\ |w(s(q_t))-w(s(q_{-t}))|\leq\delta\}$. (Here, $q\in\mathcal{A}_d^{(p+1)N}$). If we set

$$\delta=\sqrt{\frac{(m+n+2)\ln(2/\epsilon^2)}{m(m+n)}}. \tag{4}$$

then, we have that the real and ideal states are ϵ-close in trace distance (on average over the subset choice as described in Theorem 1) with the real-state being $\frac{1}{T}\sum_t[\mathbf{t}]\otimes[\psi]$.

We first analyze the ideal case and then use this analysis to argue about security of the actual given input state from Eve. In the ideal case, the event of choosing subset t, measuring those systems in the Fourier basis and observing outcome $q\in\mathcal{A}_d^{(p+1)m}$, causes the ideal state to collapse to: $|\phi_q^t\rangle=\sum_{x\in J_q}\alpha_x|x\rangle^{\mathcal{F}}\otimes|E_x\rangle$, where: $J_q=\{x\in\mathcal{A}_d^{(p+1)n}\ :\ |w(s(x))-w(s(q))|\leq\delta\}$ By manipulating the above state, we may write it in the following form which will be more useful for us in our analysis:

$$|\phi_q^t\rangle\cong\sum_{x\in\mathcal{A}_d^{pn}}\beta_x|x\rangle_{B_1\cdots B_p}^{\mathcal{F}}\otimes\sum_{y\in J(q\,:\,x)}\beta_{y|x}|y\rangle_A^{\mathcal{F}}|F_{x,y}\rangle_E \tag{5}$$

where: $J(q\ :\ x)=\{y\in\mathcal{A}_d^n\ :\ |w(s(yx))-w(s(q))|\leq\delta\}$. Note that some of the β's in the above expression may be zero; also note that we permuted the subspaces above to place the A register to the right of the B registers - this was done

only to make the algebra in the remainder of the proof easier to follow.

Our goal now is to compute a lower bound on the conditional quantum min entropy following a Z basis measurement on the collapsed ideal state (that is, the entropy in the above state $|\phi_q^t\rangle$, but following Alice's Z basis measurement on her A register). Tracing out B's system yields:

$$\sigma_{AE} = \sum_{x \in \mathcal{A}_d^{p \cdot n}} |\beta_x|^2 \underbrace{P\left(\sum_{y \in J(q\,:\,x)} \beta_{y|x} |y\rangle_A^{\mathcal{F}} |F_{x,y}\rangle_E\right)}_{\sigma_{AE}^{(x)}}, \quad (6)$$

where $P(|z\rangle) = [\mathbf{z}]$.

From Equation 1, we have $H_\infty(A_Z|E)_\sigma \geq \min_x H_\infty(A_Z|E)_{\sigma^{(x)}}$. Fix a particular x and consider the mixed state: $\chi_{AE}^{(x)} = \sum_{y \in J(q\,:\,x)} |\beta_{y|x}|^2 [\mathbf{y}]_A^{\mathcal{F}} \otimes [\mathbf{F}_{\mathbf{x},\mathbf{y}}]_E$. From Lemma 1, we have: $H_\infty(A_Z|E)_{\sigma^{(x)}} \geq H_\infty(A_Z|E)_{\chi^{(x)}} - \log_2 |J(q\,:\,x)|$. We first compute a bound on the size of $J(q\,:\,x)$. Let $\mathcal{I} = \{y \in \mathcal{A}_d^n\,:\,|w(y) - w(s(q))| \leq \delta\}$. We claim $|J(q\,:\,x)| \leq |\mathcal{I}|$. Indeed, pick $y \in J(q\,:\,x)$ and let $z = s(yx)$. Then $z \in \mathcal{I}$. Furthermore, for any $y, y' \in J(q\,:\,x)$ with $y \neq y'$, it holds that $s(yx) \neq s(y'x)$. Thus the claim follows. Now, since $|\mathcal{I}| \leq d^{nH_d(w(s(q))+\delta)}$ by the well known bound on the volume of a Hamming ball, we have an upper-bound on the size of the set $J(q\,:\,x)$ as a function of the observed value q. Note that, ideally, $w(s(q)) = 0$ with non-zero values representing error in the channel, and so the size of this set should be "small" for low noise levels. As the noise increases, our entropy bound will decrease (thus ultimately decreasing the overall key-rate as expected).

What remains is to compute $H_\infty(A_Z|E)_\chi$. Following a Z basis measurement on the A register in χ, we are left with the post-measured state:

$$\chi_{A_Z E} = \sum_y |\beta_{y|x}|^2 \sum_{z \in \mathcal{A}_d^n} p(z|y) [\mathbf{z}]_A [\mathbf{F}_{\mathbf{x},\mathbf{y}}]_E, \quad (7)$$

where $p(z|y)$ is the conditional probability of observing outcome $|z\rangle$ given input state $|y\rangle^{\mathcal{F}}$. Now, consider the following state where we add an additional, classical, ancilla:

$$\chi_{A_Z E Y} = \sum_y |\beta_{y|x}|^2 [\mathbf{y}]_Y \otimes \underbrace{\sum_{z \in \mathcal{A}_d^n} p(z|y) [\mathbf{z}]_A [\mathbf{F}_{\mathbf{x},\mathbf{y}}]_E}_{\chi^{(y)}}.$$

Then we have $H_\infty(A_Z|E)_\chi \geq H_\infty(A_Z|EY)_\chi \geq \min_y H_\infty(A_Z|E)_{\chi^{(y)}}$ where we used Equation 1 for the last inequality. Since the E and A_Z registers are independent in $\chi^{(y)}$ we have $H_\infty(A_Z|E)_{\chi^{(y)}} = H_\infty(A_Z)_{\chi^{(y)}} = -\log_2 \max_z p(z|y)$. It is not difficult to see that $p(z|y) = d^{-n}$ for all $y, z \in \mathcal{A}_d^n$. Thus $H_\infty(A_Z|E)_\chi \geq n \log_2 d$. Note that our bound here, and also on $|J(q\,:\,x)|$, are independent of x. Thus, concluding, we have the following bound on the entropy in the ideal state:

$$H_\infty(A_Z|E)_\sigma \geq n\left(\log_2 d - \frac{H_d(w(s(q)) + \delta)}{\log_d 2}\right). \quad (8)$$

Of course, this was only the ideal state analysis, however, Equation 8 holds for any choice of subset t and observation q. We now use this result to derive the final security of the real state produced by Eve and show that, with high probability over the choice of subset t and measurement outcome q, the final secret key produced by the protocol will be secure.

Step 3: Real State Security - The QCKA protocol (and, indeed, most if not all QKD protocols) may be broken into three distinct modules or CPTP maps: first is a sampling module $\mathcal{S}$ which takes as input a quantum state ρ_{TABE} where the T register represents the sampling subset t used and B represents all p Bobs. Here, this module measures the T register which chooses a subset t; from this, all qudits indexed by t are measured in the Fourier basis, producing outcome $q \in \mathcal{A}_d^{m \cdot (p+1)}$. The output of this process is the subset chosen t, the observed q, and also the post-measured state $\rho_{ABE}(t, q)$. Following this, the raw-key generation module is run, denoted $\mathcal{R}$, which takes as input the previous post measured state and measures the remaining systems in the Z basis resulting in raw keys for all parties. The output of this module is the raw key produced along with a post-measured state for Eve. Finally, a post-processing module is run, denoted $\mathcal{P}$, which will run an error correction protocol and privacy amplification, yielding the final secret key. The output of this last CPTP map is the actual secret key produced along with Eve's final quantum ancilla. This module requires as input the raw keys along with q (needed to determine the final secret key size). We want to show, with high probability over the choice of sampling subset and test measurement outcome, that the final secret key is ϵ_{PA}-close to the ideal secret key as defined by Equation 2.

Recall, $|\psi\rangle_{AB_1 \cdots B_p E}$ is the actual state produced by the adversary and sent to each of the parties. We may assume this is a pure state as a mixed state would lead to greater uncertainty for Eve. Of course, in the real case, the choice of subset is independent of the state produced by Eve and so we write the complete real state as $\rho_{TABE} = \sum_t \frac{1}{T} [\mathbf{t}] \otimes [\psi]$ where $T = \binom{N}{m}$. From this, an ideal state of the form $\sum_t \frac{1}{T} [\mathbf{t}] \otimes \left[\phi^{\mathbf{t}}\right]_{ABE}$ may be defined as was analyzed previously in the second step of the proof. We may write the action of the composition $\mathcal{P} \circ \mathcal{R} \circ \mathcal{S} = \mathcal{PRS}$ as follows:

$$\mathcal{PRS}\left(\sum_t \frac{1}{T} [\mathbf{t}]_T [\psi]\right) = \sum_{q,t} p(q,t) [\mathbf{q}, \mathbf{t}] \mathcal{P}_q \mathcal{R}\left(\left[\psi_{\mathbf{q}}^{\mathbf{t}}\right]_{ABE}\right)$$

$$\mathcal{PRS}\left(\sum_t \frac{1}{T} [\mathbf{t}]_T [\phi^{\mathbf{t}}]\right) = \sum_{q,t} \tilde{p}(q,t) [\mathbf{q}, \mathbf{t}] \mathcal{P}_q \mathcal{R}\left(\left[\phi_{\mathbf{q}}^{\mathbf{t}}\right]_{ABE}\right).$$

Above, $p(q,t)$ is the probability of choosing subset t and observing outcome q in the real state and $\tilde{p}(q,t)$ is similar but for the ideal state. The post-measured state after sampling are denoted $|\psi_q^t\rangle$ in the real case and $|\phi_q^t\rangle$ in the ideal case (see Equation 5 for what this state looks like in the ideal case). Note that, conditioning on a particular q, t, these states are pure.

Let $\ell(q, \lambda) = n(\log_2 d - \frac{1}{\log_d 2} H_d(w(s(q)) + \delta)) - \lambda - 2\log_2\left(\frac{1}{\epsilon}\right)$ where λ will be used to denote the leaked information due to error correction. Then, from Equation 2

and our analysis on the min entropy of the post-measured ideal state in Equation 8, we know that for any t and observed q, if privacy amplification shrinks the raw key to a size of ℓ, it holds that: $\left|\left|\mathcal{P}_q\mathcal{R}\left(\left[\phi^{\mathbf{t}}_{\mathbf{q}}\right]\right) - \mathcal{U}_{\ell(q,\lambda)} \otimes tr_A\mathcal{P}_q\mathcal{R}\left(\left[\phi^{\mathbf{t}}_{\mathbf{q}}\right]\right)\right|\right| \leq \epsilon$, where $\mathcal{U}_k = \frac{1}{2^k}\sum_{i=0}^{2^k-1}[\mathbf{i}]$. Finally, note that the above of course implies that: $\left|\left|\sum_{q,t}\tilde{p}(q,t)[\mathbf{q},\mathbf{t}]\left(\mathcal{P}_q\mathcal{R}\left(\left[\phi^{\mathbf{t}}_{\mathbf{q}}\right]\right) - \mathcal{U}_{\ell(q,\lambda)}tr_A\mathcal{P}_q\mathcal{R}\left(\left[\phi^{\mathbf{t}}_{\mathbf{q}}\right]\right)\right)\right|\right|$ is upper-bounded by ϵ.

We now claim that, with high probability over t and measurement outcome q, it holds that:

$$\left|\left|\mathcal{P}_q\mathcal{R}\left(\left[\psi^{\mathbf{t}}_{\mathbf{q}}\right]\right) - \mathcal{U}_{\ell(q,\lambda)} \otimes tr_A\mathcal{P}_q\mathcal{R}\left(\left[\psi^{\mathbf{t}}_{\mathbf{q}}\right]\right)\right|\right| \leq \epsilon_{PA} \quad (9)$$

where $\epsilon_{PA} = 5\epsilon + (20\epsilon)^{1/3}$. Thus, the resulting secret key is ϵ_{PA}-secure.

Let $\Delta_{t,q} = \frac{1}{2}\left|\left|\mathcal{P}_q\mathcal{R}(\left[\psi^{\mathbf{t}}_{\mathbf{q}}\right]) - \mathcal{U}_{\ell(q,\lambda)} \otimes tr_A\mathcal{P}_q\mathcal{R}(\left[\psi^{\mathbf{t}}_{\mathbf{q}}\right])\right|\right|$. Then, it can be shown (see the full paper for details [30]) that: $\frac{5\epsilon}{2} \geq \sum_{q,t} p(q,t)\Delta_{q,t}$. We now consider $\Delta_{q,t}$ as a random variable over q and t. From the above, its expected value is upper-bounded by $5\epsilon/2$. Furthermore, since $\Delta_{t,q} \leq 1$ for all t, q (by properties of trace distance), the variance may also be upper-bounded by $5\epsilon/2$. Using Chebyshev's inequality:

$$Pr\left[\left|\Delta_{t,q} - \frac{5\epsilon}{2}\right| \leq \left(\frac{5\epsilon}{2}\right)^{1/3}\right] \geq 1 - \left(\frac{5\epsilon}{2}\right)^{1/3}, \quad (10)$$

From this, and simple algebra, it follows that, except with probability at most $\epsilon_{\text{fail}} = (5\epsilon/2)^{1/3}$, Equation 9 holds. This implies that, with high probability over the choice of subset t and test measurement outcome in the Fourier basis q, Alice and the p Bob's are left with an $\epsilon_{PA} = 5\epsilon + (20\epsilon)^{1/3}$ secure key of size:

$$\ell = n\left(\log_2 d - \frac{H_d(w(s(q)) + \delta)}{\log_d 2}\right) - \lambda - 2\log_2\frac{1}{\epsilon}, \quad (11)$$

concluding the security proof.

A. Evaluation

We now evaluate our key-rate bound for this protocol assuming a depolarization channel. This assumption is not required for our security proof which works for any channel. However, we will consider depolarization channels in order to compare with prior work (which also assume depolarization channels when evaluating key-rates). This also allows us to easily bound the error correction leakage using results in [24] and [31]. More details on our evaluation settings and how to bound the error correction leakage in this scenario may be found in the full paper [30].

In dimension two ($d = 2$), a comparison of our key-rate bound, and that derived in [24] through alternative means, is shown in Figure 1 (Left). We note that, except for a slight deviation, the two results agree (with prior results from [24] surpassing ours by a small amount). Of course, the proof and results in [24] apply only to $d = 2$; to our knowledge, we are the first to derive a high-dimensional QCKA protocol along with a rigorous finite-key proof of security.

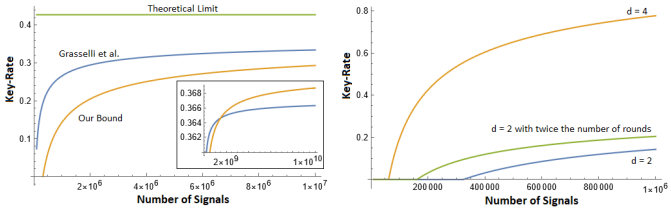

Fig. 1. Left: Comparing our new bound with that from [24] for the qubit case ($d = 2$) with 10% depolarization noise. We note that our result is slightly lower than in [24] for this dimension though they tend to converge as the number of signals increases (Inset). However, the advantage to our approach is that it can readily handle higher dimensions. Right: Showing that the advantage in key-rate for higher dimensions cannot be recovered simply by using lower-dimensional systems and increasing the number of rounds/signals.

We also evaluate our key-rate bound in higher-dimensions. In higher dimensions, we cannot compare to any other QCKA protocols as we are not aware of any other finite key security results for such protocols in high (greater than 2) dimensions. However, we note several interesting properties here. First, as the dimension increases, the number of signals needed before a positive key-rate is achieved, decreases, and the general key-rate increases, making the protocol potentially more efficient. Note that one explanation for the increased key-rate is due to the fact that one receives, for each signal, a larger number of raw-key bits as the dimension increases. However this, alone, does not explain the great increase in key-rate as the signal dimension increases. For instance, if we compare $d = 2$ and $d' = 4$, a single iteration of the protocol, in the first case, produces at most one raw key bit, while the second case would produce at most 2 raw key bits. If this were the only reason for the increase in secret key-rates, one would expect that running twice the number of iterations for the $d = 2$ case would produce the same secret key length as the $d' = 4$ case. However this is clearly not the case, as shown in Figure 1 (Right). We also note that the number of Bob's, p, does not noticeably affect the key-rate regardless of d - interestingly, this was also discovered in [24] for the qubit, $d = 2$, case.

IV. Closing Remarks

In this paper, we proved the security of a high-dimensional QCKA protocol, allowing multiple parties to establish a shared secret key. We proved security using a combination of the quantum sampling framework of [25], along with sample-based entropic uncertainty relation techniques from [26]. Our proof introduced several new methods needed to use those two frameworks in this multi-user scenario and our methods may be applicable to other multi-user quantum cryptographic protocols, especially in higher dimensions. Our work here, has shown even more evidence, beyond that already known (as discussed in the Introduction), of the potential benefits, at least in theory, of high-dimensional quantum states.

Acknowledgments: WOK would like to acknowledge support from the National Science Foundation under grant number 2006126.

REFERENCES

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep 2009. [Online]. Available: http://link.aps.org/doi/10.1103/RevModPhys.81.1301

[2] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, "Advances in quantum cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.

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

[4] A. Cabello, "Multiparty key distribution and secret sharing based on entanglement swapping," *arXiv preprint quant-ph/0009025*, 2000.

[5] M. Epping, H. Kampermann, D. Bruß *et al.*, "Multi-partite entanglement can speed up quantum key distribution in networks," *New Journal of Physics*, vol. 19, no. 9, p. 093012, 2017.

[6] F. Grasselli, H. Kampermann, and D. Bruß, "Conference key agreement with single-photon interference," *New Journal of Physics*, vol. 21, no. 12, p. 123002, 2019.

[7] Y. Wu, J. Zhou, X. Gong, Y. Guo, Z.-M. Zhang, and G. He, "Continuous-variable measurement-device-independent multipartite quantum communication," *Physical Review A*, vol. 93, no. 2, p. 022325, 2016.

[8] C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, "Modular network for high-rate quantum conferencing," *Communications Physics*, vol. 2, no. 1, pp. 1–6, 2019.

[9] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and A. Fedrizzi, "Experimental quantum conference key agreement," *Science Advances*, vol. 7, no. 23, p. eabe0395, 2021.

[10] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, "Quantum conference key agreement: A review," *Advanced Quantum Technologies*, vol. 3, no. 11, p. 2000025, 2020.

[11] H. Bechmann-Pasquinucci and W. Tittel, "Quantum cryptography using larger alphabets," *Physical Review A*, vol. 61, no. 6, p. 062308, 2000.

[12] H. F. Chau, "Unconditionally secure key distribution in higher dimensions by depolarization," *IEEE Transactions on Information Theory*, vol. 51, no. 4, pp. 1451–1468, 2005.

[13] L. Sheridan and V. Scarani, "Security proof for quantum key distribution using qudit systems," *Physical Review A*, vol. 82, no. 3, p. 030301, 2010.

[14] T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol without monitoring signal disturbance," *Nature*, vol. 509, no. 7501, pp. 475–478, 2014.

[15] H. Chau, "Quantum key distribution using qudits that each encode one bit of raw key," *Physical Review A*, vol. 92, no. 6, p. 062324, 2015.

[16] C. Vlachou, W. Krawec, P. Mateus, N. Paunković, and A. Souto, "Quantum key distribution with quantum walks," *Quantum Information Processing*, vol. 17, no. 11, pp. 1–37, 2018.

[17] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," *Physical review letters*, vol. 88, no. 12, p. 127902, 2002.

[18] G. M. Nikolopoulos and G. Alber, "Security bound of two-basis quantum-key-distribution protocols using qudits," *Physical Review A*, vol. 72, no. 3, p. 032320, 2005.

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

[20] G. M. Nikolopoulos, K. S. Ranade, and G. Alber, "Error tolerance of two-basis quantum-key-distribution protocols using qudits and two-way classical communication," *Physical Review A*, vol. 73, no. 3, p. 032325, 2006.

[21] Z.-Q. Yin, S. Wang, W. Chen, Y.-G. Han, R. Wang, G.-C. Guo, and Z.-F. Han, "Improved security bound for the round-robin-differential-phase-shift quantum key distribution," *Nature communications*, vol. 9, no. 1, pp. 1–8, 2018.

[22] M. Doda, M. Huber, G. Murta, M. Pivoluska, M. Plesch, and C. Vlachou, "Quantum key distribution overcoming extreme noise: simultaneous subspace coding using high-dimensional entanglement," *Physical Review Applied*, vol. 15, no. 3, p. 034003, 2021.

[23] M. Pivoluska, M. Huber, and M. Malik, "Layered quantum key distribution," *Physical Review A*, vol. 97, no. 3, p. 032312, 2018.

[24] F. Grasselli, H. Kampermann, and D. Bruß, "Finite-key effects in multipartite quantum key distribution protocols," *New Journal of Physics*, vol. 20, no. 11, p. 113014, 2018.

[25] N. J. Bouman and S. Fehr, "Sampling in a quantum population, and applications," in *Annual Cryptology Conference*. Springer, 2010, pp. 724–741.

[26] W. O. Krawec, "Quantum sampling and entropic uncertainty," *Quantum Information Processing*, vol. 18, no. 12, pp. 1–18, 2019.

[27] R. Renner, "Security of quantum key distribution," *International Journal of Quantum Information*, vol. 6, no. 01, pp. 1–127, 2008.

[28] W. 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.

[29] K. Yao, W. O. Krawec, and J. Zhu, "Quantum sampling for finite key rates in high dimensional quantum cryptography," *IEEE Transactions on Information Theory*, 2022.

[30] O. Amer and W. O. Krawec, "High-dimensional quantum conference key agreement," *arXiv:2202.00140*, 2022.

[31] K. Brádler, M. Mirhosseini, R. Fickler, A. Broadbent, and R. Boyd, "Finite-key security analysis for multilevel quantum key distribution," *New Journal of Physics*, vol. 18, no. 7, p. 073030, 2016.