Quantum Information Processing (2022) 21: 319
https://doi.org/10.1007/s11128-022-03663-x

Improved semi-quantum key distribution with two almost-classical users

Saachi Mutreja[1] · **Walter O. Krawec**[2]

Received: 20 March 2022 / Accepted: 23 August 2022 / Published online: 17 September 2022

Abstract
Semi-quantum key distribution (SQKD) protocols attempt to establish a shared secret key between users, secure against computationally unbounded adversaries. Unlike standard quantum key distribution protocols, SQKD protocols contain at least one user who is limited in their quantum abilities and is almost "classical" in nature. In this paper, we revisit a mediated semi-quantum key distribution protocol, introduced by Massa et al. (Experimental quantum cryptography with classical users, 2019. arXiv preprint arXiv:1908.01780), where users need only the ability to detect a qubit, or reflect a qubit; they do not need to perform any other basis measurement; nor do they need to prepare quantum signals. Users require the services of a quantum server which may be controlled by the adversary. In this paper, we show how this protocol may be extended to improve its efficiency and also its noise tolerance. We discuss an extension which allows more communication rounds to be directly usable; we analyze the key-rate of this extension in the asymptotic scenario for a particular class of attacks and compare with prior work. Finally, we evaluate the protocol's performance in a variety of lossy and noisy channels.

Keywords Quantum key distribution · Semi-quantum cryptography · Security · Information theory

1 Introduction

Semi-quantum key distribution (SQKD) allows two parties, Alice and Bob, to establish a shared secret key that is secure against computationally unbounded adversaries. Unlike standard quantum key distribution, with SQKD, at least one party is restricted to being "classical" in nature—namely, at least one party is restricted to operating in

✉ Walter O. Krawec
walter.krawec@uconn.edu

1 UC Berkeley, Berkeley, CA 94720, USA

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

a single, publicly known, basis, or to disconnecting from the quantum channel and reflecting all qubits back to the sender. This limited "classical" party is not permitted to measure or send qubits in arbitrary bases. Semi-quantum key distribution was introduced originally in 2007 in [1] and, since then, has led to a growing area of research interest with new protocols and security proofs for both QKD [2–11] and alternative cryptographic primitives such as secret sharing [12–14], secure direct communication [15–19], private comparison [20, 21], and secure identification protocols [22, 23]. It is also experimentally realizable [24, 25]. For a general survey of semi-quantum cryptography, the reader is referred to [26], while for a general survey of QKD, the reader is referred to [27–29].

Recently, a form of *mediated semi-quantum key distribution* (M-SQKD) protocol (a model originally introduced in [30]) was developed in [24]. Here, two parties wish to establish a shared secret key; however, these parties are only able to detect the presence of a photon, or to reflect a photon back to a sender. They cannot even prepare new quantum signals. Clearly, such a protocol cannot be secure (or even correct) without the help of a third-party who is capable of performing some alternative quantum operations. This third-party, called a quantum server, is responsible for creating the initial quantum state, and later performing a particular quantum measurement and reporting the outcome. This protocol was also experimentally implemented. Interestingly, as proven in [24], the server need not be trusted and may in fact be adversarial; security is still possible even though users are so restricted. A variant of this protocol was shown to be partially device independent in [10].

The protocol described in [24] (which we call here MZ-M-SQKD19 as it is a Mach-Zehnder-based Mediated SQKD protocol developed in 2019) though proven secure in the finite-key setting under practical device constraints (e.g., imperfect detectors and weak coherent sources) and collective attacks, was inefficient. Under ideal scenarios, the key-rate of the protocol was only $1/8$ meaning that 8 qubits were required to distill 1 secret key bit assuming no noise or loss (if there is noise and/or loss, the key-rate, of course, drops even more). This inefficiency is due to the fact that users must discard numerous rounds and only use particular rounds where things "go right" (namely, a random measurement from the server produces the right outcome).

In this work, we revisit this original protocol of [24] and extend it to increase its efficiency. We also demonstrate that our extension can increase the protocol's noise tolerance. Our work is primarily concerned with improving the efficiency of this original protocol and, to evaluate, we conduct an information theoretic proof of security assuming single photons and lossy channels, though assuming an adversarial server. We compute the protocol's key-rate in the asymptotic scenario under a particular form of i.i.d. attack. Our extension adds a potential second "sub-round" for every protocol round; this greatly complicates the security analysis and our methods may be useful in other (S)QKD protocols. Importantly, our methods in improving the efficiency of this M-SQKD protocol may be useful to other experimentally realizable semi-quantum protocols, such as [8, 9] as we show how previously discarded events may be utilized in the semi-quantum model, through careful use of a second sub-round. Finally, we evaluate the protocol's performance in a variety of scenarios including noisy and lossy channels and adversarial servers.

2 Notation and preliminaries

Given a quantum state ρ_A (a Hermitian positive semi-definite operator of unit trace) acting on some Hilbert space $\mathcal{H}_A$. We write $H(A)_\rho$ to mean the von Neumann entropy of the system. Namely $H(A)_\rho = -\text{tr}(\rho_A \log \rho_A)$, where all logarithms in this paper are base two unless otherwise specified. Given a bipartite state ρ_{AE}, we write $H(A|E)_\rho$ to be the conditional von Neumann entropy, namely $H(A|E)_\rho = H(AE)_\rho - H(E)_\rho$. If both systems are classical, then $H(A|E)_\rho$ is the Shannon entropy (in which case we will often forgo writing the subscript when there is no ambiguity). We use $h(x)$ to mean the binary Shannon entropy, namely $h(x) = -x \log x - (1-x)\log(1-x)$. Given a pure state $|\psi\rangle$, we write:

$$[\psi] = |\psi\rangle \langle\psi| .$$

In general, QKD protocols (semi-quantum or otherwise) will first utilize the quantum channel and authenticated classical channel to establish a *raw key* of size N bits; this process requires sending $M \geq N$ qubits (in general, $N = p_{\text{acc}} M$, where p_{acc} is the probability that a round is "accepted" and not discarded by users). These raw keys are classical bit strings, one held by Alice and another by Bob, which are partially correlated and partially secret. Following this, an error correction protocol and privacy amplification protocol are run, establishing a final secret key of size ℓ bits. Two important metrics for any QKD protocol are its key rate $r = \ell/N$ and its effective key rate $r' = \ell/M$. In the asymptotic scenario, where $M \to \infty$, and assuming collective attacks, we may use the Devetak–Winter keyrate equation [31, 32] to evaluate these rates leading to:

$$r = H(A|E)_\rho - H(A|B) \tag{1}$$

The effective key-rate, r', is typically found by relating the number of qubits sent to the size of the raw key (e.g., if $N = p_{\text{acc}} M$, then $r' = p_{\text{acc}} r$). Above, ρ_{ABE} is the state of the system modeling a single quantum communication round, conditioned on it being accepted (i.e., conditioned on it leading to a raw key bit being generated).

To actually compute the key-rate, we will therefore need a bound on the entropy $H(A|E)_\rho$ and $H(A|B)$. The latter is typically easy to compute directly since it is a function of Alice and Bob only (who, through standard sampling arguments, may fully know their joint AB distribution and thus evaluate $H(A|B)$ directly). Bounding the quantum entropy $H(A|E)_\rho$ is the more difficult challenge and usually the key ingredient in any security proof. For that, we will later use the following result from: [33]:

Theorem 1 (From [33] though generalized for our application here) *Given a quantum state ρ_{AE} of the form:*

$$\rho_{AE} = \frac{1}{N}[\mathbf{0}]_A \otimes \left(\sum_{i=0}^{m} [\mathbf{E_i}]\right) + \frac{1}{N}[\mathbf{1}]_A \otimes \left(\sum_{i=0}^{m} [\mathbf{F_i}]\right), \tag{2}$$

then for every $0 \leq m' \leq m$ *it holds that:*

$$H(A|E)_\rho \geq \sum_{i=0}^{m'} \left(\frac{\langle E_i|E_i\rangle + \langle F_i|F_i\rangle}{N} \right) \cdot \left(h\left(\frac{\langle E_i|E_i\rangle}{\langle E_i|E_i\rangle + \langle F_i|F_i\rangle} \right) - h(\lambda_i) \right), \quad (3)$$

with:

$$\lambda_i = \frac{1}{2}\left(1 + \frac{\sqrt{(\langle E_i|E_i\rangle - \langle F_i|F_i\rangle)^2 + 4|\langle E_i|F_i|E_i|F_i\rangle|^2}}{\langle E_i|E_i\rangle + \langle F_i|F_i\rangle}\right). \quad (4)$$

Note that the states $|E_i\rangle$ *and* $|F_i\rangle$ *may be arbitrary states (not necessarily normalized nor orthogonal) in Eve's ancilla.*

Note that the above is a slight generalization of the theorem as presented in [33]; for a proof that this indeed follows, the reader is referred to [34]. In particular, the above theorem says that, given a classical-quantum state ρ_{AE} of the form described above, namely where Eve's system is the sum of rank one operators, then the entropy can be computed if one has information on the inner product of the various states in Eve's ancilla. Note that the ordering of the sum for Eve's system does not actually matter—any "pairing" of E and F states will give a lower bound. Some pairings, however, produce more optimal lower bounds. Note that it holds that any classical-quantum state may actually be represented in the above manner and so the above theorem can be used for any collective attack analysis.

3 The protocol

We now describe the protocol in detail. We assume that a two way quantum channel connects the server (C) to Alice and Bob. In the ideal scenario, this should constitute a folded Mach–Zehnder interferometer; however, since the server may be adversarial, we do not assume this in our security proof later. An authenticated classical channel connects Alice and Bob; an unauthenticated classical channel connects the server to Alice and Bob. See Fig. 1. We will call our protocol here MZ-M-SQKD19-ext (to distinguish from the original one in [24] which we extend and which, as mentioned, we refer to as MZ-M-SQKD19).

We introduce the protocol assuming an honest server for clarity, however will later prove security against a potentially corrupt server. The protocol consists of N independent *rounds*, each round consists of two *sub-rounds* with the second sub-round only being used in certain circumstances. The original protocol from [24] consists only of the first sub-round; our extension here adds this second sub-round in an effort to improve efficiency. A single round consists of the following process:

1. The server C prepares a quantum state of the form $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, with $|0\rangle$ representing a photon traveling to Alice and $|1\rangle$ representing a photon traveling to Bob. Such a state may be created by sending a single photon through a beamsplitter in a Mach–Zehnder interferometer. See Fig. 1.

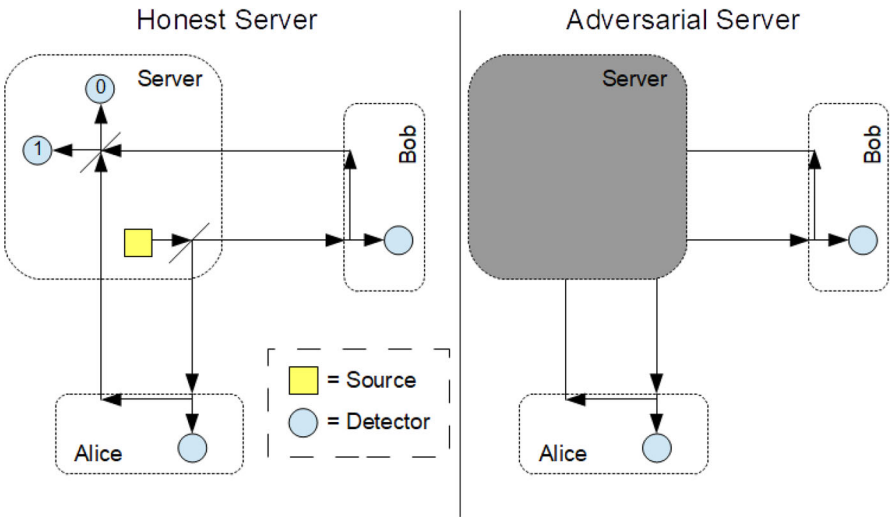

Fig. 1 Left: High-level diagram of the protocol assuming an honest server. The server should send a single photon through a beamsplitter causing the qubit to travel towards Alice and Bob in a superposition. Alice and Bob may independently choose to `Reflect` or `Measure`. If `Reflect`, the signal is sent directly back to the server; otherwise, if `Measure`, the signal is routed to a photon detector. Note that Alice and Bob cannot create new quantum systems. The server, on return, should pass the signal through a second beamsplitter and report which of the two detectors (if any) received a signal. The key is derived from users choices—in particular, when users choose *opposite* actions. Right: In our security analysis, we do not assume an honest server. Instead the server is potentially adversarial and so we cannot assume the server is actually implementing the interferometer, as is specified by the protocol. We do assume ideal single photons, however, in our analysis. See Sect. 4 for more details on our security model

2. Alice and Bob, independently, choose to `Reflect` or `Measure`. If `Measure`, the photon is routed to a photon detector; otherwise, it is routed back to the server. If a party chooses `Measure` and detects the photon, they will later signal to discard this round. Otherwise, if the measuring party does not detect the photon, Alice will use the raw-key encoding scheme that a choice of `Reflect` means a key-bit of 0 and `Measure` means a key-bit of 1; Bob will use the opposite encoding scheme. The goal of the protocol, at this point, is for Alice and Bob to guess at the action of the other party without the server (or another third-party adversary) determining what choice was actually made. Notably, it is the actions of the parties that dictate their raw key, not an actual measurement outcome.
3. The server will pass the returning signal through the second half of the interferometer (again, see Fig. 1) and report the measurement outcome, either "0," "1," or "*vac*." Here the message "*vac*" is used to indicate that the server did not detect a photon (i.e., the server detected the vacuum state). Normally, if both parties choose `Reflect`, the interferometer should be calibrated so that the message "0" is always sent. Of course natural noise (or adversarial interference) will alter this and any other value will be considered noise that must be taken into account when deriving the key rate.
4. If the server sends the message "*vac*", then Alice and Bob discard this round and repeat from step 1 with a new round; if the server sends the message "1" then Alice

Table 1 The possible outcomes of a single sub-round of the protocol under analysis assuming ideal conditions and an honest server

A	B	A_{key}	B_{key}	C's message
`Reflect`	`Measure`	0	0	"0", "1", or "vac"
`Measure`	`Reflect`	1	1	"0", "1", or "vac"
`Reflect`	`Reflect`	0	1	"0"
`Measure`	`Measure`	1	0	"vac"

This table applies to both the original MZ-M-SQKD19 and our extension here. Alice and Bob's keys are derived from their actions. Note that, whenever the server sends the message "1," users can be certain they chose *opposite* actions, thus the need to reverse the action-to-key encoding for Alice and Bob. In the original protocol, any other message from the server was discarded as it was inconclusive for users. Here, we propose an extension so that whenever the server sends the message "0," users run a second sub-round where they flip their actions. This second sub-round is discarded only if the server sends the message "vac" or users detect the photon in a measurement. See text for greater explanation

and Bob use this round to contribute towards their raw key and users are finished with this round, proceeding to the next (starting above at step 1). Ideally, if the server sends the message "1," users can be certain they chose *opposite* actions. See Table 1.

5. **Extension:** Otherwise, if the server sends the message "0", then parties will begin *Sub-Round 2*. The server will repeat the above process (from step 1) but Alice and Bob will invert their action choice. In this sub-round, when the server sends its second message, they will reject this entire round only if the server sends "vac"—otherwise, if the server sends the message "0" or "1", they will use this round to contribute towards their raw key. In particular, they will use the encoding chosen in sub-round 1.

Note that, importantly, Alice and Bob's choice of actions are independently chosen each round; however if the second sub-round is used, their actions depend on their choice in the first sub-round.

After the completion of a round (which may consist of both sub-rounds or just the first sub-round depending on the server's message), the protocol repeats with a new round. Following the completion of a sufficient number of rounds (in this paper we will consider the asymptotic scenario where the number of rounds goes to infinity), Alice and Bob will disclose a random subset of all measurement outcomes and choices to perform parameter estimation. In particular, users will choose a random subset and disclose all actions and results on those rounds chosen. Any key material from those rounds chosen for parameter estimation are, of course, discarded. Following this, assuming the error rate is "low enough" (to be discussed), they will perform an error correction and privacy amplification process to distill their final secret key.

We comment that this protocol extends the original MZ-M-SQKD19 protocol from [24] by adding the additional sub-round 2. That is, the original protocol consisted of steps 1–4 above; our extension adds the additional step 5, repeating the above for a second sub-round The original protocol would reject any round where the server did

not send the message "1." Our protocol extension here, by utilizing a second sub-round where users flip their action choice, allows for the potential contribution of message "0" to be used towards the raw key. As we show later, this extension can greatly improve the secret key generation rate of this protocol, even when counting for the potential need to send two photons on a single round (i.e., even the effective key rate is improved with our extension). Interestingly, our extension also improves the noise tolerance of the protocol as we show later.

It is clear that our protocol is correct—namely, in the absence of noise and if the server is honest, then Alice and Bob will agree on the same raw-key. Indeed, under ideal conditions, the only time the server can send the message "1" is if one of Alice or Bob, but not both, chose `Measure` and the measuring party did not detect the photon. Furthermore, in this event, it is always clear to users that the other party choose the opposite action. Now, in the event the server sends the message "0" on sub-round 1, it is not immediately clear to parties whether they choose opposite actions or if both parties choose `Reflect` (see Table 1). Thus, the original protocol [24] discarded this event leading to waste. Our extension, by utilizing a second sub-round *where users flip their actions* can potentially salvage these rounds by having the server send a second qubit and parties flipping their action choices. Note that, the ambiguity of a message "0" arises only if both parties choose `Reflect` (in which case the server will always send "0" in ideal conditions). Thus, by flipping their actions in this case, both parties, in sub-round 2 will choose `Measure` causing the server to always send the message "*vac*" (ideally) in which case parties discard the round. However, if one party chose `Measure` and the other chose `Reflect`, in the next sub-round they will choose `Reflect` and `Measure`, respectively; thus, any message of "0" or "1" by the server in this second sub-round lets parties know they are choosing opposite actions without ambiguity, thus leading to a correlation for their key.

The reader may now wonder if this is really more efficient than the original protocol in terms of number of photons sent since, for some rounds, two photons are required. We show later that our protocol, even with adversarial noise, can be more efficient than the original.

4 Security analysis

The goal of this section is to compute a bound on the key-rate of our protocol. From Eq. 1, this involves, primarily, computing a bound on the von Neumann entropy of the system. To do this, we must first model a single round of the protocol, conditioning on a key-generation event (from which $H(A|E)$ must be computed). In our security analysis, we will assume single qubits and lossy channels—that is, we do not consider multi-photon events. These are important to consider, of course, and though considered for the original protocol [24], we only consider single qubits and lossy channels here in order to demonstrate how improvements may be made to the protocol in theory, leaving practical issues as interesting future work. We will also consider only i.i.d. attacks on each sub-round. In particular, each sub-round will consist of the same (potentially probabilistic) attack operation. In general, this is weaker than a collective attack which would have the second sub-round attack dependent on the first. However, we feel that

analyzing security even in this case is still a notable contribution and furthermore, if one were to consider the multi-mediated SQKD model introduced in [34], or a variant of the protocol where users "shuffle" individual rounds into appropriate sub-rounds when needed, then it is equivalent to a general collective attack. Analyzing full collective attacks for a single server without this shuffling process would be interesting future work (though out of scope for this paper), and our method below may serve as a foundation for such an analysis.

Finally, we note that any third party adversary attack may be "absorbed" into an adversarial server's attack. Thus, in our security analysis, we only consider adversarial servers—any third party adversary's attack will be analyzed also as a consequence. Because of this, we actually consider the server to be only adversary and call the server, in this case, Eve.

Based on these assumptions, the server will begin the protocol by sending a state of the form:

$$|\phi_0\rangle = \alpha\,|0, c_0\rangle + \beta\,|1, c_1\rangle + \gamma\,|v, c_v\rangle \tag{5}$$

Note that the α, β, and γ may be real numbers as any alternative phase may simply be absorbed into the corresponding $|c_i\rangle$ ancilla state. Above, $|0\rangle$ represents a single photon traveling towards Alice; $|1\rangle$ represents a photon traveling towards Bob; and $|v\rangle$ represents a vacuum state. The $|c_i\rangle$ states are arbitrary ancilla states that the (adversarial) server may use to attempt to extract information later. If Alice chooses to `Measure`, then, with probability α^2, Alice observes the photon and, ultimately, the round will be discarded. Otherwise, with probability $1-\alpha^2$, Alice does not observe the photon in which case it collapses to $(\beta\,|1, c_1\rangle + \gamma\,|v, c_v\rangle)/\sqrt{1-\alpha^2}$. This will then be the state that returns to the server. If Bob chooses `Measure`, similar identities may be derived. Of course if both parties choose `Measure` and neither detect the photon, then it collapses to $|v, c_v\rangle$, an event that happens with probability γ^2.

Following Alice and Bob's actions, a quantum signal, or a vacuum state, returns to Eve. From this, she may apply any quantum operation; however, she must send a classical message to Alice and Bob. We may assume that this message is the same to both parties (that is, Eve does not send one message to Alice and a different message to Bob on a single round)—this is easily enforced by having Alice forward all messages she receives from the server directly to Bob over the authenticated channel and any discrepancies will cause Bob to signal to abort the protocol.

As shown in [24, 30], the most general way to model such an attack is through a quantum instrument [35] which, using standard techniques [36], may be dilated to a unitary operator. This attack, as shown in [30], then consists of Eve taking the return signal, applying an isometry U mapping it to a state living in some Hilbert space $\mathcal{H}_{cl} \otimes \mathcal{H}_E$, where in this case $\mathcal{H}_{cl}$ is spanned by $\{|0\rangle, |1\rangle, |v\rangle\}$ where these three basis states represent the three possible messages Eve could send to Alice and Bob. Following the application of U to the returned signal, Eve measures the *cl* register—the outcome determines the message she sends to the parties, while the post measured E portion represents her ancilla in this event. For a proof that this is identical to a general quantum instrument attack, see [30].

More formally, Eve's second attack is an isometry (which may, subsequently, be dilated to a unitary operator, though we do not require this detail in this section):

$$U : \mathcal{H}_T \otimes \mathcal{H}_{E_0} \to \mathcal{H}_{cl} \otimes \mathcal{H}_E, \tag{6}$$

where $\mathcal{H}_T$ is the "Transit" register modeling the traveling qubit (this is three dimensional spanned by $|vac\rangle$, $|0\rangle$, and $|1\rangle$) and $\mathcal{H}_{E_0}$ is Eve's (the adversarial server's) initial private ancilla (storing the $|c_i\rangle$ states used in the initial state, Eq. 5). This is mapped into the Hilbert space modeling the classical message sent (spanned by $|0\rangle$, $|1\rangle$, and $|v\rangle$) along with a new, enlarged, private ancilla for Eve (the server). Note that the original qubit is "absorbed" into this new ancilla allowing Eve maximum ability to attempt to extract useful information later. In particular, this takes into account that the server may not be performing an honest measurement at the end of the protocol round.

Without loss of generality, we may describe the action of this attack operator on basis states using the following notation:

$$\begin{aligned} U\,|0, c_0\rangle &= |0\rangle_{cl}\,|e_0\rangle_E + |1\rangle_{cl}\,|e_1\rangle_E + |v\rangle_{cl}\,|e_v\rangle_E \\ U\,|1, c_1\rangle &= |0\rangle_{cl}\,|f_0\rangle_E + |1\rangle_{cl}\,|f_1\rangle_E + |v\rangle_{cl}\,|f_v\rangle_E \\ U\,|v, c_v\rangle &= |0\rangle_{cl}\,|g_0\rangle_E + |1\rangle_{cl}\,|g_1\rangle_E + |v\rangle_{cl}\,|g_v\rangle_E \end{aligned} \tag{7}$$

Note that, in the following text, we often forgo writing the subscripts in the above states. Also note that U's action on basis states differing from those appearing on the left-hand side of the above expressions may be arbitrary as such states never show up in the analysis.

There are four main paths which can lead to a key being distilled based on the choices of Alice and Bob. Consider, first, the case when Alice and Bob both choose `Reflect` (in which case, should the round be accepted and not rejected, Alice will have a key-bit of 0 and Bob a key-bit of 1—note this is an error event and so, ideally, the probability of it being discarded should be one or close to one). We trace the protocol's execution in this event in order to derive a density operator describing the state of Alice, Bob, and Eve's registers in this case along with any public communication sent. Of course, as we only care about cases that lead to a key bit being distilled, we condition on events leading to a successful key generation event. In the first sub-round, since both parties choose `Reflect`, the state returns to the server unchanged, namely the state returning is $|\psi_0\rangle$. Note that, as is normal in QKD security proofs, we assume all noise is caused by the adversary's attack and that, in fact, the adversary replaces the noisy quantum channel with a perfect channel, allowing her to "hide" within the natural noise. Thus, in the event both parties choose `Reflect`, the state returning is unchanged. Eve at this point applies U evolving the state to:

$$\begin{aligned} U\,|\psi_0\rangle = {} & |0\rangle_{cl}\,(\alpha\,|e_0\rangle + \beta\,|f_0\rangle + \gamma\,|g_0\rangle) \\ & + |1\rangle_{cl}\,(\alpha\,|e_1\rangle + \beta\,|f_1\rangle + \gamma\,|g_1\rangle) \\ & + |v\rangle_{cl}\,(\alpha\,|e_v\rangle + \beta\,|f_v\rangle + \gamma\,|g_v\rangle). \end{aligned}$$

Now, the protocol discards the round if the server sends the message "v" while, if the server sends the message "1" they will use this round immediately and proceed to the next round. In this case, the state of the system is:

$$[\mathbf{01}]_{AB} \otimes \left([\mathbf{1}]_{cl} \otimes P\left(\alpha \left|e_1\right\rangle + \beta \left|f_1\right\rangle + \gamma \left|g_1\right\rangle\right) \otimes [\boldsymbol{v_0}] + \sigma_{\text{reject}}\right)$$

where, above, $[\boldsymbol{v_0}]$ is some state in Eve's ancilla used by her when the second sub-round is not used (without loss of power to Eve, this is a pure state) and σ_{reject} is the state of the system in the case that Alice and Bob signal to discard this round (this state will later be projected out when we condition on this round's acceptance and so we do not bother to derive what it is). We also define $P(|z\rangle) = [\mathbf{z}]$ to simplify the expressions.

Finally, if the server sends the message "0" parties run the second sub-round, flipping their actions to `Measure`. In this case, as discussed in our security model, Eve prepares, for sub-round 2, the same state as before, sending $|\psi_0\rangle$. Alice and Bob both then `Measure` and discard if they see a photon. Thus, focusing on the part of the state that will ultimately not be rejected (in particular, Alice and Bob do not observe the photon when it arrives, thus causing the state to collapse to $|v, c_v\rangle$ then returning to Eve), we find the final state for Alice, Bob, and Eve to be:

$$\begin{aligned}[\mathbf{01}]_{AB} \otimes \left([\mathbf{1}]_{cl} \otimes P\left(\alpha \left|e_1\right\rangle + \beta \left|f_1\right\rangle + \gamma \left|g_1\right\rangle\right) \otimes v_0 \right.\\ \left. + [\mathbf{0}]_{cl} \otimes P(\alpha \left|e_0\right\rangle + \beta \left|f_0\right\rangle + \gamma \left|g_0\right\rangle) \otimes \left[[\mathbf{0}]_{cl}[\mathbf{g_0}] + [\mathbf{1}]_{cl}[\mathbf{g_1}]\right] + \sigma_{\text{reject}}\right),\end{aligned}$$

where the AB registers are used to store Alice and Bob's classical raw key choice. Note that $|v_0\rangle$ is a state in the Hilbert space used to model the classical message and Eve's ancilla in the second sub-round assuming that sub-round is not used. Using similar techniques, one may trace the protocol for the other three cases of actions, leading to the following results (ignoring any "reject" states which, of course, appear in all the cases below):

$$\begin{aligned}&[\mathbf{10}]_{AB} \otimes ([\mathbf{1}]_{cl}[\mathbf{g_1}] \otimes [\boldsymbol{v_0}] \\ &\quad + [\mathbf{0}]_{cl} \otimes [\mathbf{g_0}] \otimes [[\mathbf{1}]_{cl} \otimes P(\alpha \left|e_1\right\rangle + \beta \left|f_1\right\rangle + \gamma \left|g_1\right\rangle) + [\mathbf{0}]_{cl} \otimes P(\alpha \left|e_0\right\rangle + \beta \left|f_0\right\rangle + \gamma \left|g_0\right\rangle)]) \\ &[\mathbf{00}]_{AB} \otimes ([\mathbf{1}]_{cl} \otimes P\left(\alpha \left|e_1\right\rangle + \gamma \left|g_1\right\rangle\right) \otimes [\boldsymbol{v_0}] \\ &\quad + [\mathbf{0}]_{cl} \otimes P(\alpha \left|e_0\right\rangle + \gamma \left|g_0\right\rangle) \otimes \left[[\mathbf{0}]_{cl} \otimes P(\beta \left|f_0\right\rangle + \gamma \left|g_0\right\rangle) + [\mathbf{1}]_{cl} \otimes P(\beta \left|f_1\right\rangle + \gamma \left|g_0\right\rangle)\right] \\ &[\mathbf{11}]_{AB} \otimes ([\mathbf{1}]_{cl} \otimes P\left(\beta \left|f_1\right\rangle + \gamma \left|g_1\right\rangle\right) \otimes [\boldsymbol{v_0}] \\ &\quad + [\mathbf{0}]_{cl} \otimes P(\beta \left|f_0\right\rangle + \gamma \left|g_0\right\rangle) \otimes \left[[\mathbf{0}]_{cl} \otimes P(\alpha \left|e_0\right\rangle + \gamma \left|g_0\right\rangle) + [\mathbf{1}]_{cl} \otimes P(\alpha \left|e_1\right\rangle + \gamma \left|g_0\right\rangle)\right]\end{aligned}$$

To clean up the resulting density operator, we introduce the following notation:

$$\begin{aligned}\left|r_1\right\rangle &= \alpha \left|e_1\right\rangle + \beta \left|f_1\right\rangle + \gamma \left|g_1\right\rangle \\ \left|r_0\right\rangle &= \alpha \left|e_0\right\rangle + \beta \left|f_0\right\rangle + \gamma \left|g_0\right\rangle \\ \left|s_1\right\rangle &= \beta \left|f_1\right\rangle + \gamma \left|g_1\right\rangle \\ \left|s_0\right\rangle &= \beta \left|f_0\right\rangle + \gamma \left|g_0\right\rangle\end{aligned}$$

$$
\begin{aligned}
|t_1\rangle &= \alpha\,|e_1\rangle + \gamma\,|g_1\rangle \\
|t_0\rangle &= \alpha\,|e_0\rangle + \gamma\,|g_0\rangle
\end{aligned} \tag{8}
$$

Using this, we derive the following density operator ρ_{ABE} which models the entire joint state of the protocol conditioning on the round not being rejected (i.e., we now project out the "reject" states above and re-normalize):

$$
\begin{aligned}
\rho_{ABE} = &\frac{1}{N}[\mathbf{00}]_{AB} \otimes ([\mathbf{1}, \mathbf{t_1}, \boldsymbol{v_0}] + [\mathbf{0}, \mathbf{t_0}, \mathbf{0}, \mathbf{s_0}] + [\mathbf{0}, \mathbf{t_0}, \mathbf{1}, \mathbf{s_1}]) \\
&+ \frac{1}{N}[\mathbf{11}]_{AB} \otimes ([\mathbf{1}, \mathbf{s_1}, \boldsymbol{v_0}] + [\mathbf{0}, \mathbf{s_0}, \mathbf{0}, \mathbf{t_0}] + [\mathbf{0}, \mathbf{s_0}, \mathbf{1}, \mathbf{t_1}]) \\
&+ \frac{1}{N}[\mathbf{01}]_{AB} \otimes ([\mathbf{1}, \mathbf{r_1}, \boldsymbol{v_0}] + [\mathbf{0}, \mathbf{r_0}, \mathbf{0}, \mathbf{g_0}] + [\mathbf{0}, \mathbf{r_0}, \mathbf{1}, \mathbf{g_1}]) \\
&+ \frac{1}{N}[\mathbf{10}]_{AB} \otimes ([\mathbf{1}, \mathbf{g_1}, \boldsymbol{v_0}] + [\mathbf{0}, \mathbf{g_0}, \mathbf{0}, \mathbf{r_0}] + [\mathbf{0}, \mathbf{g_0}, \mathbf{1}, \mathbf{r_1}])
\end{aligned} \tag{9}
$$

where N is the normalization term:

$$
\begin{aligned}
N = &\langle t_1|t_1\rangle + \langle t_0|t_0\rangle\langle s_0|s_0\rangle + \langle t_0|t_0\rangle\langle s_1|s_1\rangle \\
&+ \langle s_1|s_1\rangle + \langle s_0|s_0\rangle\langle t_0|t_0\rangle + \langle s_0|s_0\rangle\langle t_1|t_1\rangle \\
&+ \langle r_1|r_1\rangle + \langle r_0|r_0\rangle\langle g_0|g_0\rangle + \langle r_0|r_0\rangle\langle g_1|g_1\rangle \\
&+ \langle g_1|g_1\rangle + \langle g_0|g_0\rangle\langle r_0|r_0\rangle + \langle g_0|g_0\rangle\langle r_1|r_1\rangle.
\end{aligned} \tag{10}
$$

Our goal is to compute $H(A|E)_\rho$. Applying Theorem 1 and simplifying the resulting expression yields:

$$
\begin{aligned}
H(A|E)_\rho \geq &\frac{\langle t_1|t_1\rangle + \langle s_1|s_1\rangle}{N}\left[H\left(\frac{\langle t_1|t_1\rangle}{\langle t_1|t_1\rangle + \langle s_1|s_1\rangle}\right) - H(\lambda_1)\right] \\
&+ \frac{2\langle t_0, s_0|t_0, s_0\rangle}{N}\left[1 - H(\lambda_2)\right] \\
&+ \frac{\langle t_0, s_1|t_0, s_1\rangle + \langle s_0, t_1|s_0, t_1\rangle}{N}\left[H\left(\frac{\langle t_0, s_1|t_0, s_1\rangle}{\langle t_0, s_1|t_0, s_1\rangle + \langle s_0, t_1|s_0, t_1\rangle}\right) - H(\lambda_3)\right] \\
&+ \frac{\langle r_1|r_1\rangle + \langle g_1|g_1\rangle}{N}\left[H\left(\frac{\langle r_1|r_1\rangle}{\langle r_1|r_1\rangle + \langle g_1|g_1\rangle}\right) - H(\lambda_4)\right] \\
&+ \frac{2\langle r_0, g_0|r_0, g_0\rangle}{N}\left[1 - H(\lambda_5)\right] \\
&+ \frac{\langle r_0, g_1|r_0, g_1\rangle + \langle g_0, r_1|g_0, r_1\rangle}{N}\left[H\left(\frac{\langle r_0, g_1|r_0, g_1\rangle}{\langle r_0, g_1|r_0, g_1\rangle + \langle g_0, r_1|g_0, r_1\rangle}\right) - H(\lambda_6)\right]
\end{aligned} \tag{11}
$$

where:

$$
\lambda_1 = \frac{1}{2}\left(1 + \frac{\sqrt{(\langle t_1|t_1\rangle - \langle s_1|s_1\rangle)^2 + 4|\langle t_1|s_1\rangle|^2}}{(\langle t_1|t_1\rangle + \langle s_1|s_1\rangle)}\right)
$$

$$\lambda_2 = \frac{1}{2}\left(1 + \frac{|\langle t_0, s_0|s_0, t_0\rangle|}{\langle t_0, s_0|t_0, s_0\rangle}\right)$$

$$\lambda_3 = \frac{1}{2}\left(1 + \frac{\sqrt{(\langle t_0, s_1|t_0, s_1\rangle - \langle s_0, t_1|s_0, t_1\rangle)^2 + 4|\langle t_0, s_1|s_0, t_1\rangle|^2}}{(\langle t_0, s_1|t_0, s_1\rangle + \langle s_0, t_1|s_0, t_1\rangle)}\right)$$

$$\lambda_4 = \frac{1}{2}\left(1 + \frac{\sqrt{(\langle r_1|r_1\rangle - \langle g_1|g_1\rangle)^2 + 4|\langle r_1|g_1\rangle|^2}}{(\langle r_1|r_1\rangle + \langle g_1|g_1\rangle)}\right)$$

$$\lambda_5 = \frac{1}{2}\left(1 + \frac{|\langle r_0, g_0|r_0, g_0\rangle|}{\langle r_0, g_0|r_0, g_0\rangle}\right)$$

$$\lambda_6 = \frac{1}{2}\left(1 + \frac{\sqrt{(\langle r_0, g_1|r_0, g_1\rangle - \langle g_0, r_1|g_0, r_1\rangle)^2 + 4|\langle r_0, g_1|g_0, r_1\rangle|^2}}{(\langle r_0, g_1|r_0, g_1\rangle + \langle g_0, r_1|g_0, r_1\rangle)}\right)$$

We must now show how those inner products appearing in the above expression may be bounded through observable quantities (i.e., through the probabilities of certain observable events occurring). This will allow us to calculate a lower-bound on the key-rate of our protocol based only on observable quantities.

4.1 Parameter estimation

To evaluate our entropy bound derived above (in order to evaluate the key-rate of the protocol using Eq. 1), we require bounds on the inner products of those vectors appearing in Eq. 11. This can be done for any arbitrary channel, though to actually evaluate our bound and compare with prior work, we derive expressions for a symmetric depolarization attack. This is a common approach in QKD security proofs and so, by doing so, will allow us to compare with prior work and protocols. Note that our security proof above does not require this as an assumption; it is only done to evaluate the performance on a standard channel scenario. The steps we use to derive these expressions may be used, however, for any observed channel.

We may parameterize the channel statistics using a few parameters. We use ϕ to be the phase error of the channel and p_l to be the probability of loss in one direction (the server to users and the users back to the server). Finally, we use p_d to denote the dark count rate of the server's detectors. Note that if the server is adversarial, it may have perfect detectors but try to "hide" its attack by simulating a suitable dark count rate.

Now, we consider what observable statistics are available to users. We denote by $P_{0|RR}$ to be $\Pr(C = 0 \mid A = B = \texttt{Reflect})$, namely the probability that, conditioning on both Alice and Bob choosing `Reflect`, the server sends the message "0." Similarly, we can define $P_{i|RR}$ along with quantities of the form $P_{i|MR}$, $P_{i|RM}$, and $P_{i|MM}$, where the later are conditioning on Alice choosing `Measure` and Bob choosing `Reflect`; Alice choosing `Reflect` and Bob choosing `Measure`; and finally both Alice and Bob choosing `Measure`, respectively. Note that, when working with a probability involving a party choosing `Measure`, the probability is also over the measuring party not detecting the photon.

Using these parameters, we can compute important bounds on the inner products appearing in our entropy expression. Full details on these derivations are described in "Appendix A.1". We are able to determine the following:

$$
\begin{aligned}
P_{1|RR} &= \langle r_1|r_1\rangle = \frac{p_l p_d}{2} + (1-p_l)\left(\frac{p_l p_d}{2} + (1-p_l)\phi\right)\\
P_{0|RR} &= \langle r_0|r_0\rangle = \frac{p_l p_d}{2} + (1-p_l)\left(\frac{p_l p_d}{2} + (1-p_l)(1-\phi)\right)\\
P_{1|MR} &= \langle s_1|s_1\rangle = \frac{p_l p_d}{2} + \frac{1-p_l}{2}\left(\frac{p_l p_d}{2} + \frac{1-p_l}{2}\right)\\
P_{0|MR} &= \langle s_0|s_0\rangle = \frac{p_l p_d}{2} + \frac{1-p_l}{2}\left(\frac{p_l p_d}{2} + \frac{1-p_l}{2}\right)\\
P_{1|RM} &= \langle t_1|t_1\rangle = \frac{p_l p_d}{2} + \frac{1-p_l}{2}\left(\frac{p_l p_d}{2} + \frac{1-p_l}{2}\right)\\
P_{0|RM} &= \langle t_0|t_0\rangle = \frac{p_l p_d}{2} + \frac{1-p_l}{2}\left(\frac{p_l p_d}{2} + \frac{1-p_l}{2}\right)\\
P_{1|MM} &= \langle g_1|g_1\rangle = \frac{p_l p_d}{2}\\
P_{0|MM} &= \langle g_0|g_0\rangle = \frac{p_l p_d}{2}
\end{aligned}
$$

These let us easily compute N using Eq. 10 and the above. We also have:

$$
\begin{aligned}
|\alpha|^2 = |\beta|^2 &= \frac{1-p_l}{2}\\
|\gamma|^2 &= p_l,
\end{aligned}
$$

Finally, we can also derive the following bounds (again, see "Appendix A.1" for details):

$$
|\langle s_1|t_1\rangle| \geq \frac{\langle t_1|t_1\rangle + \langle s_1|s_1\rangle - \langle r_1|r_1\rangle}{2} - \frac{3}{2}\langle g_1|g_1\rangle - (\alpha\gamma + \beta\gamma)\sqrt{\langle g_1|g_1\rangle}, \quad (12)
$$

$$
|\langle s_0|t_0\rangle| \geq \frac{\langle t_0|t_0\rangle + \langle s_0|s_0\rangle - \langle r_1|r_1\rangle}{2} - \frac{3}{2}\langle g_1|g_1\rangle - (\alpha\gamma + \beta\gamma)\sqrt{\langle g_1|g_1\rangle}. \quad (13)
$$

The only remaining inner products we require are $\langle r_0|g_0\rangle$ and $\langle g_1|r_1\rangle$. However, we were unable to find a non-trivial bound for these based only on observed statistics. Our analysis shows that Eve can always set these to be orthogonal states without inducing additional noise. Note that by making these orthogonal, Eve has maximal information gain from these particular states. Thus, to work around this, we take advantage of the fact that Theorem 1 allows us to remove summation terms *while still generating a lower-bound on the entropy*. Therefore, we will instead use the following entropy bound, which can only be lower than the one in Eq. 11 (thus this bound gives more advantage to the adversary):

$$H(A|E)_\rho \geq \frac{\langle t_1|t_1\rangle + \langle s_1|s_1\rangle}{N}\left[H\left(\frac{\langle t_1|t_1\rangle}{\langle t_1|t_1\rangle + \langle s_1|s_1\rangle}\right) - H(\lambda_1)\right] + \frac{2\langle t_0, s_0|t_0, s_0\rangle}{N}\left[1 - H(\lambda_2)\right] + \frac{\langle t_0, s_1|t_0, s_1\rangle + \langle s_0, t_1|s_0, t_1\rangle}{N}\left[H\left(\frac{\langle t_0, s_1|t_0, s_1\rangle}{\langle t_0, s_1|t_0, s_1\rangle + \langle s_0, t_1|s_0, t_1\rangle}\right) - H(\lambda_3)\right] \tag{14}$$

Though we do not use it in our evaluation, we keep Eq. 11 in this paper to aid future researchers. If it is possible to derive a non-trivial bound for those inner products appearing in λ_4, λ_5, or λ_6, the key-rate bound can only improve. We derive a lower bound here that may not be optimal—yet, despite this, we show improved performance over the original protocol (as we soon show).

4.2 Evaluation

This gives us everything we need to evaluate our key-rate bound. In Fig. 2, we show how our protocol behaves as the probability of loss increases, while in Fig. 3, we show how the protocol behaves when noise varies and see that the maximal phase noise ϕ allowed is 9.8% when there is no loss (as the probability of loss increases, the maximal noise tolerance of course decreases as expected).

We also compare to the original MZ-M-SQKD19 protocol introduced in [24] which our protocol extends. For this comparison, we look at the ideal case of no loss and no dark counts for both. To perform this comparison, we note that the original protocol is the single-round version of the extension presented here. Thus, to compute it's key-rate, we simply discard all double-round terms appearing in our entropy and key-rate expressions. That is, we use only the terms involving λ_1 and λ_4. We also change the normalization term to remove the terms involving the second round. The resulting expression is then easily evaluated and, furthermore, the expression agrees exactly with the key-rate expression described in [24] for the ideal case.

This comparison is shown in Fig. 4. We note that the key-rate is significantly improved for our new protocol for the same channel noise scenario. We also compare to BB84's key rate of $1 - 2h(\phi)$ [32, 37]. Of course, BB84 outperforms as expected; however, our extension does bring the key-rate closer to that of BB84 (in the ideal scenario which is all we consider here).

Next, we consider the effective key-rate which is defined to be the number of secret bits over the total number of signals sent. The previous graphs were the number of secret bits over the raw key size, a value that is higher than the effective rate as the effective rate takes into account rounds that were discarded and the fact that some rounds require two qubits as the second sub-round was invoked. Let Q be the number of photons sent (in the combined sub-round 1 and sub-round 2 for all used rounds), and let M be the total number of rounds (where a round can consist of one or two sub-rounds; thus a round can contribute one or two photons to the total number of photons sent). Note that with most QKD protocols, and in particular the original MZ-M-SQKD19 protocol, it holds that $Q = M$; but this is not the case for our protocol. Finally, let K be the size of the raw key. We have computed, above, the

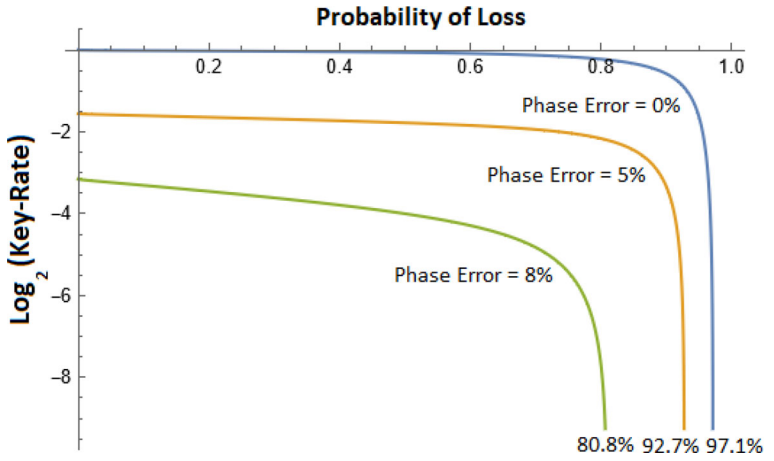

Fig. 2 Evaluating our protocol's key-rate as the probability of loss increases for fixed phase error rate ϕ. Here we set $p_d = 10^{-6}$ (a typical value for detector dark counts). Blue (top): $\phi = 0$; Yellow (middle): $\phi = 5\%$; Bottom (green): 8%. Note that this is assuming single qubits and lossy channels—if multi-photon attacks were analyzed the maximal supported probability of loss would be significantly lower; however, potentially decoy state methods [38–41] may be used to improve that though we leave that as interesting future work (Color figure online)

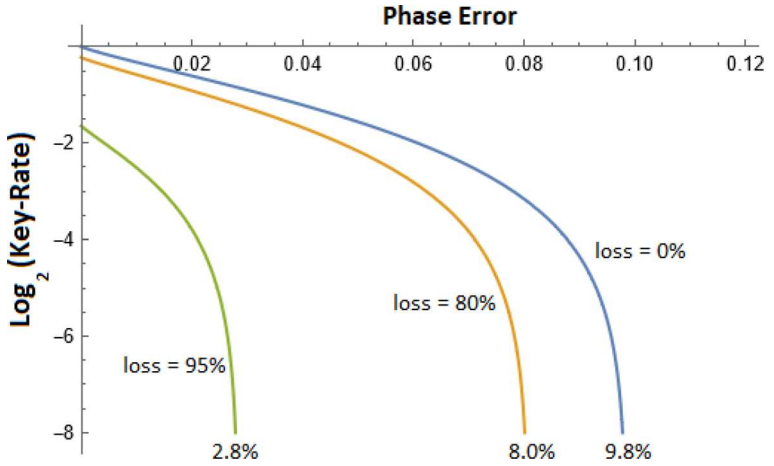

Fig. 3 Evaluating our protocol's key-rate as the phase error rate ϕ increases, for fixed loss rate. Blue (top): $p_l = 0$; Yellow (middle): $p_l = 0.8$; Green (bottom): $p_l = 0.95$. For all evaluations, we set $p_d = 10^{-6}$ (Color figure online)

ratio ℓ/K as $K \to \infty$. We next derive ℓ/Q and for this, we must express Q as a function of K. Normally, these values may all be observed; however to evaluate this and compare we will again continue to assume our symmetric noise model. This is not required, as mentioned before, it simply makes the algebra easier. It is clear that $Q = M + M \cdot \Pr(\text{Sub-Round 2 is Used}) = M(1 + \Pr(C \text{ sends "0" on Sub-Round 1}))$. Let $p_0 = \Pr(C \text{ sends "0" on Sub-Round 1})$; in our symmetric noise model, we find this to be:

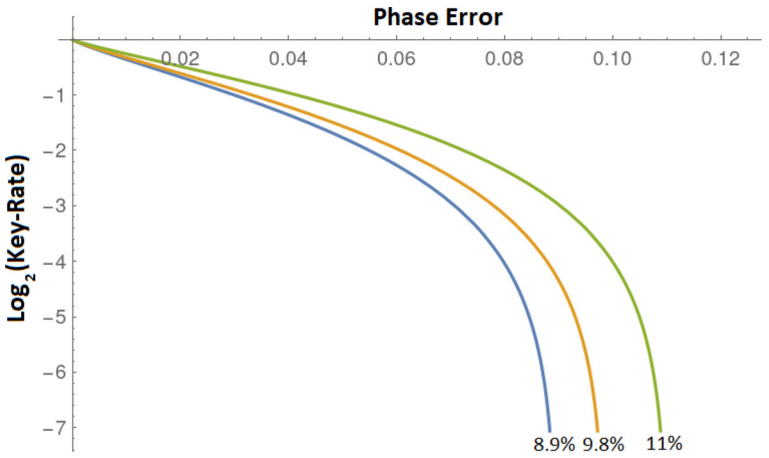

Fig. 4 Comparing our protocol's key rate (Yellow, middle) with the original MZ-M-SQKD19 protocol in [24] (Blue, bottom) with similar parameters; also comparing with BB84 (Green, top). Here, we consider no loss and no dark counts, while we vary the phase error ϕ. We note that the extension we propose here has a higher noise tolerance and higher key-rate than the original MZ-M-SQKD19 (Color figure online)

$$p_0 = \frac{1}{4}\left(2p_l p_d + (1-p_l)\left(p_l p_d + \frac{1-p_l}{2} + (1-p_l)(1-\phi)\right)\right)$$

It is clear that $K = p_{\text{acc}} M$, where p_{acc} is the probability of accepting any particular round (i.e., the probability that a round leads to a raw key bit generation). This is easily seen to be $p_{\text{acc}} = \frac{1}{4}N$, where N is given in Eq. 10. Thus, combining everything, we have:

$$K = \frac{p_{\text{acc}} Q}{1+p_0} = \frac{NQ}{4(1+p_0)} \Longrightarrow Q = \frac{4(1+p_0)K}{N},$$

and so we find the effective key-rate $r' = \frac{\ell}{Q}$ to be:

$$r' = \frac{\ell}{Q} = \frac{N\ell}{4(1+p_0)K} = \frac{N}{4(1+p_0)} r.$$

In Fig. 5, we compare the effective key-rate of our extended protocol with the original MZ-M-SQKD19 protocol. We note that even when factoring in the need for an additional qubit, our extended version is still more efficient overall. In Fig. 6, we show the overall improvement between the two protocols. We note that as the noise increases, the percentage of increase in effective key-rate of our extension also increases. Thus, our extension becomes highly useful the noisier the channel becomes.

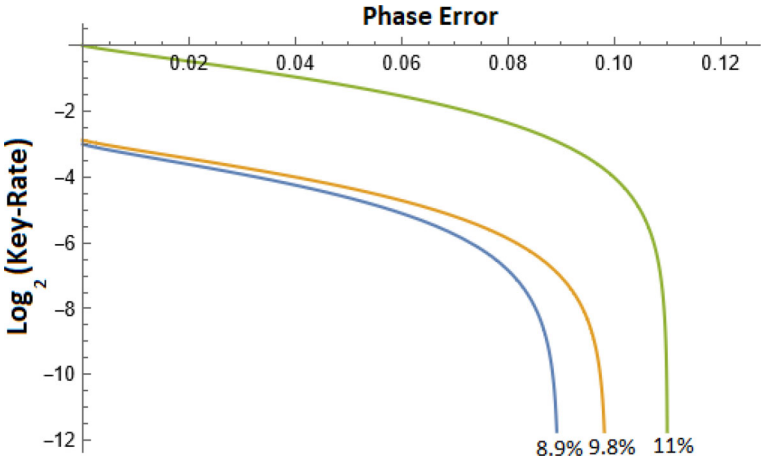

Fig. 5 Comparing our protocol's *effective* key rate (Yellow, middle) with the original MZ-M-SQKD19 protocol in [24] (Blue, bottom) with similar parameters; also comparing with BB84 (Green, top). Here we consider no loss and no dark counts while we vary the phase error ϕ. We note that even when considering the occasional need for two quantum signals per raw key bit (in the case a second sub-round is used), our extension is still more efficient and noise tolerant with similar parameters (Color figure online)

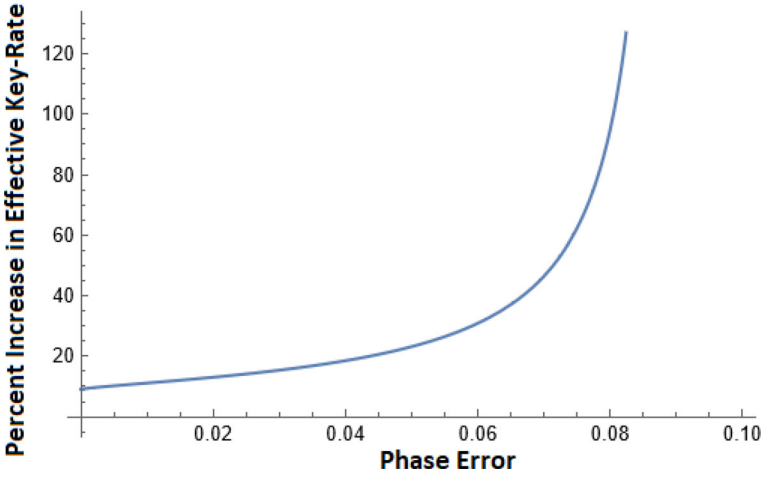

Fig. 6 The percent improvement in effective key rate of our extension compared to the original MZ-M-SQKD19 protocol under a noisy but lossless channel and no dark counts. That is, we plot $\frac{r'_{\text{new}} - r'_{\text{old}}}{r'_{\text{old}}}$ for varying levels of phase noise ϕ. Note that for $\phi > 8.9\%$, $r'_{\text{old}} = 0$ while our extension maintains a positive key-rate until 9.8% thus the reason for the asymptote

5 Closing remarks

In this paper, we introduced an extension to the mediated SQKD protocol introduced in [24]. Our extension was designed to improve efficiency of the overall system by discarding fewer rounds. Even though our extension occasionally requires the use of

two signals per round, overall effective secret key rates are still improved even under noisy channels. Interestingly, our extension also improves the noise tolerance of the protocol.

Many interesting open problems remain. First, would be a full security analysis of general attacks—techniques from [42] in reducing mediated SQKD protocols to entanglement-based versions may be useful, though those techniques do not immediately apply and some new insights are required. Also of interest would be to extend the original protocol further in an effort to not waste the vacuum events. One candidate protocol we may consider is to activate sub-round 2 if the server sends the message "0" *or* "*vac*" on sub-round 1. It is clear that this would be correct and lead to improved efficiency, especially on lossy channels. We tried to analyze the security of this protocol; however, the entropy expression contained over 18 terms and the analysis became intractable; thus, alternative methods may be required to rigorously prove security of this candidate extension. Finally, we comment that this protocol contains a high level of asymmetry in error rates. Referring to Table 1 shows that the only way to get an error of Alice$=1$ and Bob$=0$ is through a dark-count event (which are typically small). It would be interesting to see if this can be harnessed somehow to improve key-rates, perhaps even through a new classical process (e.g., a version of classical advantage distillation [43–45]) that takes into account this asymmetry.

Acknowledgements WOK would like to acknowledge support from the National Science Foundation under Grant Number 1812070. SM would like to acknowledge the support of National Science Foundation grant number CNS-1950600, which supported her during a summer REU at the University of Connecticut.

Data availability statement Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Appendix

A.1 Parameter estimation

In this appendix, we determine bounds on the needed inner products (required to evaluate Eq. 14) by considering various, observable, events such as the probability of the server sending the message "1" given that both parties choose `Reflect` (this should be small for instance). This can be done for arbitrary channels; however as discussed in the text, we derive expressions for a symmetric depolarization attack, a common approach in QKD security proofs. Note that our security proof does not require this as an assumption—it is only done in order to evaluate the performance on a standard channel scenario. Our steps below, however, may be followed for any observed channel. Under these evaluation conditions, we may parameterize the channel statistics as follows: ϕ will be the phase error of the channel; p_l is the probability of loss in one direction (the server to users and the users to the server); and p_d is the dark count rate of the server's detectors.

Recall the density operator describing one round of the protocol (Eq. 9) which we copy here:

$$\begin{aligned}\rho_{ABE} = &\frac{1}{N}[\mathbf{00}]_{AB} \otimes ([\mathbf{1}, \mathbf{t_1}, \boldsymbol{v_0}] + [\mathbf{0}, \mathbf{t_0}, \mathbf{0}, \mathbf{s_0}] + [\mathbf{0}, \mathbf{t_0}, \mathbf{1}, \mathbf{s_1}]) \\ &+ \frac{1}{N}[\mathbf{11}]_{AB} \otimes ([\mathbf{1}, \mathbf{s_1}, \boldsymbol{v_0}] + [\mathbf{0}, \mathbf{s_0}, \mathbf{0}, \mathbf{t_0}] + [\mathbf{0}, \mathbf{s_0}, \mathbf{1}, \mathbf{t_1}]) \\ &+ \frac{1}{N}[\mathbf{01}]_{AB} \otimes ([\mathbf{1}, \mathbf{r_1}, \boldsymbol{v_0}] + [\mathbf{0}, \mathbf{r_0}, \mathbf{0}, \mathbf{g_0}] + [\mathbf{0}, \mathbf{r_0}, \mathbf{1}, \mathbf{g_1}]) \\ &+ \frac{1}{N}[\mathbf{10}]_{AB} \otimes ([\mathbf{1}, \mathbf{g_1}, \boldsymbol{v_0}] + [\mathbf{0}, \mathbf{g_0}, \mathbf{0}, \mathbf{r_0}] + [\mathbf{0}, \mathbf{g_0}, \mathbf{1}, \mathbf{r_1}]) \end{aligned} \tag{15}$$

We begin by considering $\Pr(C = 1 \mid A = B = \texttt{Reflect}) = P_{1|RR}$ which is the probability that conditioning on both Alice and Bob choosing `Reflect`, the server sends the message 1. It is clear, from the analysis in Sect. 4 and the state ρ_{ABE}, that this is $P_{1|RR} = \langle r_1 | r_1 \rangle$. Under our symmetric attack scenario, we set this to $P_{1|RR} = \frac{p_l p_d}{2} + (1 - p_l)\left(\frac{p_l p_d}{2} + (1 - p_l)\phi\right)$. Similarly, we find the following:

$$\begin{aligned} P_{1|RR} &= \langle r_1 | r_1 \rangle = \frac{p_l p_d}{2} + (1 - p_l)\left(\frac{p_l p_d}{2} + (1 - p_l)\phi\right) \\ P_{0|RR} &= \langle r_0 | r_0 \rangle = \frac{p_l p_d}{2} + (1 - p_l)\left(\frac{p_l p_d}{2} + (1 - p_l)(1 - \phi)\right) \end{aligned}$$

$$\begin{aligned} P_{1|MR} &= \langle s_1 | s_1 \rangle = \frac{p_l p_d}{2} + \frac{1 - p_l}{2}\left(\frac{p_l p_d}{2} + \frac{1 - p_l}{2}\right) \\ P_{0|MR} &= \langle s_0 | s_0 \rangle = \frac{p_l p_d}{2} + \frac{1 - p_l}{2}\left(\frac{p_l p_d}{2} + \frac{1 - p_l}{2}\right) \end{aligned}$$

$$\begin{aligned} P_{1|RM} &= \langle t_1 | t_1 \rangle = \frac{p_l p_d}{2} + \frac{1 - p_l}{2}\left(\frac{p_l p_d}{2} + \frac{1 - p_l}{2}\right) \\ P_{0|RM} &= \langle t_0 | t_0 \rangle = \frac{p_l p_d}{2} + \frac{1 - p_l}{2}\left(\frac{p_l p_d}{2} + \frac{1 - p_l}{2}\right) \end{aligned}$$

$$\begin{aligned} P_{1|MM} &= \langle g_1 | g_1 \rangle = \frac{p_l p_d}{2} \\ P_{0|MM} &= \langle g_0 | g_0 \rangle = \frac{p_l p_d}{2} \end{aligned}$$

Note that, in the above, we are defining $P_{i|RM} = P_{i|MR}$ to be the probability of the server sending message i and the measuring party not detecting the photon. These let us easily compute N using Eq. 10 and the above.

It is also clear that the values of α, β, and γ may be observed based on Alice and Bob's measurements. Namely, $|\alpha|^2$ is the probability that conditioning on both parties choosing `Measure` that Alice detects the photon. Similar observations may be made for $|\beta|^2$, while $|\gamma|^2$ is the probability that neither party detects a photon. Thus, these

are:

$$|\alpha|^2 = |\beta|^2 = \frac{1-p_l}{2}; |\gamma|^2 = p_l,$$

Next, we bound $|\langle s_1|t_1\rangle|$ and $|\langle s_0|t_0\rangle|$. From Eq. 8, we have:

$$\begin{aligned}\langle r_1|r_1\rangle = \alpha^2\langle e_1|e_1\rangle + \beta^2\langle f_1|f_1\rangle + \gamma^2\langle g_1|g_1\rangle \\ + 2\alpha\beta\text{Re}\langle e_1|f_1\rangle + 2\beta\gamma\text{Re}\langle f_1|g_1\rangle + 2\gamma\alpha\text{Re}\langle g_1|e_1\rangle\end{aligned}$$

Thus,

$$\begin{aligned}\alpha\beta\text{Re}\langle e_1|f_1\rangle &= \frac{1}{2}(\langle r_1|r_1\rangle - \alpha^2\langle e_1|e_1\rangle - \beta^2\langle f_1|f_1\rangle - \gamma^2\langle g_1|g_1\rangle \\ &\quad - 2\beta\gamma\text{Re}\langle f_1|g_1\rangle - 2\gamma\alpha\text{Re}\langle g_1|e_1\rangle) \\ &= \frac{1}{2}(\langle r_1|r_1\rangle - \alpha^2\langle e_1|e_1\rangle - \beta^2\langle f_1|f_1\rangle - \gamma^2\langle g_1|g_1\rangle) \\ &\quad - \beta\gamma\text{Re}\langle f_1|g_1\rangle - \gamma\alpha\text{Re}\langle g_1|e_1\rangle \end{aligned} \tag{16}$$

Now, we can write $\text{Re}\langle s_1|t_1\rangle$ as:

$$\text{Re}\langle s_1|t_1\rangle = \alpha\beta\text{Re}\langle f_1|e_1\rangle + \beta\gamma\text{Re}\langle f_1|g_1\rangle + \alpha\gamma\text{Re}\langle g_1|e_1\rangle + \gamma^2\langle g_1|g_1\rangle$$

By substituting in Eq. 16 and noting that $\text{Re}\langle e_1|f_1\rangle = \text{Re}\langle f_1|e_1\rangle$, we have:

$$\begin{aligned}\text{Re}\langle s_1|t_1\rangle &= \frac{1}{2}(\langle r_1|r_1\rangle - \alpha^2\langle e_1|e_1\rangle - \beta^2\langle f_1|f_1\rangle - \gamma^2\langle g_1|g_1\rangle) \\ &\quad - \beta\gamma\text{Re}\langle f_1|g_1\rangle - \gamma\alpha\text{Re}\langle g_1|e_1\rangle + \beta\gamma\text{Re}\langle f_1|g_1\rangle + \alpha\gamma\text{Re}\langle g_1|e_1\rangle + \gamma^2\langle g_1|g_1\rangle \\ &= \frac{1}{2}\langle r_1|r_1\rangle - \frac{1}{2}\alpha^2\langle e_1|e_1\rangle - \frac{1}{2}\beta^2\langle f_1|f_1\rangle + \frac{1}{2}\gamma^2\langle g_1|g_1\rangle \end{aligned} \tag{17}$$

Next we may find an expression for $\alpha^2\langle e_1|e_1\rangle$ by looking at $\langle t_1|t_1\rangle$ (which is an observable quantity as discussed above, namely $P_{1|RM}$):

$$\begin{aligned}&\langle t_1|t_1\rangle = \alpha^2\langle e_1|e_1\rangle + \gamma^2\langle g_1|g_1\rangle + 2\alpha\gamma\text{Re}\langle e_1|g_1\rangle \\ &\implies \alpha^2\langle e_1|e_1\rangle = \langle t_1|t_1\rangle - \gamma^2\langle g_1|g_1\rangle - 2\alpha\gamma\text{Re}\langle e_1|g_1\rangle\end{aligned}$$

Of course $\langle t_1|t_1\rangle$ is an observable probability for Alice and Bob and, later, we may use Cauchy–Schwarz to bound $|\langle e_1|g_1\rangle|$ thus allowing them to bound $\alpha^2\langle e_1|e_1\rangle$ used in the expansion of $\langle s_1|t_1\rangle$. Similarly, we find:

$$\begin{aligned}&\langle s_1|s_1\rangle = \beta^2\langle f_1|f_1\rangle + \gamma^2\langle g_1|g_1\rangle + 2\beta\gamma\text{Re}\langle f_1|g_1\rangle \\ &\implies \beta^2\langle f_1|f_1\rangle = \langle s_1|s_1\rangle - \gamma^2\langle g_1|g_1\rangle - 2\beta\gamma\text{Re}\langle f_1|g_1\rangle\end{aligned}$$

Combining this into Eq. 17 and using the (reverse) triangle inequality yields:

$$\begin{aligned}|\langle s_1|t_1\rangle| \geq |\mathrm{Re}\langle s_1|t_1\rangle| &= \frac{1}{2}\,|\langle t_1|t_1\rangle + \langle s_1|s_1\rangle - \langle r_1|r_1\rangle - 3\langle g_1|g_1\rangle - 2\alpha\gamma\mathrm{Re}\langle e_1|g_1\rangle \\ &\quad -2\beta\gamma\mathrm{Re}\langle f_1|g_1\rangle| \\ &\geq \frac{\langle t_1|t_1\rangle + \langle s_1|s_1\rangle - \langle r_1|r_1\rangle}{2} \\ &\quad - \frac{3}{2}\langle g_1|g_1\rangle - (\alpha\gamma+\beta\gamma)\sqrt{\langle g_1|g_1\rangle}, \end{aligned} \tag{18}$$

where, for the last inequality, we used the fact that $|\langle e_1|g_1\rangle| \leq \sqrt{\langle e_1|e_1\rangle\langle g_1|g_1\rangle} \leq \sqrt{\langle g_1|g_1\rangle}$. (Similarly for $\langle f_1|g_1\rangle$.) Similarly we may bound:

$$|\langle s_0|t_0\rangle| \geq \frac{1}{2}\,|\langle t_1|t_1\rangle + \langle s_1|s_1\rangle - \langle r_1|r_1\rangle - 3\langle g_1|g_1\rangle - 2\alpha\gamma\mathrm{Re}\langle e_1|g_1\rangle - 2\beta\gamma\mathrm{Re}\langle f_1|g_1\rangle| \tag{19}$$

$$\geq \frac{\langle t_0|t_0\rangle + \langle s_0|s_0\rangle - \langle r_1|r_1\rangle}{2} - \frac{3}{2}\langle g_1|g_1\rangle - (\alpha\gamma+\beta\gamma)\sqrt{\langle g_1|g_1\rangle}. \tag{20}$$

References

1. Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical Bob. Phys. Rev. Lett. **99**, 140501 (2007)
2. Boyer, M., Gelles, R., Kenigsberg, D., Mor, T.: Semiquantum key distribution. Phys. Rev. A **79**, 032341 (2009)
3. Zou, X., Qiu, D., Li, L., Wu, L., Li, L.: Semiquantum-key distribution using less than four quantum states. Phys. Rev. A **79**(5), 052312 (2009)
4. He, J., Li, Q., Wu, C., Chan, W.H., Zhang, S.: Measurement-device-independent semiquantum key distribution. Int. J. Quantum Inf. **16**(02), 1850012 (2018)
5. Amer, O., Krawec, W.O.: Semiquantum key distribution with high quantum noise tolerance. Phys. Rev. A **100**(2), 022319 (2019)
6. Vlachou, C., Krawec, W., Mateus, P., Paunković, N., Souto, A.: Quantum key distribution with quantum walks. Quantum Inf. Process. **17**(11), 1–37 (2018)
7. Iqbal, H., Krawec, W.O.: High-dimensional semiquantum cryptography. IEEE Trans. Quantum Eng. **1**, 1–17 (2020)
8. Boyer, M., Katz, M., Liss, R., Mor, T.: Experimentally feasible protocol for semiquantum key distribution. Phys. Rev. A **96**(6), 062335 (2017)
9. Krawec, W.O.: Practical security of semi-quantum key distribution. In: Quantum Information Science, Sensing, and Computation X, vol. 10660, pp. 1066009. International Society for Optics and Photonics (2018)
10. Silva, M., Faleiro, R., Mateus, P.: Semi-device-independent quantum key distribution based on a coherence equality (2021). arXiv preprint arXiv:2103.06829
11. Chongqiang, Y., Jian, L., Xiubo, C., Yuan, T., Yanyan, H.: An efficient semi-quantum key distribution protocol and its security proof. IEEE Commun. Lett. **26**, 1226–1230 (2022)
12. Li, Q., Chan, W.H., Long, D.-Y.: Semiquantum secret sharing using entangled states. Phys. Rev. A **82**(2), 022303 (2010)
13. Lin, J., Yang, C.-W., Tsai, C.-W., Hwang, T.: Intercept-resend attacks on semi-quantum secret sharing and the improvements. Int. J. Theor. Phys. **52**(1), 156–162 (2013)
14. Wang, J., Zhang, S., Zhang, Q., Tang, C.-J.: Semiquantum secret sharing using two-particle entangled state. Int. J. Quantum Inf. **10**(05), 1250050 (2012)

15. Zou, X.F., Qiu, D.W.: Three-step semiquantum secure direct communication protocol. Sci. China Phys. Mech. Astron. **57**(9), 1696–1702 (2014)
16. Gu, J., Lin, P., Hwang, T.: Double C-NOT attack and counterattack on 'three-step semi-quantum secure direct communication protocol'. Quantum Inf. Process. **17**(7), 1–8 (2018)
17. Xie, C., Li, L., Situ, H., He, J.: Semi-quantum secure direct communication scheme based on bell states. Int. J. Theor. Phys. **57**(6), 1881–1887 (2018)
18. Sun, Y., Yan, L., Chang, Y., Zhang, S., Shao, T., Zhang, Y.: Two semi-quantum secure direct communication protocols based on bell states. Mod. Phys. Lett. A **34**(01), 1950004 (2019)
19. Rong, Z., Qiu, D., Mateus, P., Zou, X.: Mediated semi-quantum secure direct communication. Quantum Inf. Process. **20**(2), 1–13 (2021)
20. Thapliyal, K., Sharma, R.D., Pathak, A.: Orthogonal-state-based and semi-quantum protocols for quantum private comparison in noisy environment. Int. J. Quantum Inf. **16**(05), 1850047 (2018)
21. Chongqiang, Y., Jian, L., Xiubo, C., Yuan, T.: Efficient semi-quantum private comparison without using entanglement resource and pre-shared key. Quantum Inf. Process. **20**(8), 1–19 (2021)
22. Wen, X.-J., Zhao, X.-Q., Gong, L.-H., Zhou, N.-R.: A semi-quantum authentication protocol for message and identity. Laser Phys. Lett. **16**(7), 075206 (2019)
23. Zhou, N.-R., Zhu, K.-N., Bi, W., Gong, L.-H.: Semi-quantum identification. Quantum Inf. Process. **18**(6), 1–17 (2019)
24. Massa, F., Yadav, P., Moqanaki, A., Krawec, W.O., Mateus, P., Paunković, N., Souto, A., Walther, P.: Experimental quantum cryptography with classical users (2019). arXiv preprint arXiv:1908.01780
25. Gurevich, P., Orenstein, M., Mor, T.: Experimental Quantum Key Distribution with Clasical Alice. PhD thesis, Computer Science Department, Technion (2013)
26. Iqbal, H., Krawec, W.O.: Semi-quantum cryptography. Quantum Inf. Process. **19**(3), 1–52 (2020)
27. Pirandola, S., Andersen, U.L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., et al.: Advances in quantum cryptography. Adv. Opt. Photon. **12**(4), 1012–1236 (2020)
28. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N., Peev, M.: The security of practical quantum key distribution. Rev. Mod. Phys. **81**, 1301–1350 (2009)
29. Amer, O., Garg, V., Krawec, W.O.: An introduction to practical quantum key distribution. IEEE Aerosp. Electron. Syst. Mag. **36**(3), 30–55 (2021)
30. Krawec, W.O.: Mediated semiquantum key distribution. Phys. Rev. A **91**(3), 032323 (2015)
31. Devetak, I., Winter, A.: Distillation of secret key and entanglement from quantum states. Proc. R. Soc. A Math. Phys. Eng. Sci. **461**(2053), 207–235 (2005)
32. Renner, R., Gisin, N., Kraus, B.: Information-theoretic security proof for quantum-key-distribution protocols. Phys. Rev. A **72**, 012332 (2005)
33. Krawec, W.O.: Quantum key distribution with mismatched measurements over arbitrary channels. Quantum Inf. Comput. **17**(3 and 4), 209–241 (2017)
34. Krawec, W.O.: Multi-mediated semi-quantum key distribution. In: 2019 IEEE Globecom Workshops (GC Wkshps), pp. 1–6. IEEE (2019)
35. Davies, E.B., Lewis, J.T.: An operational approach to quantum probability. Commun. Math. Phys. **17**(3), 239–260 (1970)
36. Wilde, M.M.: From classical to quantum Shannon theory (2011). arXiv preprint arXiv:1106.1445
37. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441 (2000)
38. Hwang, W.-Y.: Quantum key distribution with high loss: toward global secure communication. Phys. Rev. Lett. **91**, 057901 (2003)
39. Lo, H.-K., Ma, X., Chen, K.: Decoy state quantum key distribution. Phys. Rev. Lett. **94**, 230504 (2005)
40. Wang, X.-B.: Beating the photon-number-splitting attack in practical quantum cryptography. Phys. Rev. Lett. **94**, 230503 (2005)
41. Lim, C.C.W., Curty, M., Walenta, N., Xu, F., Zbinden, H.: Concise security bounds for practical decoy-state quantum key distribution. Phys. Rev. A **89**(2), 022307 (2014)
42. Guskind, J., Krawec, W.O.: Mediated semi-quantum key distribution with improved efficiency (2021). arXiv preprint arXiv:2111.01627
43. Maurer, U.M.: Secret key agreement by public discussion from common information. IEEE Trans. Inf. Theory **39**(3), 733–742 (1993)
44. Bae, J., Acín, A.: Key distillation from quantum channels using two-way communication protocols. Phys. Rev. A **75**(1), 012334 (2007)

45. Chau, H.F.: Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate. Phys. Rev. A **66**(6), 060302 (2002)