IEEE Transactions on Quantum Engineering

Received June 29, 2020; accepted August 6, 2020; date of publication August 20, 2020; date of current version September 23, 2020.

Digital Object Identifier 10.1109/TQE.2020.3018133

High-Dimensional Semiquantum Cryptography

HASAN IQBAL AND WALTER O. KRAWEC
University of Connecticut, Storrs, CT 06296 USA

This work was supported in part by the National Science Foundation under Grant 1812070. Corresponding author: Walter O. Krawec (walter.krawec@gmail.com).

ABSTRACT A semiquantum key distribution (SQKD) protocol allows two users, one of whom is restricted in their quantum capabilities to being nearly classical, to establish a shared secret key, secure against an all-powerful adversary. The study of such protocols helps to answer the fundamental question of "how quantum" must a protocol be to gain an advantage over classical communication. In this article, we design a new SQKD protocol using high-dimensional quantum states and conduct an information theoretic security analysis. We show that, similar to the fully quantum key distribution case, high-dimensional systems can increase the noise tolerance in the semiquantum case. Furthermore, we prove several general security results which are applicable to other (S)QKD protocols (both high-dimensional ones and standard qubit-based protocols) utilizing a two-way quantum channel.

INDEX TERMS Quantum cryptography, quantum information theory, quantum key distribution.

I. INTRODUCTION

It is well known that secure key distribution, using only classical communication, is impossible unless computational assumptions are placed on the power of the adversary. If both A and B are able to communicate using quantum resources, however, perfect security is possible and the only assumption on the adversary required is that she obey the laws of quantum physics. Quantum key distribution (QKD) protocols allow two parties (Alice, A, and Bob, B) to establish a shared secret key, secure against an all-powerful adversary (Eve, E). Since the first QKD protocol developed by Bennett and Brassard in 1984 (the so-called BB84 protocol [1]), both the theory and practice of QKD has been increasing dramatically. For a general survey of QKD, both the theory and practice, the reader is referred to [2]–[4].

Since perfect security for key distribution is impossible if both A and B are restricted to classical communication while it *is* possible if both A and B are "quantum capable," a natural question to ask is "what is the middle ground?" A communication model designed to help answer this question is the so-called semiquantum model of cryptography, first introduced in 2007 by Boyer *et al.* [5]. In this model, one party is "fully quantum" in that they can do anything the protocol requires of them so long as it is possible according to quantum mechanics. The second party, however, is restricted to operations which are mathematically equivalent to classical communication. Thus, one party is quantum while the other party is "classical." Since its original introduction in 2007, there have been numerous new semiquantum key distribution (SQKD) protocols developed [6]–[12]. There have also been extensions to the model beyond basic key distribution including secret sharing [13]–[15], identification [16], and state comparison [17]–[19].

(S)QKD protocols operate in two stages: first is a *quantum communication stage* whereby users utilize the quantum channel, along with the classical authenticated channel (which is a classical communication channel that is authenticated, but not secret), to establish a *raw key*. A and B both have their own raw key which is a string of classical bits that are partially correlated (there may be some errors due to an adversary's attack or just natural noise) and partially secret (an adversary may have some information on this raw key). Thus, this raw key by itself cannot be used directly as a secret key. Users, therefore, must run a second stage where, at a minimum, they will execute an error correction protocol using the authenticated classical channel (leaking additional information to E) followed by a privacy amplification protocol which takes the error-corrected raw key and hashes it down to a smaller secret key. The relative size of the secret key compared to the initial raw key (called the *key-rate* of the protocol) is a statistic of great importance in QKD research and bounding it, as a function of observed noise in the quantum channel, is the main challenge in any (S)QKD security proof. A related statistic is the *noise tolerance* of the protocol which specifies the noise threshold after which the adversary has too much information and so users must simply abort (e.g., BB84's noise tolerance is 11% [20], [21]). Before this tolerance threshold is reached, privacy amplification is able to give a positive, though potentially small, key (the size of the secret key decreases as the noise increases due to the

direct correlation between noise and adversarial information gain).

As far as semiquantum cryptography is concerned, there have been, by now, several proofs of security based on key-rate computations for SQKD protocols and, rather surprisingly, despite the limitations on one of the users, along with the increased attack strategy space afforded to the adversary (due to the requirement of a two-way quantum channel allowing quantum resources to travel from A, to B, then back to A), noise tolerances compare favorably to several fully quantum protocols. In particular, in [22], the noise tolerance of the original Boyer *et al.*, protocol can approach 11%, the same as BB84. However, this optimistic result required looking at numerous *mismatched statistics* (a technique introduced in [23], extended for one-way channels in [24]–[26], and expanded for two-way quantum channels in [22]). Without these statistics, and only looking at the error rate, Boyer *et al.*, protocol has a noise tolerance of 6.14%, though this is only a lower bound and future refinements to the security proof techniques may improve this to the 11% found with mismatched measurements. Currently, the best-known noise tolerance for an SQKD protocol is from [27] which can attain a tolerance of 17.8% or even as high as 26% for certain, practical, quantum channels (a result comparable to BB84 with classical advantage distillation [28], [29]). Again, this high tolerance bound required looking at numerous mismatched measurements.

Designing protocols with increased noise tolerance is an important task. Encouraged by recent theoretical successes in fully-quantum QKD using high-dimensional carriers [30]–[41] and, in particular, these protocols' ability to withstand high channel noise levels [30]–[32], [34] (some approaching 50% noise tolerance as the dimension of the quantum carrier approaches infinity [33]), or other interesting properties, such as the "round-robin" protocol which can bound Eve's information based only on the dimension of the signal [38], we ask, can a high-dimensional quantum communication channel also benefit semiquantum key distribution? Or does this substantial improvement in noise tolerance require two fully quantum users to truly harness? We note that a high-dimensional SQKD protocol was introduced in [34], using a quantum walk as the information carrier, however, a noise tolerance computation was not performed due to the great complexity of that protocol and so this question still remained open (*though the methods we develop in this article may be applicable to other protocols such as this quantum-walk based protocol*).

Besides potential increases in noise tolerance, high-dimensional systems afford other advantages, namely that greater communication efficiency is possible per signal (meaning potentially more bits may be sent per signal due to the increased dimension). Such systems are experimentally feasible also through, for example, time-bin encoding [42], [43], or space division multiplexing [44] just to list some examples. Finally, some protocols, such as the so-called "round-robin" protocol [38] actually allow users to bound Eve's information based only on the dimension instead of the observed noise. Naturally, there are also disadvantages to high-dimensional systems, namely in their increased implementation complexity. However, in this article, we focus primarily on theoretical behavior of these systems, leaving implementation complexity for future work. For a general survey of high-dimensional quantum communication, along with additional information on the advantages and disadvantages of using these systems, the reader is referred to [45].

In this article, we show high-dimensional states can benefit semiquantum communication and in doing so, make several contributions in this article. We design a new high-dimensional SQKD protocol and conduct an information theoretic security analysis allowing us to compute a lower bound on its key-rate based on observed channel noise. *Our security proof introduces several new techniques which may be applicable to other (S)QKD protocols (both standard qubit-based and future-developed high-dimensional ones including, perhaps, the quantum-walk SQKD protocol developed in [34]).* Semiquantum protocols rely on a two-way quantum channel giving the adversary a greater attack strategy space making security analyses for semiquantum protocols difficult, especially in higher dimensions (all past work involving key-rate computations have been for the qubit case). As such, our new methods may prove beneficial not only for other semiquantum protocols, but also fully quantum protocols reliant on a two way quantum channel (of which there are several [46]–[51]).

One of the main contributions of our security proof method is to show how a large class of two-way high-dimensional SQKD protocol may be reduced to an equivalent one-way fully quantum protocol, making it easier to analyze. This extends an earlier result of ours in a conference paper [52] to higher dimensions and a larger class of SQKD protocol. The techniques here may be applicable to other two-way protocols. Note that in [48], it was shown how to reduce some two-way fully quantum QKD protocols to one-way protocols. However, that method only applied if a certain symmetry condition was met—a condition that is not possible to attain for semiquantum protocols and, indeed, for other "limited-resource" QKD protocols. Thus, our new methods may shed light on how to prove security for other two-way QKD protocols, semiquantum or otherwise, which, to this point, have been intractable to analyze.

Finally, we evaluate our protocol's performance and determine its noise tolerance for varying dimensions and show that, indeed, high-dimensional carriers do benefit the noise tolerance and efficiency of semiquantum protocols. We show that our protocol's noise tolerance tends to 30% as the dimension increases; this result is without requiring any mismatched statistics. While this is not as high as the 50% achieved in the fully quantum case [33], this is still higher than any other SQKD protocol to-date and, considering that this is a semiquantum protocol, where one participant is severely limited in their capabilities, is still a very positive result. This article paves the way for future research in

higher dimensional systems for semiquantum or two-way quantum cryptography. By analyzing semiquantum protocols with high-dimensional systems, we further map out the "gap" between classical and quantum communication systems.

In this article, we are primarily concerned with a theoretical protocol and not practical attacks or complications involving its implementation. Though, we do mention one potential practical version of our protocol later, we leave its full security analysis as future work. We note that several fully quantum high-dimensional QKD protocols have been experimentally implemented and the experimental generation of high-dimensional entangled states has seen rapid progress lately [53]–[56]. However, we do not concern ourselves with an exact analysis of practical implementations of this system in the semiquantum setting. Instead, we are solely interested in understanding how high-dimensional quantum states may benefit the semiquantum model of cryptography, leaving an exact study of practical issues as future work.

II. PRELIMINARIES

If ρ_{AB} is a *density operator* (i.e., a Hermitian positive semidefinite operator of unit trace) acting on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, then, we write ρ_A to mean the partial trace over the B portion, namely $\rho_A = tr_B \rho_{AB}$. Similarly for other, or multiple, systems. Given a system ρ_{AB} which is unmeasured, and an orthonormal basis $V = \{|v_1\rangle, \ldots, |v_d\rangle\}$ for the A system (which is of dimension d), then, we write $\rho_{A^V B}$ to mean the density operator resulting from a measurement of the A register in this V basis. We use $[\psi]$ to mean $|\psi\rangle\langle\psi|$.

We use $H(A)_\rho$ to mean the entropy function—either the classical Shannon entropy (if ρ is a classical state) or the quantum von Neumann entropy (the context will always be clear which we mean). Note this implies ρ is a density operator acting on *at least* some A register (if it acts on others, we first trace out those additional spaces and compute the entropy in the resulting A space only). von Neumann entropy is defined: $H(A)_\rho = H(\rho_A) = -tr(\rho_A \log \rho_A)$ (where all logarithms in this article are base two). The conditional entropy is denoted $H(A|B)_\rho$ and defined $H(AB)_\rho - H(A)_\rho$. If ρ_{AB} is an unmeasured quantum state, then by $H(A^V|B)_\rho$ we mean the conditional entropy in the operator resulting from measuring the A portion of ρ_{AB} in the V basis (the B portion remains unmeasured). By $H(A^V|B^V)_\rho$ we mean the same, but after also measuring the B portion (in which case the entire state is classical and so Shannon entropy is used). If the context is clear, we may drop the subscript. Finally, for a real number $x \in [0, 1]$, we write $H(x)$ to mean the binary Shannon entropy, namely $H(x) = -x \log x - (1-x)\log(1-x)$.

Given operator X, we write $||X||$ to mean the trace distance. If X is Hermitian and finite dimensional, then this is simply the sum of the absolute values of the eigenvalues of X.

Finally, let ρ_{ABE} be a quantum state where the A portion is d-dimensional and let $V = \{|v_1\rangle, \ldots, |v_d\rangle\}$ and $U = \{|u_1\rangle, \ldots, |u_d\rangle\}$ be two orthonormal bases. An important *entropic uncertainty relation* which will be used later, was proven in [57] and states that for any quantum state ρ_{ABE}, it holds that

$$H(A^V|E)_\rho + H(A^U|B) \geq -\log c \tag{1}$$

where $c = \max_{i,j} |\langle v_i|u_j\rangle|^2$. This will be used in our proof of security later.

A. SEMIQUANTUM CRYPTOGRAPHY

The semiquantum model, as introduced in [5], consists of at least one "fully quantum" user (typically A) and one "classical" or "semiquantum" user (typically B). This classical user is only allowed to interact with the quantum channel in a very restricted way. In particular, he can choose to do one of two things on receiving any quantum state from A.

1) `Reflect`: If he chooses this option, he will disconnect from the quantum channel, creating a loop back to A. In this case, the quantum user is simply "talking to herself" over a large, looped, quantum channel.
2) `Measure and Resend`: If he chooses this option, he will perform a measurement of the quantum state in a single, publicly known, basis (typically the computational basis). Based on his measurement result, he will then send a new quantum state, prepared in this same basis, back to A.

Clearly, if both users are semiquantum and can only perform these two operations, the system is mathematically equivalent to a classical communication protocol as both users would be restricted to only operating directly in a single, publicly known, basis. Thus, the interest in semiquantum cryptography is to see how security holds when one user is quantum, but the other is classical according to the above functionality.

Note that we are not considering practical device security in this article and are only interested in the theoretical properties of semiquantum communication. Thus, we do not concern ourselves with such attacks as the photon tagging attack [58], [59] or multiphoton attacks (especially problematic when B chooses `Measure and Resend` as he must reprepare qubits in the observed state). Though interesting, these are outside the scope of this article—techniques from [7] may prove beneficial to securing our protocol against these attacks but we leave this as interesting future work.

As mentioned earlier, (S)QKD protocols operate, first, through a quantum communication stage. This stage utilizes the quantum communication channel and the authenticated classical channel to output a *raw key* of size N bits. From this, error correction and privacy amplification are run outputting a secret key of size $\ell(N)$ bits. The *key-rate* is defined to be the ratio $\ell(N)/N$. We are interested in the theoretical asymptotic limit. In this case, assuming collective attacks (i.i.d. attacks where E is free to store a quantum memory system for measurement at any future point in time [2]), it was shown in [21]

and [60] that

$$r = \lim_{N\to\infty} \frac{\ell(N)}{N} = \inf(H(A|E)_\rho - H(A|B)_\rho) \qquad (2)$$

where ρ_{ABE} is a density operator describing a single iteration of the quantum communication stage, conditioned on that iteration being used to distill raw key material (i.e., not on an iteration used only for error checking or an iteration that is later discarded due to an incompatible basis choice). The infimum is over all collective attacks that induce the observed noise statistics. Above, the A and B registers are the actual classical raw key bit registers and only the E portion is quantum. It is this entropy equation, and in particular the von Neumann entropy $H(A|E)$, that we are interested in computing and is the main challenge (computing $H(A|B)$ is generally trivial given the observed noise statistics).

Our protocol uses higher dimensional systems and, as such, we must define the bases we work with. For the classical user, we will use the computational basis of dimension 2^n, namely $\{|0\cdots00\rangle, |0\cdots01\rangle, \ldots, |1\cdots11\rangle\}$ which, when needed to simplify notation, we will also label equivalently as $\{|0\rangle, |1\rangle, \ldots, |2^n-1\rangle\}$. We use $\mathcal{Z}$ to denote this basis.

The quantum user, of course, is not restricted to operating in only one basis and so we also define the following "$\mathcal{F}$" basis:

$$\mathcal{F} = \{|F_0\rangle, |F_1\rangle, \ldots, |F_{2^n-1}\rangle\} \qquad (3)$$

where $|F_x\rangle = \mathcal{F}|x\rangle$ and $\mathcal{F}$ is the quantum Fourier transform, namely

$$\mathcal{F}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \exp(-\pi i xy/2^{n-1})|y\rangle . \qquad (4)$$

Of course, one may consider other bases that the quantum user may utilize. However, our protocol will make use of both the $\mathcal{Z}$ and $\mathcal{F}$ bases. Note that, for the classical user, if he chooses `Measure and Resend` or `Reflect`, that operation is performed on an entire n-qubit signal state (e.g., he cannot reflect "half" the qubits and measure the other half in our model).

III. PROTOCOL

Our protocol is shown in Protocol 1. The protocol operates by having A send signals of n-qubits each. For each iteration, B will either `Measure and Resend` the entire n-qubit state or he will `Reflect` the entire state. Whenever A sends a $\mathcal{Z}$ basis state and B chooses to `Measure and Resend`, they will add n bits to their raw key. Once a sufficiently large raw key has been established, standard error correction and privacy amplification are run. In the next section, we will compute a lower bound on the key-rate of this protocol. We will consider a noisy, but loss-less, quantum channel and ideal devices. Practical security concerns, though interesting, are outside the scope of this article and would provide interesting future work. Any collective attack against this protocol consists of two unitary operators (U_F, U_R) where U_F is applied in the forward channel and U_R is applied in the reverse.

Protocol 1: n-Dimensional SQKD: Π^{SQKD}.

Public Parameters: n: the number of qubits to send per signal; p_M, the probability of choosing `Measure and Resend`; p_Z, the probability of A choosing the $\mathcal{Z}$ basis.

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

1) With probability p_Z, A prepares a randomly chosen $\mathcal{Z}$ basis state; otherwise she prepares a randomly chosen $\mathcal{F}$ basis state. She records her choice of basis and the choice of state and sends the resulting n-qubit state to B.
2) B chooses, with probability p_M to `Measure and Resend`, measuring all n qubits in the computational basis and recording the result and then resending the observed state back to A. Otherwise, with probability $1-p_M$, he chooses `Reflect` in which case he reflects all n qubits back to A.
3) A measures the returning n qubit system in the same basis she used to prepare.
4) A and B, using the authenticated classical channel, divulge their choices (B his choice of "`Measure and Resend`" or "`Reflect`" and A her choice of basis). If A chose the $\mathcal{Z}$ basis and B chose `Measure and Resend`, they will use this iteration to contribute towards their raw key; namely, B will append his n-bit measurement result string and A will append her initial state she prepared to their respective raw keys (in this case, A's subsequent measurement result is not used). We call this a *key-distillation iteration*. Otherwise, this iteration (along with a suitably chosen random subset of key-distillation iterations) may be used for error detection in the obvious way.

IV. SECURITY ANALYSIS

We now analyze the security of our protocol. As with other (S)QKD protocols, we show security against collective attacks. We will comment on general attacks later. Our security analysis extends ideas introduced in our conference paper [52] but to the higher dimensional case and consists of two main parts: First, we will prove that it is sufficient to analyze a particular *one-way* fully quantum protocol and, once security is proven there assuming the same channel observations are made, security of our SQKD protocol follows immediately. *This reduction is very general and can apply to other SQKD protocols*. Thus, to analyze security of the two-way semiquantum protocol, it suffices to consider a particular one-way protocol which is easier to analyze as E

only attacks once. Second, we analyze the security of this one-way protocol through the use of entropic uncertainty relations, and continuity of conditional von Neumann entropy. The techniques we develop in both steps are often general and may be applicable to other two-way (S)QKD protocols.

A. REDUCTION TO A ONE-WAY PROTOCOL

In this section, we show how certain SQKD protocols, of arbitrary dimensions, may be reduced to a one-way protocol. Note that in [48], a method of reducing two-way fully quantum protocols to one-way, entanglement-based protocols was shown, however, that method only applies if the original protocol admits a certain symmetry property which semiquantum protocols necessarily lack (due to B's use of `Measure and Resend`). As a first step, we first consider an intermediate, two-way, SQKD protocol, which we denote by $\Pi^{\texttt{ent}}$. This intermediate protocol is no longer prepare-and-measure, but instead has A preparing entangled qudits and B performing a CNOT gate whenever he chooses `Measure and Resend`. The protocol is shown in Protocol 2. It is not difficult to see that security of $\Pi^{\texttt{ent}}$ implies security of $\Pi^{\texttt{SQKD}}$ (i.e., $\Pi^{\texttt{ent}} \Rightarrow \Pi^{\texttt{SQKD}}$ where "$\Rightarrow$" means "implies security of"). Indeed, A's prepare-and-measure scheme in $\Pi^{\texttt{SQKD}}$ is equivalent to her preparing the entangled state of $2n$ qubits $|\psi_0\rangle = \frac{1}{2^{n/2}} \sum_a |a, a\rangle$ and sending the right register (consisting of n qubits) to B while keeping the left-half to herself. If B chooses to reflect, this is nothing more than an identity operation whereas if he chooses to `Measure and Resend`, then by applying CNOT gates targeting his register and then measuring at some future time, this is equivalent to him measuring immediately. Finally, when qubits return to A, she may measure both n qubit registers in the same basis—standard arguments [2], [6] show that her measurement of the A_1 register is equivalent to her initially preparing the state she observes at this later point. Furthermore, a collective attack against this protocol is identical to the $\Pi^{\texttt{SQKD}}$ case, namely two unitary attack operators (U_F, U_R).

Next, we introduce our one-way protocol, shown in Protocol 3 and denoted $\Pi^{\texttt{OW}}$. At first glance, the two protocols, $\Pi^{\texttt{ent}}$ (which is semiquantum and uses a two-way quantum channel) and $\Pi^{\texttt{OW}}$ (which is one-way and fully quantum) do not appear similar. However, we will prove that security of $\Pi^{\texttt{OW}}$ implies security of $\Pi^{\texttt{ent}}$ (which, in turn, implies security of our actual protocol $\Pi^{\texttt{SQKD}}$). We do this by showing that, for any attack against $\Pi^{\texttt{ent}}$, there exists an attack against $\Pi^{\texttt{OW}}$ which causes E to gain as much information on the raw key as in $\Pi^{\texttt{ent}}$ and, furthermore, the view according to A, B, and E are identical in both cases (i.e., the two cases are indistinguishable). Thus, if we analyze $\Pi^{\texttt{OW}}$ (which is easier to do since it is one-way), we automatically cover any attack against $\Pi^{\texttt{ent}}$. Ultimately, this technique is an extension of a result in our conference paper [52] to the arbitrary, N-dimensional case (only the qubit, $N = 2$ case was considered before). However, beyond being more general, our proof here is also more refined as it does not require an additional "simplification" step that was necessary in [52].

Protocol 2: Entanglement-Based n-Dimensional SQKD: $\Pi^{\texttt{ent}}$.

Public Parameters: n: the number of qubits to send per signal; p_M, the probability of choosing `Measure and Resend`; p_Z, the probability of A measuring in the $\mathcal{Z}$ basis.

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

1) A prepares the $2n$-qubit state: $|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{a=0}^{2^n-1} |a, a\rangle_{A_1 T}$ and sends the "T" portion to B.
2) B chooses, with probability p_M to `Measure and Resend` in which case he applies the operator $CNOT^{\otimes n}$, acting on the T space and his own private B register (also of n qubits). Otherwise, with probability $1 - p_M$, he chooses `Reflect` and applies $I^{\otimes n}$ to the T portion (thus, his B register will remain independent of the system in this case). Either way, the T register is then returned to A. Once returned, we rename the T register as the A_2 register.
3) A chooses to measure in the $\mathcal{Z}$ basis (with probability p_Z) or the $\mathcal{F}$ basis (with probability $1 - p_Z$). She measures both the A_1 register and the returned T register (now called the A_2 register) in the same basis (either both $\mathcal{Z}$ or both $\mathcal{F}$). At this point, B will measure his register in the $\mathcal{Z}$ basis if he chose `Measure and Resend`.
4) A and B divulge their choices (B his choice of "`Measure and Resend`" or "`Reflect`" and A her choice of basis). If A choose the $\mathcal{Z}$ basis and B chose `Measure and Resend`, they will save their measurement results and append the resulting value (as a bit-string) to their respective raw keys (A will use her result from the A_1 register, discarding the A_2 register in this case).

Let $N = 2^n$. An attack against $\Pi^{\texttt{OW}}$ consists of a probability distribution $\{p(b)\}$ for all $b = 0, 1, \ldots, N-1$ along with a *single* attack operator U acting on $2n$ qubits and E's quantum ancilla. Note that E gets to choose the values $p(b)$ which B uses to prepare his states—thus, E has partial control over B's source device in $\Pi^{\texttt{OW}}$; the reason for this necessity will be apparent later in our proof. We now prove it is sufficient to consider security of $\Pi^{\texttt{OW}}$ (in which case we have $\Pi^{\texttt{OW}} \Rightarrow \Pi^{\texttt{ent}} \Rightarrow \Pi^{\texttt{SQKD}}$).

Theorem 1: Let (U_F, U_R) be a collective attack against $\Pi^{\texttt{ent}}$ and let ρ_{ABE} be the resulting density operator describing a single iteration of $\Pi^{\texttt{ent}}$ in the event this attack is used. Then, there exists an attack of the form $(\{p(b)\}_{b=0}^{2^n-1}, U)$ against $\Pi^{\texttt{OW}}$ such that, if σ_{ABE} is the resulting density operator of a single iteration of $\Pi^{\texttt{OW}}$ in this case, it holds that

Protocol 3: One-Way n-Dimensional QKD: Π^{OW}.

Public Parameters: n: the number of qubits to send per signal; p_M, the probability of choosing `Measure and Resend`; p_Z, the probability of A measuring in the $\mathcal{Z}$ basis; $\{p(b)\}_{b=0}^{2^n-1}$, probability values set by the adversary but known to all parties.

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

1) B chooses, with probability p_M operation "`Measure and Resend`" otherwise he chooses "`Reflect`." Note that the terminology `Measure and Resend` and `Reflect` do not have any operational meaning in this protocol—we simply use them so that the reduction later from our SQKD protocol Π^{SQKD} makes sense. If he chooses `Reflect`, he prepares a $3n$ qubit state of the form

$$|\phi_R\rangle = \sum_{b=0}^{2^n-1} \sqrt{p(b)}\,|b,b\rangle_{A_1A_2} \otimes |0\rangle_B \tag{5}$$

where the right-most B register contains n qubits in the state $|0\rangle$. Otherwise, if he chooses `Measure and Resend`, he prepares a $3n$ qubit state of the form

$$|\phi_{MR}\rangle = \sum_{b=0}^{2^n-1} \sqrt{p(b)}\,|b,b,b\rangle_{A_1A_2B}\,. \tag{6}$$

Regardless of his choice, he sends the A_1A_2 register (consisting of $2n$ qubits) to A.

2) Same as step (3) of Π^{ent}.

3) Same as step (4) of Π^{ent}.

$\sigma_{ABE} = \rho_{ABE}$. In particular, there is no advantage to E in either case and, furthermore, no party A, B, or E can distinguish between the two scenarios.

Proof: Fix an attack (U_F, U_R). Without loss of generality, we may write U_F's action on basis states as

$$U_F\,|a\rangle \otimes |\chi\rangle_E = \sum_{b=0}^{N-1} |b, e_{a,b}\rangle$$

where $N = 2^n$ and $|e_{a,b}\rangle$ are arbitrary states in E's ancilla (we assume, without loss of generality in the collective attack case, that E's ancilla starts in some pure state $|\chi\rangle_E$). Unitarity, of course, imposes some restrictions on these states. In particular, for every a it holds that

$$\sum_{b=0}^{N-1} \langle e_{a,b}|e_{a,b}\rangle = 1. \tag{7}$$

Given this attack, we construct $(\{p(b)\}, U)$, an attack against Π^{OW}, that satisfies the theorem statement. To do so, we follow a technique first introduced in our conference paper [52] but generalized here for higher dimensions. First, we set the values $p(b)$ to

$$p(b) = \frac{1}{N}\sum_{a=0}^{N-1} \langle e_{a,b}|e_{a,b}\rangle\,. \tag{8}$$

Clearly $p(b) \geq 0$ for all b. Furthermore, from (7), it follows that

$$\sum_b p(b) = \frac{1}{N}\sum_b\sum_a \langle e_{a,b}|e_{a,b}\rangle = \frac{1}{N}\sum_a\sum_b \langle e_{a,b}|e_{a,b}\rangle = 1.$$

Thus this is a valid probability distribution, and so a valid attack setting.

Now, consider the following operator **Rw** which we call the "rewind" operator as, in a way, it "rewinds" the channel so that a state prepared by B in the one-way case (i.e., protocol Π^{OW}) appears *to all three parties* as if it had been prepared by A in the two-way case (i.e., Π^{ent}). In particular, it will "setup" the A_1 register and E's quantum memory as if this had been performed in the two-way Π^{ent} case. The only thing that cannot be "rewound" is B's measurement distribution, thus the need for E to set this separately through the $p(b)$ values. This operator acts on basis states $|b,b\rangle$ (sent by B in the one-way protocol Π^{OW}) as follows:

$$\mathbf{Rw}\,|b,b\rangle_{A_1A_2} = \frac{\sum_{a=0}^{N-1}|a,b,e_{a,b}\rangle}{\sqrt{N\cdot p(b)}}. \tag{9}$$

It is not difficult to see that **Rw** is an isometry. Indeed, given $|b,b\rangle$ and $|b',b'\rangle$ for $b \neq b'$, we have

$$0 = \langle b,b|b',b'\rangle = \frac{1}{N\sqrt{p(b)p(b')}}\sum_{a,a'}\langle a,b,e_{a,b}|a',b',e_{a',b'}\rangle = 0.$$

Furthermore, it is noticeable that

$$1 = \langle b,b|b,b\rangle = \frac{1}{N\cdot p(b)}\sum_{a,a'}\langle a,b,e_{a,b}|a',b,e_{a',b}\rangle = \frac{1}{N\cdot p(b)}\sum_a \langle e_{a,b}|e_{a,b}\rangle = 1.$$

Thus, **Rw** is an isometry and may be extended, using standard techniques, to a unitary operator implying it is an operation that E may do within the laws of quantum physics. We claim that $U = (I_{A_1}\otimes U_R)\mathbf{Rw}$ is the desired attack operator satisfying the theorem statement.

Refer to Fig. 1. Consider the case when B chooses `Measure and Resend`. At time t^* (after E attacks with U_F and B's operation, but *before* E attacks a second time with U_R), the joint state held by A, B, and E using protocol Π^{ent} is found to be

$$|\psi_{MR}^{ent}\rangle = \frac{1}{\sqrt{N}}\sum_a |a\rangle_A \sum_b |b,e_{a,b},b\rangle_{TEB}\,. \tag{10}$$

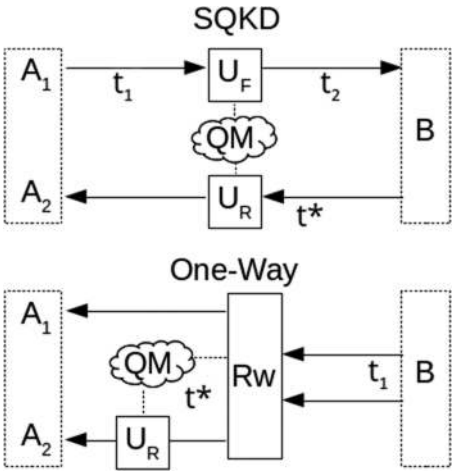

FIGURE 1. Showing the reduction from the semiquantum protocol (Π^{SQKD} and Π^{ent}, top) to the fully quantum one-way protocol (Π^{OW} bottom). For the SQKD protocol, *A* prepares qubits at time t_1, Eve attacks, and then *B* performs an operation `Measure and Resend` or `Reflect`. Time t^* is after *B*'s operation. On the other hand, for the fully quantum protocol, *B* prepares two qubits and sends both to *A*. *E* attacks with a specially designed **Rw** operator resulting in a state at time t^*. We claim a suitable **Rw** operator can be constructed so that the density operators in both cases at time t^* are identical. Later, when proving general security of the one-way protocol, we do not require any special attack; clearly security of the SQKD protocol, then, would follow. QM stands for *E*'s quantum memory.

Now, referring to Fig. 1, consider the same case (namely, B choosing `Measure and Resend`) but with the Π^{OW} protocol. In this event, B prepares the state $\sum_b \sqrt{p(b)}\,|b, b, b\rangle_{A_1A_2B}$ and E attacks with **Rw**. The joint system then, at time t^* is

$$\begin{aligned}|\phi_{MR}\rangle &= \sum_b \sqrt{p(b)}\left(\frac{\sum_a |a, b, e_{a,b}\rangle}{\sqrt{N\cdot p(b)}}\right)\otimes |b\rangle_B \\ &= \frac{1}{\sqrt{N}}\sum_a |a\rangle_{A_1}\sum_b |b, e_{a,b}, b\rangle_{A_2EB} \\ &= |\psi^{ent}_{MR}\rangle\,.\end{aligned}$$

Thus, after applying **Rw**, the state of the joint system for the case of Π^{OW} is identical to that of Π^{ent}. Of course, after applying U_R (which happens in both scenarios since we constructed $U = (I_{A_1}\otimes U_R)\mathbf{Rw}$), the systems will remain the same. *Thus, any measurement outcomes or entropy computations will be identical in both scenarios.* It is trivial to show the same holds true in the `Reflect` case for both protocols (in that case, the additional $|b\rangle$ term is no longer there but the algebra remains the same otherwise). Thus, if one were to write out a density operator description of both protocols, tracing their evolution, they would be identical as the underlying systems are identical in all cases. Note that the only thing E could not "rewind" with **Rw** is the probability distribution of B's measurements (since he is now preparing). Thus, it is required that E gets to choose the distribution $p(b)$ so that the probability distribution in Π^{OW} matches that observed in Π^{ent}. ■

Theorem 1 implies that it is sufficient to prove security of the one-way protocol Π^{OW}. Since any attack against Π^{ent} can also be transformed into an attack against Π^{OW}, if we analyze a general attack against the latter, this automatically gives security against the former. Indeed, there may be more attack strategies for E against Π^{OW} as E has access to both n qubit registers simultaneously; despite this, it is easier to analyze as it is a one-way protocol. Furthermore, note that no party can distinguish between the two scenarios and, as a consequence, observed channel noise in the "real" SQKD protocol Π^{ent} translate directly to observed statistics in the one-way protocol Π^{OW}. Our goal is to prove security of Π^{ent} (which proves security of Π^{SQKD}) and, given observed noise statistics there, if we prove security of Π^{OW} given those same statistics, the key-rate can only be better in Π^{ent} (since Π^{OW} has potentially more attack strategies as mentioned).

B. PROOF OF SECURITY FOR Π^{OW}

We now prove security of Π^{OW}. In the following, we define $N = 2^n$ where n is the user-defined number of qubits sent per iteration of our protocol. Our proof of security is in three steps. First, we compute the conditional entropy $H(A|E)$ in the case where B chooses `Reflect`. This, of course, is useless for key distillation as B is completely independent of the state in this case, but it will be used later to argue about the entropy in the actual key-distillation state (i.e., when B chooses `Measure and Resend`). Second, we argue that E's optimal attack must take on a particular form if A and B use the $\mathcal{Z}$ or $\mathcal{F}$ basis. Third, and finally, we use these results, along with Winter's continuity bound on conditional entropy [61], to compute the entropy of A's register conditioned on E's quantum memory in the actual key-distillation state when B chooses `Measure and Resend` giving us the desired key-rate.

First, we need a channel scenario for the real Π^{ent} protocol (which translates, as discussed, to observations for Π^{OW}). Keeping in line with other high-dimensional QKD analyses [32], [34], we consider a symmetric attack modeled as a depolarization channel (*which may even be enforced by users*)

$$\mathcal{E}_Q(\sigma) = \left(1 - \frac{N}{N-1}Q\right)\sigma + \frac{Q}{N-1}I \tag{11}$$

where σ is any N-dimensional quantum state.

We will assume the noise in the forward channel and reverse channel are the same and parameterized by Q (though our analysis follows even if they are different, though the algebra complexity increases). In the "reflect" case, we will use a depolarization parameter Q_F—this captures the practical case that, for certain fiber channels, reflecting a quantum state back can "undue" some noise (but in the `Measure and Resend` case this cannot happen as the "measurement" breaks any entanglement in the channel) [48], [62].

Let $p(x|y)$ be the probability that a party observes x given the sender sent y (in the $\mathcal{Z}$ or $\mathcal{F}$ basis) in either the forward

or reverse channel. From this model, we have

$$p(x|y) = \begin{cases} 1-Q & \text{if } x = y \\ \frac{Q}{N-1} & \text{otherwise.} \end{cases} \tag{12}$$

In $\Pi^{\texttt{ent}}$, the probability that A_1^Z (i.e., after measuring) is a, for any particular a, is simply $p(a) = 1/N$. Furthermore, the probability that B measures b is $\sum_a p(b|a)p(a) = \frac{1}{N}(1 - Q + (N-1)\frac{Q}{N-1}) = 1/N$. Thus, we set $p(b) = 1/N$ when analyzing $\Pi^{\texttt{OW}}$ (E's choice here must conform to the observed statistics in the "real" protocol $\Pi^{\texttt{ent}}$).

Let $p(a, b, c)$ be the probability that, in the case of `Measure and Resend`, if all parties measure in the $\mathcal{Z}$ basis, A_1 measures a, B measures b, and A_2 measures c (recall A_1 is A's first n-qubit register and A_2 is her second register). Then, since this is a classical probability distribution, by the chain rule it holds that

$$p(a, b, c) = p(c|b, a) \cdot p(b|a) \cdot p(a). \tag{13}$$

We will assume that *in the* `Measure and Resend` *case* of $\Pi^{\texttt{ent}}$, the two channels act independently and, so, $p(c|b, a) = p(c|b)$. That is, A's measurement in the return channel, depends only on what B actually sends. This is a very realistic noise scenario *and can even be enforced by the users*—A and B will simply abort if they do not observe this (natural) behavior. Of course, as discussed, we do not assume the two channels act independently if B chooses to `Reflect` (such an assumption would not be natural nor could it be enforced and so we do not make it here). Under these assumptions, it is not difficult to see that

$$p(a, b, c) = \frac{1}{N} \times \begin{cases} \beta^2 & \text{if } c = b \text{ and } b = a \\ \alpha\beta & \text{if } c \neq b \text{ and } b = a \\ \alpha\beta & \text{if } c = b \text{ and } b \neq a \\ \alpha^2 & \text{if } c \neq b \text{ and } b \neq a \end{cases} \tag{14}$$

where

$$\alpha = \frac{Q}{N-1} \quad \beta = 1 - Q. \tag{15}$$

Given these observed channel statistics in $\Pi^{\texttt{ent}}$, we now turn to $\Pi^{\texttt{OW}}$ using this same distribution on measurement events. Ultimately, our goal is to compute a lower bound on the key-rate: $H(A_1^Z|E)_\mu - H(A_1^Z|B_1^Z)_\mu$, where $\mu_{A_1B_1E}$ is the density operator describing an iteration of the protocol in the `Measure and Resend` case.

First Step—Entropy in the Reflect Case: Let $\rho_{A_1A_2BE}$ be the density operator describing the state of the system (*before measurements are made by any party*) if B chooses `Reflect`. Similarly, let $\mu_{A_1A_2BE}$ be the density operator in the case B chooses `Measure and Resend`. Since key-bits are only distilled in this `Measure and Resend` case, to compute the key-rate of the protocol, we will require a bound on the von Neumann entropy $H(A_1^Z|E)_\mu$. However, we will actually, first, bound $H(A_1^Z|E)_\rho$ and later argue that, due to continuity of entropy [61], the difference in entropy between the two systems, ρ and μ, cannot be "too large."

Consider the state $\rho_{A_1A_2BE}$. In this `Reflect` case, B's system is completely independent of all other systems; thus $\rho_{A_1A_2BE} \equiv \rho_{A_1A_2E} \otimes [\mathbf{0}]_B$ and so the B portion does not factor into any entropy equations and may be ignored. Using the entropic uncertainty relation proven in [57] [see (1)], we know

$$H(A_1^Z|E)_\rho \geq n - H(A_1^F|A_2)_\rho \geq n - H(A_1^F|A_2^F)_\rho$$

where the second inequality follows from the fact that measurements cannot decrease uncertainty. If we could distill a key from ρ, we would be finished—in fact, the above would be the case when A_1 is attempting to distill a key with herself, "A_2" which, of course, is meaningless from a practical standpoint. However, as we now show, knowing the entropy in ρ allows us to bound the entropy in μ (which is what we actually want in order to compute the key-rate of our protocol).

Consider E's attack operator U against $\Pi^{\texttt{OW}}$. Without loss of generality, we may write U's action on basis states of the form $|b, b\rangle$ as follows:

$$U\,|b, b\rangle \otimes |\chi\rangle_E = \sum_{a=0}^{N-1} \sum_{c=0}^{N-1} |a, c, e_{a,b,c}\rangle \tag{16}$$

where the $|e_{a,b,c}\rangle$ are arbitrary states in E's ancilla (again, we assume without loss of generality that E's ancilla is cleared to some initial pure state $|\chi\rangle_E$). Note that we are not assuming a particular structure to this attack (e.g., we do not assume it consists of the **Rw** operator used in the proof of Theorem 1—instead, it may be arbitrary and if we prove security here, we will gain security of $\Pi^{\texttt{ent}}$ since it will cover any attack against that protocol).

Consider $\rho_{A_1^ZE}$, i.e., the state of the system after A measures the A_1 register in the $\mathcal{Z}$ basis and tracing out A_2. Tracing the evolution of the state in this case, and recalling that $p(b) = 1/N$ due to our (enforceable) symmetry assumption, we find

$$\rho_{A_1^ZE} = \frac{1}{N} \sum_{a=0}^{N-1} [\mathbf{a}] \otimes \left(\sum_{c=0}^{N-1} P \left[\sum_{b=0}^{N-1} |e_{a,b,c}\rangle \right] \right) \tag{17}$$

where $P(z) = zz^*$.

On the other hand, tracing the evolution of the protocol in the case when B chooses `Measure and Resend`, gives us the following operator:

$$\mu_{A_1^ZE} = \frac{1}{N} \sum_{a=0}^{N-1} [\mathbf{a}] \otimes \left(\sum_{c=0}^{N-1} \sum_{b=0}^{N-1} [\mathbf{e_{a,b,c}}] \right). \tag{18}$$

Our goal in the remainder of the security proof is to bound the difference between $H(A_1^Z|E)_\rho$ and $H(A_1^Z|E)_\mu$. To do so, we will use Winter's continuity bound [61] and in particular, the case derived for classical-quantum states. This bound states that (rewriting in terms of our notation of course)

$$|H(A_1^Z|E)_\rho - H(A_1^Z|E)_\mu| \leq \Delta \log A_1^Z + (1+\Delta) H\left(\frac{\Delta}{1+\Delta}\right) \tag{19}$$

where

$$\Delta = \frac{1}{2}\left|\left|\rho_{A_1^Z E} - \mu_{A_1^Z E}\right|\right|.$$

Of course $\log A_1^Z = n$. Thus, our goal is to determine an upper bound on the trace distance Δ. Note that an upper bound will only increase the distance between the two entropies causing the key-rate to drop. Thus, by finding an upper bound, we determine a worst-case key-rate and the actual key-rate can only be higher.

By elementary properties of trace distance, along with the triangle inequality, we have

$$\Delta \leq \frac{1}{2N}\sum_{a,c=0}^{N-1} \underbrace{\left|\left| P\left(\sum_{b=0}^{N-1} |e_{a,b,c}\rangle\right) - \sum_{b=0}^{N-1} [\mathbf{e_{a,b,c}}] \right|\right|}_{\Delta_{a,c}}$$

$$= \frac{1}{2N}\sum_{a,c} \Delta_{a,c}. \tag{20}$$

Second Step—Structure of E's Attack Operator: Before computing Δ, we argue now that E's optimal attack operator has a particular structure to it. As discussed earlier, let $p(a, b, c)$ denote the probability that measuring A_1 results in a; measuring B results in b; and measuring A_2 results in c (where these measurements are performed in the $\mathcal{Z}$ basis in the `Measure and Resend` case; thus $a, b, c \in \{0, 1, \ldots, N-1\}$). It is not difficult to see that $p(a, b, c) = \langle e_{a,b,c}|e_{a,b,c}\rangle / N$. Indeed, note that the state $\mu_{A_1^Z A_2^Z BE}$ (i.e., the case where B chooses `Measure and Resend`, but before tracing out A_2^Z and B which we did for (18)) is found to be

$$\mu_{A_1^Z A_2^Z BE} = \frac{1}{N}\sum_{a,b,c} [\mathbf{a}]_{A_1} \otimes [\mathbf{c}]_{A_2} \otimes [\mathbf{b}]_B \otimes [\mathbf{e_{a,b,c}}]$$

from which it is clear that $p(a, b, c) = \langle e_{a,b,c}|e_{a,b,c}\rangle / N$. Since N is known and since $p(a, b, c)$ is a value that can be observed by the parties running the protocol, this implies $\langle e_{a,b,c}|e_{a,b,c}\rangle$ is also an observable quantity.

We now claim that it is to E's advantage to choose her attack such that for any *fixed* a, c, it holds that

$$\langle e_{a,b,c}|e_{a,b',c}\rangle = \begin{cases} N \cdot p(a, b, c) & \text{if } b = b' \\ 0 & \text{if } b \neq b'. \end{cases} \tag{21}$$

Indeed, orthogonal ancilla states cannot increase her uncertainty, thus the only reason to make these states nonorthogonal would be if, by doing so, she could make some other, potentially "more important" vectors closer to orthogonal (e.g., the nonerror cases such as $\langle e_{0,0,0}|e_{1,1,1}\rangle$) while still falling within the observed noise statistics. But the inner product $\langle e_{a,b,c}|e_{a,b',c}\rangle$ does not contribute to the observed noise in any way, assuming basis $\mathcal{F}$ is used, and thus she might as well set them to be orthogonal potentially decreasing her overall uncertainty (but certainly not increasing it).

Clearly the inner product $\langle e_{a,b,c}|e_{a,b',c}\rangle$ does not contribute to the $\mathcal{Z}$ basis noise when $b \neq b'$. We thus consider the $\mathcal{F}$ basis noise. Consider the case when B chooses `Reflect` in which case the state arriving to A, before measuring, is

$$\frac{1}{2^{n/2}}\sum_{a,c} |a, c\rangle\, |g_{a,c}\rangle \tag{22}$$

where $|g_{a,c}\rangle = \sum_b |e_{a,b,c}\rangle$. Since the above is normalized, it holds that

$$\frac{1}{2^n}\sum_{a,c} \langle g_{a,c}|g_{a,c}\rangle = 1. \tag{23}$$

Now, changing basis, we may write $|j\rangle = \sum_x \beta_{x,j} |F_x\rangle$, where $\beta_{x,j} = \langle F_x|j\rangle$. Clearly, due to our choice of basis $\mathcal{F}$, it holds that $|\beta_{x,j}|^2 = 1/2^n$. Taking (22) and changing basis in both the A_1 and A_2 registers yields

$$\frac{1}{2^{n/2}}\sum_{x,y} |F_x, F_y\rangle \left(\sum_{a,c} \beta_{x,a}\beta_{y,c}\, |g_{a,c}\rangle\right).$$

Thus, the probability that A_1 measures F_x and A_2 measures F_y, for any x, y is

$$\frac{1}{2^n}\left|\sum_{a,c} \beta_{x,a}\beta_{y,c}\, |g_{a,c}\rangle\right|^2$$

$$= \frac{1}{2^n}\sum_{a,c}\frac{1}{2^{2n}}\langle g_{a,c}|g_{a,c}\rangle + \sum_{(a,c)\neq(a',c')} \beta_{x,a}\beta^*_{x,a'}\beta_{y,c}\beta^*_{y,c'}\langle g_{a,c}|g_{a',c'}\rangle$$

$$= \frac{1}{2^{2n}} + \sum_{(a,c)\neq(a',c')} \beta_{x,a}\beta^*_{x,a'}\beta_{y,c}\beta^*_{y,c'}\langle g_{a,c}|g_{a',c'}\rangle$$

where for the third equality, we use (23). Note that $\langle g_{a,c}|g_{a',c'}\rangle$, for $(a, c) \neq (a', c')$ has no terms of the form $\langle e_{a,b,c}|e_{a,b',c}\rangle$ (since either a' or c' will not equal a or c). Thus, the $\langle e_{a,b,c}|e_{a,b',c}\rangle$ inner product cannot affect any observed noise statistic. Therefore, there is no advantage to E in making it nonorthogonal as it cannot benefit her by "hiding" other states in the noise of the channel (e.g., she cannot use $\langle e_{a,b,c}|e_{a,b',c}\rangle$ to increase the orthogonality of other vectors to her advantage while still keeping within the observed noise statistics). We may therefore assume the attack operator U is such that (21) applies. Note that this proof would not hold if $|\beta_{i,j}|^2 \neq 1/2^n$ for all i, j.

Thus, for any fixed a and c, we may define an orthonormal basis $\{|\nu_b^{(a,c)}\rangle\}_{b=0}^{N-1}$ and write

$$|e_{a,b,c}\rangle = \sqrt{N \cdot p(a, b, c)}\, |\nu_b^{(a,c)}\rangle.$$

Note that we do not assume any relation between these vectors for differing a and c. I.e., we do not make any assumptions on the value $\langle \nu_b^{(a,c)}|\nu_{b'}^{(a',c')}\rangle$ when $a \neq a'$ or $c \neq c'$.

Third Step—Continuity Bound Analysis: From the above analysis on the structure of E's optimal attack operator, we may write $\Delta_{a,c}$, defined in (20), as

$$\begin{aligned}\Delta_{a,c} &= \left\| P\left(\sum_{b=0}^{N-1}\sqrt{N\cdot p(a,b,c)}\,|v_b^{(a,c)}\rangle\right)\right. \\ &\quad \left. -\sum_{b=0}^{N-1} N\cdot p(a,b,c)[v_{\mathbf{b}}^{(\mathbf{a},\mathbf{c})}]\right\| \\ &= N\left\| P\left(\sum_{b=0}^{N-1}\sqrt{p(a,b,c)}\,|b\rangle\right) - \sum_{b=0}^{N-1} p(a,b,c)[\mathbf{b}]\right\| \end{aligned} \tag{24}$$

where the last equality follows from the fact that trace distance is invariant to changes in basis and, again, we use $P(z) = zz^*$.

Recall our description of the channel, and in particular the value of $p(a, b, c)$ given in (14). Note that, if $Q = 0$, then it is easy to see that $\Delta_{a,c} = 0$ for all a, c and so we are done. Thus, in the following, we will consider $0 < Q < 1/2$. Due to the symmetry in a depolarization channel as clearly seen in the expression for $p(a, b, c)$ in (14) (*again, this may even be enforced by users)*, there are two cases to consider, first when $c = a$ and second when $c \neq a$. For the first, we have

$$\begin{aligned}\Delta_{a,a} &= N\left\| P\left(\sum_{b=0}^{N-1}\sqrt{p(a,b,a)}\,|b\rangle\right) - \sum_{b=0}^{N-1} p(a,b,a)[\mathbf{b}]\right\| \\ &= N\left\|\sum_{b\neq b'}\sqrt{p(a,b,a)p(a,b',a)}\,|b\rangle\langle b'|\right\|. \end{aligned} \tag{25}$$

Let X be the operator

$$X = N\sum_{b\neq b'}\sqrt{p(a,b,a)\cdot p(a,b'a)}\,|b\rangle\langle b'|.$$

Thus, $\Delta_{a,a} = ||X||$. Since it is Hermitian, we may decompose X as

$$X = \sum_{j=0}^{N-1}\lambda_j[\mathbf{v_j}] \tag{26}$$

where $\{|v_j\rangle\}$ are orthogonal eigenvectors and λ_j are (real) eigenvalues; thus $X|v_j\rangle = \lambda_j|v_j\rangle$ for all $j = 0, \ldots, N-1$ and, of course, $||X|| = \sum_j |\lambda_j|$. Consider a particular eigenvector $|v\rangle = |v_j\rangle = \sum_i x_i|i\rangle$. Then

$$\begin{aligned}X|v\rangle &= N\sum_{b=0}^{N-1}\underbrace{\left(\sum_{\substack{i=0\\ i\neq b}}^{N-1} x_i\sqrt{p(a,b,a)\cdot p(a,i,a)}\right)}_{y_b}|b\rangle \\ &= N\sum_b y_b|b\rangle. \end{aligned}$$

Thus, for $\lambda = \lambda_j$ to be the corresponding eigenvalue, it must hold that $Ny_b = \lambda x_b$ for all $b = 0, \ldots, N-1$. Note that, when $b = a$, it holds that

$$\begin{aligned} & Ny_a = \lambda x_a \\ \iff & N\sum_{\substack{i=0\\ i\neq a}}^{N-1} x_i\sqrt{p(a,a,a)\cdot p(a,i,a)} = \lambda x_a \\ \iff & \alpha\beta\sum_{i\neq a} x_i = \lambda x_a. \end{aligned} \tag{27}$$

When $b \neq a$, then Ny_b simplifies to

$$\begin{aligned} & N\sum_{i\neq b} x_i\sqrt{p(a,b,a)\cdot p(a,i,a)} \\ &= N\cdot x_a\sqrt{p(a,b,a)\cdot p(a,a,a)} \\ &\quad + N\sum_{\substack{i\neq b\\ i\neq a}} x_i\sqrt{p(a,b,a)\cdot p(a,i,a)} \end{aligned} \tag{28}$$

and thus it must hold that

$$\alpha\beta x_a + \alpha^2\sum_{\substack{i\neq b\\ i\neq a}} x_i = \lambda x_b. \tag{29}$$

Now, assume that there exists a $k \neq k'$ such that $x_k \neq x_{k'}$ and both k and k' are not equal to a (we will handle the case when this is not true afterwards). From (29), we have, using the case when $b = k$ and $b = k'$, respectively

$$\alpha\beta x_a + \alpha^2\sum_{\substack{i\neq k\\ i\neq a}} x_i = \lambda x_k$$

$$\alpha\beta x_a + \alpha^2\sum_{\substack{i\neq k'\\ i\neq a}} x_i = \lambda x_{k'}.$$

Subtracting these two expressions yields

$$\begin{aligned} & \alpha^2(x_{k'} - x_k) = \lambda(x_k - x_{k'}) \\ \Rightarrow\ & \lambda = -\alpha^2. \end{aligned} \tag{30}$$

We next claim, the geometric multiplicity of this eigenvalue is $N-2$ and, thus, this eigenvalue appears $N-2$ times in (26). Consider the operator $X - \lambda I$. By choosing a suitable basis, we may write this in matrix form as

$$X - \lambda I = \begin{pmatrix} -\lambda & \alpha\beta & \alpha\beta & \cdots & \alpha\beta \\ \alpha\beta & -\lambda & \alpha^2 & \cdots & \alpha^2 \\ \alpha\beta & \alpha^2 & -\lambda & \cdots & \alpha^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha\beta & \alpha^2 & \alpha^2 & \cdots & -\lambda \end{pmatrix}. \tag{31}$$

Substituting $\lambda = -\alpha^2$ it is clear that the rank of $X - (-\alpha^2)I$ is at most two. Thus, the geometric multiplicity is at least $N-2$ (and indeed is exactly $N-2$ except when $Q = 0$ or $Q = 1 - 1/N$; but the first case is considered separately as mentioned, and the second case implies $Q > 1/2$ which is much larger than our evaluations later and so not considered).

Therefore, exactly $N-2$ of the eigenvalues of X are $-\alpha^2 = -\frac{Q^2}{(N-1)^2}$.

The remaining two eigenvalues are found when there does not exist $k \neq k'$ (where $k \neq a$ and $k' \neq a$) such that $x_k \neq x_{k'}$. In this case, we have $x_k = x_{k'} = x$ for all k, k' not equal to a. Using (27), we find

$$\alpha\beta(N-1)x = \lambda x_a \implies x_a = \frac{\alpha\beta(N-1)x}{\lambda}.$$

Note that the above equation forces $x \neq 0$ as, otherwise, x_a is also 0 and so $|v\rangle$ would be the zero vector and not an eigenvector of Hermitian operator X. Substituting this into (29) (for any $b \neq a$) we find

$$\alpha\beta\left(\frac{\alpha\beta(N-1)x}{\lambda}\right) + \alpha^2(N-2)x = \lambda x$$
$$\iff \lambda^2 - \alpha^2(N-2)\lambda - \alpha^2\beta^2(N-1) = 0$$

thus leading us to the two remaining eigenvalues, which we denote $\lambda_{\pm}^X$

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

Since there was no dependence on a in the above analysis, this leads us to conclude that

$$\Delta_{a,a} = (N-2)\frac{Q^2}{(N-1)^2} + |\lambda_+^X| + |\lambda_-^X|. \tag{32}$$

We next consider the case when $c \neq a$ and compute $\Delta_{a,c}$. Following the same logic as before, fix a particular $c \neq a$ and consider the operator $Y = N\sum_{b\neq b'}\sqrt{p(a,b,c)\cdot p(a,b',c)}\,|b\rangle\langle b'|$ (and so $\Delta_{a,c} = ||Y||$). Let $|v\rangle = \sum_i x_i |i\rangle$ be an eigenvector of Y such that $Y|v\rangle = \lambda|v\rangle$. Then

$$Y|v\rangle = N\sum_{b=0}^{N-1}\underbrace{\left(\sum_{\substack{i=0\\ i\neq b}}^{N-1} x_i\sqrt{p(a,b,c)\cdot p(a,i,c)}\right)}_{z_b}|b\rangle$$
$$= N\sum_b z_b|b\rangle.$$

To satisfy the equation $Y|v\rangle = \lambda|v\rangle$, we require $Nz_b = \lambda x_b$ for all $b = 0, \ldots, N-1$. There are three cases of b to consider here: $b = a$, $b = c$, and $b \neq a, c$. For each of these cases we find, first for $b = a$

$$Nz_a = \lambda x_a$$
$$\iff \alpha\beta x_c + \sum_{\substack{i\neq c\\ i\neq a}} x_i\sqrt{\alpha^3\beta} = \lambda x_a. \tag{33}$$

For $b = c$

$$Nz_c = \lambda x_c$$
$$\iff \alpha\beta x_a + \sum_{\substack{i\neq c\\ i\neq a}} x_i\sqrt{\alpha^3\beta} = \lambda x_c. \tag{34}$$

And, finally, for $b \neq a, c$

$$Nz_b = \lambda x_b$$
$$\iff \sqrt{\alpha^3\beta}x_a + \sqrt{\alpha^3\beta}x_c + \sum_{\substack{i\neq a\\ i\neq b\\ i\neq c}}\alpha^2 x_i = \lambda x_b. \tag{35}$$

As with the previous operator X, we break this up into several cases depending on the eigenvector $|v\rangle$. For the first case, assume there exists $k \neq k'$ with $k \neq a, c$ and $k' \neq a, c$ such that $x_k \neq x_{k'}$. Then, using (35), for $b = k$ and $b = k'$ and subtracting the resulting expressions yields

$$\alpha^2(x_{k'} - x_k) = \lambda(x_k - x_{k'}) \implies \lambda = -\alpha^2. \tag{36}$$

We claim this eigenvalue has geometric multiplicity $N-3$. Consider the operator $Y - \lambda I$ and, as before, by considering a suitable basis, we may write this in matrix form as

$$Y - \lambda I = \begin{pmatrix} -\lambda & \alpha\beta & \sqrt{\alpha^3\beta} & \cdots & \sqrt{\alpha^3\beta} \\ \alpha\beta & -\lambda & \sqrt{\alpha^3\beta} & \cdots & \sqrt{\alpha^3\beta} \\ \sqrt{\alpha^3\beta} & \sqrt{\alpha^3\beta} & -\lambda & \cdots & \alpha^2 \\ \sqrt{\alpha^3\beta} & \sqrt{\alpha^3\beta} & \alpha^2 & \cdots & \alpha^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \sqrt{\alpha^3\beta} & \sqrt{\alpha^3\beta} & \alpha^2 & \cdots & -\lambda \end{pmatrix}.$$

From this, it is evident that the rank of $Y - (-\alpha^2)I$ is three and so the geometric multiplicity of the eigenvalue $-\alpha^2$ is $N-3$ (again, assuming $Q \neq 0$ and $Q \neq 1 - 1/N$ which holds since $0 < Q < 1/2$. Thus, there are three more eigenvalues. Next, consider the case if $x_a \neq x_c$. In this case, subtracting (33) and (34) yields

$$\alpha\beta(x_c - x_a) = \lambda(x_a - x_c) \implies \lambda = -\alpha\beta. \tag{37}$$

Finally, consider the case where $x_a = x_c = x_1$ and $x_k = x_{k'} = x_2$ for every $k \neq k'$ and $k, k' \neq a, c$. In this case, (35) simplifies to

$$2\sqrt{\alpha^3\beta}x_1 + \alpha^2(N-3)x_2 = \lambda x_2. \tag{38}$$

Note that this implies $x_2 \neq 0$ as, otherwise, $x_1 = 0$ and so $|v\rangle$ is the zero vector and not an eigenvector. Equation (33) yields

$$\alpha\beta x_1 + (N-2)\sqrt{\alpha^3\beta}x_2 = \lambda x_1.$$

Note that the above equation also implies that $\lambda \neq \alpha\beta$ since if it were, we would have $x_2 = 0$ which, as already discussed, is not true. Thus, we may solve

$$x_1 = \frac{(N-2)x_2\sqrt{\alpha^3\beta}}{\lambda - \alpha\beta}.$$

Substituting this into (38) yields

$$\frac{2x_2\alpha^3\beta(N-2)}{\lambda - \alpha\beta} + \alpha^2(N-3)x_2 = \lambda x_2 \iff$$
$$2\alpha^3\beta(N-2) + \alpha^2(N-3)(\lambda - \alpha\beta) = \lambda(\lambda - \alpha\beta). \tag{39}$$

Solving the above quadratic for λ gives us the two remaining eigenvalues which we denote $\lambda_{\pm}^{Y}$. After some algebra, these eigenvalues are found to be

$$\lambda_{\pm}^{Y} = \frac{1}{2}[\alpha\beta + \alpha^2(N-3)] \pm \frac{1}{2}\alpha\sqrt{(\beta + \alpha[N-3])^2 + 4\alpha\beta(N-1)}.$$

Since the above arguments were for arbitrary $a \neq c$, this gives us the following:

$$\begin{aligned}\Delta_{a,c} &= (N-3)\alpha^2 + \alpha\beta + |\lambda_{+}^{Y}| + |\lambda_{-}^{Y}| \\ &= (N-3)\frac{Q^2}{(N-1)^2} + \frac{Q(1-Q)}{N-1} + |\lambda_{+}^{Y}| + |\lambda_{-}^{Y}|.\end{aligned} \tag{40}$$

Thus, we conclude

$$\begin{aligned}\Delta &= \frac{1}{2N}\sum_{a,c=0}^{N-1}\Delta_{a,c} \\ &= \frac{1}{2N}\sum_{a}\Delta_{a,a} + \frac{1}{2N}\sum_{a\neq c}\Delta_{a,c} \\ &= \frac{1}{2}\left((N-2)\frac{Q^2}{(N-1)^2} + |\lambda_{+}^{X}| + |\lambda_{-}^{X}| + (N-1)\right. \\ &\quad \left.\times\left[(N-3)\frac{Q^2}{(N-1)^2} + \frac{Q(1-Q)}{N-1} + |\lambda_{+}^{Y}| + |\lambda_{-}^{Y}|\right]\right).\end{aligned}$$

At first glance, this expression may seem to scale exponentially with n (since $N = 2^n$). However, note that $\lambda_{\pm}$ (for both the X and Y operators) are multiples of α, which, itself, is a multiple of $1/(N-1)$. Returning to Π^{OW}, we apply the Winter continuity bound (19) to attain

$$\begin{aligned}&H(A_1^Z|E)_\mu \\ &\geq H(A_1^Z|E)_\rho - \Delta\log N - (1+\Delta)f(\Delta) \\ &\geq n - H(A_1^F|A_2^F)_\rho - \Delta\log N - (1+\Delta)f(\Delta) \\ &\geq n(1-\Delta) - (1+\Delta)f(\Delta) - H(A_1^F|A_2^F)_\rho\end{aligned} \tag{41}$$

where $f(\Delta) = H(\Delta/[1+\Delta])$. To finish the key-rate computation, we need $H(A_1^F|A_2^F)_\rho$ and $H(A_1^Z|B^Z)_\mu$. The first is determined through the observed values $p_{i,j}^F$, which we use to denote the probability that A observes $|F_i\rangle$ (in A_1) and $|F_j\rangle$ (in A_2) conditioned on the event B choose `Reflect`; the second is determined through the observed values $p_{i,j}^Z$ which we use to denote the probability that B observes $|j\rangle$ and A observes $|i\rangle$ in A_1 (we use A_1 as this is the register used for key-distillation) conditioned on the event B choose `Measure and Resend`. In both cases, $i, j \in \{0, 1, \ldots, N-1\}$. Clearly these are observable values allowing A and B to compute these final (classical) entropy expressions. Since we are considering a symmetric attack modeled by the depolarization channel described in (12), we have $p_{i,j}^Z = \frac{1}{N}p(j|i)$ and so we compute the joint entropy as

$$\begin{aligned}H(A_1^Z B^Z)_\mu &= -\sum_{i,j} p_{i,j}^Z \log p_{i,j}^Z \\ &= -\sum_{i}\frac{p(i|i)}{N}\log_2 p(i|i) - \sum_{i\neq j}\frac{p(j|i)}{N}\log_2 p(j|i) \\ &= (1-Q)\log_2\frac{1-Q}{N} - Q\log\frac{Q}{N(N-1)} \\ &= n + Q\log_2(N-1) + H(Q).\end{aligned}$$

It is not difficult to show that $H(B^Z)_\mu = n$ (since the attack is symmetric, B's probability of observing any particular value $|j\rangle$ is uniform). Thus, the conditional entropy is simply

$$H(A_1^Z|B^Z) = Q\log_2(N-1) + H(Q).$$

The case for the $\mathcal{F}$ basis is identical, though we use a different noise parameter Q_F to parameterize the channel in this case (since the noise may be different in the reflection case as discussed earlier). In this case, we have

$$H(A_1^F|A_2^F) = Q_F\log_2(N-1) + H(Q_F).$$

Our final key-rate expression, therefore is

$$\begin{aligned}r &= H(A_1^Z|E) - H(A_1^Z|B^Z) \\ &\geq n(1-\Delta) - (1+\Delta)H\left(\frac{\Delta}{1+\Delta}\right) \\ &\quad - (Q+Q_F)\log_2\left(2^n-1\right) - H(Q) - H(Q_F).\end{aligned} \tag{42}$$

Note that the above assumed collective attacks. Ordinarily, one may extend such computations done for the collective attack case to prove security against arbitrary, general, attacks by using de Finetti style arguments or postselection techniques [63], [64]. We suspect that this result holds for our protocol, however, we leave a complete proof of that for future work.

C. EVALUATION

We evaluate our key-rate bound, (42), in two scenarios. First, we assume in the *reflection* case, that the reverse channel is *independent* of the forward and, so, $Q_F = 2Q(1-Q)$ shown in Fig. 2. In the second *dependent* case, we assume $Q_F = Q$ shown in Fig. 3. We note that, similar to the fully quantum case [32], [33], as the dimension increases, the noise tolerance also surpasses the single qubit case. Thus, we prove that this high-dimensional advantage, known for fully quantum protocols, also applies to the semiquantum model. We also observe numerically that, as n increases, the maximal noise tolerance tends to approach 26% in the independent case and 30% in the dependent case. As mentioned, some fully quantum high-dimensional QKD protocols can tolerate up to 50% error as the dimension increases [33]; thus, while

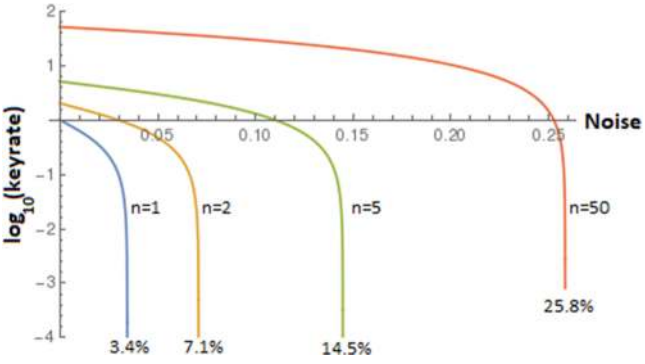

FIGURE 2. Key-rate of our high-dimensional SQKD protocol for the independent channel case, namely when $Q_F = 2Q(1-Q)$. We consider various number of qubits used by A and B, namely $n = 1, 2, 5,$ and 50 (for a total dimension of $2, 2^2, 2^5,$ and 2^{50}. The x-axis represents the depolarization noise in the channel, namely Q in (12). As shown and discussed in the text, as the dimension of the quantum system increases, the efficiency increases (as more bits may be carried per signal) but also the noise tolerance increases, allowing for potential secure communication over noisier channels. As discussed in the text, this behavior is also known for fully-quantum protocols. Our work here shows, for the first time, this behavior applies also to semiquantum communication.

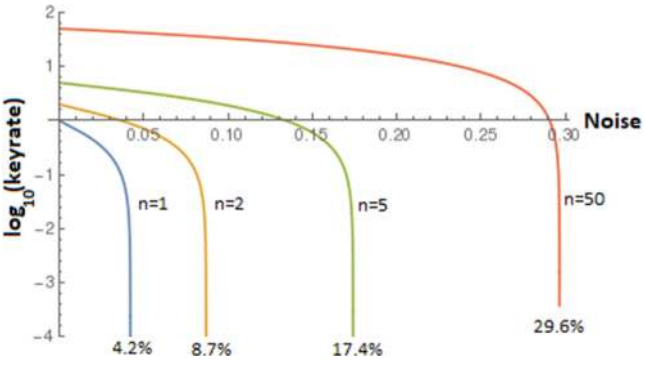

FIGURE 3. Similar to Fig. 2, showing the key-rate of our high-dimensional SQKD protocol however now for the dependent channel case, when $Q_F = Q$. Here we plot the case for $n = 1, 2, 5,$ and 50. As with the independent case, where the $\mathcal{F}$ basis noise is higher, we see the same benefit to using higher dimensional systems both in noise tolerance and efficiency for the depolarization channel.

not as high as the fully quantum case (which, perhaps, is to be expected), it is higher than any other semiquantum protocol to-date. Indeed, the highest known semiquantum protocol [27] can tolerate up to 17.8% in the independent case (as opposed to 26% here) and 26% in the dependent case (as opposed to 30% here). Of course, (42) is only a lower bound—future work may improve this. In particular, the use of mismatched measurements (needed to attain a high noise tolerance in [27]) may greatly benefit our analysis here. This we leave as an interesting future research direction.

Note that our protocol is a semiquantum version of a higher dimensional BB84 (HD-BB84), first introduced in [35]. So we compare our key-rate with it. Description of this protocol is given in Protocol 4.

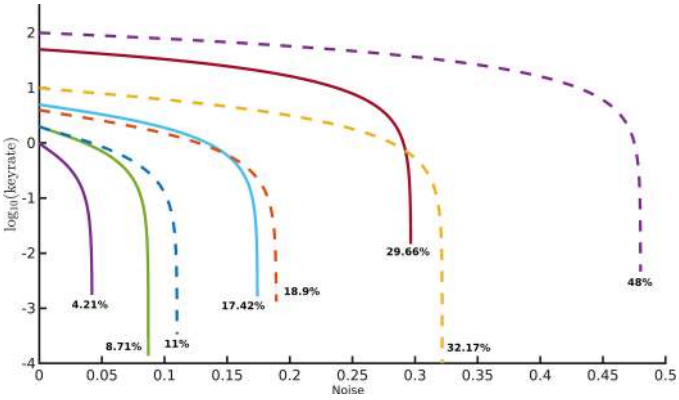

FIGURE 4. Here, we compare the key-rate of our protocol (solid lines) with HD-BB84 (dashed lines) as a function of the depolarization noise [Q, see (12)]. Comparing for various dimensions $n = 1, 2, 5, 50$ with n, in this graph, increasing from left to right. Note the total dimension is, of course, 2^n. We note that, though HD-BB84 (dashed) outperforms our protocol both in efficiency and noise tolerance for all dimension settings, this is not too surprising since HD-BB84 is a fully quantum protocol. We note, however, that our security proof is only a lower bound so the actual performance of our protocol may be higher.

Protocol 4: n-Dimensional BB84.

Public Parameters: n: the number of qubits to send per signal;

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

1) A prepares a randomly chosen $\mathcal{Z}$ basis state; otherwise she prepares a randomly chosen $\mathcal{F}$ basis state. She records her choice of basis and the choice of state, then sends the resulting n-qubit state to B.
2) Similarly, B chooses $\mathcal{Z}$ or $\mathcal{F}$ basis states randomly, measures the incoming qudit in this basis.

Classical Communication Stage: A and B, using the authenticated classical channel, divulge their choices. If both A and B chose the $\mathcal{Z}$ basis, they use this iteration to contribute toward their raw key. Otherwise, if both of them chose the X basis, then this iteration can be used to gather statistics on the channel.

To calculate the key-rate r_{BB84} in this protocol, we use key-rate equation from [60] suited to our notation and see that

$$\begin{aligned} r_{BB84} &= H(A^Z|E) - H(A^Z|B) \\ &\geq n - H(A^F|B^F) - H(A^Z|B^Z) \\ &= n - 2(H(A^Z B^Z) + H(B^Z))) \end{aligned} \tag{43}$$

where the inequality follows from the entropic uncertainty relation from [57] and $n = \max_{j,k} |\langle\psi_j|\phi_k\rangle|^2$, where ψ_j and ϕ_k are eigenvectors of $\mathcal{Z}$ and $\mathcal{F}$, respectively. We are also using the fact that measurement cannot decrease entropy. $H(A^Z B^Z)$ is the entropy of the joint distribution of Alice and Bob's choices and $H(B^Z)$ is Bob's entropy. Because

Alice and Bob choose $\mathcal{Z}$ or $\mathcal{F}$ basis with equal probability, the conditional entropy is the same in either case. For the depolarization channel that we are considering, (43) can be simplified to

$$r_{BB84} \geq n - 2(h(Q) + Q\log(2^n - 1)).$$

Because we have two-way communication channel in our protocol, it is only fair to run HD-BB84 independently twice and sum their results before comparing. Fig. 4 depicts the key-rate comparison of the two protocols as a function of channel noise. In addition to noise-tolerance comparison, we also look at the key-rate as a function of bit-error rate (BER) for these protocols. BER is the expected number of wrong bits in Bob's outcome in a single iteration of a protocol. It is defined as

$$\text{BER}(n) = \frac{1}{n}\sum_{a\in\mathcal{Z}}\sum_{b\in\mathcal{Z}} \Pr(b \wedge a) w(a \oplus b) \tag{44}$$

where $w(x)$ is the Hamming weight of bit string x. $Pr(b \wedge a)$ represents the probability that Bob receives $|b\rangle$, if $|a\rangle$ was sent by Alice. We can make two observations that would simplify the BER calculation. Because the depolarization channel treats each basis state in the same way and Alice would choose any of those states with equal probability, it is noticeable that for $a_1 \neq a_2 \in \mathcal{Z}$

$$\sum_{b\in\mathcal{Z}} w(a_1 \oplus b) = \sum_{b\in\mathcal{Z}} w(a_2 \oplus b) = \sum_{b\in\mathcal{Z}} w(b).$$

Moreover, $\Pr(x \wedge y) = \frac{Q}{2^n-1}$ for all $x \neq y \in \mathcal{Z}$. Using these two observations and a standard result from combinatorics, (44) can be simplified in the following way:

$$\begin{aligned}
\text{BER}(n) &= \frac{1}{n}\sum_{a\in\mathcal{Z}}\sum_{b\in\mathcal{Z}} \Pr(b \wedge a) w(a \oplus b) \\
&= \frac{Q}{n(2^n-1)2^n}\sum_{a\in\mathcal{Z}}\sum_{b\in\mathcal{Z}} w(a \oplus b) \\
&= \frac{Q}{n(2^n-1)2^n}\sum_{a\in\mathcal{Z}}\sum_{k=0}^{n} k\binom{n}{k} \\
&= \frac{Q}{n(2^n-1)2^n}\sum_{a\in\mathcal{Z}} n2^{n-1} \\
&= \frac{2^{n-1}}{2^n-1}Q.
\end{aligned}$$

Fig. 5 shows the comparison of our key rate r with $2r_{BB84}$ as a function of BER. It is noticeable from Figs. 4 and 5 that, HD-BB84 has a higher key-rate than our protocol. This is expected as our protocol imposes restriction on Bob's measurement capability.

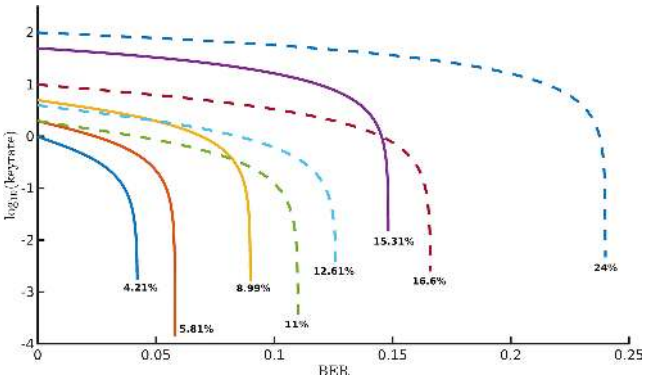

FIGURE 5. Comparing the key-rate of our protocol (solid lines) with HD-BB84 (dashed lines) as a function of the BER which is, itself of course, a function of the depolarization noise Q [see (44)]. We graph various dimensions $n = 1, 2, 5, 50$ where n is the number of qubits (hence the total dimension is 2^n). In the graph, n increases from left to right. We make the same observations as in Fig. 4 that HD-BB84 outperforms our protocol. However, we do note that our SQKD protocol, for high enough n, can establish a key when the BER is higher than 11%, similar to HD-BB84, at least for the depolarization channel.

V. DISCUSSION OF PRACTICAL SYSTEMS

As discussed, our work here is primarily interested in the theoretical aspects of high-dimensional systems applied to semiquantum cryptography. However, in light of recent practical and experimental SQKD implementations for qubit-based protocols [7], [65], it is worthwhile to consider whether, and how, high-dimensional systems may be used practically for semiquantum communication. One problem with semiquantum cryptography from a practical standpoint is the need for the `Measure and Resend` operation. As the most practical (S)QKD implementation utilizes photons as information carriers, this `Measure and Resend` operation leads to the destruction of the original photon and the creation of a new, fresh, photon to resend. Such a process leads to several practical attacks as discussed in [58].

To counter this, a practical SQKD protocol must not require the classical user to prepare fresh photons. The so-called "mirror" protocol, introduced in [7], was the first such SQKD protocol. Here, time-bin encoding is typically performed, where $|i\rangle$ represents a photon in time bin i (for $i = 0, 1$). Of course $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ represents a single photon in a superposition of both time bins. In the mirror protocol, `Reflect` acts as expected, reflecting the entire signal back to A. However, the `Measure and Resend` operation is subdivided into multiple operations allowing B to only "look" at a particular time-bin while reflecting the other. That is, B has a controllable "mirror" (hence the name), permitting him to place a photon counter at time bin $|i\rangle$ while reflecting $|1 - i\rangle$. If his detector clicks, the photon is destroyed and a vacuum is sent to A; if his detector does not click, then the state collapses to $|1 - i\rangle$ and the same photon is returned to A. The critical point is that, first, he is able to determine the state of the photon by this measurement and, second, he never prepares a fresh photon. This counters the practical attacks from [58].

Protocol 5: Mirror-Based N-Dimensional SQKD.

Public Parameters: N: the number of time bins; p_M, the probability of choosing `Measure and Resend`; p_Z, the probability of A choosing the $\mathcal{Z}$ basis.

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

1) With probability p_Z, A prepares a randomly chosen $\mathcal{Z}$ basis state, preparing a single photon in the chosen time bin. Otherwise she prepares a randomly chosen $\mathcal{F}$ basis state, preparing a single photon in an appropriate superposition of time-bins. She records her choice of basis and the choice of state.
2) B chooses, with probability $1 - p_M$, operation `Reflect` in which case he reflects all N time bins back to A. Otherwise, he chooses `Measure and Resend` in which case, he chooses a random time-bin i (out of the N available bins) and performs operation `Measure and Resend` $- i$ as discussed in the text and Fig. 6. He records the outcome of this measurement (either j if he observed the photon at time-bin $|j\rangle$ or i if he does not observe anything). Note that, if he observes j, the photon is destroyed and A should observe a vacuum later; if he observes i, then the photon collapses to the $|i\rangle$ time bin and is returned to A (importantly, this is not a new photon, however).
3) A measures the returning system in the same basis she used to prepare.
4) A and B, using the authenticated classical channel, divulge their choices. Namely, B his choice of "`Measure and Resend`" (but *not* his choice of i in this case) or "`Reflect`" and A her choice of basis. B also discloses whether he detected a photon or not. If A chose the $\mathcal{Z}$ basis and B chose `Measure and Resend` *and did not observe a photon*, they will use this iteration to contribute towards their raw key; namely, B will append the bit-string representation of i to his raw key while A will append her initial state she prepared (in this case, A's subsequent measurement result is not used).

To consider a practical implementation of our high-dimensional protocol, we propose that this mirror terminology may be extended. Now, a single photon may be prepared in different time bins $|i\rangle$ for $i = 1, \cdots N$ or a superposition of those time bins. The classical user may reflect the entire signal or may choose to reflect only a single time bin $|i\rangle$ while measuring the other time bins $|j\rangle$ for $j \neq i$. If his detector clicks at time j, a vacuum is sent back to A and he knows the result of his $\mathcal{Z}$ basis measurement was $|j\rangle$. If his detector does not click, the state collapses to $|i\rangle$ while he also knows that the measurement resulted in outcome $|i\rangle$. We denote this operation `MeasureandResend` $- i$. See Fig. 6. Critically, he never prepares a fresh photon meaning that the practical photon tagging attacks [58] are not applicable here. The exact protocol we describe in Protocol 5.

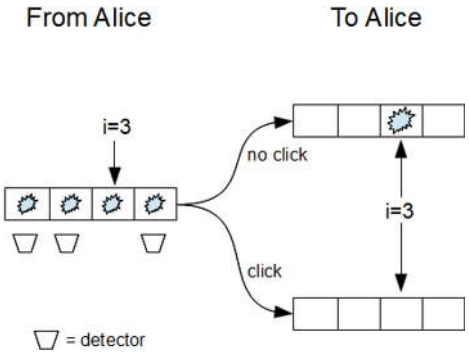

FIGURE 6. High-level overview of the measurement apparatus for the potential experimental high-dimensional SQKD protocol discussed in Protocol 5. Here, Alice prepares time-bin encoded states where a single photon may be in a superposition of multiple time bins (here the number of time bins is four). Bob has a controllable "mirror" based on an idea originally introduced in [7] but extended here for multiple dimensions. This measurement allows him to choose a specific time bin to "ignore" (i) while being able to measure any other time bin. If he observes a photon ("click"), a vacuum state is sent back to Alice whereas if he does not detect a photon ("no click"), he knows the measurement outcome is $|i\rangle$ and the original photon collapses to time-bin i and returns to A. Such an operation allows him to perform the `Measure and Resend` operation without requiring him to prepare a fresh photon. We leave the security analysis of this protocol, including when devices are imperfect, as future work.

Note that, any iteration where B did observe a photon must be discarded, as in the original qubit-based mirror protocol of [7]. This causes a drop in efficiency, however the advantage is the system is potentially practical in that fresh photons are not needed. An exact security analysis of this protocol, both in the ideal and in practical device settings, we leave as future work. We only propose this protocol to show that there is a potential for practical implementations of high-dimensional SQKD protocols. We do not claim security of this candidate practical Protocol 5 and leave a security analysis as future work.

VI. CLOSING REMARKS

In this article, we designed a new high-dimensional semiquantum key distribution protocol and performed an information theoretic security analysis. To conduct this security analysis, we developed several new techniques for high-dimensional protocols over two-way quantum channels which may be applicable to other (S)QKD protocols. In particular, we showed how one may reduce a two-way, high-dimensional, semiquantum protocol to a one-way protocol which is easier to analyze. Thus, we produced new security results of broad application. We also proved that high-dimensional quantum systems can benefit communication in the semiquantum model just as they do in fully QKD.

Many interesting future problems remain open. For one thing, it would be interesting to see if our proof technique can be applied to the high-dimensional quantum-walk based SQKD protocol introduced in [34]. If so, we would then be

able to compare noise tolerance properties of the two protocols. It would also be interesting to see if we can improve our bound and technique here. One factor contributing to a potentially lower key-rate bound is our use of a continuity bound. Other methods may produce more optimistic results. Finally, a security analysis of Protocol 5 would be very exciting.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, 1984, pp. 175–179. [Onine]. Available: https://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf

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

[3] A. Shenoy-Hejamadi, A. Pathak, and S. Radhakrishna, "Quantum cryptography: Key distribution and beyond," *Quanta*, vol. 6 no. 1, pp. 1–47, 2017, doi: 10.12743/quanta.v6i1.57.

[4] M. Razavi, A. Leverrier, X. Ma, B. Qi, and Z. Yuan, "Quantum key distribution and beyond: introduction," *J. Opt. Soc. Amer. B*, vol. 36, no. 3, pp. QKD1–QKD2, Mar. 2019, doi: 10.1364/JOSAB.36.00QKD1.

[5] M. Boyer, D. Kenigsberg, and T. Mor, "Quantum key distribution with classical Bob," in *Proc. 2007 1st Int. Conf. Quantum, Nano, Micro Technologies (ICQNM'07)*, Jan. 2007, doi: 10.1109/ICQNM.2007.18.

[6] M. Boyer, R. Gelles, D. Kenigsberg, and T. Mor, "Semiquantum key distribution," *Phys. Rev. A*, vol. 79, Mar. 2009, Art. no. 032341, doi: 10.1103/PhysRevA.79.032341.

[7] M. Boyer, M. Katz, R. Liss, and T. Mor, "Experimentally feasible protocol for semiquantum key distribution," *Phys. Rev. A*, vol. 96 no. 6, 2017, Art. no. 062335, doi: 10.1103/PhysRevA.96.062335.

[8] X. Zou, D. Qiu, L. Li, L. Wu, and L. Li, "Semiquantum-key distribution using less than four quantum states," *Phys. Rev. A*, vol. 79, May 2009, Art. no. 052312, doi: 10.1103/PhysRevA.79.052312.

[9] X. Zou, D. Qiu, S. Zhang, and P. Mateus, "Semiquantum key distribution without invoking the classical party's measurement capability," *Quantum Inf. Process.*, 2015, pp. 1–16, doi: 10.1007/s11128-015-1015-z.

[10] W. O. Krawec, "Mediated semiquantum key distribution," *Phys. Rev. A*, vol. 91, Mar. 2015, Art. no. 032323, doi: 10.1103/PhysRevA.91.032323.

[11] N.-R. Zhou, K.-N. Zhu, and X.-F. Zou, "Multi-party semi-quantum key distribution protocol with four-particle cluster states," *Annalen der Physik*, vol. 531, 2019, Art. no. 1800520, doi: 10.1002/andp.201800520.

[12] P.-H. Lin, C.-W. Tsai, and T. Hwang, "Mediated semi-quantum key distribution using single photons," *Annalen der Physik*, vol. 531, 2019, Art. no. 1800347, doi: 10.1002/andp.201800347.

[13] Q. Li, W. H. Chan, and D.-Y. Long, "Semiquantum secret sharing using entangled states," *Phys. Rev. A*, vol. 82, Aug. 2010, Art. no. 022303, doi: 10.1103/PhysRevA.82.022303.

[14] L. Li, D. Qiu, and P. Mateus, "Quantum secret sharing with classical Bobs," *J. Phys. A, Math. Theor.*, vol. 46, no. 4, 2013, Art. no. 045304, doi: 10.1088/1751-8113/46/4/045304.

[15] J. Wang, S. Zhang, Q. Zhang, and C.-J. Tang, "Semiquantum secret sharing using two-particle entangled state," *Int. J. Quantum Inf.*, vol. 10, no. 5, 2012, Art. no. 1250050, doi: 10.1142/S0219749912500505.

[16] N.-R. Zhou, K.-N. Zhu, W. Bi, and L.-H. Gong, "Semi-quantum identification," *Quantum Inf. Process.*, vol. 18 no. 6, 2019 Art. no. 197, doi: 10.1007/s11128-019-2308-4.

[17] K. Thapliyal, R. D. Sharma, and A. Pathak, "Orthogonal-state-based and semi-quantum protocols for quantum private comparison in noisy environment," *Int. J. Quantum Inf.*, vol. 16, no. 5, 2018, Art. no. 1850047, doi: 10.1142/S0219749918500478.

[18] W.-H. Chou, T. Hwang, and J. Gu, "Semi-quantum private comparison protocol under an almost-dishonest third party," 2016, *arXiv:1607.07961*.

[19] L. Y.-Feng, "Semi-quantum private comparison using single photons," *Int. J. Theor. Phys.*, vol. 57, no. 10, pp. 3048–3055, 2018, doi: 10.1007/s10773-018-3823-2.

[20] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, Jul. 2000, doi: 10.1103/PhysRevLett.85.441.

[21] R. Renner, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum-key-distribution protocols," *Phys. Rev. A*, vol. 72, no. 1, 2005, Art. no. 012332, doi: 10.1103/PhysRevA.72.012332.

[22] W. O. Krawec, "Quantum key distribution with mismatched measurements over arbitrary channels," *Quantum Inf. Comput.*, vol. 17, no. 3/4, pp. 209–241, 2017.

[23] S. M. Barnett, B. Huttner, and S. J. D. Phoenix, "Eavesdropping strategies and rejected-data protocols in quantum cryptography," *J. Modern Opt.*, vol. 40, no. 12, pp. 2501–2513, 1993, doi: 10.1080/09500349314552491.

[24] S. Watanabe, R. Matsumoto, and T. Uyematsu, "Tomography increases key rates of quantum-key-distribution protocols," *Phys. Rev. A*, vol. 78, no. 4, 2008, Art. no. 042316, doi: 10.1103/PhysRevA.78.042316.

[25] R. Matsumoto and S. Watanabe, "Key rate available from mismatched measurements in the BB84 protocol and the uncertainty principle," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. 91, no. 10, pp. 2870–2873, 2008, doi: 10.1093/ietfec/e91-a.10.2870.

[26] R. Matsumoto and S. Watanabe, "Narrow basis angle doubles secret key in the BB84 protocol," *J. Phys. A, Math. Theor.*, vol. 43, no. 14, 2010, Art. no. 145302, doi: 10.1088/1751-8113/43/14/145302.

[27] O. Amer and W. O. Krawec, "Semiquantum key distribution with high quantum noise tolerance," *Phys. Rev. A*, vol. 100, no. 2, 2019, Art. no. 022319, doi: 10.1103/PhysRevA.100.022319.

[28] G. O. Myhr, J. M. Renes, A. C. Doherty, and N. Lütkenhaus, "Symmetric extension in two-way quantum key distribution," *Phys. Rev. A*, vol. 79, no. 4, 2009, Art. no. 042329, doi: 10.1103/PhysRevA.79.042329.

[29] H. F. Chau, "Practical scheme to share a secret key through a quantum channel with a 27.6 percent bit error rate," *Phys. Rev. A*, vol. 66, no. 6, 2002, Art. no. 060302, doi: 10.1103/PhysRevA.66.060302.

[30] H. Bechmann-Pasquinucci and W. Tittel, "Quantum cryptography using larger alphabets," *Phys. Rev. A*, vol. 61, no. 6, 2000, Art. no. 062308, doi: 10.1103/PhysRevA.61.062308.

[31] H. F. Chau, "Unconditionally secure key distribution in higher dimensions by depolarization," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1451–1468, Apr. 2005, doi: 10.1109/TIT.2005.844076.

[32] L. Sheridan and V. Scarani, "Security proof for quantum key distribution using qudit systems," *Phys. Rev. A*, vol. 82, no. 3, 2010, Art. no. 030301, doi: 10.1103/PhysRevA.82.030301.

[33] H. F. Chau, "Quantum key distribution using qudits that each encode one bit of raw key," *Phys. Rev. A*, vol. 92, no. 6, 2015, Art. no. 062324, doi: 10.1103/PhysRevA.92.062324.

[34] C. Vlachou, W. Krawec, P. Mateus, N. Paunković, and A. Souto, "Quantum key distribution with quantum walks," *Quantum Inf. Process.*, vol. 17, no. 11, 2018, Art. no. 288, doi: 10.1007/s11128-018-2055-y.

[35] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," *Phys. Rev. Lett.*, vol. 88, no. 12, 2002, Art. no. 127902, doi: 10.1103/PhysRevLett.88.127902.

[36] G. M. Nikolopoulos and G. Alber, "Security bound of two-basis quantum-key-distribution protocols using qudits," *Phys. Rev. A*, vol. 72, no. 3, 2005, Art. no. 032320, doi: 10.1103/PhysRevA.72.032320.

[37] 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," *Phys. Rev. A*, vol. 73, no. 3, 2006, Art. no. 032325, doi: 10.1103/PhysRevA.73.032325.

[38] T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol without monitoring signal disturbance," *Nature*, vol. 509, no. 7501, 2014, Art. no. 475, doi: 10.1038/nature13303.

[39] Z.-Q. Yin *et al.*, "Improved security bound for the round-robin-differential-phase-shift quantum key distribution," *Nature Commun.*, vol. 9, no. 1, 2018, Art. no. 457, doi: 10.1038/s41467-017-02211-x.

[40] R. Wang *et al.*, "Security proof for single-photon round-robin differential-quadrature-phase-shift quantum key distribution," *Phys. Rev. A*, vol. 98, no. 6, 2018, Art. no. 062331, doi: 10.1103/PhysRevA.98.062331.

[41] 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," 2020, *arXiv:2004.12824*.

[42] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, "Provably secure and high-rate quantum key distribution with time-bin qudits," *Sci. Adv.*, vol. 3, no. 11, 2017, Art. no. e1701491, doi: 10.1126/sciadv.1701491.

[43] I. Vagniluca *et al.*, "Efficient time-bin encoding for practical high-dimensional quantum key distribution," *Phys. Rev. Appl.*, vol. 14, no. 1, Jul. 2020, Art. no. 014051.

[44] Y. Ding *et al.*, "High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits," *npj Quantum Inf.*, vol. 3, no. 1, pp. 1–7, 2017, doi: 10.1038/s41534-017-0026-2.

[45] D. Cozzolino, B. Da Lio, D. Bacco, and L. K. Oxenløwe, "High-dimensional quantum communication: Benefits, progress, and future challenges," *Adv. Quantum Technol.*, vol. 2, no. 12, 2019, Art. no. 1900038, doi: 10.1002/qute.201900038.

[46] M. Lucamarini and S. Mancini, "Secure deterministic communication without entanglement," *Phys. Rev. Lett.*, vol. 94, no. 14, 2005, Art. no. 140501, doi: 10.1103/PhysRevLett.94.140501.

[47] K. Boström and T. Felbinger, "Deterministic secure direct communication using entanglement," *Phys. Rev. Lett.*, vol. 89, no. 18, 2002, Art. no. 187902, doi: 10.1103/PhysRevLett.89.187902.

[48] N. J. Beaudry, M. Lucamarini, S. Mancini, and R. Renner, "Security of two-way quantum key distribution," *Phys. Rev. A*, vol. 88, Dec. 2013, Art. no. 062302, doi: 10.1103/PhysRevA.88.062302.

[49] Q. Zhuang, Z. Zhang, J. Dove, F. N. C. Wong, and J. H. Shapiro, "Floodlight quantum key distribution: A practical route to gigabit-per-second secret-key rates," *Phys. Rev. A*, vol. 94, Jul. 2016, Art. no. 012322, doi: 10.1103/PhysRevA.94.012322.

[50] C. Ottaviani, S. Mancini, and S. Pirandola, "Two-way gaussian quantum cryptography against coherent attacks in direct reconciliation," *Phys. Rev. A*, vol. 92, no. 6, 2015, Art. no. 062323, doi: 10.1103/PhysRevA.92.062323.

[51] Q. Zhuang, Z. Zhang, N. Lütkenhaus, and J. H. Shapiro, "Security-proof framework for two-way Gaussian quantum-key-distribution protocols," *Phys. Rev. A*, vol. 98, no. 3, 2018, Art. no. 032332, doi: 10.1103/PhysRevA.98.032332.

[52] W. O. Krawec, "Key-rate bound of a semi-quantum protocol using an entropic uncertainty relation," in *Proc. IEEE Int. Symp. Inf. Theory*, 2018, pp. 2669–2673, doi: 10.1109/ISIT.2018.8437303.

[53] J.-Y. Guan *et al.*, "Experimental passive round-robin differential phase-shift quantum key distribution," *Phys. Rev. Lett.*, vol. 114, no. 18, 2015, Art. no. 180502, doi: 10.1103/PhysRevLett.114.180502.

[54] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, "Experimental quantum key distribution without monitoring signal disturbance," *Nature Photon.*, vol. 9, no. 12, 2015, Art. no. 827, doi: 10.1038/nphoton.2015.173.

[55] N. T. Islam, C. Cahall, A. Aragoneses, A. Lezama, J. Kim, and D. J. Gauthier, "Robust and stable delay interferometers with application to d-dimensional time-frequency quantum key distribution," *Phys. Rev. Appl.*, vol. 7, no. 4, 2017, Art. no. 044010, doi: 10.1103/PhysRevApplied.7.044010.

[56] S. Wang *et al.*, "Proof-of-principle experimental realization of a qubit-like qudit-based quantum key distribution scheme," *Quantum Sci. Technol.*, vol. 3, no. 2, 2018, Art. no. 025006, doi: 10.1088/2058-9565/aaace4.

[57] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, "The uncertainty principle in the presence of quantum memory," *Nature Phys.*, vol. 6, no. 9, pp. 659–662, 2010, doi: 10.1038/nphys1734.

[58] Y.-G. Tan, H. Lu, and Q.-Y. Cai, "Comment on 'quantum key distribution with classical Bob'," *Phys. Rev. Lett.*, vol. 102, Mar. 2009, Art. no. 098901, doi: 10.1103/PhysRevLett.102.098901.

[59] M. Boyer, D. Kenigsberg, and T. Mor, "Boyer, Kenigsberg, and Mor reply to the comment by Yong-gang Tan, Hua Lu, and Qing-yu Cai," *Phys. Rev. Lett.*, vol. 102, Mar. 2009, Art. no. 098902, doi: 10.1103/PhysRevLett.102.098902.

[60] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," *Proc. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 461, no. 2053, pp. 207–235, 2005, doi: 10.1098/rspa.2004.1372.

[61] A. Winter, "Tight uniform continuity bounds for quantum entropies: Conditional entropy, relative entropy distance and energy constraints," *Commun. Math. Phys.*, vol. 347, no. 1, pp. 291–313, Oct. 2016, doi: 10.1007/s00220-016-2609-8.

[62] M. Lucamarini and S. Mancini, "Quantum key distribution using a two-way quantum channel," *Theor. Comput. Sci.*, vol. 560, pp. 46–61, 2014, doi: 10.1016/j.tcs.2014.09.017.

[63] R. König and R. Renner, "A de Finetti representation for finite symmetric quantum states," *J. Math. Phys.*, vol. 46, no. 12, 2005, Art. no. 122108, doi: 10.1063/1.2146188.

[64] M. Christandl, R. König, and R. Renner, "Postselection technique for quantum channels with applications to quantum cryptography," *Phys. Rev. Lett.*, vol. 102, no. 2, 2009, Art. no. 020504, doi: 10.1103/PhysRevLett.102.020504.

[65] F. Massa *et al.*, "Experimental quantum cryptography with classical users," 2019, *arXiv:1908.01780*.