Semi-Quantum Cryptography

Hasan Iqbal¹ and Walter O. Krawec^{*1}

¹Department of Computer Science and Engineering, University of Connecticut, Storrs, CT 06269 USA

October 15, 2019

Abstract

Quantum key distribution (QKD) protocols allow two parties to establish a shared secret key, secure against an all powerful adversary. This is a task impossible to achieve through classical communication only; indeed, to distribute a secret key through classical means requires one to assume computationally bounded adversaries. If, however, both parties are "quantum capable" then security may be attained assuming only that the adversary must obey the laws of physics. But "how quantum" must a protocol actually be to gain this advantage over classical communication? This is one of the questions semi-quantum cryptography seeks to answer.

Semi-quantum communication, a model introduced in 2007 by M. Boyer, D. Kenigsberg, and T. Mor (PRL 99 140501), involves the use of fully-quantum users and semiquantum, or "classical" users. These classical users are only allowed to interact with the quantum channel in a limited, classical manner. Originally introduced to study the key-distribution problem, semi-quantum research has since expanded, and continues to grow, with new protocols, security proof methods, experimental implementations, and new cryptographic applications beyond key distribution. Research in the field of semi-quantum cryptography requires new insights into working with restricted protocols and, so, the tools and techniques derived in this field can translate to results in broader quantum information science. Furthermore, other questions such as the connection between quantum and classical processing, including how classical information processing can be used to counteract a quantum deficiency in a protocol, can shed light on important theoretical questions.

This work surveys the history and current state-of-the-art in semi-quantum research. We discuss the model and several protocols offering the reader insight into how protocols are constructed in this realm. We discuss security proof methods and how classical post-processing can be used to counteract users' inability to perform certain quantum operations. Moving beyond key distribution, we survey current work in other

^{*}Email: walter.krawec@uconn.edu

semi-quantum cryptographic protocols and current trends. We also survey recent work done in attempting to construct practical semi-quantum systems including recent experimental results in this field. Finally, as this is still a growing field, we highlight, throughout this survey, several open problems that we feel are important to investigate in the hopes that this will spur even more research in this topic.

1 Introduction

Through most of history, *cryptography* was an *art* primarily focused on hiding and sending information secretly (i.e., encryption). Numerous ciphers were used through history, many of which are now considered insecure by modern standards. In fact, it wasn't until very recently in the mid 20th century that cryptography transformed from an art to a *science*. Now we have rigorous methods and techniques to argue and measure security of cryptographic systems. Interestingly, along with these new techniques came a great extension to the underlying applications beyond encryption, such as authentication, secret sharing, signatures (just to name a few), along with a great explosion in user base.

In general, there are two flavors to modern cryptography: private key and public key (also known as symmetric key and asymmetric key respectively). In a private key setting, all users of the underlying primitive (whether it be encryption, authentication, or some other task), share the same secret key k (i.e., this key is privately shared and all users have the same symmetric information concerning this key). In a public key setting, one user has a public/private key pair while all other users, including potential adversaries, hold the public key. Thus there is an asymmetry to the overall system with one user having additional information.

While public key cryptography is an incredibly useful mechanism, allowing for users with only public information to, for instance, send information securely to a single party holding the secret key (namely, public key encryption), it is also orders of magnitude slower than symmetric key systems. Furthermore, while some symmetric key systems can be proven information theoretic secure (i.e., secure without requiring computational assumptions), this is impossible with public key cryptography where security must *always* depend on some unproven computational assumption. Thus, despite public key cryptography's great appeal, it is still desirable in practice to use symmetric key cryptography whenever possible. But how do parties agree on a secret key k without an adversary learning it? This is exactly the *key distribution* problem. For more information on these issues, the reader is referred to [1].

Of course, if distances are short and the user-base is small, a secret key could be agreed on by meeting in person. Obviously this solution does not scale. Today, we use public key cryptography to distribute secret keys (for instance in a TLS/SSL connection, public key encryption is used to transfer a randomly generated shared session key between parties [2] thus, public key cryptography is used to "boot-strap" symmetric key mechanisms which are much faster). But the security of such systems, then, depend entirely on the security of the underlying public key system used to distribute the key.

Rather interestingly, it is a mathematical impossibility for two parties to agree on a

shared secret key which is secure against a computationally unbounded adversary, when using only *classical communication*. Instead, one must always make assumptions on the power of the adversary. Thankfully, this impossibility result does not hold when parties switch to *quantum communication*. Indeed, if users utilize quantum information (in addition to classical information), it is possible to establish a shared secret key, secure against an allpowerful adversary (i.e., an adversary who is bounded only by the laws of physics, and not necessarily by some computational hardness assumption). Requiring only that the adversary live in a physical universe, as opposed to the adversary having difficulty solving certain mathematical problems, is an arguably safer assumption for securing our communication infrastructure.

Quantum Key Distribution (QKD) was initially discovered in 1984 by Bennett and Brassard [3] and, independently, in 1991 by Ekert [4], however it wasn't until many years later in 2001 that a full proof of security was developed [5]. An alternative, information theoretic proof technique was developed in 2004 by Renner et al. [6]. Such protocols require the two users, whom we refer throughout this work as the customary Alice (A) and Bob (B), to both be capable of manipulating qubits in certain manners (e.g., being able to prepare and measure qubits in arbitrary bases). Both parties must, therefore, be quantum capable.

But is this always needed? If both parties are capable only of classical communication, perfectly secure key distribution is impossible; if both parties are quantum capable, then it is possible. What is the middle-ground and what exactly happens in this "gap" between classical and quantum communication? This is the question which *semi-quantum cryptography* seeks to shed light on. Introduced originally in 2007 by M. Boyer, D. Kenigsberg, and T. Mor in [7], this field has seen growing interest over the years with new protocols, new cryptographic primitives, and new security proofs leading to a growing research area. Furthermore, as our society begins to move towards practical implementations of quantum communication networks [8, 9, 10, 11], the semi-quantum model may hold unique benefits allowing for potentially cheaper devices (as less "quantum capable hardware" may be required) or devices that are more robust to hardware faults (as one may switch to a semi-quantum mode of operation if some devices fail). Finally, the theoretical and practical innovations necessary to study the semi-quantum model, where users are highly restricted in their abilities, may lead to great innovations in the broader field of quantum information science.

This paper surveys the development and the latest state of the art in the field of semiquantum cryptography. We will begin by discussing basic (fully) quantum key distribution topics that are relevant. After this, we will present the semi-quantum model in detail along with the first protocols developed for key distribution - so called *semi-quantum key distribution* (SQKD) protocols. We will cover in detail semi-quantum key distribution protocols, past and current along with the research being done to reduce quantum resource requirements even further. Following this, a detailed review of security results and methods will be presented, including proof techniques and noise tolerance results. The last topic in keydistribution will be a survey of multi-user SQKD protocols, including protocols where multiple classical users establish a key through the use of an untrusted (adversarial) quantum server. Semi-quantum cryptography now spreads beyond key distribution so we will then survey other applications of the model to primitives such as secret sharing, secure direct communication, and private state comparison. We will conclude with a survey on current practical SQKD research, including recent experimental implementations.

1.1 Quantum Key Distribution

Before discussing the semi-quantum model of cryptography, we review here some basic facts about quantum key distribution. We only review some important facts needed to put into context the work done in the semi-quantum model - for a more complete survey of standard (i.e., "fully-quantum") quantum cryptographic protocols and technology, the reader is referred to [8, 9, 10, 11]. This survey, of course, will focus on semi-quantum communication and cryptography.

QKD protocols utilize both quantum and classical communication. A quantum channel connects users allowing them to send quantum resources to one another (e.g., qubits); an authenticated classical channel is also available on which users may send authenticated, but not secret, messages to one another. A QKD protocol generally consists of two stages: first is a *quantum communication stage* followed by a second *post processing stage*. Much research is often spent in the first stage, while the second generally consists of standard classical cryptographic processes (though, we note, developing new, faster, and more efficient systems for this second stage is also an area of active research and interest). Certainly, in the semi-quantum field, at the moment all research has been on the first stage, using standard techniques and methods for the second stage.

The quantum communication stage of a protocol typically operates over numerous, independent, iterations. Each iteration consists of random choices by users, however the choice is independent of previous iterations. Thus, when presenting a protocol later, we generally write out only a single iteration of the quantum communication stage - it is understood, then, that what is written would be repeated a sufficiently large amount of time as required by the users. The goal of this stage is to utilize the quantum communication channel and the classical authenticated channel, to establish what is called a raw key. These are two strings of classical bits, one string held by A and one by B, which are partially correlated and partially secret. Due to noise in the quantum channel (either natural or adversarially generated), the strings will inevitably have errors in them. Furthermore, one must assume the worst case that an adversary has some classical or quantum system correlated or entangled with this raw key. Thus, the raw key, by itself, cannot be used directly for cryptographic applications. Instead it must be further processed through the second stage of a QKD protocol. Before this, however, a second output of the quantum communication stage is some form of sampling data on the quantum channel determining, at a minimum, the noise level in the quantum channel. We refer to this data as the channel's *noise signature*. Exactly what data this consists of depends on the protocol.

The second stage, the classical post processing stage, takes as input the raw key and the noise signature and, first, runs an error correction protocol. This uses the authenticated classical channel thus leaking additional information to E; this additional leakage must be

taken into account in any security proof. Following this a privacy amplification protocol is run, taking the error corrected raw key and hashing it down to a secret key. Privacy amplification is done using a two-universal hash function [6]. Namely, A will choose a hash function f randomly from a family of two-universal hash functions. She will send a description of f to B using the authenticated channel (thus the adversary then knows which function f is used). Following this, both users run their raw key through the hash function resulting in a secret key K_A and K_B of size ℓ bits.

If the protocol is correct, it should hold that $K_A = K_B$ with high probability (i.e., they should differ only with negligible probability as determined by some user specified security parameter). If the protocol is secure, it should be that any adversary's system should be independent of the final secret key and, furthermore, the secret key should be no different from one chosen uniformly at random.

More formally, let ρ_{KE} be the state of the system describing the generated secret key K (known to A and B) and E's system (which includes anything learned from error correction and the chosen privacy amplification hash function). Then, the protocol is considered secure if:

$$\left|\left|\rho_{KE} - I_K/2^\ell \otimes \rho_E\right|\right| \le \epsilon,\tag{1}$$

where ||X|| is the trace distance of operator X. In essence, the above says that, after execution, the actual protocol state, ρ_{KE} , is ϵ -indistinguishable from an ideal state consisting of a key chosen uniformly at random and completely independent of E's system. One is very often interested in the key rate of a (S)QKD protocol, defined to be the ratio of secret bits (ℓ) to either the size of the raw-key N, or the number of qubit signals sent (the latter of which is, of course, never smaller than N and can, in fact, be much larger depending on how efficient the protocol is); note that the latter term is smaller and is often called the *effective* key-rate. We will return to these notions later when we discuss key-rate computations for SQKD protocols.

As we will see later, an important question, given a new (S)QKD protocol, is to determine a bound on its key-rate ℓ/N , either in the finite key setting or the asymptotic setting (the latter being when N approaches infinity). This bound should be a function only of observed noise statistics (the noise signature). Once this is computed, one is also interested in a (S)QKD protocol's *noise tolerance* - namely the maximal observed noise for which the keyrate remains positive. We will return to these concepts later.

2 Semi-Quantum Key Distribution

The question, "how quantum does a protocol or system need to be to gain an advantage over its classical counterpart" is an important one both theoretically and practically. This question has been studied in various manners, but it wasn't until Boyer et al., introduced the semi-quantum model for key distribution that this question was first extended to the field of *cryptography* [7].

A semi-quantum key distribution (SQKD) protocol typically consists of two users: a *fully* quantum user Alice (A) and a classical user Bob (B) (though the names may occasionally



Figure 1: The typical setup of an SQKD protocol. A fully quantum user A begins by sending quantum states to B. This user, A, is allowed to prepare any state required by the protocol. This qubit passes through the *forward channel* to the semi-quantum or classical user B. This user, B, is only allowed to perform certain operations, namely ignore the qubit (Reflect) or interact with the qubit in the computational Z basis only (e.g., Measure and Resend). B may also only prepare Z basis qubits. The *reverse channel* then carries qubits back to A. Note that, B, the classical user, can only interact with the channel directly in the Z basis, or disconnect from the channel, in which case A is sending quantum information to herself in a large loop. When qubits return to A through the reverse channel, she is allowed to perform any operation on them.

be reversed in some references, it is irrelevant to our discussion). Before introducing actual protocols, it is important to more rigorously understand and define exactly what a "classical" user is in the context of this problem. Indeed, what does it even mean for a so-called "classical" user to interact with a quantum channel?

2.1 The Semi-Quantum Model

The quantum user has access to a quantum channel which starts at her lab, travels out, and returns to her. The *classical user* (sometimes called the *semi-quantum user*) B can access a portion of this channel. Thus, semi-quantum protocols operate over a two-way quantum channel where qubits, or other quantum carriers, travel first from the quantum user A, to the classical user B, then return to the quantum user. See Figure 1.

Besides the requirement of a two-way quantum channel, SQKD protocols place a further restriction on the classical user. Namely, he is only allowed to interact with the quantum channel by performing a Z basis measurement or sending Z basis qubits. Alternatively, he can simply ignore the channel, disconnect from it, in which case A, the quantum user, is simply "talking to herself." More specifically, for every qubit received, B may choose one of the following options:

- 1. Measure: Subject the incoming qubit to a Z basis measurement.
- 2. Prepare: Prepare a Z basis state and send it to A on the reverse channel.

- 3. Measure and Resend: Subject the incoming qubit to a Z basis measurement and then resend the result back to A as a Z basis qubit (a combination of the above two operations, though with the restriction that B always sends the same state he observes this is actually important for security as discussed later in this paper).
- 4. Reflect: Reflect the qubit back to A undisturbed. This is equivalent to simply disconnecting from the quantum channel and forwarding everything back to the sender (e.g., A). The classical user does not learn anything about the state of the qubit in this case.
- 5. **Permute**: Reorder the qubits received (or a subset of qubits received) without otherwise disturbing them. The classical user does not learn anything about the underlying states of the qubits, he only permutes their order.

Protocols that utilize Reflect and Measure and Resend are generally called *measure-resend* protocols while those that require Permute are usually called *randomization based* protocols [12]. Note that B can only directly work in the Z basis; otherwise he can disconnect from the quantum channel in which case A, the fully quantum user, is simply "talking to herself." We comment that, occasionally, new semi-quantum research introduces new operations that the semi-quantum user B may perform and we will comment on these other operations as they arise in our survey.

Note that if both A and B were restricted to these operations (either working in a single Z basis or disconnecting from the quantum channel), the resulting protocol would be no different, from a mathematical standpoint, from a purely classical protocol and, thus, could never be unconditionally secure. The question is, can one user be classical in this sense (in that he can only operate in a single basis or ignore the channel) while still maintaining security? As it turns out, the answer is, indeed, yes.

2.2 First Protocols

In their seminal paper, Boyer et al. [7], introduced two SQKD protocols to demonstrate the model. Here we discuss these protocols to give the reader some idea as to how SQKD protocols typically operate.

As with QKD protocols, SQKD protocols operate in two stages. The quantum communication stage of the original measure-resend style SQKD protocol from [7], which we denote here BKM07, operates by repeating the following:

Protocol: BKM07 [7]

- 1. A prepares one of the four states $|0\rangle$, $|1\rangle$, $|+\rangle$, or $|-\rangle$ with uniform probability, remembering her choice. She sends the resulting qubit to the classical user B.
- 2. B will choose to either Measure and Resend or to Reflect the incoming qubit.

- 3. A will measure the returning qubit in the same basis she initially used to prepare it (Z or X).
- 4. A discloses her choice of basis while B discloses his choice of operation. Measurement results and initial state preparation choices remain secret.
- 5. If A choose to send a Z basis qubit and if B choose Measure and Resend, parties may use this round for their raw-key. In particular, A will use her initial preparation choice while B will use his measurement result (these should be correlated). All other iterations, along with a suitably sized random sample of raw-key iterations, are used for sampling the quantum channel error rates.

Note that the protocol could be written equivalently with A using her measurement result for her key-bit instead of her initial state preparation choice. Indeed, A can choose later which option to follow based on the observed noise - if the noise in the forward channel is higher than the reverse, it would make sense to switch (this way there will be a higher correlation between A and B's raw key results). For sampling, note that due to the two way quantum channel, several statistics can be gathered, namely:

- $p_{i,j}^{A \to B}$: The probability that B measures a $|j\rangle$ given that A sent a $|i\rangle$ and B choose Measure and Resend, for $i, j \in \{0, 1\}$.
- $p_{i,j}^{B\to A}$: The probability that A measures a $|j\rangle$ given that B sent a $|i\rangle$ (for $i, j \in \{0, 1\}$).
- $p_{i,R,j}^{A \to A}$: The probability that A measures a $|j\rangle$ given that she initially sent a $|i\rangle$ and B choose Reflect (now, for $i, j \in \{0, 1, +, -\}$).

Note that, while users can measure the Z basis noise (e.g., a $|i\rangle$ flipping to a $|1-i\rangle$ for i = 0, 1) in each of the forward and reverse channels, they can only measure the X basis noise in the entire joint channel. Since B cannot measure or prepare in the X basis, it is impossible to observe the X basis error in either channel separately. This opens up potential attack strategies for an adversary and makes security analyses difficult (we comment on current security techniques later in this paper).

The second SQKD protocol introduced by the same authors in [12], utilized the Permute operation as opposed to the Measure and Resend.

Protocol: BGKM09 [12]

- 1. A prepares N qubits, each qubit prepared randomly in one of the four states $|0\rangle$, $|1\rangle$, $|+\rangle$, or $|-\rangle$. She sends all N qubits to B.
- 2. For each qubit, *B* chooses randomly to Measure or to Reflect. For those qubits he chooses to Reflect, he also permutes the qubits before returning them. That is, he does not disturb their state through any measurement, however he re-orders them before resending. Those qubits he measures he does not resend.

- 3. A stores the returning qubits in a quantum memory. At this point, B will inform her which qubits he choose Reflect and also the order he reflected them back. The quantum user A then undoes the permutation and measures the returned qubits in the same basis she initially sent them.
- 4. A discloses which qubits she sent in the Z basis. Whenever A sent a Z basis qubit and B choose to Measure, users now have a correlation used for their raw key.

Note that the above protocol requires a quantum memory on the part of the quantum user. It also, in a way, requires more advanced capabilities on the part of the classical user in that he must be able to randomly permute qubits (perhaps, through delay lines [12]). Note that, if B does not "resend" then he must "permute" otherwise the protocol becomes susceptible to the so-called double CNOT attack [12]. Indeed, in this case, E can apply a CNOT gate to all qubits traveling in the forward direction. If B measures, but does not resend, E will notice a vacuum leaving his lab in which case a measurement of her ancilla provides full information to her. If B chooses to Reflect, then E will simply apply a CNOT gate in the reverse channel, undoing the initial state (since B's operation is the identity operation in this event and so the two CNOT gates invert each other) and thus avoid detection. Therefore, it is vital for any point-to-point SQKD protocol to have the classical user "resend" or "permute."

The above protocols were *prepare-and-measure* protocols whereby qubits are prepared and subsequently measured (similar to BB84). Additionally, *entanglement based* SQKD protocols were also subsequently proposed where the fully quantum user prepares entangled states, sending one particle to the other (classical) user and holding the other locally (similar to an E91 style protocol [4]). For instance, [13] proposed two protocols in this line where the quantum user prepares a Bell state, sending a particle to the classical user. This user then performs the Reflect or Measure and Resend operation, returning the state to A. Whenever B performed Reflect, A will measure the qubit pair in the Bell basis - she should receive the same Bell state she originally prepared. On other iterations, she measures her qubit in the Z basis, creating a correlation between the two parties that is used as their raw key (A's qubit measurement in the Z basis should match B's). A similar protocol was described in that same reference where B also uses the Permute option.

An alternative entanglement based protocol was presented in [14]. Here a different encoding scheme was used in that a key bit of 0 is encoded by sending a Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ while a key bit of 1 is encoded by sending a Bell state $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. Namely, on each iteration of the protocol A prepares, randomly, a Bell state $|\Phi^+\rangle$ or $|\Psi^+\rangle$; her choice determines her random raw key bit for this iteration. It is, therefore, the goal of B to guess which Bell state A prepared. This is done by A sending one particle to B, keeping the remaining one private. B then chooses Measure and Resend or Reflect. Finally, when a qubit returns to A, she will measure both particles either in the Bell basis or the computational basis. Parties then disclose their operations. When B choose Reflect and A chose to measure in the Bell basis, she should receive the same outcome that she initially prepared (other outcomes being counted as errors). For all iterations where A measured in the computational basis, however, she will disclose the measurement result of the qubit she kept private (i.e., she discloses 0 or 1 based on the computational basis measurement of the qubit she initially kept private). This disclosure, combined with B's measurement outcome (which he keeps private) allows him to determine which of the two Bell states A prepared, thus allowing him to guess A's raw key bit for that iteration. Note that for E to guess this also, she would have to know the measurement result of the qubit particle that traveled between parties - however such a measurement on her part would have caused a disturbance in the cases where B choose Reflect. We discuss general security issues later in this work, however this encoding scheme is interesting in that it allows a classical party to, in a way, determine the result of a Bell state preparation with help from A.

2.3 Reducing Resource Requirements

Numerous SQKD protocols have been developed, beyond those mentioned in the previous section, each with various advantages, disadvantages, and theoretical interests. One of the primary theoretical goals of semi-quantum cryptography is to better understand "how quantum" a protocol must be to gain an advantage over its classical counterpart; thus, one important research direction in semi-quantum communication is in further reducing the quantum resource requirements on the part of the two users. This includes both the fully-quantum user, and the semi-quantum user. As this is a vital area of research in semi-quantum cryptography, we spend some time here surveying the recent progress in this area.

The first result in this line of investigation came in 2009 with a paper by Zou et al., [15]. In this work it was shown, for the first time, that the fully-quantum user can also have reduced resource requirements. Namely, five new protocols were proposed. These protocols required fully-quantum Alice to send only three, two, or even a single state to B. On return, of course, the fully-quantum user must be able to measure in two bases. In light of their work, one may classify SQKD protocols as *n*-state SQKD protocols where *n* is the number of states that the quantum user A may choose to prepare. If n = 1 we call the protocol a single state protocol; otherwise it is a multi state protocol. Zou et al., [15] presented the first single state protocol along with 2 and 3 state protocols. Note that BKM07 is a 4-state protocol.

The so-called *single state* SQKD protocol from [15] is of particular interest as it sparked several additional protocols along this line; furthermore, such protocols actually admit certain nice reductions in their security proofs which we will comment on later. The quantum communication stage of this protocol repeats the following process:

Protocol: Single State SQKD [15]

- 1. A prepares a single qubit in the state $|+\rangle$ and sends it to B.
- 2. *B* chooses randomly to Measure and Resend or to Reflect recording his choice and, if applicable, his measurement outcome.

- 3. A chooses to measure in the Z or the X basis randomly.
- 4. Users A and B disclose their choices. If B chose to Measure and Resend and if A chose to measure in the Z basis, they should share a correlated bit to be used for their raw key. If B chose Reflect and if A chose to measure in the X basis, she should observe outcome |+⟩ and any other outcome is considered an error.

This single state protocol is remarkably simple and demonstrated that the fully quantum user need not have advanced source preparation capabilities. Rather remarkably, as we comment later, the security properties of this protocol were also shown to be optimistically comparable to certain fully-quantum protocols, at least in the perfect qubit scenario (we will discuss this later when we talk about security of SQKD protocols).

Since Zou et al.'s 2009 paper [15], several other single-state protocols have been proposed. In 2014 it was shown that a key need not be distilled from measurement choices, but instead may be distilled from *B*'s action [16]. While the BKM07 protocol may be considered a semi-quantum version of the BB84 protocol (since all four BB84 states are transmitted on the return channel) and the Single State SQKD protocol may be considered a semi-quantum three-state BB84 [17, 18] (since only three states, $|0\rangle$, $|1\rangle$, and $|+\rangle$ are transmitted on the return channel), this new protocol is, in a way, a version of the Extended B92 [19] protocol. This is due to the fact that three states are transmitted on the return channel ($|+\rangle$, $|0\rangle$, and $|1\rangle$) and, furthermore, the encoding scheme is based on alternative basis choice (as determined by *B*'s actual operation) and not based on the qubit state directly. This singlestate protocol operates as follows:

Protocol: Reflection-Based SQKD [16]

- 1. A prepares a single qubit in the state $|+\rangle$, sending it to B.
- 2. B chooses a random bit k_B . If $k_B = 0$, he will choose to Reflect the qubit, and furthermore he sets a private internal register \texttt{accept}_B to TRUE with 1/2 probability (otherwise it is set to FALSE). If $k_B = 1$ he chooses to Measure and Resend setting $\texttt{accept}_B = \texttt{TRUE}$ only if he observes $|0\rangle$.
- 3. A chooses randomly to measure in the Z or X basis. If she chooses the Z basis and observes outcome $|1\rangle$, she sets $k_A = 0$ and $\operatorname{accept}_A = \operatorname{TRUE}$. If she chose the X basis and observes outcome $|-\rangle$, she sets $k_A = 1$ and $\operatorname{accept}_A = \operatorname{TRUE}$. All other measurement outcome possibilities result in her setting $\operatorname{accept}_A = \operatorname{FALSE}$ (in which case k_A is set arbitrarily).
- 4. Users A and B both divulge their value of accept_A and accept_B respectively. If both are TRUE, they will keep their bits k_A and k_B to contribute towards their raw key. Otherwise, the iteration is discarded.

It is not difficult to see the similarity between the above protocol and a B92-style protocol. Indeed, the key is transmitted only when B chooses **Reflect** (which should result in him sending a $|+\rangle$) or when he chooses **Measure and Resend** and observes $|0\rangle$. However, there is one very significant difference - namely, B cannot be certain he is sending a $|+\rangle$ when he chooses **Reflect**. Indeed, an adversary will attack the forward channel (see Figure 1), altering this state. Unlike security proofs of standard one-way protocols, security proofs of semi-quantum protocols must take into account that what B sends is affected by E's forward channel attack. This complicates security analyses. Another protocol based also on this reflection-based encoding scheme was developed in [20] which is, in a way, the semiquantum version of B92 (the non-extended version).

In [21], a two state SQKD protocol was proposed where the quantum user prepares a random X basis state (either $|+\rangle$ or $|-\rangle$) and sends it to the classical user. Note that in their paper, they referred to the quantum user as B and the classical user as A (thus flipping the labels with B now initiating the communication). However, to remain consistent throughout this work, we will maintain the notion that A is the quantum user who initiates the communication and B is the classical user. Obviously the exact labeling is irrelevant. Following this state preparation, the classical user chooses one of two operations Measure and Resend or Reflect; finally the quantum user will choose to measure in a random basis Z or X. Both parties disclose their choices and the key is distilled from those iterations where B, the classical user, chose Measure and Resend and the quantum user A chose the Z basis. Thus, it is, in a way, a two-state version of the BKM07 protocol.

Another single-state protocol, along with a new four-state protocol, was proposed in [22]. This paper increased B's abilities by allowing him to choose a Measure and Prepare option (as opposed to simply resending whatever he observed). This option gives B the ability to measure a qubit in the Z basis, but prepare any Z basis state he likes, regardless of his measurement outcome (normally the Measure and Resend option forces him to always send the basis state he measured). This augmentation allows for the construction, also, of a secure direct communication protocol.

Attack on B's Send Operation: Rather interestingly, it was recently shown in [23] that by allowing B this extra ability (namely the ability to prepare any Z basis state regardless of measurement outcome), only partial security may be achieved. Thus, rather interestingly, if both parties are fully quantum, secure protocols exists (e.g., BB84 [3]); if B is classical in that he only chooses Reflect, Measure and Resend, or Permute, the protocol may also be secure (e.g., BKM07 [7]); however if we take this and add a little extra power to B, security may break down. The attack discovered in [23] operates as discussed below, though we generalize it slightly here to show how it may be applied to arbitrary protocols which operate using the Measure and Prepare operation (where the prepared Z basis qubit may be in a different state than what was measured) as opposed to the Measure and Resend operation - that is, their attack described in [23] can be applied to arbitrary semi-quantum protocols whenever B deviates from sending exactly the Z basis state he measured:

1. In the forward channel (refer to Figure 1), Eve applies a CNOT gate, using the traveling

qubit as a control and her private ancilla as a target. Her private ancilla is initially in a $|0\rangle_E$ state.

2. In the reverse channel, E applies the following operator which acts on the traveling qubit (denoted the T space) and her private ancilla as follows:

$$\begin{aligned} U_R & |00\rangle_{TE} = |00\rangle_{TE} \\ U_R & |11\rangle_{TE} = |10\rangle_{TE} \\ U_R & |01\rangle_{TE} = |02\rangle_{TE} \\ U_R & |10\rangle_{TE} = |13\rangle_{TE} . \end{aligned}$$

Note that we assume E's ancilla is four dimensional, spanned by basis states $|0\rangle, \dots, |3\rangle$. Also note that the operator U_R as described is an isometry and so may be dilated to a unitary operator through standard techniques (thus, it is an operation E could physically perform).

Now, on any particular iteration of a SQKD protocol, Alice will send a state of the form $\alpha |0\rangle + \beta |1\rangle$. These α and β may be chosen randomly if the protocol is a multi-state one, or they may be publicly known if the protocol is a single state one. After the initial CNOT gate, the joint system becomes $\alpha |0,0\rangle_{TE} + \beta |1,1\rangle_{TE}$. If *B* chooses **Reflect**, the state returning to *E* is exactly this; *E* will then apply U_R evolving the joint state to $(\alpha |0\rangle + \beta |1\rangle) \otimes |0\rangle_E$ thus creating no detectable disturbance.

On the other hand, if B chooses to Measure and Prepare, he will detect $|0\rangle$ with probability $|\alpha|^2$ or $|1\rangle$ with probability $|\beta|^2$, the same probability had E chosen to not attack and, so far at least, her attack is not detected. We may write the resulting state as a density operator:

$$\left|\alpha\right|^{2}\left|0\right\rangle\left\langle 0\right|_{B}\otimes\left|0\right\rangle\left\langle 0\right|_{E}+\left|\beta\right|^{2}\left|1\right\rangle\left\langle 1\right|_{B}\otimes\left|1\right\rangle\left\langle 1\right|_{E},$$

where we introduced a *B* register storing *B*'s measurement result. Next, *B* chooses to prepare a fresh qubit (unlike Measure and Resend, the state he sends may be different from that he observed). If he sends a $|0\rangle$, the resulting state, again modeling as a density operator due to *B*'s measurement, is:

$$\left|\alpha\right|^{2}\left|0\right\rangle\left\langle0\right|_{B}\otimes\left|00\right\rangle\left\langle00\right|_{TE}+\left|\beta\right|^{2}\left|1\right\rangle\left\langle1\right|_{B}\otimes\left|01\right\rangle\left\langle01\right|_{TE}\right\rangle$$

which becomes, after applying U_R :

$$\rho_0 = |\alpha|^2 |0\rangle \langle 0|_B \otimes |00\rangle \langle 00|_{TE} + |\beta|^2 |1\rangle \langle 1|_B \otimes |02\rangle \langle 02|_{TE}.$$

$$\tag{2}$$

Following the same logic, had B chosen to send $|1\rangle$, we have density operator:

$$\rho_1 = |\alpha|^2 |0\rangle \langle 0|_B \otimes |13\rangle \langle 13|_{TE} + |\beta|^2 |1\rangle \langle 1|_B \otimes |10\rangle \langle 10|_{TE}.$$
(3)

The T qubit is passed to A. It is not difficult to see that this attack goes undetected. However, by measuring her ancilla, if E observes $|2\rangle_E$ she knows for certain that B choose to Measure and Prepare, that he originally observed $|1\rangle$ and that he sent $|0\rangle$. If E observes $|3\rangle_E$ she knows that B originally observed $|0\rangle$ and sent $|1\rangle$. In these cases, E has full information on B and A, thus causing a security break. Of course this attack does not always work. Indeed, it fails whenever B chooses to send exactly the same state he measured (i.e., he ends up using Measure and Resend)! Thus, by increasing B's capabilities, we actually cause a security break. Since this attack does not work all of the time (some iterations will give E no information) it leads to a partially secure system (i.e., it may be *partially robust* as defined in [7] though we will return to this notion of "robustness" later in this work).

Open Problem 1: While security is broken when B sends an alternative state than what he observed for key distillation, are there potential advantages to this, perhaps, in better categorizing E's attack? Additional noise statistics may be gathered which could help security so long as those iterations where B sends the opposite state are never used for the key.

Research has shown that decreasing A's source preparation ability (e.g., single-state protocols) can still lead to secure key distribution systems. Interestingly it is also possible to decrease her ability to measure. In [24], it was shown that A need only measure in the X basis and send three states. In [25], it was shown that A needed only to prepare two states, a $|0\rangle$ and a state $|a\rangle$ where $|\langle 0|a\rangle| \in (0, 1)$ while only measuring using a three outcome POVM. This last paper provided an SQKD protocol that could smoothly transition from classical communication to (semi) quantum communication and proposed a method of measuring the affects this transition has on secure communication rates. However, their security analysis required a three outcome POVM - while weaker than a two basis measurement, it is not as weak as simply measuring in a single basis as in [24] (though *that* paper required three states). This leads to a rather interesting open problem:

Open Problem 2: Does there exist an SQKD protocol where A sends only two (non orthogonal) states and only performs a measurement in a single basis?

Clearly, a single state SQKD protocol where A measures only in one basis cannot exist. This is easy to see: assume such a protocol exists - then, since A sends only a single state, no key material can be transferred on the forward channel, instead it must be transmitted somehow using the reverse or loop channels. But, since A can only measure in a single basis, and since this basis is public knowledge (due to Kerckhoffs' principle [1], the basis choice should be public knowledge), Eve could simply also measure in this basis any qubit arriving to A. Thus A and E's systems will be fully correlated and no key can be distilled. Thus, to have any hope of further reducing resource requirements on the quantum user, a two state, one basis protocol is the only possibility. It is unclear if such a protocol can exist.

One candidate was proposed in [25], but it is not clear that it is secure. While it was shown to be secure against a single Intercept/Resend attack in [25], beyond this no proof of security (or insecurity) exists. Since single-state with two basis measurement protocols exist [15, 16, 20, 21], and since three state, one basis measurement protocols exist [24], a two-state, one basis measurement protocol would be an interesting development in SQKD research and represent the minimal resource requirements on the part of the quantum user, in a point-to-point SQKD system (there are other models of semi-quantum communication involving third parties which are outside of this question's scope and which we discuss later).

Continuing our discussion on reducing resource requirements, a protocol where B does not need to actually perform a measurement was shown in [26]. This protocol required the Measure and Permute operations. Namely, on receipt of a qubit stream from A, B will choose to discard a random subset of the qubits and prepare fresh Z basis ones in place of them (these qubits are not first measured). He then applies the Permute operation sending these qubits back to A. Another protocol in [27] was introduced where B needs only to be able to Reflect or discard a qubit (he need not measure nor must he prepare a qubit). This required a third party however. The protocol consisted of A sending qubits to B who can choose to drop them, or forward them (the Reflect operator in this case) to the third party server. This third party was responsible for applying a unitary gate to the qubits received and sending them back to B. This classical user B may again choose to discard or forward them back to the third party who then measures the qubits.

2.4 Other SQKD Protocols

While a large portion of research has been in the direction of further reducing resource requirements for an SQKD protocol (either for the fully quantum or the semi quantum user), other novel protocols with interesting theoretical insights have also been developed. One area of research has been in attempting to develop "authenticated SQKD protocols" which do not utilize an authenticated channel (instead relying on a pre-shared key). Protocols of this nature have been proposed in [28, 29]. Security in this regime, however, is difficult to define and attacks have been shown in [30]. There has not been a complete information theoretic security analysis for these protocols as of writing this, instead security is generally shown against certain classes of attacks.

Strategically utilizing the two-way quantum channel is another possible research direction to take when designing new SQKD protocols. In [31] a new SQKD protocol was developed where A uses information from both the forward and reverse channels. This results in a loss of efficiency but results in a drastic increase in protocol noise tolerance - something we will comment on later when discussing security results.

Efficiency is an important consideration to take into account when designing new SQKD protocols. In [32, 33] protocols were proposed to improve efficiency by biasing choices to improve their overall efficiency (e.g., by leading to fewer discarded iterations due to incompatible choices), similar to what is done for fully-quantum protocols [34].

Other encoding schemes are also worth investigating. In [35], two qubits were used in a form of time-bin encoding. The encoding was done in a way so as to allow for robust protection against dephasing noise. A six-qubit encoding scheme was presented in [36] (subsequently improved in [37]) allowing for protection against dephasing and rotation noise.

While the majority of SQKD research is in reducing resource requirements, some work in [38, 39] has been done in high-dimensional (beyond a small fixed constant number of qubits per signal) SQKD. Since it is now known that the use of high-dimensional quantum states for fully quantum key distribution provides several benefits, especially in noise tolerance (see

[40, 41, 42, 43, 44] for a few references), it is interesting to see that this also translates to the semi-quantum case.

When working with high-dimensional semi-quantum communication, one must define what the classical user's capabilities are when interacting with high-dimensional states. The natural approach (used also in [38, 39]) is for A, the fully quantum user, to send an arbitrary state $|\psi\rangle$, now living in a d-dimensional space (instead of the usual d=2). B, when receiving this state, can either choose **Reflect** in which case he reflects the entire *d*-dimensional state, or he can choose Measure and Resend in which case he performs a measurement in the d-dimensional computational basis, namely $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$ and prepares a fresh ddimensional state based on his measurement outcome. Of course when d = 2 this agrees completely with Boyer et al.'s original definitions [7]; furthermore, if both A and B are restricted to these operations, the protocol is no different, mathematically, from a classical one and, so, this seems the natural way to extend semi-quantum communication to higher dimensions. In [38], a high-dimensional SQKD protocol based on the use of quantum walks was presented (here, the states A prepared were results from evolving a quantum walk [45, 46]). In [39] a high-dimensional version of BKM07 was presented which was shown to tolerate high levels of noise as the dimension of the quantum state increases (similar to what occurs in the fully-quantum setting [41]). Future work in developing high-dimensional semi-quantum protocols may prove very interesting in further discovering the differences, and similarities, between the semi-quantum and fully-quantum models of communication.

3 Security Results

In this section we discuss research on security aspects of SQKD protocols in the perfect qubit scenario (we leave practical security issues for a later section). There are two main challenges to performing a security analysis of a semi-quantum protocol. First is the fact that at least one party (potentially both as discussed above) is limited in some nature and, therefore, users cannot make certain measurements on the noise in the quantum channel. For instance, they cannot measure the X basis noise in the forward channel (from A to B). Second is the fact that E has two opportunities to interact with the qubit in flight - first when it travels to B and second on its return. Indeed, as shown in [47], attacking twice can allow an adversary greater information gain than simply attacking one channel, at least for some SQKD protocols. In this section we review general techniques for arguing about the security of SQKD protocols.

3.1 Robustness

The first notion of security for a semi-quantum protocol was *robustness*. This was a term introduced by Boyer et al., in the original SQKD paper [7] and states that an SQKD protocol is *robust* if any attack which causes an adversary to learn non-zero information on the raw key of the protocol must necessarily induce a detectable disturbance in the quantum channel. That is, the adversary cannot get any information without risking detection. The notion



Figure 2: Showing the attack scenario considered in Boyer et al.'s proof of robustness [12]. Each U_i is a unitary probe acting on all N qubits and E's quantum ancilla.

of *partial robustness* was introduced in that same paper which weakens the definition to allowing the adversary to gain some information without being detected, but any attack which gains full information on the raw key must induce a detectable disturbance.

To prove an SQKD protocol robust, one must show that for any attack, if E's ancilla is somehow correlated with A or B's raw key bit register, then this attack cannot go undetected with unit probability. In general, there are two main methods of proving a protocol robust. The first, introduced in [12] involves the following:

- 1. First, assume that E is able to capture all N qubits leaving A's lab in bulk. Before forwarding them to B, E applies a unitary probe U_0 acting jointly on all qubits and E's private ancilla.
- 2. Following this probe, E forwards the first qubit to B. After B's operation, the qubit returns to A however E captures it again. At this point, the adversary once again holds all N qubits and applies a new unitary probe U_1 which, as with U_0 , acts jointly on all qubits and E's private ancilla (the same ancilla throughout).
- 3. E then repeats the above, sending the next qubit to B, capturing it on its return, and probing it with a new unitary operator U_i .
- 4. Once all N qubits have gone through this process, E returns the N qubits to A who completes the protocol.

This process is depicted in Figure 2. It is obviously a very strong attack model allowing E to capture these qubits in bulk.

The second method of showing robustness was introduced first in [15] by Zou et al., and makes the assumption that A only sends a subsequent qubit to B after receiving the previous

one back from him. This assumption restricts E from storing all N qubits simultaneously, however the probe E uses need not be the same for every iteration. This assumption generally simplifies the security proof and allows for an inductive style argument to prove robustness. Indeed, consider the BKM07 protocol - an inductive style of robustness proof could proceed along these lines: Consider the first iteration of the protocol. Then, A sends a qubit state of the form $|i\rangle_T$ for $i \in \{0, 1, +, -\}$ (we use "T" to represent the transit space - i.e., the two-dimensional Hilbert space modeling the qubit in transit between parties). Let $U_F^{(1)}$ be E's first probe in the forward direction. Since this is the first iteration, E's ancilla is cleared to some default pure state $|\chi\rangle_E$ which we may assume is known to E (note, the state is pure to E's advantage). The action of this first probe on basis states may be written as:

$$U_F^{(1)} |0\rangle_T \otimes |\chi\rangle_E = |0, e_0\rangle_{TE} + |1, e_1\rangle_{TE}$$
$$U_F^{(1)} |1\rangle_T \otimes |\chi\rangle_E = |0, e_2\rangle_{TE} + |1, e_3\rangle_{TE}$$

where the $|e_i\rangle$ are arbitrary states in E's private ancilla (these are not assumed to be normalized or orthogonal). However, with non-zero probability this iteration will be used for error detection. Thus, to avoid detection, E must set $|e_1\rangle \equiv |e_2\rangle \equiv 0$, that is, both must be the zero vector. When the qubit returns (recall, this second model of robustness from [15] assumes A will not send another qubit until this one returns - thus E is forced to probe the qubit immediately on return from B), E applies a second probe $U_R^{(1)}$ whose action we may write as:

$$U_R^{(1)} |0, e_0\rangle_{TE} = |0, f_0\rangle_{TE} + |1, f_1\rangle_{TE}$$
$$U_R^{(1)} |1, e_3\rangle_{TE} = |0, f_2\rangle_{TE} + |1, f_3\rangle_{TE}$$

where, like the $|e_i\rangle$ states, the $|f_j\rangle$ are arbitrary states in E's ancilla. Note that $U_R^{(1)}$'s action on states not of the form $|0, e_0\rangle$ and $|1, e_3\rangle$ is irrelevant as they never appear. As before, this iteration may be used for error detection with non zero probability. Thus to avoid detection, namely to avoid inducing any Z basis noise in the reverse channel, E must set $|f_1\rangle \equiv |f_2\rangle \equiv 0$. Now, with non-zero probability A might have sent $|+\rangle$ and B may have chosen Reflect. In this case, the state returning to A is found to be:

$$U_{R}^{(1)}U_{F}^{(1)}|+,\chi\rangle_{TE} = U_{R}^{(1)}\left(\frac{1}{\sqrt{2}}|0,e_{0}\rangle + \frac{1}{\sqrt{2}}|1,e_{3}\rangle\right)$$
$$= \frac{1}{\sqrt{2}}|0,f_{0}\rangle + \frac{1}{\sqrt{2}}|1,f_{3}\rangle$$
$$= \frac{1}{2}|+\rangle\left(|f_{0}\rangle + |f_{3}\rangle\right) + \frac{1}{2}|-\rangle\left(|f_{0}\rangle - |f_{3}\rangle\right), \tag{4}$$

where the last equality arises from changing the transit space from the Z to the X basis. At this point, it is clear that to avoid detection, it must hold that $|f_0\rangle = |f_3\rangle$. Thus, E's ancilla after this first iteration is completely independent of the transit space and A and B's measurements. Through induction, one sees that this holds for each subsequent iteration for probes $U_F^{(i)}$ and $U_R^{(i)}$ (though note that the initial state $|\chi\rangle_E$ is potentially different each iteration, but remains independent of A and B's state).

Proving robustness in the first model introduced by Boyer et al., in [7] is more involved. It is an interesting open problem, however, to know whether or not this iterative attack as assumed in the Boyer model of robustness gives E any advantage.

3.2 Information Theoretic Analysis

The notion of robustness gives a good security guarantee in that any adversary who attempts to learn something about the raw key risks being detected. Beyond this, it is often useful, however, to know exactly *how much* an adversary could have learned given a certain amount of detectable noise. As current quantum communication systems are not perfect there will always be natural noise that cannot be avoided. As we assume all-powerful adversaries, we must actually assume, therefore, the worst case that the adversary replaces the noisy quantum channel with a perfect one. She then hides her attack within the expected natural noise. Thus, as is typical with standard QKD research [8, 9, 10, 11], we must assume that any detectable noise is the result of an adversary. The question then is how much information can an adversary gain? And, furthermore, how much noise is "too much." Similar questions also involve the protocol's efficiency as determined by its key-rate.

Recall that a (S)QKD protocol is considered secure if, after privacy amplification, Equation 1 holds. If we consider collective attacks [8] (i.i.d. attacks where E is free to postpone measurement of her ancilla until any future point in time and, furthermore, is free to perform a joint coherent measurement on her ancilla at that point to attempt to extract maximal information), let N be the size of the raw key *before* error correction and privacy amplification are run. Let ℓ be the size of the secret key satisfying Equation 1; then it was shown in [6] that, in the asymptotic limit it holds that:

$$\lim_{N \to \infty} \frac{\ell}{N} = \inf \left[S(A|E) - H(A|B) \right],\tag{5}$$

where the infimum is over all collective attacks which induce the observed noise statistics (e.g., error rates). Here, S(A|E) is the von Neumann entropy of A's raw-key bit register conditioned on E's quantum memory system while H(A|B) is the classical Shannon entropy of A's raw-key bit register conditioned on B's. This equation is very intuitive: it states that the key-rate increases when E has a lot of uncertainty (measured by S(A|E)) and B has little uncertainty (measured by H(A|B)). The goal of a (S)QKD security proof in this manner is to determine a lower-bound on r, given only the observed noise statistics. That is, one cannot compute S(A|E) with certainty since we do not know exactly what attack E used however, one can attempt to lower-bound E's uncertainty based on the noise assuming she chose an optimal attack which induces that observed noise. Note that an alternative, and equivalent, version of Equation 5, derived in [48], is:

$$\lim_{N \to \infty} \frac{\ell}{N} = \inf \left[I(A:B) - I(A:E) \right],\tag{6}$$

where I(A : E) is the quantum mutual information and I(A : B) is the classical mutual information. That these two versions of the key-rate expression are the same follows immediately from the definition of mutual information and the fact that the systems under consideration, namely A and B's classical raw-key registers and E's quantum register, are classical-classical-quantum states.

The question, then, becomes: given certain observed channel statistics (e.g., noise rates in the quantum channel(s)), what is a protocol's key-rate?

Individual Attacks: The first papers to attempt to answer this question were [21] and [49] which both considered information gain as functions of observed noise assuming *in-dividual attacks*, namely attacks whereby the adversary attacks each qubit identically and, furthermore, is forced to measure her ancilla immediately thus leading to a classical memory.

In [21], the authors introduced a new SQKD protocol which we discussed in an earlier section. Security for their protocol was proven in terms of an individual attack on the reverse channel (an argument was made that attacking the forward channel for their specific protocol under the assumption of individual attacks did not provide her with any additional information). Under this attack, they derived the following expression for the mutual information held between A and E, namely:

$$I(A:E) = 1 - h\left(\frac{1+x}{2}\right),\tag{7}$$

where:

$$x = 2\sqrt{Q_X(1 - Q_X)},\tag{8}$$

and Q_X is the observed X basis error rate in the channel whenever B chooses Reflect. Of course I(A : B) is simply 1 - h(Q) where $h(\cdot)$ is the binary Shannon entropy function and Q is the probability of a Z basis error in the reverse channel (note that the reverse channel is used to carry key material for this particular protocol). A graph of the resulting key rate r = I(A : B) - I(A : E) is shown in Figure 3. Interestingly, the noise tolerance of this protocol in this attack model is 14.6% (when $Q_X = Q$) which is exactly that which BB84 can tolerate against individual attacks [50]. This connection in noise tolerance between semi-quantum and fully-quantum key distribution is something we will comment on again later when looking at stronger security models and shows that, even though semi-quantum protocols are limited in their quantum capabilities, they hold similar security properties to that of fully quantum protocols, at least in ideal qubit channels (practical issues surrounding semi-quantum cryptography remain a large area of open research which we address later in this paper). It would be interesting to investigate SQKD protocols in other attack models where an adversary is limited in their quantum abilities and compare to the fully-quantum counterpart.

Open Problem 3: It has been demonstrated that the noise tolerance of SQKD protocols are comparable, or equal, to that of fully quantum protocols in the individual attack scenario and, as we discuss later, against stronger collective attacks. Does this relation hold for security models that may be weaker than individual attacks? For instance, intercept-resend



Figure 3: Showing the key-rate of the two-state protocol introduced in [21] assuming individual attacks. For the Solid Line, we consider $Q_X = Q$; for the Dashed Line, we consider $Q_X = 2Q(1-Q)$.

attacks (where E must measure in a particular basis and forward a result - i.e., she cannot probe the qubit sent any other way).

In [49], an analysis of Zou's single state protocol (introduced in [15]) was performed also assuming individual attacks. There, the mutual information between A and E was found to be:

$$I(A:E) \le 2\sqrt{Q_X + 6Q^{1/4}}.$$
 (9)

This is the first upper-bound on the mutual information for the single-state SQKD protocol, at least for individual attacks. It also hints at robustness as, when $Q_X = Q = 0$, then I(A : E) = 0; that is, when there is no noise, E cannot extract information. Of course, robustness should not assume that E measures her ancilla which is an assumption made when handling individual attacks. Note that this result is only an upper-bound and, as shown in Figure 4, is very pessimistic as E's information gain is potentially very large even for small disturbances. More optimistic bounds for this protocol have since been shown also assuming a stronger attack model as we discuss later. However, the paper [49] was one of the first to actually derive a connection between noise and information gain for a semi-quantum protocol and remains an important work.

Restricted Attacks:

One of the challenges with proving security of an SQKD protocol, either in terms of robustness, or some other security model, is that the adversary is allowed two opportunities to attack the qubit as it travels. However, there are currently two techniques for reducing this complexity.

We consider, now, collective attacks where E attacks the forward channel with an operator U_F and the reverse with an operator U_R . Both of these are unitary and act on the two dimensional qubit space and E's private ancilla (of arbitrary dimension). This can be used to prove robustness in Zou's model [15] or for an information theoretic analysis of noise tolerance against collective attacks which we discuss next.



Figure 4: Showing the *upper bound* on the mutual information held between A and E as derived in [49] for Zou's single-state protocol introduced originally in [15]. This assumes E is restricted to individual attacks. New work has since determined more optimistic bounds, but this original result remains important as one of the first to derive a relation between disturbance and information gain for an SQKD protocol.

First, it was shown in [16] that for any *single-state* SQKD protocol using only the Measure and Resend and Reflect operations, the forward attack operator does not need to entangle the traveling qubit with E's quantum ancilla. Instead, it is sufficient to bias the state's probability amplitudes. However, beyond this, the attack does not provide E with any additional information. Note this result is not true if B is allowed to use an operation beyond Measure and Resend or Reflect. Of course it is also not true if B is more powerful than semi-quantum.

More formally, as proven in [16], to prove security against collective attacks, or robustness in Zou et al.'s model, it suffices to consider an attack whereby E sends to B a qubit state:

$$\left|\psi\right\rangle = \sqrt{\frac{1}{2} + b} \left|0\right\rangle + \sqrt{\frac{1}{2} - b} \left|1\right\rangle,\tag{10}$$

for some real bias parameter $b \in [-1/2, 1/2]$. Any arbitrary collective attack of the form (U_F, U_R) can be "reduced" to this *restricted collective attack* without loss of advantage to an all-powerful adversary. This allows for simplified security analyses as one must only consider the forward channel bias and not any entanglement with an adversarial system. In fact, one may even enforce a symmetry to E's attack in that, if A was supposed to send a $|+\rangle$ state, B can enforce that b = 0 and abort otherwise (such a symmetry assumption is often made in S(QKD) security proofs). Regardless, however, it is clear that this value b is an observable parameter that may be used in any security proof.

This restricted attack definition was recently extended to arbitrary *multi-state* SQKD protocols in [51]. For multi-state protocols, E need only apply a restricted forward attack

operator \mathcal{F} which acts as follows:

$$\begin{split} \mathcal{F} \left| 0 \right\rangle_T \otimes \left| \chi \right\rangle_E &= q_0 \left| 0, 0 \right\rangle_{TE} + \sqrt{1 - q_0^2} \left| 1, e \right\rangle_{TE} \\ \mathcal{F} \left| 1 \right\rangle_T \otimes \left| \chi \right\rangle_E &= q_2 \left| 1, f \right\rangle_{TE} + \sqrt{1 - q_2^2} \left| 1, 0 \right\rangle_{TE}. \end{split}$$

where, q_i are positive real numbers no greater than one and, furthermore, one may assume that:

$$\begin{split} |e\rangle_{E} &= \eta_{0} |0\rangle_{E} + \sqrt{1 - |\eta_{0}|^{2}} |1\rangle_{E} \\ |f\rangle_{E} &= \eta_{1} |0\rangle_{E} + \sqrt{1 - |\eta_{1}|^{2}} |1\rangle_{E} \end{split}$$

where η_0 and η_1 are complex numbers such that $|\eta_i| \leq 1$. Note that, unlike the single-state case, for a multi-state protocol one must consider E entangling the qubit with her quantum ancilla in the forward channel. However, the dimension of E's memory need only be two dimensional. Furthermore, rather interestingly, the state of her ancilla is essentially a "right" or "wrong" state - namely it is $|0\rangle_E$ when \mathcal{F} does not flip the input while it is one of the $|e\rangle$ or $|f\rangle$ otherwise. Such simplified attacks can help to perform a security analysis of any SQKD protocol which relies on operations Measure and Resend and Reflect. For singlestate protocols, one should use the restricted bias-only version [16]; for others, one must use the alternative definition for multi state protocols from [51].

Open Problem 4: Do equivalent restricted attacks exist for protocols where B uses **Permute**? Proofs of equivalency from [16, 51] normally employ the following strategy: Fix an attack against the protocol. Work out the density operator describing the protocol when the particle(s) return to Eve for the second time. Next, show that, if a restricted attack were used, the returning state can be "fixed" via a unitary operator so that it is equal to the general case. If this is possible, there is no advantage to E using a full attack, she might as well use the simplified attack. Note that one must also be careful to ensure that A and Bcannot tell the difference (e.g., the two attacks should induce the same observable statistics in both cases). Can a definition of restricted attack for the **Permute**, or other semi-quantum, operations be defined and proven?

Key Rate Computations:

Moving beyond robustness, it is important to understand how a protocol behaves when faced with noise. In detail, one wishes to derive an information theoretic bound on the keyrate of a protocol (see Equation 5) as a function only of observable parameters. This allows for the better understanding of a protocol's performance (e.g., its noise tolerance) and also allows us to better compare semi-quantum protocols with fully-quantum ones. Since one of the main theoretical goals of the semi-quantum model of cryptography is to better map out the "gap" between fully quantum and partially quantum protocols, having a rigorous way to gauge relative performance of two protocols is vital. Key-rate under certain noise conditions makes for an excellent measure to compare.

The first information theoretic analysis of an SQKD protocol was in 2015 in [52] with several other protocols analyzed since then. Assuming collective attacks in the asymptotic scenario, doing so ultimately requires bounding the entropy term S(A|E), where ρ_{AE} is a density operator describing a single iteration of the protocol conditioning on that iteration being used for raw-key distillation. In general, there seem to be three main methods currently for deriving key-rate computations for SQKD protocols:

- 1. Compute a lower bound on S(A|E) based on strong subadditivity.
- 2. For single state-protocols, use biased-restricted attacks to argue that when the bias is 0 (see Equation 10), the SQKD protocol is equivalent to a known one-way protocol for which the entropy is known; next, argue using the continuity of von Neumann entropy [53, 54, 55], that as the bias changes, the entropy cannot differ "too much." Thus the key-rate cannot decrease "too much" based on b.
- 3. Reduce the protocol to an equivalent one-way entanglement based protocol (shown in [51, 39] to be possible at least for *some* SQKD protocols) and use entropic uncertainty relations [56, 57, 58, 59].

First Key-Rate Proof Method: Perhaps the most generally applicable approach is to compute S(A|E) directly and this seems to be the approach used for the majority of SQKD key-rate computations. First used in [52] but improved in [60], one must begin by writing out a density operator description of a single iteration of the protocol assuming that iteration is used to distill a raw key bit. Namely, one must condition on events leading to a raw-key iteration. Taking into account also E's attack (one may take advantage, here, of the restricted attack results for single-state [16] or multi-state [51] protocols as discussed earlier) this results in a classical-classical-quantum state (ccq-state) of the form:

$$\rho_{ABE} = \frac{1}{N} \sum_{i,j \in \{0,1\}} |i,j\rangle \langle i,j|_{AB} \otimes \rho_E^{(i,j)},\tag{11}$$

where $\rho_E^{(i,j)}$ is a density operator modeling E's attack in the event A's raw key bit happens to be *i* and B's raw key bit is *j* and where N is a normalization term.

The operators $\rho_E^{(i,j)}$ can always be written as a sum of the form:

$$\rho_E^{(i,j)} = \sum_k |E_k^{(i,j)}\rangle \left\langle E_k^{(i,j)} \right|,$$

where $|E_k^{(i,j)}\rangle$ are vectors (possibly sub normalized if the above sum has more than one element) in E's ancilla. The fact that one may write the operators $\rho_E^{(i,j)}$ in this form is a basic fact of linear algebra. However, the exact structure of these operators usually is found through the derivation of ρ_{ABE} and so, generally, no additional work is needed to decompose the operators in this structure (after tracing the protocol to derive ρ_{ABE}).

In [60] a general theorem was derived allowing one to compute the conditional entropy of a state shown in Equation 11:

Theorem 1. (From [60]): Let ρ_{AE} be a state of the form:

$$\rho_{AE} = \frac{1}{N} |0\rangle \langle 0|_A \otimes \left(\sum_{k=0}^M |E_k^{(0)}\rangle \langle E_k^{(0)}| \right) + \frac{1}{N} |1\rangle \langle 1|_A \otimes \left(\sum_{k=0}^M |E_k^{(1)}\rangle \langle E_k^{(1)}| \right)$$
(12)

and denote by N_k^i to mean $N_k^i = \langle E_k^{(i)} | E_k^{(i)} \rangle$. Then it holds that:

$$S(A|E) \ge \sum_{k=1}^{M} \left(\frac{N_k^0 + N_k^1}{N}\right) S_k,\tag{13}$$

where:

$$S_{k} = \begin{cases} h\left(\frac{N_{k}^{0}}{N_{k}^{0} + N_{k}^{1}}\right) - h(\lambda_{k}) & \text{if both } N_{k}^{0} > 0 \text{ and } N_{k}^{1} > 0 \\ 0 & \text{otherwise} \end{cases}$$
(14)

and finally:

$$\lambda_k = \frac{1}{2} \left(1 + \frac{\sqrt{(N_k^0 - N_k^1)^2 + 4Re^2 \langle E_k^{(0)} | E_k^{(1)} \rangle}}{N_k^0 + N_k^1} \right).$$
(15)

Note that this theorem is very general and can be applied to any cq-state - either one produced by a SQKD protocol, or one produced by some other protocol, quantum or semiquantum. It states that one may compute the conditional entropy simply by knowing (or bounding) the inner products of states $\langle E_k^{(i)} | E_k^{(i)} \rangle$ (in an SQKD protocol these are typically found by looking at the Z basis noise in the quantum channel) and the overlap between $|E_k^{(0)}\rangle$ and $|E_k^{(1)}\rangle$ (which in an SQKD protocol can usually be bounded by looking at the X basis noise in the case when B chooses Reflect).

We make three comments on the above theorem. First, one may always write a density operator ρ_{AE} in the form shown in Equation 12. This is due to the fact that the theorem allows some $|E_k^{(j)}\rangle$ to be zero vectors and so the total number of terms in the 0 and 1 case may both be M.

Secondly, the ordering of the terms appearing in the E portion of the density operators in Equation 12 is irrelevant. Indeed, one may apply any permutation $\pi : \{1, \dots, M\} \rightarrow \{1, \dots, M\}$ and consider the (equivalent) density operator:

$$\rho_{AE} = \frac{1}{N} |0\rangle \langle 0|_A \otimes \left(\sum_{k=0}^M |E_k^{(0)}\rangle \langle E_k^{(0)}| \right) + \frac{1}{N} |1\rangle \langle 1|_A \otimes \left(\sum_{k=0}^M |E_{\pi(k)}^{(1)}\rangle \langle E_{\pi(k)}^{(1)}| \right).$$

Theorem 1 will provide a lower-bound on S(A|E) for any such ordering, even though, now, one considered inner-products of the form $Re \langle E_k^{(0)} | E_{\pi(k)}^{(1)} \rangle$. For all permutations, all lowerbounds are correct bounds on the entropy in the state ρ_{AE} . Thus, when applying this theorem to key-rate computations, one must arrange the terms strategically to get the most optimistic lower-bound. In general, the "rule of thumb" appearing in most SQKD papers using this result is to arrange vectors so that $|E_k^{(0)}\rangle$ and $|E_k^{(1)}\rangle$ have both similar weights (i.e., N_k^0 is close to or equal to N_k^1) and appear in E's system when similar events occur (e.g., when there is no error in the quantum channel or when there is a double-error). Of course, this is just a guideline - when working with this theorem, it is important to keep in mind that an alternative arrangement of the terms may lead to more optimistic results (but all orderings lead to technically correct lower-bounds on S(A|E)).

Third, and finally, one may actually get a more optimistic bound on S(A|E) by defining λ_k as:

$$\lambda_k = \frac{1}{2} \left(1 + \frac{\sqrt{(N_k^0 - N_k^1)^2 + 4|\langle E_k^{(0)} | E_k^{(1)} \rangle|^2}}{N_k^0 + N_k^1} \right).$$
(16)

That is, instead of using only the real part of $\langle E_k^{(0)} | E_k^{(1)} \rangle$, one should use both real and imaginary to get a tighter bound. This fact is easily seen from the proof of Theorem 1 from [60]. Though, in key-rate proofs, it is often easier to determine a bound on only the real part, thus the original statement, using only the real part, has, so far, been more useful.

To demonstrate its application, we consider the original Boyer et al., protocol [7], BKM07. The following proof is from [60], we highlight the main details here. Consider a particular collective attack as a pair of unitary operators U_F applied in the forward channel and U_R applied in the reverse. Since we are considering collective attacks, we may assume E's ancilla is initially cleared to some default state $|\chi\rangle_E$. Then, without loss of generality, we may write the action of E's attack operators as follows:

$$U_F |0, \chi\rangle_{TE} = |0, e_0\rangle + |1, e_1\rangle$$

$$U_F |1, \chi\rangle_{TE} = |0, e_2\rangle + |1, e_3\rangle$$
(17)

$$U_R |i, e_j\rangle_{TE} = |0, e_{i,j}^0\rangle + |1, e_{i,j}^1\rangle.$$

where the various $|e_i\rangle$ and $|e_{i,j}^k\rangle$ states are arbitrary states which are not necessarily normalized nor orthogonal in E's ancilla.

Now, one must construct the ccq-state ρ_{ABE} . Full details can be found in [52, 60], however, tracing the protocol's execution, including E's attack, and conditioning on the iteration being used for key-distillation (thus, one need only consider A sending a Z basis state, B choosing Measure and Resend and A measuring again in the Z basis), one finds the following operator:

$$\rho_{ABE} = \frac{1}{2} |00\rangle \langle 00|_{AB} \otimes \left(|e_{0,0}^{0}\rangle \langle e_{0,0}^{0}| + |e_{0,2}^{0}\rangle \langle e_{0,2}^{0}| \right)$$

$$+ \frac{1}{2} |11\rangle \langle 11|_{AB} \otimes \left(|e_{1,3}^{1}\rangle \langle e_{1,3}^{1}| + |e_{1,1}^{1}\rangle \langle e_{1,1}^{1}| \right)$$

$$+ \frac{1}{2} |01\rangle \langle 01|_{AB} \otimes \left(|e_{1,3}^{0}\rangle \langle e_{1,3}^{0}| + |e_{1,1}^{0}\rangle \langle e_{1,1}^{0}| \right)$$

$$+ \frac{1}{2} |10\rangle \langle 10|_{AB} \otimes \left(|e_{0,0}^{1}\rangle \langle e_{1,0}^{1}| + |e_{0,2}^{1}\rangle \langle e_{0,2}^{1}| \right) .$$
(18)

Tracing out B yields:

$$\rho_{AE} = \frac{1}{2} |0\rangle \langle 0|_A \otimes \left(|e^0_{0,0}\rangle \langle e^0_{0,0}| + |e^0_{0,2}\rangle \langle e^0_{0,2}| + |e^0_{1,3}\rangle \langle e^0_{1,3}| + |e^0_{1,1}\rangle \langle e^0_{1,1}| \right)$$

$$+ \frac{1}{2} |1\rangle \langle 1|_A \otimes \left(|e^1_{1,3}\rangle \langle e^1_{1,3}| + |e^1_{1,1}\rangle \langle e^1_{1,1}| + |e^1_{0,0}\rangle \langle e^0_{0,0}| + |e^1_{0,2}\rangle \langle e^1_{0,2}| \right).$$

$$(19)$$

Note that the structure of this state is already in the form of Equation 12 needed to apply Theorem 1. The states have been paired according to the general rule as mentioned earlier; indeed, note that $\langle e_{0,0}^0 | e_{0,0}^0 \rangle$ and $\langle e_{1,3}^1 | e_{1,3}^1 \rangle$ are the highest weighted vectors since they appear when there is no Z basis noise in the forward and reverse channel. The inner products $\langle e_{i,j}^k | e_{i,j}^k \rangle$ (needed to compute the resulting lower bound from the theorem) can all be computed by observing the Z basis noise in the channel. If Q is the observed Z basis noise in the forward and reverse channel, one finds [60]:

$$\begin{split} \langle e^0_{0,0} | e^0_{0,0} \rangle &= \langle e^1_{1,3} | e^1_{1,3} \rangle = (1-Q)^2 \\ \langle e^0_{0,2} | e^0_{0,2} \rangle &= \langle e^1_{1,1} | e^1_{1,1} \rangle = Q(1-Q) \\ \langle e^1_{0,0} | e^1_{0,0} \rangle &= \langle e^0_{1,3} | e^0_{1,3} \rangle = Q(1-Q) \\ \langle e^0_{1,1} | e^0_{1,1} \rangle &= \langle e^1_{0,2} | e^1_{0,2} \rangle = Q^2. \end{split}$$

The above are all found simply by tracing the evolution of the qubit and using Equation 17. To finish the computation, one requires also bounds on the inner-products $E_1 = Re \langle e_{0,0}^0 | e_{1,3}^1 \rangle$, $E_2 = Re \langle e_{1,1}^1 | e_{0,2}^0 \rangle$, $E_3 = Re \langle e_{0,0}^1 | e_{1,3}^0 \rangle$ and $E_4 = Re \langle e_{1,1}^0 | e_{0,2}^1 \rangle$. These are more involved - for complete details see [60]. However if one assumes a symmetric channel, the final entropy expression simplifies to:

$$S(A|E) \ge (1-Q)^2 [1-h(\lambda_1)] + Q(1-Q)[1-h(\lambda_2)]$$

$$+ Q(1-Q)[1-h(\lambda_3)] + Q^2 [1-h(\lambda_4)],$$
(20)

where:

$$\lambda_{1} = \frac{1}{2} \left(1 + \frac{|E_{1}|}{(1-Q)^{2}} \right) \qquad \lambda_{4} = \frac{1}{2} \left(1 + \frac{|E_{4}|}{Q^{2}} \right)$$
$$\lambda_{2} = \frac{1}{2} \left(1 + \frac{|E_{2}|}{Q(1-Q)} \right) \qquad \lambda_{3} = \frac{1}{2} \left(1 + \frac{|E_{3}|}{Q(1-Q)} \right).$$

Finally, it can be shown that $E_1 = 1 - 2Q_X - E_2 - E_3 - E_4$, where Q_X is the observed X basis noise whenever B chooses **Reflect** and A measures in the X basis (having sent an X basis state initially). To compute S(A|E), therefore, one must minimize over all E_2 , E_3 , and E_4 subject to the constraints $|E_2|, |E_3| \leq Q(1-Q)$ and $|E_4| \leq Q^2$ (these bounds were derived from the Cauchy-Schwarz inequality). For complete details on this proof method, the reader is referred to [60]. Computing H(A|B), necessary to finish the key-rate bound, is trivial given the observed error rates in the raw key (in this case, it is H(A|B) = h(Q)).

A plot of the resulting key-rate is shown in Figure 5. Generally, when evaluating keyrates for protocols relying on a two-way quantum channel (fully quantum or otherwise), one



Figure 5: Showing an evaluation of the key-rate of the BKM07 protocol as derived in [60], namely Equation 20. We consider both dependent (Solid Line, when $Q_X = Q$) and independent (Dashed Line, when $Q_X = 2Q(1-Q)$) channels - see text for explanation.

often considers independent channels and dependent channels [61, 60]. For the first, it is assumed that the observed X basis noise in the entire joint forward-reverse channel (when B chooses Reflect) is 2Q(1-Q); for the dependent channel, the observed X basis noise is simply Q, the error in each channel individually. Note that certain fiber channels can exhibit this dependent case [61, 62]. Of course, these two assumptions are not necessary for security - instead they are just used to evaluate the key-rate and determine noise tolerances. Since these are commonly used, they also provide good comparison cases.

Evaluating the key-rate expression (Figure 5), one notes that the noise tolerance for a dependent channel is 11% exactly that of BB84 [3, 5, 6]. For an independent channel, where the X basis noise is roughly twice as high, the noise tolerance drops to 7.9%. However, for a similar X basis noise, this is also the noise tolerance of BB84. In fact, the key-rate equation shown in Equation 20 numerically agrees with BB84 on these two channels. This demonstrates that the semi-quantum model, at least from a theoretical perspective, can attain just as high noise tolerances and similar security properties to that of fully quantum protocols!

In general, Theorem 1 allows one to derive a bound on the key-rate expression allowing for fine-grained control over the result through the use of numerous statistics. This method has been used, now, for several other SQKD protocols beyond BKM07. Compared with the other methods for proving SQKD security, this has, so far, given the most optimistic results. However, this method can also result in cumbersome expressions and, for certain protocols, more direct and efficient proof methods are available which we discuss next.

Second Key-Rate Proof Method: When working with a single state protocol, as mentioned, it is sufficient to consider E's forward channel attack as simply biasing B's measurement result. This opens up an alternative proof strategy consisting of the following three steps [63]:

1. First, consider E's bias to be 0 (see Equation 10). In this case, E is actually performing the identity operator on the forward channel and, so, the protocol reduces to a one-way protocol consisting of three states. Namely, the protocol reduces to a protocol where B

(who is no longer classical) prepares $|\psi_0\rangle$ or $|0\rangle$ or $|1\rangle$. Eve attacks the reverse channel normally through a unitary probe, and A performs her operations as dictated by the original protocol. Since this is essentially a one-way protocol (as E is not attacking the forward channel when the bias is 0), its security analysis may be potentially easier (or, even, already completed in past work since, often, the protocol reduces to one that is mathematically equivalent to a known one-way QKD protocol) thus giving a bound on $S(A|E)_{\rho_0}$ in this case.

2. Next, consider a fixed reverse attack probe but now alter the bias parameter b. Let ρ_b be the resulting density operator for a bias value of b (where this b is the actual observed bias in the operation of the protocol). We need to compute $S(A|E)_{\rho_b}$, the conditional entropy for the actual attack we observe. Since we know, from the first step, the value of $S(A|E)_{\rho_0}$ (i.e., when there is no bias), we may compute $S(A|E)_{\rho_b}$ using the continuity of von Neumann entropy [53, 54, 55]. Indeed, using a continuity bound in [55], we may write (since dim $\mathcal{H}_A = 2$):

$$S(A|E)_{\rho_b} \ge S(A|E)_{\rho_0} - \delta - (1+\delta)h\left(\frac{\delta}{1+\delta}\right),\tag{21}$$

where:

$$\delta = \frac{1}{2} ||\rho_b - \rho_0||. \tag{22}$$

Thus, the goal of this second step, is to compute a bound on δ as a function only on observed noise parameters, including the observed bias b. Of course when b = 0, we obtain $S(A|E)_{\rho_b} = S(A|E)_{\rho_0}$ as expected. As the bias increases (e.g., as E's forward channel attack becomes stronger), δ increases, thus causing $S(A|E)_{\rho_b}$ (the actual conditional entropy of the protocol operation) to decease, thus causing the keyrate to also decrease.

3. Finally, the two steps are combined, however care must be taken in that, on step (1), the entropy $S(A|E)_{\rho_0}$ was bounded as a function of the observed noise - however on the one hand, the observed X basis noise (when B chooses Reflect) is a function now of both forwards and reverse attacks, whereas the entropy bound from step (1) assumes it is only in the reverse channel. That is, E's attack in the reverse may actually emit more X basis noise by itself (when b = 0) then the actual observed noise. Therefore, to complete the proof, given Q_X , the observed X basis noise and given the bias b, determine a bound on \tilde{Q}_X , the noise produced only in the reverse channel by the unitary probe.

Ultimately, the above method leads to simpler security proofs. Step (1) is often achieved by recognizing that the protocol, when the bias is set to zero, reduces to a well known protocol such as the Three State BB84 [17, 18] (as is the case of the Zou et al., protocol [15]) or the Extended B92 protocol [19] (as is the case of the Reflection-Based protocol introduced in [16]). However, the use of a continuity bound gives a worst-case result. Indeed, the first method has, so far, always led to more optimistic results (all results have been lower-bounds, so there is no contradiction). The first method also allows for finer-grained control of the result. Indeed, as shown in [64], the bias can positively and negatively affect E's uncertainty (as expected) - however this observation is not possible when using the second method as any bias automatically leads to a decrease in uncertainty (as δ increases); i.e., it leads to a worst-case bound.

Third Key-Rate Proof Method: Finally, the third method of proof involves reducing the SQKD protocol to a one-way, fully quantum protocol and then analyzing that protocol directly. It was proven in [51] that the BKM07 protocol can be reduced to an equivalent one-way protocol (where, now, both parties are actually fully quantum) of the following form:

Protocol: Equivalent One-Way Protocol for BKM07 [51]

- 1. *B*, who is now a fully quantum user, prepares either the state $\frac{1}{\sqrt{2}}(|00\rangle_{A_1A_2} + |11\rangle_{A_1A_2}) \otimes |0\rangle_B$ or the state $\frac{1}{\sqrt{2}}(|000\rangle_{A_1A_2B} + |111\rangle_{A_1A_2B})$, choosing randomly each iteration (with the same probability that he normally would have chosen **Reflect** or **Measure and Resend** respectively in the original SQKD protocol). He then sends the A_1A_2 qubits to Alice (*E* is allowed to attack both qubits simultaneously).
- 2. A measures both the A_1 and A_2 qubits in either the Z basis or the X basis, choosing randomly.
- 3. A discloses her choice of basis and B his choice of state preparation. If B choose to prepare the GHZ state $\frac{1}{\sqrt{2}}(|000\rangle_{A_1A_2B}+|111\rangle_{A_1A_2B})$, and if A chose to measure in the Z basis, this iteration may be used for raw key distillation (they should share a correlated bit). Otherwise, the iteration may be used for error estimation.

The proof that security of this one-way fully quantum protocol implies security of the original BKM07 protocol can be found in [51]. A similar reduction was recently proven for a higher dimensional SQKD protocol in [39]. It is currently an open problem as to which families of SQKD protocols have a similar reduction.

Open Problem 5: Do all SQKD protocols have an equivalent one-way protocol that they may be reduced to?

Regardless, once reduced, the one-way protocol may be analyzed through standard techniques, for instance using entropic uncertainty relations [57, 58, 59]. This then may be translated to a key-rate bound for the semi-quantum protocol. As with the second method, this leads to a clear and concise security bound, but it does not give as optimistic a result as the first method (due, perhaps, in part to the fact that the one-way protocol affords E more attack opportunities than in the actual two-way SQKD protocol, thus causing a less than optimistic bound on security to the adversary's advantage). Indeed, while the first method described earlier can show that BKM07 can suffer 11% noise tolerance [60], this third method shows only 6.14% [51]. However, that is not an entirely fair comparison: the first method relied on the collection of numerous mismatched measurements (thus allowing for a tighter bound on the entropy) whereas the third method did not use any mismatched measurements - only the error rate. It is unclear if mismatched measurements are necessary to attain this high noise tolerance and, perhaps, the 6.14% as determined by this third method is actually tight for this protocol without these statistics.

Mismatched Measurements:

As discussed, three methods of computing the key-rate of an SQKD protocol have so far been developed. The first method, direct computation of S(A|E), combined with *mismatched measurements* have so far given the most optimistic results. Mismatched measurements are a technique originally introduced in 1993 by Barnett et al., in [65] for fully-quantum protocols. Later the technique became more refined in [66, 67, 68] showing that substantial improvements in noise tolerance and asymptotic efficiency are possible for fully-quantum protocols with restricted resources such as the Three State BB84 [17, 18] or the Extended B92 [19] protocols - indeed for the Three State BB84 protocol, despite A's inability to send the $|-\rangle$ state, noise tolerance can be as high as the standard four-state BB84 as shown in [69, 70].

This technique of using mismatched measurements was extended in [60] to two-way quantum channels and semi-quantum users using two bases and extended in [31] for three bases. Using this method, one may show that the noise tolerance of the BKM07 protocol, assuming E's attack is symmetric (an enforceable assumption), is as high as BB84 as discussed in the previous section. To compute this key-rate requires looking at 18 different measurement statistics as shown in Table 1. Without these statistics, the current best result is based on reducing to a one-way protocol and using an entropic uncertainty bound - using such a method does not require collecting all of these statistics (it only requires looking at error rates) but the (lower-bound bound on) noise tolerance drops to 6.14% [51]. Whether mismatched measurements are necessary for the BKM07 protocol to attain this high noise tolerance is still an open question. Indeed, the 6.14% tolerance from [51] is only a lower bound.

Open Problem 6: Are mismatched statistics necessary for the BKM07 protocol to attain the same noise tolerance as BB84, namely 11%? Or can this tolerance be achieved by looking only at error statistics?

Note that we did not ask the question in regards to *any* semi-quantum protocol. In fact, it was shown in [24, 25] that for some SQKD protocols (specifically the two developed in those references), mismatched measurements are necessary to attain any level of security. That is, *without mismatched measurements, there are semi-quantum protocols that are completely insecure.* This seems to suggest that mismatched measurements may be necessary for all SQKD protocols (either to show any form of security or, in the case of BKM07, to improve security bounds) though an exact proof of this is elusive. It is interesting to note, however, that by dropping the resource requirements of users (namely, when moving from the fully quantum to the semi-quantum setting), one can use additional classical post processing (e.g., mismatched measurements), to compensate. This seems to suggest the semi-quantum model of communication can shed light on interesting fundamental connections between classical

Error Statistics	$\begin{array}{c} p^{A \rightarrow B}_{i,1-i} \\ p^{A \rightarrow A}_{i,j,1-j} \\ p^{A \rightarrow A}_{i,R,1-i} \\ p^{A \rightarrow A}_{\pm,R,\mp} \end{array}$	Forward channel Z basis noise Reverse channel Z basis noise Z basis noise when B chooses Reflect X basis noise when B chooses Reflect
Mismatched Statistics	$\begin{array}{c} p^{A \rightarrow B}_{+,i} \\ p^{A \rightarrow A}_{i,j,+} \\ p^{A \rightarrow A}_{+,R,0} \\ p^{A \rightarrow A}_{i,R,+} \end{array}$	Forward channel $X \to Z$ statistic. Reverse channel $Z \to X$ statistic. Loop channel $X \to Z$ statistic Loop channel $Z \to X$ statistic

Table 1: Showing all observable statistics used in the key-rate computation for the BKM07 protocol in [60]. Here, $i, j \in \{0, 1\}$ and we use $p_{i,j}^{A \to B}$ to denote the probability that B observes $|j\rangle$ given that A initially sent $|i\rangle$ and B chooses Measure and Resend; $p_{i,j,k}^{A \to A}$ is the probability that A observes $|k\rangle$ (for $k \in \{0, 1, +, -\}$) conditioned on A initially sending $|i\rangle$, B choosing Measure and Resend and actually observing $|j\rangle$, and finally A choosing to measure in the correct basis to observe $|k\rangle$; finally $p_{i,R,k}^{A \to A}$ is similar, but now conditioning on B choosing Reflect. In [31], this was extended to allow the quantum user to choose from three bases, Z, X, or Y; while this increases noise tolerance, it also roughly doubles the number of statistics needed for mismatched measurements. Note that by "Loop channel" above, we mean the joint channel when B chooses Reflect.

Original Protocol	Noise	Proof	Comments
	Tolerance	Reference	
BKM07 [7]	11%	[60]	
Single State by Zou et al., [15]	9.65%	[71]	
Reflection-Based [16]	5.36%	[64]	
Semi-Quantum B92 [20]	3.46%	[20]	
Single-A-Measurement [24]	11%	[24]	MM Required
Classical-to-Quantum [25]	< 1%	[25]	MM Required; Noise
			tolerance depends on
			distance from classical.
High-Noise-SQKD M2 [31]	16.4%	[31]	
High-Noise-SQKD M3 [31]	26%	[31]	
High-Dimensional SQKD [39]	30%	[39]	Noise tolerance increases
			to 30% as dimension
			approaches infinity

Table 2: Showing state of the art best noise tolerances for those SQKD protocols which have this analysis performed. "MM Required" means that mismatched measurements are required for the protocol to be secure at all (i.e., the protocol is completely insecure without them); note that mismatched measurements may be used in the above results for other protocols besides those specifically marked as such, but it is not required for security - see text for discussion.

and quantum information processing.

Overall, as of writing this, several SQKD protocols have a key-rate analysis lower-bound thus giving us a lower-bound on the protocol's noise tolerance. A summary of the current best case noise tolerances are shown in Table 2. Noise tolerances are reported here based on the Z basis error in the forward and reverse channel, denoted here as Q (we also assume $Q_X = Q$). In particular, the value reported is the maximal Q for which the resulting key-rate r is positive. Note that many key-rate proofs for SQKD protocols support different noise scenarios, including different Z basis noise rates in the forward and reverse channels; we only report the symmetric case here for simplicity in presentation. Where appropriate we also assume depolarization channel noise. Complete details for alternative scenarios, if available, can be found in the original reference for the proof of security provided in the table.

4 Multi-User SQKD

While the vast effort in SQKD research (i.e., research specific to key distribution in the semiquantum model) is in trying to discover, and prove secure, novel protocols requiring fewer resources on the part of the users, other directions have also seen great interest. Perhaps the most fruitful as of writing this is the development of multi-user protocols. Multi-user protocols within the semi-quantum realm come in two flavors: first is trusted quantum user



Figure 6: Based on an image in [74] showing the assumed network topology for their protocol in that reference. Each B_i and A_i is a classical user while T is a fully quantum user.

(where this quantum user is trusted and, generally, shares the secret key) and the second is the mediated model (where the quantum user is adversarial and should not share the key).

The first multi-user SQKD protocols were introduced independently in [21] and [72]. The network topology assumed by their protocols is circular in that users communicate in sequence. Here, one fully quantum user, who is trusted and is one of the key-holders, transmits quantum resources to the first classical user B_1 . This user then can perform some semi-quantum operation (e.g., Measure and Resend or Reflect), forwarding a qubit to the next classical user B_2 . This repeats for the next user and so on until B_n at which point the qubit returns to the quantum user who is free to measure in any basis. After the protocol, all B_i 's transmit their choice of operation and A will transmit her basis choice. It is assumed this broadcast communication is done in an authenticated manner, though the classical communication mechanism required for this to operate successfully is not discussed. In general, whenever two B's choose Measure and Resend those users share a key bit. Key bits are shared with the quantum user A whenever a B_i chooses Measure and Resend and the quantum A chooses to measure in the Z basis. Thus, these protocols permit different subgroups of users to share different keys.

Other multi-user protocols in the semi quantum model have also been proposed. In [73] a protocol based on a trusted server preparing GHZ states was described and security analyzed with regards to certain attacks including some attacks based on an adversarial server. One of the main limitations to previous multi-user protocols is that, for m users to agree on a key, all m have to choose the "correct" options for that event to happen (e.g., all classical users must choose Measure and Resend in the protocol of [72]). To improve efficiency, a new multi-user protocol was proposed in [74] which uses *cluster states* [75] and an alternative network topology shown in Figure 6. Their protocol allowed for a roughly quadratic speedup in efficiency over previous work. Also provided in [74] was an information theoretic analysis of the key-rate showing a maximal noise tolerance of 2.82%.

Beyond multi-user protocols where M users all wish to agree on a key, an alternative model involving multiple users is the *mediated semi-quantum* model. This model was first introduced in 2015 in [76] and it involves a fully quantum server and two "classical" users A and B. These two users wish to agree on a secret key known only to them and *not* the server. Furthermore, they do not trust the server who may even be adversarial. Two forms



Figure 7: Based on an image in [76] showing the structure of a mediated SQKD protocol. Here a central, fully quantum, server C (which may be adversarial) prepares and measures quantum states. A and B are classical users. An authenticated classical channel connects the two users while a standard (unauthenticated) classical channel connects the server to each user.

of adversarial models were considered: first a semi-honest server who follows the protocol but may attempt to learn additional information later; alternatively a stronger fully adversarial model is also considered. A general scenario of this framework is shown in Figure 7. The original mediated protocol consisted of the following steps:

Protocol: Mediated SQKD [76]

- 1. The server prepares a Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, sending one particle to A and the other to B.
- 2. Each user, A and B, choose, independently, to either Measure and Resend or to Reflect.
- 3. When both particles return to the server, the fully quantum server performs a Bell measurement, sending the classical message "-" if and only if the outcome is $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle |11\rangle)$. For any of the other three potential outcomes, the server sends the classical message "+".
- 4. A and B both divulge their choice of operation. If the server sent the message "-" and if both users chose Measure and Resend, they will use their measurement results as their raw key. Note that if both users chose Reflect, the server should always send the message "+" and any other result is counted as an error.

Proof of security in [76] (improved in [77]) assumes an adversarial server may prepare any arbitrary state on step (1) (possibly entangled with its quantum ancilla) and, furthermore, may perform any quantum operation on step (3). Furthermore, there may be third-party adversaries attacking the quantum channel and the classical communication between the server and the users (the classical channel connecting A and B needs to be authenticated, however the classical channel between the users and the server is not authenticated and so

subject to manipulation by an adversary - security is still possible). This shows that even with classical capabilities, users may enforce security of a more powerful quantum server. Furthermore, as shown in [77], the noise tolerance can approach 22.05% if the server is semi-honest or 13.04% if the server is fully adversarial. As shown in [78], if two independent mediators are used by A and B (referred to in that source as the *multi-mediated SQKD model*), noise tolerance can increase to 18.7% if both servers are adversarial but do not collude with each other (compared to 13.04% with only one server).

Several other mediated protocols have since been introduced, mostly with the goal of providing greater efficiency (indeed, the original mediated protocol is very inefficient with many iterations being lost due to incompatible choices or measurement results), or fewer resource requirements on the users or server. In [79], a mediated SQKD protocol was proposed where classical users did not have to measure (assuming perfect qubit channels) but, instead, could choose to **Reflect** or **Permute**. This protocol also had greater efficiency than the original mediated SQKD protocol. The authors of [80] developed a new mediated SQKD protocol where the server needs to only send single photons and perform single photon measurements. Users must choose either Reflect or Measure and Resend. This protocol decreases the quantum complexity of the server, a useful direction to move towards as this mediated model may prove to be a practically beneficial quantum communication infrastructure. Other "lightweight" mediated protocols were presented in [81, 82] designed to help mitigate trojan horse attacks against the classical users. Finally, in [83], a new mediated protocol was designed where users need only to Measure (but not resend; thus users do not need a single photon source for this protocol) or **Reflect**. This protocol, which was also experimentally implemented, shows that the mediated model of SQKD is a practical possibility. We will discuss this protocol in more detail when we turn our attention to practical issues of semi-quantum cryptography.

5 Beyond Key Distribution

The original application of semi-quantum cryptography, much like standard, fully-quantum cryptography, was to solve the key distribution problem. Investigating this makes sense as it is a much celebrated result showing a very clear advantage to quantum communication over classical communication (key distribution using only classical communication, as mentioned in the introduction, requires one to make computational assumptions on the adversary's capabilities). However, the semi-quantum model of communication, involving at least one fully quantum party and one (or more) limited, "classical" parties, can be, and has been, applied to other problems.

5.1 Secret Sharing

Perhaps the first application of semi-quantum communication outside of the key-distribution problem was to the task of *secret sharing* [84, 85]. Secret sharing is a primitive used in numerous other cryptographic protocols and consists of a *dealer* (who has some secret s)

and n other parties. The dealer creates n shares of this secret and sends one share to each party (there are n parties). In its simplest form, it should be that if t or more parties come together with their respective shares, the original secret may be recovered; however if one has strictly less than t shares, the secret cannot be learned. While information theoretic secret sharing is possible using classical communication only, one of the advantages to using quantum protocols is the additional ability to detect eavesdropping [86, 87] or to potentially decrease share size (thus increasing communication efficiency) [88]. Alternatively, quantum protocols must be used if the original secret itself is quantum.

The first semi-quantum secret sharing (SQSS) protocol was developed in 2010 by Qin Li et al., in [89]. Here the dealer, A, is quantum while two parties B and C are both classical. The threshold t is set to 2 (thus both B and C must come together to recover the secret) and the secret itself is classical data. Two protocols were presented, one requiring the **Permute** operation, the other using only **Reflect** and **Measure and Resend**. We present the second here as it is easier to follow:

Protocol: First Semi-Quantum Secret Sharing Protocol [89]

1. A, the fully-quantum dealer who holds the secret s (a bit string), creates N GHZ states, each of the form:

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|+++\rangle + |---\rangle). \tag{23}$$

She sends one particle to B, another to C, and keeps the third private in her own lab.

- 2. When each user receives a qubit, parties choose either to Measure and Resend or to Reflect.
- 3. When the qubits return to A, she stores them and alerts B and C. The two parties then disclose their choice of operation for each qubit.
- 4. For each of the N triplets, and based on B and C's choice, A performs the following operations:
 - Case 1: B = Measure and Resend and C = Measure and Resend. Then A measures her qubit in the Z basis.
 - Case 2: B = Measure and Resend and C = Reflect. Then A performs a Bell measurement with her qubit and C's reflected qubit.
 - Case 3: B = Reflect and C = Measure and Resend. Then A performs a Bell measurement on her qubit and B's qubit.
 - Case 4: B = Reflect and C = Reflect. Then A performs an appropriate three-qubit measurement where one basis state is $\frac{1}{\sqrt{2}}(|++\rangle + |---\rangle)$.

Cases 2, 3, and 4 are used only for error detection (along with a random subset of Case 1 instances). Case 1 produces a bit string k_A for the dealer A of size n < N (the length of n is expected to be N/4 - m bits where m is the size of the random subset used for error detection in the Case 1 instances). The dealer then sends $s \oplus k_A$ to B and C.

The claim for correctness and security is that the string k_A is random and independent of *B* and *C*'s individual information. However, *B* and *C* can only recover k_A by XOR'ing their measurement results. This can be seen by rewriting Equation 23 in the *Z* basis:

$$|\psi_0\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle_A \otimes \frac{|00\rangle_{BC} + |11\rangle_{BC}}{\sqrt{2}} + |1\rangle_A \otimes \frac{|01\rangle_{BC} + |10\rangle_{BC}}{\sqrt{2}} \right).$$

Note that B and C's bits are randomly distributed and that by XOR'ing their results, they recover A's bit.

In [90], a SQSS protocol was proposed which only required the dealer to prepare N copies of the state $\frac{1}{\sqrt{2}}(|+,0\rangle + |-,1\rangle)$, sending one particle to B and the other to C. Both these first papers [89, 90] showed secret sharing is possible with semi-quantum users, however it required the generation of entangled states (e.g., Equation 23) and the protocol only worked with two parties. In [91], both issues were considered and improved on. First, a protocol was proposed for n classical parties, extending the technique of [89]. For this to operate, the dealer must prepare a state of the form:

$$\frac{1}{2^{(n+1)/2}}\left(\left|+\right\rangle^{\otimes n+1}+\left|-\right\rangle^{\otimes n+1}\right).$$

Exact details of the protocol may be found in [91], however, this still requires the generation of a highly entangled state. To mitigate this, the same authors in [91] propose a two-party SQSS protocol where the dealer need only prepare separable states of the form $|+\rangle |+\rangle$, sending one particle to *B* and the other to *C*. For the multiparty case, the dealer must prepare the *n* qubit state $|+\rangle^{\otimes n}$ thus creating a more practical system (though, as pointed out in [91], efficiency of the protocol may be problematic for large *n*).

So far these SQSS protocols shared a secret through the use of a randomly generated pad. That is, before the protocol executed, the dealer had no way to deliberately create shares based on the secret itself. An alternative SQSS protocol was devised in [92] where the actual creation of shares depends on the secret - thus, there was no need for an additional transmission of $s \oplus k_A$ as was required with these other protocols discussed so far. In their protocol, the secret is a single bit $b \in \{0, 1\}$ (though this may be increased simply by running multiple instances of the protocol in sequence). At the start, A prepares N states of the form $\frac{1}{\sqrt{2}}(|+++\rangle + (-1)^b |---\rangle)$ (thus N quantum states are required for a secret of one bit). One particle is sent to B, another to C, and a third is kept private. At the end, the secret bit can only be recovered if all three users (including the dealer in this protocol) present their final classical shares, distributed during the quantum stage of the protocol. In the same paper, an n party protocol was also developed, though still requiring N quantum states per classical bit of the secret and requiring the generation of entangled states. In [93] an intercept-resend attack was shown against this protocol allowing a participant to recover the message without having to collaborate. While a fix was presented in that paper, it required parties to be fully quantum (in that they should also measure in the X basis). However, an alternative fix was presented in [94] which is semi-quantum.

Numerous other SQSS protocols have been proposed in addition to these. In [95], a new SQSS protocol was proposed using higher-dimensional states that affords greater efficiency. A "circular" SQSS protocol was developed in [96] which only required single particles and removed the need for measurements (though it does require the **Permute** operation). This protocol is "circular" in its network topology, requiring these single particles to travel from the dealer A to B, then to C, and finally return to the fully-quantum A.

An SQSS protocol without the need for measurement was proposed in [97]. A *d*-dimensional protocol was proposed in [98] which also did not require classical users to measure and supported multiple (beyond two) classical users. A secret sharing protocol using *W*-states for encoding (as opposed to Bell states or GHZ states) was developed in [99].

In [100] a new multi-user (i.e., where the number of parties was greater than two) protocol was developed with greater efficiency than prior multi-user versions at the time of its publication; also it was proven in that reference that multi-user SQSS protocols may be converted to SQKD protocols and a construction was given (furthermore, some simulations were performed on the IBM quantum computer). Bell states were used to create an SQSS protocol in [101] (where classical users applied Reflect or Measure and Resend) though a security flaw was found in [102] (no fix was provided leaving this an open question); an alternative SQSS protocol using Bell states was developed in [103] though where classical users need also the Permute operation. An interesting encoding scheme for SQSS was developed in [104] allowing a secret to be shared by A preparing multiple, initially unspecified, entangled states (their protocol also works for more than two classical users); though in [105] an attack was found on this protocol, however possible fixes were also presented. A scalable SQSS protocol was developed in [106] allowing users to be added or removed by the dealer.

One interesting observation is that all current SQSS protocols have the dealer as the fully-quantum user. This makes sense from a practical standpoint (it should be the dealer who has the most capabilities). However, from a theoretical stand-point can one construct other scenarios?

Open Problem 7: Does there exist an SQSS protocol where the dealer is classical? There are two possible variants: first, one of the participants is fully quantum and "helps" by getting the protocol started (e.g., sending quantum resources to the classical dealer). A second is in line with mediated SQKD protocols as discussed earlier: namely, the dealer and all participants are classical, but there is an untrusted quantum server to perform the needed quantum operations. Showing protocols exist for both settings would be an interesting theoretical result; showing a protocol in the mediated case may also be interesting from a practical standpoint as one could envision a future communication infrastructure where untrusted servers help facilitate both key distribution (through mediated SQKD protocols) and other cryptographic protocols (such as secret sharing) performed by classical users.

Finally, does sharing a *quantum* state make sense in the semi-quantum setting? In [107],

the authors proposed a protocol where a quantum state may be shared between classical A and quantum B (the dealer is also quantum and, of course, only the quantum user can recover the secret later). Further research in this may prove interesting.

5.2 Secure Direct Communication

Secure direct communication (SDC) is the task of sending a message directly from A to B, through a quantum channel, without having to first establish a shared secret key (beyond that needed for authentication of classical information). SDC protocol development in the fully-quantum model dates back to the early 2000's and there have been several protocols since with various advantages and disadvantages (see [108, 109, 110, 111, 112] for just a few instances in the fully-quantum setting).

The first semi-quantum SDC protocol was developed in [113] showing that, like with key distribution, the task of SDC is also possible in the semi-quantum model. In their protocol, the sender of the message $m \in \{0,1\}^n$ is the classical user (B) while the receiver is the quantum user (A). Their protocol utilizes a hash function $h : \{0,1\}^n \to \{0,1\}^k$ for some k < n. The protocol operates as follows:

Protocol: First Semi-Quantum SDC Protocol [113]

- 1. A prepares $N \approx 4(n+k)$ qubits, each of which is prepared independently at randomly as one of the four states $|0\rangle$, $|1\rangle$, $|+\rangle$, or $|-\rangle$. She sends these qubits to the classical user B (who is the message sender).
- 2. When B receives the qubits, half are selected randomly for error testing, the other half for message encoding. Those selected for error testing are subjected to a random choice of Reflect or Measure and Resend. When these qubits return to A, B informs her of their indices (he is still, through a delay line, holding on to the other half of the qubits) allowing parties to check for eavesdroppers in the standard way. If this is detected, parties immediately abort.
- 3. Assuming no eavesdropping was detected on the test half, B will choose n + k random qubits from the remaining portion and measure them in the Z basis. He then computes the classical bit string $\hat{M} = M || h(M)$ where || represents bit-string concatenation. Finally, for each measured qubit and for each bit in \hat{M} he will prepare a new Z basis qubit either in the same state he measured if that bit of \hat{M} is 0 or he will prepare the opposite Z basis state if the bit of \hat{M} is 1. All qubits (both those he measured and encoded the message and hash in and those others he is choosing Reflect), are returned to the quantum user (the receiver of the message). Notice that, due to the random choice of qubit preparation, the message, at this point, is encoded using a classical one time pad which only A and B know the key to.
- 4. A receives all qubits and is told from B which are those he encoded his message in and which were reflected. Security is verified on all reflected qubits; for the others, A

measures in the Z basis to receive the classical string $\hat{M}' = M' || H'$ and verifies that H' = h(M') ensuring that an adversary did not tamper with the message.

Note that, in its original form as described above, the protocol was actually shown in [114] to be susceptible to a Double CNOT attack; two potential solutions were presented in that reference, however, such as changing the protocol so that B uses the **Permute** operation before sending any qubits back to the quantum user.

Other semi-quantum SDC protocols have been proposed. While the above protocol from [113] allows a classical user to send a message to a quantum user, the reverse direction, namely sending a message from the quantum user to the classical user, was considered in [115] where a novel protocol was developed allowing for this functionality. A protocol utilizing EPR pairs allowing a classical user to send a message to the quantum user was developed in [116, 117]. Two protocols were proposed in [118] which also used Bell states though claimed higher qubit efficiency.

Another protocol developed in [119] removed the need for an authenticated channel by assuming a pre-shared secret key is first agreed on (though, this key must be linear in the size of the message). A so-called *delay attack* on these authenticated style protocols was discovered in [120] along with a new protocol to counter it (this new protocol also had the added advantage that it required less resource requirements on the part of the classical user). This was further improved in [121, 122] which reduced the required resources on the part of the quantum user also, though added the requirement again of an authenticated classical channel. An authenticated SDC protocol using only single qubits was proposed in [123]. Finally, [124] proposed two new SDC protocols allowing quantum A to send a message to classical B in such a way that both users can verify the authenticity of the message (assuming a pre-shared key was already shared) using quantum error correction codes.

The notion of *Quantum Dialog*, first introduced for fully quantum users in [125, 126], is similar to SDC except that it allows for a message to be transmitted from A to B and a separate message from B to A. This was extended to the semi-quantum domain first in [127] (which also proposed a novel semi-quantum SDC protocol) and an alternative protocol in [128]. A quantum dialog protocol consisting of two classical users and an untrusted server was presented in [129]; their protocol could also tolerate certain noisy channels.

5.3 Other Cryptographic Protocols

While secret sharing and secure direct communication seem to be the two largest avenues of research in semi-quantum cryptography, outside of key distribution, other cryptographic primitives have recently begun to be investigated.

One avenue, similar to key distribution, is quantum key agreement [130, 131, 132]. Here, the goal is to ensure that both A and B contribute to the generated raw key equally and that no one party can bias the result. Protocols achieving this in the semi-quantum case have been proposed in [127, 133, 134, 135].

Private state comparison is a cryptographic primitive where parties A and B each hold some data i_A and i_B respectively (e.g., parties hold two numbers) and they wish to compare their data to determine, for instance, who has the larger number or, in the case of private state comparison, whether they are equal or unequal. However, they wish to do so in a way that does not reveal their data to the other party. This is a particular instance of Secure Multiparty Computation (SMC), an important area of research in cryptography [136, 137]. This task has been extended to the quantum domain through several works [138, 139, 140] (this is hardly an exhaustive list of fully-quantum results - see [141] for a review); of course, Lo [142] proved that the equality function cannot be computed securely even using quantum means. Thus, research in this area often involves the use of a third party or weaker security models. Recently, and relevant to us, this task has been extended to semi-quantum communication.

The first semi-quantum private comparison (SQPC) protocols were developed independently in [143, 144] where the two users A and B were classical but the third-party was fully quantum. A holds classical data M_A and B holds M_B ; parties wish to know if $M_A = M_B$ without A learning M_B or B learning M_A (also, the third party should not learn either M_A or M_B). To give some idea how these protocols operate, we present the main details from the protocol in [143]:

Protocol: SQPC Protocol [143]

- 1. Parties A and B, using the fully quantum third-party, first run a mediated SQKD protocol (such as the one in [76]) to establish a shared secret key which only A and B know, but not the third party. Call this key k_{AB} .
- 2. Next, each party separately establishes a private key with the third party using a standard SQKD protocol (e.g., BKM07). Call these keys k_{AT} (held by A and the third party) and k_{BT} (between B and the third party).
- 3. The quantum third party prepares a sufficient number of Bell states, choosing randomly from all four possibilities. One particle of each pair is sent to A and the other to B. These parties then, independently, choose either to Measure and Resend or to Reflect.
- 4. For each returning Bell state pair, the third party performs a Bell measurement on them. If the result was the same Bell state that was initially prepared, the third party sends the classical message "0" to both parties; if the Bell state observed is different (due to one party choosing Measure and Resend for instance), then the third party sends the message "1."
- 5. A and B disclose their choices and run a suitable error-checking protocol comparing their measurement results and the third party's response on a suitably chosen random subset of states. On all other iterations where both parties choose Measure and Resend, they now share a correlated string K_A and K_B (the third party discloses his initial Bell state preparation allowing B to "flip" the correct bits of K_B so that $K_A = K_B$).

6. A sends the message:

$$C_A = M_A \oplus K_A \oplus K_{AB} \oplus K_{AT}$$

while B sends:

$$C_B = M_B \oplus K_B \oplus K_{AB} \oplus K_{BT}$$

to the third party

7. Finally, the third party computes $C_A \oplus C_B \oplus K_{AT} \oplus K_{BT}$ and announces the result. Note that if this is the zero string then $M_A = M_B$; otherwise $M_A \neq M_B$.

A security analysis and also the effects of noise, was performed on this protocol in [143].

Other SQPC protocols have been proposed. In [145, 146], protocols requiring only single photons were presented. Another protocol in [135] was developed which used a new semiquantum key agreement protocol developed in the same reference. A protocol where the quantum third party was not required to prepare entangled states was developed in [147].

Semi-quantum protocols for identity verification were developed recently in [148, 149]. These protocols allow quantum A and classical B to verify their identities assuming a preshared secret key. In [150], a protocol was developed allowing a classical user to securely query a database entry owned by another classical user. Here, the database owner should not know the query and the user asking should not learn anything else about the database. This protocol required a quantum third party of course.

Finally, a form of measurement device independent protocol was constructed in [151]. Here a quantum A sends qubits to both the third party measurement device and to classical B. In this protocol B is allowed to Reflect (in this case reflecting to the third party measurement device) or discard the qubit, preparing a fresh Z basis state (since B does not measure, he cannot perform Measure and Resend exactly thus he is dropping the qubit from A and preparing a fresh one independent of the state received). The third party measurement device must perform a Bell measurement. Also, an oblivious transfer (OT) protocol was presented in [152] and a quantum signature scheme developed in [153]. More research in device independence, along with alternative cryptographic primitives (such as OT or signatures, perhaps using alternative security models such as bounded storage [154, 155] or noisy storage [156, 157]) for semi-quantum protocols would be highly valuable.

6 Practical Semi-Quantum

While the original motivating factor behind the semi-quantum model of communication is to study the theoretical question "how quantum must a protocol be to gain an advantage over its classical counterpart" [7], as QKD technology matures, it is worth also considering the question: can practical SQKD systems be implemented? Indeed, in the fully-quantum setting (e.g., BB84), companies already exist producing commercial QKD systems and QKD has been used in several real-world applications. Outside of these applications, there continues to be rapid progress in experimental research involving QKD systems. For a general survey of fully-quantum cryptography, the reader is again referred to [11].

When it comes to implementing a semi-quantum protocol, several major challenges quickly arise. First, semi-quantum protocols require a two-way quantum channel. Second, many theoretical protocols require the classical user to Measure and Resend - in practice this would be implemented through a photon detector which absorbs the photon and, so, to "resend" B would need to prepare a fresh photon opening the door to multiple attacks [158, 159, 160]. Third, the act of switching between Measure and Resend and Reflect requires fast, low noise, switching capabilities. Finally, device imperfections need to be considered and finite-key security proofs must be derived.

As it turns out, the first major challenge, the dependence on a two-way quantum channel, may not be as much a hindrance as initially one might think and may, in fact, be advantageous in some scenarios. Indeed, several fully-quantum QKD systems, especially in the continuous variable (CV) model [161, 162, 163, 164, 165, 166, 167], have been proposed and experimentally implemented, using a two-way channel and, furthermore, have shown in some cases to hold an advantage to one-way quantum communication in terms of noise tolerance [161] or efficiency [167]; they are also potentially more secure against source preparation noise [163]. It would be interesting to see if these CV techniques could be applied to the semi-quantum scenario. Of course, for this, the notion of "semi-quantum" must be defined for continuous variables.

Open Problem 8: Can a rigorous definition of continuous variable semi-quantum communication be developed? What kinds of protocols can be discovered in such a setting and what are their advantages, especially with regards to two-way quantum communication?

For the semi-quantum case, it has been shown, at least in the ideal theoretical perfect qubit case, that two-way channels can be used advantageously to promote the noise tolerance of protocols [31]. While this is the perfect qubit scenario, it does show that two-way channels can be advantageous for semi-quantum communication. Furthermore, the techniques there may perhaps be applied to practical SQKD systems.

The second major challenge is perhaps the most critical to overcome. If B prepares fresh qubits after performing a measurement, this opens the system to photon tagging attacks [158] or trojan horse attacks [160]. Thus, for any SQKD protocol to be practical, it would seem that B should never prepare a fresh photon when performing the theoretical Measure and Resend operation. As it turns out three SQKD protocols [168, 169, 83], so far, have been proposed which are able to choose Reflect and Measure and Resend yet, when choosing the latter, do not actually result in a new photon being created.

The first protocol to achieve this is the so-called *mirror protocol* and it was the first SQKD protocol designed with practical implementation issues in mind [168]. To describe the protocol, we require the use of the Fock basis, where, briefly, we write $|i, j\rangle$ to mean a state consisting of *i* photons in the $|0\rangle$ state and *j* photons in the $|1\rangle$ state (physically, these may be polarization, time-bin, spatial encoding, or some other encoding as needed by the protocol). We write $|i, j\rangle_X$ to mean a similar thing but now in the X basis. *B*'s allowed operations were then refined to allow the classical user to only measure $|0\rangle$ states, ignoring $|1\rangle$ states; only measure $|1\rangle$ states, ignoring $|0\rangle$ states; or measure both $|0\rangle$ and $|1\rangle$ states. However he does not need to "prepare" or "resend" a photon which is critical for

practical SQKD security. This operation can be done in a classical manner through the use of time-bin encoding. For instance, to observe only photons in the $|0\rangle$ state, *B* needs to be able to detect photons in time bin t_0 while reflecting the photons in time bin t_1 (the $|1\rangle$) states. This requires the use of a controllable mirror (hence the name "mirror protocol"). The protocol, which is a single-state protocol, operates as follows:

Protocol: Mirror Protocol [168]

- 1. Fully-quantum A sends a single photon in the $|+\rangle$ state which, in Fock notation, is $|1,0\rangle_X = \frac{1}{\sqrt{2}}(|0,1\rangle + |1,0\rangle).$
- 2. *B* chooses randomly either to Reflect or to Measure. If he chooses the latter, he chooses one of three options: Measure-All, Measure-0, or Measure-1. These operations are described in the text above. If he chooses one of these measure operations, he records whether he received a "click" (a detection) or not. Note that if he chose, say, Measure-0, and assuming the state arriving at his lab is the correct $|1,0\rangle_X = \frac{1}{\sqrt{2}}(|1,0\rangle + |0,1\rangle)$, he will only see a click with probability 1/2. If he does not see a click, the state is projected to the unobserved state (e.g., the other time bin).
- 3. A measures the returning state in either the Z or X basis, choosing randomly.
- 4. Following her measurement, A discloses her basis choice. B discloses the following information: whether he reflected, or measured and, if the latter, whether he got a detection or not. Note that he does *not* disclose which of the three measurement choices he made he only discloses that he chose one of them and whether that led to a detection or not.
- 5. If A choose the Z basis, and if B choose to measure and did not see a photon, they will use this iteration for their raw key. Namely, A will use her measurement result and B will use the opposite measurement choice he made (i.e., if he chose Measure-j and did not see the photon, his raw key bit will be 1 j).
- 6. A suitable subset of all iterations are chosen and all choices and results are disclosed on this subset to determine the error in the channel.

In the same paper, this protocol was proven to be robust. Note that it never requires B to send newly-prepared qubits. Instead, the idea is that he makes a partial measurement of only the $|0\rangle$ or the $|1\rangle$ states; if he does not see the photon (which happens, ideally, with probability 1/2) then he knows it's been projected to the opposite state. That is, if he uses Measure-j and does not see the photon, it should be leaving his lab in the state $|1 - j\rangle$). Then, when A later measures in the Z basis, she should receive the outcome 1 - j. A version of this protocol was experimentally implemented in [170]. Interestingly, it was shown in [171] that if this protocol is simplified to remove the Measure-All operation, the protocol is insecure.

An alternative SQKD protocol for practical implementations was presented in [169], based off of the Reflection-Based SQKD protocol from [16]. Again, the protocol was constructed so that B never had to prepare fresh photons. Security was shown only against a few practical attacks, namely an unambiguous state discrimination attack similar to the one used against B92 [172], and a multi-photon attack assuming imperfect devices.

Finally, a mediated SQKD protocol was developed in [83] where a fully quantum server prepares and later measures photons. The two classical users need only to choose Reflect or to Measure. They do not need to prepare photons; in fact, they also do not need to measure in a particular basis - they simply need to "look" at their portion of the quantum channel thus showing key distribution is possible with very minimal resources. In the same paper, a complete security proof against collective attacks in the finite-key setting was derived, including device imperfections and assuming an adversarial server (which may even prepare multi-photon states maliciously). Finally, an experimental demonstration of this protocol was performed and the key-rate computed using these experimental observations thus showing its practicality and the potential for practical semi-quantum communication.

The remaining major challenges, namely the need to switch rapidly from Measure and Resend (or some equivalent operation) and **Reflect** and, finally device imperfections, remain a challenge. The latter (e.g., dark counts, loss, and detector efficiency) affects all QKD (semiquantum and otherwise) work and these should be accounted for in proofs. Indeed, in the semi-quantum case, they have been accounted for in the papers we consider in this section. For the first, perhaps new protocols can be developed which do not require rapid switching. or some alternative mechanism for switching can be developed. For instance, in [173], an alternative switching technique using only passive optics was proposed. Perhaps also the mediated model presents a solution to both: we now know practical mediated SQKD protocols can be built consisting of an (untrusted) quantum server and several classical users. In the future, as the technology becomes more capable, one can envision only requiring a few commercial centers needing to purchase this expensive technology while end-users need only basic, perhaps poorly performing (e.g., detectors with low efficiency), quantum devices. Moving forward, when investigating practical semi-quantum communication, these are issues to keep in mind, and device imperfections, along with solutions for mitigating them (perhaps through the use of central servers with good devices, thus allowing end users to have less efficient devices) is an important area of investigation.

Considering the relative ease with which fully-quantum, one-way protocols (such as BB84) may be implemented, it is important to consider how the semi-quantum model may fully contribute beneficially to practical quantum communication. It seems that several avenues are potentially available: (1) if devices "break down" theoretical work within the semi-quantum communication model show that secure communication may still be possible with fewer resources, perhaps by changing the classical post processing; (2) the techniques developed to study these "limited resource" protocols, can translate to novel practical insights creating more efficient fully-quantum systems; (3) one may "offload" expensive devices to centralized, but untrusted, servers, leaving end-users with cheap, potentially poorly performing, quantum devices yet still attain optimistic security results. *Research in semi-quantum communication*

7 Closing Remarks and Future Directions

Semi-quantum cryptography and communication was originally introduced to study the theoretical question: how quantum must a protocol be to gain an advantage over its classical counterpart. This has led to developments in quantum key distribution (namely, semiquantum key distribution) showing that it is possible to establish a shared secret key, secure against a computationally unbounded adversary, when users have fewer theoretical quantum capabilities. Namely, even when one user is restricted to "classical" operations. Beyond this, these protocols have even been shown to be comparable in noise tolerance to fully-quantum protocols, at least in ideal perfect qubit channels. Furthermore, exciting possibilities exist involving semi-quantum users with weak quantum abilities, being able to perform certain cryptographic tasks using the help of strong, but untrusted (and potentially adversarial) servers. Moving beyond key distribution, the semi-quantum model of communication has been applied to other cryptographic primitives including secret sharing, state comparison, and secure direct communication, to list a few.

This paper has surveyed the history of semi-quantum cryptography and the current state of the art. We have also discussed recent research in practical, experimental, semi-quantum communication showing that this is a potentially viable model. There still remains many interesting theoretical and experimental problems, only some of which we have highlighted throughout this review. On the theory side, it is interesting to see how far one can go in reducing resource requirements and how this affects security. On the experimental side, it is interesting to see what systems can be built and how.

We believe that research in semi-quantum cryptography can offer great insight into other fields of quantum information science. The tools and techniques that have been, and are being, developed to construct and analyze semi-quantum protocols can be applied to fullyquantum protocols. We can gain insight into when security is possible and how to compensate for limited quantum capabilities - all of which are important problems for standard, fullyquantum, systems. It also provides insight into the great importance of quantum and classical information processing - indeed, many results in semi-quantum cryptography have shown how some lack of a quantum resource may be compensated for by using purely classical means. There are still many exciting questions and research directions in this area which may shed light on fundamental issues within quantum and classical information science and cryptography.

References

[1] Jonathan Katz and Yehuda Lindell. Introduction to modern cryptography. Chapman and Hall/CRC, 2014.

- [2] William Stallings. *Network security essentials: applications and standards*. Pearson Education India, 2007.
- [3] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175. New York, 1984.
- [4] Artur K Ekert. Quantum cryptography based on bells theorem. *Physical review letters*, 67(6):661, 1991.
- [5] Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000.
- [6] Renato Renner, Nicolas Gisin, and Barbara Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72:012332, Jul 2005.
- [7] Michel Boyer, Dan Kenigsberg, and Tal Mor. Quantum key distribution with classical bob. *Phys. Rev. Lett.*, 99:140501, Oct 2007.
- [8] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009.
- [9] Akshata Shenoy-Hejamadi, Anirban Pathak, and Srikanth Radhakrishna. Quantum cryptography: Key distribution and beyond. *Quanta*, 6(1):1–47, 2017.
- [10] Mohsen Razavi, Anthony Leverrier, Xiongfeng Ma, Bing Qi, and Zhiliang Yuan. Quantum key distribution and beyond: introduction. J. Opt. Soc. Am. B, 36(3):QKD1– QKD2, Mar 2019.
- [11] S Pirandola, UL Andersen, L Banchi, M Berta, D Bunandar, R Colbeck, D Englund, T Gehring, C Lupo, C Ottaviani, et al. Advances in quantum cryptography. arXiv preprint arXiv:1906.01645, 2019.
- [12] Michel Boyer, Ran Gelles, Dan Kenigsberg, and Tal Mor. Semiquantum key distribution. Phys. Rev. A, 79:032341, Mar 2009.
- [13] Wang Jian, Zhang Sheng, Zhang Quan, and Tang Chao-Jing. Semiquantum key distribution using entangled states. *Chinese Physics Letters*, 28(10):100301, 2011.
- [14] Zhiwei Sun, Ruigang Du, and Dongyang Long. Semi-quantum key distribution protocol using bell state. arXiv preprint arXiv:1106.2910, 2011.
- [15] Xiangfu Zou, Daowen Qiu, Lvzhou Li, Lihua Wu, and Lvjun Li. Semiquantum-key distribution using less than four quantum states. *Phys. Rev. A*, 79:052312, May 2009.
- [16] Walter O Krawec. Restricted attacks on semi-quantum key distribution protocols. Quantum Information Processing, 13(11):2417–2436, 2014.

- [17] Chi-Hang Fred Fung and Hoi-Kwong Lo. Security proof of a three-state quantumkey-distribution protocol without rotational symmetry. *Phys. Rev. A*, 74:042342, Oct 2006.
- [18] Cyril Branciard, Nicolas Gisin, Norbert Lutkenhaus, and Valerio Scarani. Zero-error attacks and detection statistics in the coherent one-way protocol for quantum cryptography. Quantum Information & Computation, 7(7):639–664, 2007.
- [19] Marco Lucamarini, Giovanni Di Giuseppe, and Kiyoshi Tamaki. Robust unconditionally secure quantum key distribution with two nonorthogonal and uninformative states. *Physical Review A*, 80(3):032327, 2009.
- [20] Wei Zhang and Daowen Qiu. A single-state semi-quantum key distribution protocol and its security proof. arXiv preprint arXiv:1612.03087, 2016.
- [21] Hua Lu and Qing-Yu Cai. Quantum key distribution with classical alice. International Journal of Quantum Information, 6(06):1195–1202, 2008.
- [22] Zhi-Wei Sun, Rui-Gang Du, and Dong-Yang Long. Quantum key distribution with limited classical bob. International Journal of Quantum Information, 11(01):1350005, 2013.
- [23] Po-Hua Lin, Tzonelih Hwang, and Chia-Wei Tsai. Double cnot attack on quantum key distribution with limited classical bob. *International Journal of Quantum Information*, 17(02):1975001, 2019.
- [24] Walter O Krawec and Eric P Geiss. Semi-quantum key distribution with limited measurement capabilities. In 2018 International Symposium on Information Theory and Its Applications (ISITA), pages 462–466. IEEE, 2018.
- [25] Allison Gagliano, Walter O Krawec, and Hasan Iqbal. From classical to semi-quantum secure communication. In 2019 IEEE International Symposium on Information Theory (ISIT), pages 1707–1711. IEEE, 2019.
- [26] Xiangfu Zou, Daowen Qiu, Shengyu Zhang, and Paulo Mateus. Semiquantum key distribution without invoking the classical partys measurement capability. *Quantum Information Processing*, 14(8):2981–2996, 2015.
- [27] Qin Li, Wai Hong Chan, and Shengyu Zhang. Semiquantum key distribution with secure delegated quantum computation. *Scientific reports*, 6:19898, 2016.
- [28] Kun-Fei Yu, Chun-Wei Yang, Ci-Hong Liao, and Tzonelih Hwang. Authenticated semiquantum key distribution protocol using bell states. *Quantum Information Processing*, 13(6):1457–1465, 2014.

- [29] Chuan-Ming Li, Kun-Fei Yu, Shih-Hung Kao, and Tzonelih Hwang. Authenticated semi-quantum key distributions without classical channel. *Quantum Information Pro*cessing, 15(7):2881–2893, 2016.
- [30] A Meslouhi and Yassine Hassouni. Cryptanalysis on authenticated semi-quantum key distribution protocol using bell states. *Quantum Information Processing*, 16(1):18, 2017.
- [31] Omar Amer and Walter O Krawec. Semiquantum key distribution with high quantum noise tolerance. *Physical Review A*, 100(2):022319, 2019.
- [32] Wei Liu and Huaijun Zhou. A new semi-quantum key distribution protocol with high efficiency. In 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), pages 2424–2427. IEEE, 2018.
- [33] Ming-Ming Wang, Lin-Ming Gong, and Lian-He Shao. Efficient semiquantum key distribution without entanglement. *Quantum Information Processing*, 18(9):260, 2019.
- [34] Hoi-Kwong Lo, Hoi-Fung Chau, and M Ardehali. Efficient quantum key distribution scheme and a proof of its unconditional security. *Journal of Cryptology*, 18(2):133–165, 2005.
- [35] Ming-Hui Zhang, Hui-Fang Li, Jin-Ye Peng, and Xiao-Yi Feng. Fault-tolerant semiquantum key distribution over a collective-dephasing noise channel. *International Jour*nal of Theoretical Physics, 56(8):2659–2670, 2017.
- [36] Chih-Lun Tsai and Tzonelih Hwang. Semi-quantum key distribution robust against combined collective noise. International Journal of Theoretical Physics, 57(11):3410– 3418, 2018.
- [37] Chia-Wei Tsai and Chun-Wei Yang. Cryptanalysis and improvement of the semiquantum key distribution robust against combined collective noise. *International Jour*nal of Theoretical Physics, pages 1–7, 2019.
- [38] Chrysoula Vlachou, Walter Krawec, Paulo Mateus, Nikola Paunković, and André Souto. Quantum key distribution with quantum walks. *Quantum Information Pro*cessing, 17(11):288, 2018.
- [39] Hasan Iqbal and Walter O Krawec. High-dimensional semi-quantum cryptography. arXiv preprint arXiv:1907.11340, 2019.
- [40] H Bechmann-Pasquinucci and Wolfgang Tittel. Quantum cryptography using larger alphabets. *Physical Review A*, 61(6):062308, 2000.
- [41] HF Chau. Quantum key distribution using qudits that each encode one bit of raw key. *Physical Review A*, 92(6):062324, 2015.

- [42] Toshihiko Sasaki, Yoshihisa Yamamoto, and Masato Koashi. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature*, 509(7501):475, 2014.
- [43] Zhen-Qiang Yin, Shuang Wang, Wei Chen, Yun-Guang Han, Rong Wang, Guang-Can Guo, and Zheng-Fu Han. Improved security bound for the round-robin-differentialphase-shift quantum key distribution. *Nature communications*, 9(1):457, 2018.
- [44] Rong Wang, Zhen-Qiang Yin, Chao-han Cui, Shuang Wang, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. Security proof for single-photon round-robin differentialquadrature-phase-shift quantum key distribution. *Physical Review A*, 98(6):062331, 2018.
- [45] Julia Kempe. Quantum random walks: an introductory overview. *Contemporary Physics*, 44(4):307–327, 2003.
- [46] Salvador Elías Venegas-Andraca. Quantum walks: a comprehensive review. *Quantum Information Processing*, 11(5):1015–1106, 2012.
- [47] Arpita Maitra and Goutam Paul. Eavesdropping in semiquantum key distribution protocol. Information Processing Letters, 113(12):418–422, 2013.
- [48] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science, 461(2053):207-235, 2005.
- [49] Takayuki Miyadera. Relation between information and disturbance in quantum key distribution protocol with classical alice. International Journal of Quantum Information, 9(06):1427–1435, 2011.
- [50] Christopher A Fuchs, Nicolas Gisin, Robert B Griffiths, Chi-Sheng Niu, and Asher Peres. Optimal eavesdropping in quantum cryptography. i. information bound and optimal strategy. *Physical Review A*, 56(2):1163, 1997.
- [51] Walter O Krawec. Key-rate bound of a semi-quantum protocol using an entropic uncertainty relation. In 2018 IEEE International Symposium on Information Theory (ISIT), pages 2669–2673. IEEE, 2018.
- [52] Walter O Krawec. Security proof of a semi-quantum key distribution protocol. In 2015 IEEE International Symposium on Information Theory (ISIT), pages 686–690. IEEE, 2015.
- [53] Robert Alicki and Mark Fannes. Continuity of quantum conditional information. Journal of Physics A: Mathematical and General, 37(5):L55, 2004.
- [54] Koenraad MR Audenaert. A sharp continuity estimate for the von neumann entropy. Journal of Physics A: Mathematical and Theoretical, 40(28):8127, 2007.

- [55] Andreas Winter. Tight uniform continuity bounds for quantum entropies: conditional entropy, relative entropy distance and energy constraints. *Communications in Mathematical Physics*, 347(1):291–313, 2016.
- [56] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M Renes, and Renato Renner. The uncertainty principle in the presence of quantum memory. *Nature Physics*, 6(9):659–662, 2010.
- [57] Patrick J. Coles, Mario Berta, Marco Tomamichel, and Stephanie Wehner. Entropic uncertainty relations and their applications. *Rev. Mod. Phys.*, 89:015002, Feb 2017.
- [58] Iwo Bialynicki-Birula and Łukasz Rudnicki. Entropic uncertainty relations in quantum physics. In *Statistical Complexity*, pages 1–34. Springer, 2011.
- [59] Stephanie Wehner and Andreas Winter. Entropic uncertainty relations survey. New Journal of Physics, 12(2):025009, 2010.
- [60] Walter O. Krawec. Quantum key distribution with mismatched measurements over arbitrary channels. *Quantum Information and Computation*, 17(3 and 4):209–241, 2017.
- [61] Normand J Beaudry, Marco Lucamarini, Stefano Mancini, and Renato Renner. Security of two-way quantum key distribution. *Physical Review A*, 88(6):062302, 2013.
- [62] Marco Lucamarini and Stefano Mancini. Quantum key distribution using a two-way quantum channel. *Theoretical Computer Science*, 560:46–61, 2014.
- [63] Walter O Krawec. Semi-Quantum Key Distribution: Protocols, Security Analysis, and New Models. PhD thesis, Stevens Institute of Technology, May 2015.
- [64] Walter O Krawec. Security of a semi-quantum protocol where reflections contribute to the secret key. Quantum Information Processing, 15(5):2067–2090, 2016.
- [65] Stephen M Barnett, Bruno Huttner, and Simon JD Phoenix. Eavesdropping strategies and rejected-data protocols in quantum cryptography. *Journal of Modern Optics*, 40(12):2501–2513, 1993.
- [66] Shun Watanabe, Ryutaroh Matsumoto, and Tomohiko Uyematsu. Tomography increases key rates of quantum-key-distribution protocols. *Physical Review A*, 78(4):042316, 2008.
- [67] Ryutaroh Matsumoto and Shun Watanabe. Key rate available from mismatched measurements in the bb84 protocol and the uncertainty principle. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 91(10):2870– 2873, 2008.

- [68] Ryutaroh Matsumoto and Shun Watanabe. Narrow basis angle doubles secret key in the bb84 protocol. Journal of Physics A: Mathematical and Theoretical, 43(14):145302, 2010.
- [69] Kiyoshi Tamaki, Marcos Curty, Go Kato, Hoi-Kwong Lo, and Koji Azuma. Loss-tolerant quantum cryptography with imperfect sources. *Physical Review A*, 90(5):052314, 2014.
- [70] Walter O. Krawec. Asymptotic analysis of a three state quantum cryptographic protocol. In *IEEE International Symposium on Information Theory*, *ISIT 2016*, *Barcelona*, *July 10-15*, 2016, pages 2489–2493, 2016.
- [71] Wei Zhang, Daowen Qiu, and Paulo Mateus. Security of a single-state semi-quantum key distribution protocol. *Quantum Information Processing*, 17(6):135, 2018.
- [72] Zhang Xian-Zhou, Gong Wei-Gui, Tan Yong-Gang, Ren Zhen-Zhong, and Guo Xiao-Tian. Quantum key distribution series network protocol with m-classical bobs. *Chinese Physics B*, 18(6):2143, 2009.
- [73] Kong-Ni Zhu, Nan-Run Zhou, Yun-Qian Wang, and Xiao-Jun Wen. Semi-quantum key distribution protocols with ghz states. *International Journal of Theoretical Physics*, 57(12):3621–3631, 2018.
- [74] Nan-Run Zhou, Kong-Ni Zhu, and Xiang-Fu Zou. Multi-party semi-quantum key distribution protocol with four-particle cluster states. Annalen der Physik, page 1800520, 2019.
- [75] Robert Raussendorf and Hans J Briegel. A one-way quantum computer. Physical Review Letters, 86(22):5188, 2001.
- [76] Walter O Krawec. Mediated semiquantum key distribution. *Physical Review A*, 91(3):032323, 2015.
- [77] Walter O Krawec. An improved asymptotic key rate bound for a mediated semiquantum key distribution protocol. *Quantum Information and Computation*, 16(9 and 10):813–834, 2016.
- [78] Walter O Krawec. Multi-mediated semi-quantum key distribution. To appear: 2019 IEEE Globecom Workshops (GC Wkshps), 2019.
- [79] Zhi-Rou Liu and Tzonelih Hwang. Mediated semi-quantum key distribution without invoking quantum measurement. Annalen der Physik, 530(4):1700206, 2018.
- [80] Po-Hua Lin, Chia-Wei Tsai, and Tzonelih Hwang. Mediated semi-quantum key distribution using single photons. Annalen der Physik, page 1800347, 2019.

- [81] Chia-Wei Tsai and Chun-Wei Yang. Lightweight mediated semi-quantum key distribution protocol with a dishonest third party based on bell states. *arXiv preprint arXiv:1909.02788*, 2019.
- [82] Chia-Wei Tsai, Chun-Wei Yang, and Narn-Yih Lee. Lightweight mediated semiquantum key distribution protocol. *Modern Physics Letters A*, page 1950281, 2019.
- [83] Francesco Massa, Preeti Yadav, Amir Moqanaki, Walter O Krawec, Paulo Mateus, Nikola Paunković, André Souto, and Philip Walther. Experimental quantum cryptography with classical users. arXiv preprint arXiv:1908.01780, 2019.
- [84] Adi Shamir. How to share a secret. Communications of the ACM, 22(11):612–613, 1979.
- [85] Amos Beimel. Secret-sharing schemes: a survey. In International Conference on Coding and Cryptology, pages 11–46. Springer, 2011.
- [86] Mark Hillery, Vladimír Bužek, and André Berthiaume. Quantum secret sharing. Physical Review A, 59(3):1829, 1999.
- [87] Anders Karlsson, Masato Koashi, and Nobuyuki Imoto. Quantum entanglement for secret sharing and secret splitting. *Physical Review A*, 59(1):162, 1999.
- [88] Daniel Gottesman. Theory of quantum secret sharing. *Physical Review A*, 61(4):042311, 2000.
- [89] Qin Li, Wai Hong Chan, and Dong-Yang Long. Semiquantum secret sharing using entangled states. *Physical Review A*, 82(2):022303, 2010.
- [90] Jian Wang, Sheng Zhang, Quan Zhang, and Chao-Jing Tang. Semiquantum secret sharing using two-particle entangled state. *International Journal of Quantum Information*, 10(05):1250050, 2012.
- [91] Lvzhou Li, Daowen Qiu, and Paulo Mateus. Quantum secret sharing with classical bobs. Journal of Physics A: Mathematical and Theoretical, 46(4):045304, 2013.
- [92] Chen Xie, Lvzhou Li, and Daowen Qiu. A novel semi-quantum secret sharing scheme of specific bits. *International Journal of Theoretical Physics*, 54(10):3819–3824, 2015.
- [93] Aihan Yin and Fangbo Fu. Eavesdropping on semi-quantum secret sharing scheme of specific bits. International Journal of Theoretical Physics, 55(9):4027–4035, 2016.
- [94] Xiang Gao, Shibin Zhang, and Yan Chang. Cryptanalysis and improvement of the semi-quantum secret sharing protocol. International Journal of Theoretical Physics, 56(8):2512–2520, 2017.

- [95] Yi Xiang, Jun Liu, Ming-qiang Bai, Xue Yang, and Zhi-wen Mo. Limited resource semi-quantum secret sharing based on multi-level systems. *International Journal of Theoretical Physics*, 58(9):2883–2892, 2019.
- [96] Chong-Qiang Ye and Tian-Yu Ye. Circular semi-quantum secret sharing using single particles. *Communications in Theoretical Physics*, 70(6):661, 2018.
- [97] Zhulin Li, Qin Li, Chengdong Liu, Yu Peng, Wai Hong Chan, and Lvzhou Li. Limited resource semiquantum secret sharing. *Quantum Information Processing*, 17(10):285, 2018.
- [98] Ye Chong-Qiang, Ye Tian-Yu, He De, and Gan Zhi-Gang. Multiparty semi-quantum secret sharing with d-level single-particle states. *International Journal of Theoretical Physics*, pages 1–18, 2019.
- [99] Chia-Wei Tsai, Chun-Wei Yang, and Narn-Yih Lee. Semi-quantum secret sharing protocol using w-state. *Modern Physics Letters A*, 34(27):1950213, 2019.
- [100] Kun-Fei Yu, Jun Gu, Tzonelih Hwang, and Prosanta Gope. Multi-party semi-quantum key distribution-convertible multi-party semi-quantum secret sharing. *Quantum Information Processing*, 16(8):194, 2017.
- [101] Aihan Yin, Zefan Wang, and Fangbo Fu. A novel semi-quantum secret sharing scheme based on bell states. *Modern Physics Letters B*, 31(13):1750150, 2017.
- [102] Gan Gao, Yue Wang, and Dong Wang. Cryptanalysis of a semi-quantum secret sharing scheme based on bell states. *Modern Physics Letters B*, 32(09):1850117, 2018.
- [103] Gan Gao, Yue Wang, and Dong Wang. Multiparty semiquantum secret sharing based on rearranging orders of qubits. *Modern Physics Letters B*, 30(10):1650130, 2016.
- [104] Ai Han Yin and Yan Tong. A novel semi-quantum secret sharing scheme using entangled states. *Modern Physics Letters B*, 32(22):1850256, 2018.
- [105] Qijian He, Wei Yang, Bingren Chen, and Liusheng Huang. Cryptanalysis and improvement of the novel semi-quantum secret sharing scheme using entangled states. *Modern Physics Letters B*, 33(04):1950045, 2019.
- [106] Gang Cao, Chen Chen, and Min Jiang. A scalable and flexible multi-user semi-quantum secret sharing. In Proceedings of the 2nd International Conference on Telecommunications and Communication Engineering, pages 28–32. ACM, 2018.
- [107] Yi-you Nie, Yuan-hua Li, and Zi-sheng Wang. Semi-quantum information splitting using ghz-type states. *Quantum information processing*, 12(1):437–448, 2013.
- [108] Gui-Lu Long and Xiao-Shu Liu. Theoretically efficient high-capacity quantum-keydistribution scheme. *Physical Review A*, 65(3):032302, 2002.

- [109] Kim Boström and Timo Felbinger. Deterministic secure direct communication using entanglement. *Physical Review Letters*, 89(18):187902, 2002.
- [110] Fu-Guo Deng, Gui Lu Long, and Xiao-Shu Liu. Two-step quantum direct communication protocol using the einstein-podolsky-rosen pair block. *Physical Review A*, 68(4):042317, 2003.
- [111] G. Long. Quantum secure direct communication: Principles, current status, perspectives. In 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), pages 1–5, June 2017.
- [112] Fu-Guo Deng and Gui Lu Long. Secure direct communication with a quantum one-time pad. *Physical Review A*, 69(5):052319, 2004.
- [113] XiangFu Zou and DaoWen Qiu. Three-step semiquantum secure direct communication protocol. Science China Physics, Mechanics & Astronomy, 57(9):1696–1702, 2014.
- [114] Jun Gu, Po-hua Lin, and Tzonelih Hwang. Double c-not attack and counterattack on three-step semi-quantum secure direct communication protocol. *Quantum Information Processing*, 17(7):182, 2018.
- [115] Chen Xie, Lvzhou Li, Haozhen Situ, and Jianhao He. Semi-quantum secure direct communication scheme based on bell states. *International Journal of Theoretical Physics*, 57(6):1881–1887, 2018.
- [116] Ming-Hui Zhang, Hui-Fang Li, Zhao-Qiang Xia, Xiao-Yi Feng, and Jin-Ye Peng. Semiquantum secure direct communication using epr pairs. *Quantum Information Process*ing, 16(5):117, 2017.
- [117] LiLi Yan, YuHua Sun, Yan Chang, ShiBin Zhang, GuoGen Wan, and ZhiWei Sheng. Semi-quantum protocol for deterministic secure quantum communication using bell states. *Quantum Information Processing*, 17(11):315, 2018.
- [118] Yuhua Sun, Lili Yan, Yan Chang, Shibin Zhang, Tingting Shao, and Yan Zhang. Two semi-quantum secure direct communication protocols based on bell states. *Modern Physics Letters A*, 34(01):1950004, 2019.
- [119] Yi-Ping Luo and Tzonelih Hwang. Authenticated semi-quantum direct communication protocols using bell states. *Quantum Information Processing*, 15(2):947–958, 2016.
- [120] Saleh Almousa and Michel Barbeau. Delay and reflection attacks in authenticated semiquantum direct communications. In 2016 IEEE Globecom Workshops (GC Wkshps), pages 1–7. IEEE, 2016.
- [121] Haoye Lu, Michel Barbeau, and Amiya Nayak. Economic no-key semi-quantum direct communication protocol. In 2017 IEEE Globecom Workshops (GC Wkshps), pages 1–7. IEEE, 2017.

- [122] Haoye Lu, Michel Barbeau, and Amiya Nayak. Keyless semi-quantum point-to-point communication protocol with low resource requirements. *Scientific reports*, 9(1):64, 2019.
- [123] Ming-Ming Wang, Jun-Li Liu, and Lin-Ming Gong. Semiquantum secure direct communication with authentication based on single-photons. International Journal of Quantum Information, page 1950024, 2019.
- [124] Zheng Tao, Yan Chang, Shibin Zhang, Jinqiao Dai, and Xueyang Li. Two semiquantum direct communication protocols with mutual authentication based on bell states. *International Journal of Theoretical Physics*, pages 1–8, 2019.
- [125] Zhan-Jun Zhang and Zhong-Xiao Man. Secure direct bidirectional communication protocol using the einstein-podolsky-rosen pair block. arXiv preprint quant-ph/0403215, 2004.
- [126] Ba An Nguyen. Quantum dialogue. *Physics Letters A*, 328(1):6–10, 2004.
- [127] Chitra Shukla, Kishore Thapliyal, and Anirban Pathak. Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue. *Quantum Information Processing*, 16(12):295, 2017.
- [128] Tian-Yu Ye and Chong-Qiang Ye. Semi-quantum dialogue based on single photons. International Journal of Theoretical Physics, 57(5):1440–1454, 2018.
- [129] Lin Liu, Min Xiao, and Xiuli Song. Authenticated semiquantum dialogue with secure delegated quantum computation over a collective noise channel. *Quantum Information Processing*, 17(12):342, 2018.
- [130] Nanrun Zhou, Guihua Zeng, and Jin Xiong. Quantum key agreement protocol. *Electronics Letters*, 40(18):1149–1150, 2004.
- [131] Song-Kong Chong and Tzonelih Hwang. Quantum key agreement protocol based on bb84. Optics Communications, 283(6):1192–1195, 2010.
- [132] Chitra Shukla, Nasir Alam, and Anirban Pathak. Protocols of quantum key agreement solely using bell states and bell measurement. *Quantum information processing*, 13(11):2391–2405, 2014.
- [133] Wen-Jie Liu, Zhen-Yu Chen, Sai Ji, Hai-Bin Wang, and Jun Zhang. Multi-party semiquantum key agreement with delegating quantum computation. *International Journal* of Theoretical Physics, 56(10):3164–3174, 2017.
- [134] Li Li Yan, Shi Bin Zhang, Yan Chang, Zhi Wei Sheng, and Fan Yang. Mutual semiquantum key agreement protocol using bell states. *Modern Physics Letters A*, page 1950294, 2019.

- [135] Lili Yan, Shibin Zhang, Yan Chang, Zhiwei Sheng, and Yuhua Sun. Semi-quantum key agreement and private comparison protocols using bell states. *International Journal* of Theoretical Physics, pages 1–11, 2019.
- [136] Andrew C Yao. Protocols for secure computations. In 23rd annual symposium on foundations of computer science (sfcs 1982), pages 160–164. IEEE, 1982.
- [137] Yehida Lindell. Secure multiparty computation for privacy preserving data mining. In *Encyclopedia of Data Warehousing and Mining*, pages 1005–1009. IGI Global, 2005.
- [138] Xiu-Bo Chen, Gang Xu, Xin-Xin Niu, Qiao-Yan Wen, and Yi-Xian Yang. An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. Optics communications, 283(7):1561–1565, 2010.
- [139] Wen Liu, Yong-Bin Wang, and Zheng-Tao Jiang. An efficient protocol for the quantum private comparison of equality with w state. Optics Communications, 284(12):3160– 3163, 2011.
- [140] Wen Liu, Yong-Bin Wang, Zheng-Tao Jiang, and Yi-Zhen Cao. A protocol for the quantum private comparison of equality with χ -type state. International Journal of Theoretical Physics, 51(1):69–77, 2012.
- [141] Wenjie Liu, Chao Liu, Haibin Wang, and Tingting Jia. Quantum private comparison: a review. *IETE Technical Review*, 30(5):439–445, 2013.
- [142] Hoi-Kwong Lo. Insecurity of quantum secure computations. Physical Review A, 56(2):1154, 1997.
- [143] Kishore Thapliyal, Rishi Dutt Sharma, and Anirban Pathak. Orthogonal-state-based and semi-quantum protocols for quantum private comparison in noisy environment. *International Journal of Quantum Information*, 16(05):1850047, 2018.
- [144] Wen-Han Chou, Tzonelih Hwang, and Jun Gu. Semi-quantum private comparison protocol under an almost-dishonest third party. arXiv preprint arXiv:1607.07961, 2016.
- [145] Lang Yan-Feng. Semi-quantum private comparison using single photons. International Journal of Theoretical Physics, 57(10):3048–3055, 2018.
- [146] Po-Hua Lin, Tzonelih Hwang, and Chia-Wei Tsai. Efficient semi-quantum private comparison using single photons. *Quantum Information Processing*, 18(7):207, 2019.
- [147] Tian-Yu Ye and Chong-Qiang Ye. Measure-resend semi-quantum private comparison without entanglement. International Journal of Theoretical Physics, 57(12):3819–3834, 2018.

- [148] Xiao-Jun Wen, Xing-Qiang Zhao, Li-Hua Gong, and Nan-Run Zhou. A semi-quantum authentication protocol for message and identity. *Laser Physics Letters*, 16(7):075206, 2019.
- [149] Nan-Run Zhou, Kong-Ni Zhu, Wei Bi, and Li-Hua Gong. Semi-quantum identification. Quantum Information Processing, 18(6):197, 2019.
- [150] Min Xiao and Di-Fang Zhang. Practical quantum private query with classical participants. *Chinese Physics Letters*, 36(3):030301, 2019.
- [151] Jinjun He, Qin Li, Chunhui Wu, Wai Hong Chan, and Shengyu Zhang. Measurementdevice-independent semiquantum key distribution. *International Journal of Quantum Information*, 16(02):1850012, 2018.
- [152] Yu-Guang Yang, Rui Yang, He Lei, Wei-Min Shi, and Yi-Hua Zhou. Quantum oblivious transfer with relaxed constraints on the receiver. *Quantum Information Processing*, 14(8):3031–3040, 2015.
- [153] Xing-Qiang Zhao, Hua-Ying Chen, Yun-Qian Wang, and Nan-Run Zhou. Semiquantum bi-signature scheme based on w states. International Journal of Theoretical Physics, pages 1–13, 2019.
- [154] Ivan B Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded-quantum-storage model. SIAM Journal on Computing, 37(6):1865–1890, 2008.
- [155] Ivan B Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Secure identification and qkd in the bounded-quantum-storage model. In Annual International Cryptology Conference, pages 342–359. Springer, 2007.
- [156] Stephanie Wehner, Christian Schaffner, and Barbara M Terhal. Cryptography from noisy storage. *Physical Review Letters*, 100(22):220502, 2008.
- [157] Robert Konig, Stephanie Wehner, and Jürg Wullschleger. Unconditional security from noisy quantum storage. *IEEE Transactions on Information Theory*, 58(3):1962–1984, 2012.
- [158] Yong-gang Tan, Hua Lu, and Qing-yu Cai. Comment on quantum key distribution with classical bob. *Physical review letters*, 102(9):098901, 2009.
- [159] Michel Boyer, Dan Kenigsberg, and Tal Mor. Boyer, kenigsberg, and mor reply. Physical Review Letters, 102(9):098902, 2009.
- [160] Yu-Guang Yang, Si-Jia Sun, and Qian-Qian Zhao. Trojan-horse attacks on quantum key distribution with classical bob. *Quantum Information Processing*, 14(2):681–686, 2015.

- [161] Stefano Pirandola, Stefano Mancini, Seth Lloyd, and Samuel L Braunstein. Continuous-variable quantum cryptography using two-way quantum communication. *Nature Physics*, 4(9):726, 2008.
- [162] Carlo Ottaviani and Stefano Pirandola. General immunity and superadditivity of twoway gaussian quantum cryptography. *Scientific reports*, 6:22225, 2016.
- [163] Christian Weedbrook, Carlo Ottaviani, and Stefano Pirandola. Two-way quantum cryptography at different wavelengths. *Physical Review A*, 89(1):012309, 2014.
- [164] Carlo Ottaviani, Stefano Mancini, and Stefano Pirandola. Two-way gaussian quantum cryptography against coherent attacks in direct reconciliation. *Physical Review A*, 92(6):062323, 2015.
- [165] Quntao Zhuang, Zheshen Zhang, Norbert Lütkenhaus, and Jeffrey H Shapiro. Securityproof framework for two-way gaussian quantum-key-distribution protocols. *Physical Review A*, 98(3):032332, 2018.
- [166] Shouvik Ghorai, Eleni Diamanti, and Anthony Leverrier. Composable security of two-way continuous-variable quantum key distribution without active symmetrization. *Physical Review A*, 99(1):012311, 2019.
- [167] Quntao Zhuang, Zheshen Zhang, Justin Dove, Franco N. C. Wong, and Jeffrey H. Shapiro. Floodlight quantum key distribution: A practical route to gigabit-per-second secret-key rates. *Phys. Rev. A*, 94:012322, Jul 2016.
- [168] Michel Boyer, Matty Katz, Rotem Liss, and Tal Mor. Experimentally feasible protocol for semiquantum key distribution. *Physical Review A*, 96(6):062335, 2017.
- [169] Walter O Krawec. Practical security of semi-quantum key distribution. In Quantum Information Science, Sensing, and Computation X, volume 10660, page 1066009. International Society for Optics and Photonics, 2018.
- [170] Pavel Gurevich. Experimental Quantum Key Distribution with Classical Alice. Technion-Israel Institute of Technology, Faculty of Computer Science, 2012.
- [171] Michel Boyer, Rotem Liss, and Tal Mor. Attacks against a simplified experimentally feasible semiquantum key distribution protocol. *Entropy*, 20(7):536, 2018.
- [172] Kiyoshi Tamaki, Masato Koashi, and Nobuyuki Imoto. Security of the bennett 1992 quantum-key distribution protocol against individual attack over a realistic channel. *Physical Review A*, 67(3):032310, 2003.
- [173] GP Temporao. Passive switching scheme for two-way quantum key distribution setups. Electronics Letters, 46(7):512–513, 2010.