Semi-Quantum Random Number Generation

Julia Guskind
Department of Computer Science and Engineering
University of Connecticut
Storrs, CT USA

Walter O. Krawec
Department of Computer Science and Engineering
University of Connecticut
Storrs, CT USA
walter.krawec@uconn.edu

***Abstract*—Semi-quantum cryptography involves at least one user who is semi-quantum or "classical" in nature. Such a user can only interact with the quantum channel in a very restricted way. Many semi-quantum key distribution protocols have been developed, some with rigorous proofs of security. Here we show for the first time that quantum random number generation is possible in the semi-quantum setting. We also develop a rigorous proof of security, deriving a bound on the random bit generation rate of the protocol as a function of noise in the channel. Our protocol and proof may be broadly applicable to other quantum and semi-quantum cryptographic scenarios where users are limited in their capabilities.**

***Index Terms*—Quantum Cryptography, Quantum Random Number Generation, Quantum Information Theory, Security**

I. Introduction

Quantum Random Number Generators (QRNG) are an important cryptographic tool. By utilizing the physical randomness of a quantum source, such protocols can distill cryptographically-secure random strings which are, themselves, important necessities for other cryptographic primitives (e.g., encryption, key distillation, and so on). By now there are many QRNG protocols along with several security models. Security models range from the extreme device independent scenario [1], [2], [3], [4] (where all measurement and source devices are untrusted) to the fully trusted scenario (where all devices are trusted and completely characterized). An interesting middle-ground is the *source independent* model whereby measurement devices are trusted, but source devices may be offloaded to an untrusted party [5], [6], [7]. Such systems lead to a good security middle-ground while also providing fast experimental bit generation rates [8], [9]. For a general review of QRNG protocols the reader is referred to [10]; for a more general review on quantum cryptography, including theoretical and experimental developments, the reader is referred to [11], [12], [13].

Semi-quantum cryptography was first introduced in [14] for the key-distribution problem (QKD). In general QKD protocols, like all other quantum cryptographic protocols, require parties to be "fully-quantum" or "quantum-capable." Namely, they must be able to manipulate quantum bits in arbitrary ways. Semi-quantum protocols involve at least one user who has restrictions and is almost classical in nature. This restricted user is only able to interact with the quantum channel in a limited, classical, way: the user may measure and send in a single, publicly known basis (usually the $|0\rangle$, $|1\rangle$ basis) or to ignore the quantum channel, disconnecting from it, and returning all received signals back to the sender undisturbed. Clearly, if all parties were restricted to these operations, the entire protocol would be mathematically equivalent to a classical one. Thus, the restricted party is often called the "classical user." The goal of any semi-quantum protocol is to achieve the same end-result as the original fully-quantum version (e.g., unconditionally secure key distribution) but using fewer resources. In a way, they help us to study the "gap" between classical and quantum protocols and help us answer the question "how quantum" do protocols need to be to gain an advantage over its classical counterpart?

Most semi-quantum protocols are restricted to key-distribution [15], [16], [17], [18], [19], [20], [21], [22], [23], however there are other primitives that are also available, in particular secret sharing [24], [25], [26], secure direct communication [27], [28], [29], [30], [31], private comparison [32], [33], and identity authentication [34], [35]. Semi-quantum protocols can also be experimentally feasible [36], [37]. For a general survey of semi-quantum cryptography, the reader is referred to [38]. To our knowledge, no semi-quantum random number generation (SQRNG) protocol is available. We prove in this paper that QRNG is a viable semi-quantum primitive by designing the first SQRNG protocol and also deriving a rigorous information theoretic proof of security for it.

We make several contributions in this work. We develop a new, and to our knowledge the first, semi-quantum random number generation protocol allowing a "classical" or semi-quantum user to generate a cryptographically-secure random number. This is done using a fully-quantum server as a source and partial measurement device. However, this server need not be trusted and, in fact, may be fully controlled by an adversary. We develop an information theoretic proof of security for our protocol and derive an asymptotic random-bit generation rate, as a function of observed noise in the channel connecting the semi-quantum user to the adversarial server. Since the server performs quantum state preparation and measurement, this also gives a partial form of device independence for part of the protocol. Our proof of security involves reducing the semi-quantum protocol to an entanglement-based version and deriving a bound on the quantum entropy of the resulting system. The protocol and security proof methods may be important foundational building-blocks for future work in (semi) quantum cryptography.

II. Preliminaries

In this section we discuss some basic notation and concepts. Let $x \in \{0,1\}^n$, then we define $ct_i(x)$ to be the number of times $i \in \{0,1\}$ appears in the string x. Given a quantum state $|\psi\rangle$ we write $[\psi]$ to mean $|\psi\rangle\langle\psi|$. Given a state ρ_{AE} acting on some Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_E$, we write ρ_A to mean the state resulting from the partial trace over the E system, namely $\rho_A = tr_E \rho_{AE}$. Similarly for multiple systems.

The *von Neumann entropy* of a state ρ_A is defined to be $S(A)_\rho = -tr(\rho_A \log \rho_A)$ where all logarithms in this paper are base two unless otherwise specified. Given state ρ_{AE} we write $S(A|E)_\rho$ to mean the conditional von Neumann entropy defined to be $S(A|E)_\rho = S(AE)_\rho - S(E)_\rho$.

We will be working with quantum random number generation (QRNG). For this, a quantum protocol is run whereby Alice and Eve holds two registers - Alice's register is a classical system containing her *raw random string* while Eve's system is quantum and arbitrarily entangled. This raw random string may not be uniform or completely independent of Eve, thus a further post-processing step is required. Given a classical-quantum state ρ_{AE}, we are interested in how much uniform randomness, independent of E, can be extracted from A. The process of *privacy amplification* can be used to extract this randomness. Namely, if one chooses a random two-universal hash function sending N-bit strings to ℓ-bit strings, and maps the A register through this hash, resulting in $\rho_{F(A)E}$, then it was shown in [39] that:

$$\left|\left|\rho_{F(A)E} - \frac{I}{2^\ell} \otimes \rho_E\right|\right| \leq 2^{-\frac{1}{2}(H_\infty^\epsilon(A|E)_\rho - \ell)} + 2\epsilon, \quad (1)$$

where $H_\infty^\epsilon(A|E)$ is the smooth quantum min entropy [39]. Thus, to ensure that the resulting system is ϵ'-close to a uniform random string, independent of any adversary system, one requires a bound on the quantum min entropy. In the asymptotic scenario (which we consider in this paper), where $|A| \to \infty$ and $\epsilon \to 0$, and assuming collective attacks whereby ρ_{AE} takes a product form (and so $\rho_{AE} = \sigma_{AE}^{\otimes N}$), it holds that $\frac{1}{N} H_\infty^\epsilon(A|E)_\rho \to S(A|E)_\sigma$ (see [40]). From this, it is clear that:

$$\lim_{N\to\infty} \frac{\ell}{N} = S(A|E) \quad (2)$$

Note the similarities to the Devetak-Winter key-rate for QKD [41]; the only difference is that there is no need to worry about error correction leakage.

III. The Protocol

We now introduce our SQRNG protocol. The protocol consists of a semi-quantum user Alice and a fully quantum server capable of creating quantum signals and measuring them in the X basis (see Figure 1). A semi-quantum user is restricted to performing operations in a single, publicly known, basis (usually the computational basis $\{|0\rangle, |1\rangle\}$) or to ignoring the quantum signal and reflecting it undisturbed. Formally, the semi-quantum user is restricted to performing one of the following two operations on every qubit received from some sender:

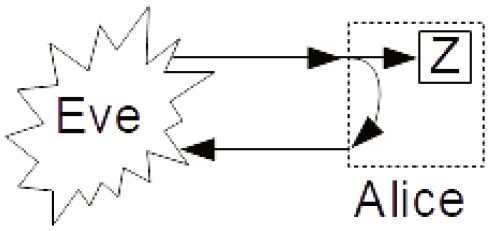

Fig. 1. The proposed SQRNG protocol. An untrusted quantum server (Eve) sends quantum signals to semi-quantum or "classical" Alice. If honest, the server should send $|+\rangle$. Alice may only measure in the computational Z basis or reflect the incoming signal. The server, if honest, will measure the returning signal in the X basis and report the outcome. We prove security assuming the server is adversarial and does not necessarily prepare the correct state or perform the correct measurement.

1) `Measure-Resend`: the semi-quantum user subjects the qubit to a Z basis measurement resulting in outcome $r \in \{0,1\}$. A qubit in the state $|r\rangle$ is then returned to the sender.
2) `Reflect`: the semi-quantum user ignores the qubit and reflects it, undisturbed, back to the sender.

Since the quantum server is untrusted, we call the server Eve. Though we will later, in our security analysis, assume the server is adversarial, for the purposes of this section, we explain the protocol's operation assuming an honest server. The protocol operates over several rounds, a single round consisting of the following actions:

1) The server prepares the state $|+\rangle$ and sends it to Alice.
2) Alice chooses randomly to `Reflect` the signal or to `Measure-Resend`, (recording the measurement result).
3) Upon receiving Alice's qubit, the server makes an X basis measurement and reports the outcome over a classical channel (this channel need not be authenticated).
   - If Alice chose `Reflect`, she should expect the message from the server to be "+" and any other response will be considered noise and will be later factored into our security analysis.
   - If Alice chose `Measure-Resend`, she will have a classical measurement outcome $a \in \{0,1\}$. Ideally, the server's message will be either "+" or "−" randomly in this event.

The above quantum portion of the protocol is repeated N times leading to a raw random string of size $n \leq N$. This raw random string is the result of Alice's measurements when she chose `Measure-Resend`. However, it may not be uniform (due to adversarial or natural noise) and Eve may have some side information on it through her quantum ancilla and her operation as the server (i.e., she need not perform an honest X basis measurement on step 3). Thus, it is next processed through privacy amplification, hashing the raw string using a two-universal hash function. As proven in [42], for QRNG, this hash function need only be chosen once and thus additional randomness is not needed on Alice's part to choose this hash function.

It is worth discussing how much seed randomness Alice needs to execute the above protocol. She requires some secret random string in order to make her operational choices each round. We may consider the protocol differently, in that Alice will choose a subset t of size m which indexes those rounds (out of the N total rounds) that will be used for testing, namely those rounds where she chooses `Reflect`. For all rounds not in t she will choose `Measure-Resend`. Choosing this subset requires $\log \binom{N}{m}$ bits of seed randomness. This seed may be replenished by the random string produced after privacy amplification. However, as we are considering the asymptotic scenario in this paper, we may choose m to be arbitrarily small compared to N and, so, as $N \to \infty$, it will hold that $\frac{1}{N} \log \binom{N}{m} \to 0$ and so we will not consider this in our subsequent analysis. In the finite signal scenario, of course, it would be important.

IV. Security Analysis

We now prove security of our protocol against general attacks in the asymptotic scenario. The security model used by our proof assumes the following:

1) The server is adversarial and may produce any arbitrary quantum state in Step 1 of the protocol. This state may be entangled with the server's private ancilla. We assume the dimension of the quantum state actually sent to Alice is 2^N where N is the number of rounds used by the protocol (a parameter set by the user Alice). That is, the server is allowed to perform any general attack in Step 1, however we assume each round consists of an ideal qubit.
2) The channel connecting the server to Alice is noisy but not lossy. However, the server, may replace the channel with a perfect one (as is typically assumed in quantum cryptographic proofs) and thus any noise detected by Alice is the result of an adversary. This assumption is to the benefit of the adversary as any natural channel noise can only cause more uncertainty for Eve.
3) Alice's measurement devices are ideal and qubits are ideal. Thus, we are not considering practical attacks such as photon tagging attacks [43], [44]
4) On Step 3 of the protocol, the server may perform any quantum operation on the returning N qubit signal and her ancilla from Step 1. However, the server must send a classical message of size N-bits (a one-bit message for every round of the protocol). This attack is modeled as a *quantum instrument* [45].
5) While there may be third party adversaries, we assume that they collude with the server. Thus, any third-party adversary attack may be "absorbed" into the adversarial server's attack strategy and we need only prove security against adversarial servers. Note that this includes attacks by third-party adversaries against the unauthenticated classical channel connecting the server to Alice. This assumption is to the benefit of the adversary.

Note, though we are proving security against general attacks here, we are not considering practical attacks. While practical attacks are important, proving security against general attacks even in the ideal-qubit scenario is challenging in itself and usually a first step (especially for semi-quantum protocols). Mirror-style adaptions may be useful here [36], [46]; however, we consider practical attacks as interesting future work, but out of scope for this paper. Note, also, that classical attack strategies are covered in our attack model.

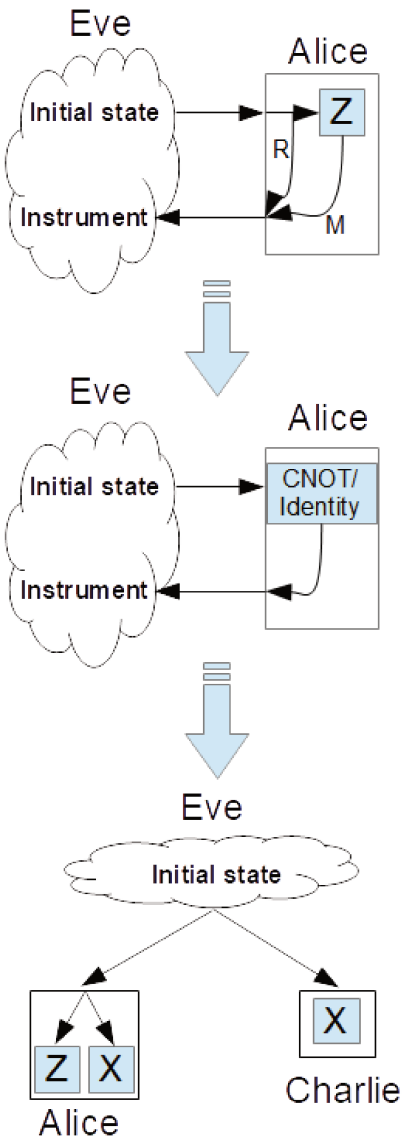

Fig. 2. A high-level overview of our security proof. Top: the actual SQRNG protocol we prove secure; here Alice can chose to `Measure-Resend` ("M") or `Reflect` ("R"); Middle: A "purified" version of the protocol where Alice applies a CNOT gate or the identity gate to each signal; Bottom: the entanglement based version where Eve creates an initial state and sends part to Alice (who is now fully quantum can can measure in the X or Z basis) and part to a trusted server Charlie (C). Note that in the top two protocols, Eve has two opportunities to attack: in the initial state creation and in the final instrument attack; in the entanglement based version, Eve only has one opportunity to attack, during the state creation. Nonetheless, we prove here that security of the entanglement based version (bottom) implies security of the SQRNG protocol (top).

Our proof works in two stages. First, we show how our

protocol can be reduced to an equivalent entanglement based version. For this we will adapt methods similar to those we developed in [47] for a particular semi-quantum key distribution protocol. This entanglement protocol is actually a QRNG protocol (i.e., a fully-quantum protocol), where the user is now fully quantum. Nonetheless, we show that security of that QRNG protocol implies security of the SQRNG version. The second step proves security of this entanglement based version (thus proving security of the actual semi-quantum prepare-and-measure protocol we developed). Note that, while we only consider this particular SQRNG protocol, we suspect our methods and our proof methodology may be broadly applicable to other quantum cryptographic protocols, especially those with device limitations and two-way quantum communication, which are generally a challenge to prove using standard proof techniques. See Figure 2.

A. Reduction to an Entanglement Based Protocol

We first show how our SQRNG protocol may be reduced to an entanglement based version denoted by e-QRNG. Our reduction is based on methods we developed in [47] for *mediated SQKD* protocols (key-distribution protocols using a quantum server [20]); we show here that these methods can be extended to work with our SQRNG protocol.

We first comment that the SQRNG protocol may be "purified" in the following sense. Instead of Eve preparing each qubit individually, she prepares a large N-qubit state where N is the number of rounds used by the protocol, possibly entangled with her private ancilla. There is no assumption that this state be a product state. Next, Alice, on receipt of these qubits, will choose a subset Θ. For each $i = 1, \cdots, N$, if $\Theta_i = 0$, she will `Reflect` the i'th signal (namely perform an identity operation); otherwise she will `Measure-Resend` the qubit. However, instead of actually performing a destructive measurement at this point, Alice will simply apply a CNOT gate with the control register being the i'th qubit sent from the server and the target being a blank qubit cleared to the $|0\rangle$ state. She may then later measure this private register in the Z basis. It is clear that this later measurement will simulate the case where Alice measures the qubits immediately. Following this operation by Alice (either the Identity operation or the CNOT operation), the entire signal of N qubits returns to Eve who performs a quantum instrument mapping the N qubits and her initial private ancilla to a classical N-bit message space (modeled as a quantum ancilla) and an updated ancilla from which Eve will attempt to learn as much as possible about Alice's measurement results (or, rather, Alice's private register which she will subsequently measure). Quantum instruments may be used to model scenarios where a quantum state undergoes some quantum operation (including potential measurements) yielding a classical and quantum state as output. The classical part represents the message Eve sends to Alice while the quantum part represents Eve's ancilla in the event she chose to send that particular message. In the purified case, this instrument may be dilated to an isometry (and subsequently a unitary) operator using standard techniques [48]. The fact that this purified version is identical to the standard prepare-and-measure one follows through standard methods; the advantage to it is that the quantum state remains a pure state which will be easier to argue about in terms of security.

Now, we show how this purified SQRNG protocol can be reduced to an entanglement QRNG, denoted e-QRNG. The e-QRNG protocol is a fully quantum protocol (not a semi-quantum one) with three parties: Alice, a Trusted Server (who may also be Alice), and Eve. Alice will have choices similar to the SQRNG case, namely `Measure-Resend` and `Reflect` though these operations are different here and, in fact, have no operational meaning in the e-QRNG protocol. We show later that, the operation of `Reflect` in the e-QRNG case (which is not actually a reflection but a particular measurement) will "simulate" a true `Reflect` operation in the SQRNG case; similarly for the `Measure-Resend` operation.

The entanglement protocol (e-QRNG) operates as follows:

1) Our quantum source, Eve, prepares an entangled state $|\tau\rangle_{ACE} \in \mathcal{H}_A \otimes \mathcal{H}_C \otimes \mathcal{H}_E$. The A and C registers are each of dimension 2^N for user specified N (as before, N is the number of rounds used by the protocol). The A system is sent to Alice while the C register is sent to the trusted server (who may also be Alice). Eve keeps the E register private.
2) Alice, on receipt of the state, has two choices for each round (i.e., each of the N qubits), as in the SQRNG protocol. We call these two choices here `Measure-Resend` and `Reflect` to keep the notation consistent with the SQRNG case, however the operations are different in the e-QRNG case. If Alice chooses `Reflect`, she will measure that qubit in the X basis, and *abort the entire protocol* if she observes $|-\rangle$. That is, to simulate a true "reflection" in the semi-quantum case, A will only continue with the protocol if she measures and observes $|+\rangle$. We say Alice *accepts* the state if she observes $|+\rangle$. Alternatively, if Alice chooses `Measure-Resend`, she will measure that particular qubit in the Z basis.
3) The trusted server, on receipt of the C system, simply measures all N qubits in the X basis, and *publicly reports the outcome*. Note that in the e-QRNG case, the server is honest in this measurement and, in fact, this C register measurement may even be done by Alice. Note that this may be done before, in parallel to, or after Alice's operations in step 2.

We comment that this e-QRNG protocol is highly inefficient due to the high probability of aborting (regardless of the noise level). *However, this e-QRNG protocol is not one users would actually run, but rather only used as a theoretical tool to prove security of the actual SQRNG protocol (which only aborts if the noise level is too high).* It is important to note that the protocol completely aborts if Alice observes $|-\rangle$ on her `Reflect` test case. The reason for this is that, as we show later, an observation of $|+\rangle$ will exactly simulate a true

`Reflect` in the SQRNG case whereas an observation of $|-\rangle$ produces a quantum system that cannot exist in the SQRNG case and, so, should not be analyzed.

Theorem 1. Let $\mathcal{E}$ be an attack against the SQRNG protocol (which, itself, consists of an initial state description and a quantum instrument to apply after Alice's operation) and let Θ be Alice's choice of operation in the SQRNG protocol. Let $|\psi(\mathcal{E},\Theta)\rangle_{AME}$ be the resulting state of operating the purified SQRNG protocol under these conditions (where A is Alice's register; E is Eve's private ancilla; and M is the register storing the classical message sent from the adversarial server to Alice). Then, there exists a quantum state $|\tau(\mathcal{E})\rangle_{ACE}$ for the e-QRNG protocol, depending only on $\mathcal{E}$, such that: (1) the probability of Alice not aborting, assuming she measures those qubits in A with $\Theta_i = 0$, (i.e., she accepts $|\tau\rangle$) is non-zero and exactly $p_a = 1/2^{ct_0(\Theta)} > 0$ for any Θ; (2) conditioning on accepting, let $|\tau(\mathcal{E},\Theta)\rangle$ be the resulting quantum state (which clearly does depend on Θ), then it holds that $|\tau(\mathcal{E},\Theta)\rangle = |\psi(\mathcal{E},\Theta)\rangle$; and (3) if the SQRNG protocol is attacked using a collective attack (namely the produced state is a product state), then the constructed state $|\tau\rangle$ is also a product state $|\tau\rangle = |\tau_0\rangle^{\otimes N}$ (the result of a collective attack) and, furthermore, the probability of observing a $|-\rangle$ on any individual signal in the e-QRNG case is exactly $1/2$.

Proof. Let's consider the (purified) SQRNG protocol. In this case, a general attack consists of Eve first preparing an arbitrary quantum state $|\psi_0\rangle_{AE}$ which, without loss of generality, we may write as:

$$|\psi_0\rangle = \sum_{a\in\{0,1\}^N} \alpha_a |a\rangle |E_a\rangle ,$$

where the $|E_a\rangle$ are arbitrary normalized states in Eve's private ancilla. The A portion is sent to Alice who chooses Θ which dictates whether to `Measure-Resend` or to `Reflect`. Whenever $\Theta_i = 1$ she will apply a CNOT gate as discussed. Since her ancilla is initially cleared to a zero state, the result of this action on $|\psi_0\rangle$ is easily seen to be:

$$|0\cdots 0\rangle_A \otimes |\psi_0\rangle \to |\psi_0'\rangle = \sum_{a\in\{0,1\}^N} \alpha_a |a\wedge\Theta, a\rangle_{AT} |E_a\rangle ,$$

where $a\wedge\Theta$ denotes the bit-wise AND operation and the $|a\wedge\Theta\rangle_A$ is Alice's private ancilla after applying CNOT gates whenever $\Theta_i = 1$. The T (Transit) register represents the quantum state that will return to Eve.

At this point, the T register will return to Eve's control who applies a quantum instrument to the system. As shown in [20], this is equivalent to applying an isometry U mapping Eve's ancilla and the Transit register into a quantum ancilla for Eve and a Hilbert space spanned by all possible classical messages that could have been sent (namely, a Hilbert space of dimension 2^N since for every round there are only two classical messages Eve is allowed to send). After applying the isometry U to the returning system and Eve's ancilla from her initial state preparation, she measures the message Hilbert space. The measurement outcome determines the message transcript she sends to Alice while the post measured system represents her quantum ancilla in the event she had sent that message using the quantum instrument attack.

Without loss of generality, we may define U's action on basis states as follows:

$$U|a, E_a\rangle = \sum_{m\in\{+,-\}^N} |m, F_{a,m}\rangle_{M,E} ,$$

where the M register is Eve's classical message. Note that U's action on basis states of the form $|a, E_b\rangle$ for $a \neq b$ may be arbitrary as these do not appear in the system under investigation.

Applying U to the returning state $|\psi_0'\rangle$ yields:

$$|\psi\rangle = \sum_{a\in\{0,1\}^N} \alpha_a |a\wedge\Theta\rangle \otimes \sum_{m\in\{+,-\}^N} |m, F_{a,m}\rangle_{cl,E} \quad (3)$$

Eve will then measure the M register dictating her message.

We now claim that there is an equivalent attack strategy against the e-QRNG protocol, producing an identical quantum system in the event the entanglement based protocol does not abort. That is, any attack against the SQRNG protocol can be translated to an equivalent attack against the e-QRNG protocol and, therefore, if the e-QRNG protocol is secure, the SQRNG protocol must also be (since e-QRNG can only have more attacks against it).

Consider, now, the entanglement based protocol. Assume Eve prepares the initial state:

$$\begin{aligned} |\tau\rangle_{ACE} &= U\left(\sum_{a\in\{0,1\}^N} \alpha_a |a, E_a\rangle\right) \\ &= \sum_{a\in\{0,1\}^N} \alpha_a |a\rangle_A \otimes \sum_{m\in\{+,-\}^N} |m, F_{a,m}\rangle_{CE} . \end{aligned} \quad (4)$$

The A and C registers are sent to Alice and the trusted server respectively (as discussed, the trusted server may in fact be Alice in the e-QRNG protocol case).

We first show the second claim of the theorem namely that, conditioning on Alice accepting the e-QRNG state, it agrees with the SQRNG state. For this, we note that we can decompose the sum over $a \in \{0,1\}^N$ in $|\psi\rangle$ (Equation 3) into two parts: a part where $\Theta_i = 0$ and a part where $\Theta_i = 1$. In particular, we can write $a = \pi_\Theta(a_0, a_1)$ for some permutation π depending on Θ. Here, $|a_0| = ct_0(\Theta)$ and $|a_1| = ct_1(\Theta)$. The function π_Θ simply maps the first argument into the appropriate bit-position of a where Θ is zero; similarly for the second argument. Thus Equation 3 (the SQRNG case) becomes:

$$|\psi\rangle = \sum_{a_0,a_1} \alpha_{\pi_\Theta(a_0,a_1)} |\pi_\Theta(0\cdots 0, a_1)\rangle \otimes \sum_m |m, F_{\pi_\Theta(a_0,a_1),m}\rangle . \quad (5)$$

Of course the sum above is over all $a_0 \in \{0,1\}^{ct_0(\Theta)}$ and $a_1 \in \{0,1\}^{ct_1(\Theta)}$.

Now, we may similarly decompose the initial state prepared by Eve in the e-QRNG case (Equation 4) as follows:

$$
\begin{aligned}
|\tau\rangle &= \sum_{a_0,a_1} \alpha_{\pi_\Theta(a_0,a_1)} \left|\pi_\Theta(a_0,a_1)\right\rangle \otimes \sum_m |m, F_{\pi_\Theta(a_0,a_1)}\rangle \\
&= \frac{1}{\sqrt{2^m}} \sum_{a_0,a_1} \alpha_{\pi_\Theta(a_0,a_1)} \left|\pi_\Theta(+^m,a_1)\right\rangle \sum_m |m, F_{\pi_\Theta(a_0,a_1)}\rangle \\
&+ |\mu\rangle_{AE} \\
&\cong \frac{1}{\sqrt{2^{ct_0(\Theta)}}} |\psi\rangle + |\mu\rangle .
\end{aligned}
$$

where $m = ct_0(\Theta)$, $+^m = + \cdots +$ (m times), and $|\mu\rangle_{AE}$ is some state that has at least one $|-\rangle$ where $\Theta_i = 0$ in Alice's register (and, thus, would lead to the protocol aborting). It is clear, then, that conditioned on Alice not aborting the e-QRNG protocol (i.e., accepting the state $|\tau\rangle$), the state collapses to $|\psi\rangle$, the same state that would have been produced if the SQRNG protocol had been run.

It is also clear that, since $\langle\psi|\psi\rangle = 1$ and $\langle\psi|\mu\rangle = 0$, the probability of Alice not aborting is strictly positive (and, thus, we do not condition on a probability zero event). In fact, the probability of not aborting (i.e., accepting) is exactly $\frac{1}{\sqrt{2^{ct_0(\Theta)}}}$ proving claim (1) of the theorem.

Finally, to prove claim (3), we note that if Equation 3 were produced by a collective attack, then Equation 4 would be a product state also and the probability of accepting will remain $\frac{1}{\sqrt{2^{ct_0(\Theta)}}}$ implying that the probability of accepting any particular signal is exactly $1/2$ completing the proof. □

Theorem 1 implies that any attack against the SQRNG protocol (whose security we want to prove) can be translated to an attack against the e-QRNG protocol which: (1) produces the same quantum system for Alice and Eve conditioned on Alice accepting the e-QRNG state (thus any entropy computation will be identical and any observed statistics will also be identical in the accepting case); and (2) the probability of accepting is strictly positive and known. Note that, even though the e-QRNG protocol is highly inefficient, this is not relevant as we are only interested in bounding the quantum entropy of the e-QRNG protocol conditioned on a non-abort. This will translate directly to a bound on the entropy of the SQRNG protocol (which never aborts, unless Alice determines the noise is too high - a threshold which we can compute later). Thus, even though the e-QRNG protocol is highly inefficient, this does not matter as it is only a theoretical tool for the security proof and not an actual protocol to run in practice. Note, also, that there are many more attacks against the e-QRNG protocol, including attacks which would cause it to always abort; however analyzing those "denial of service" attacks are not relevant as they would never appear in the SQRNG protocol.

B. Secure Bit Rate Analysis

Our goal is to derive an asymptotic bit generation rate for the SQRNG protocol. Consider a run of the SQRNG protocol where Eve employed some (unknown) attack described by $\mathcal{E}$, and Θ was Alice's choice of operations resulting in state $|\psi_{SQRNG}\rangle$. From Theorem 1, there exists an equivalent quantum state $|\psi\rangle$ produced by the e-QRNG protocol. We will derive a bit generation rate for this e-QRNG state which will translate directly to a bit-generation rate for the SQRNG protocol. Since $\mathcal{E}$ and Θ were arbitrary, our method will work for any attack and choice of Θ for the SQRNG protocol thus proving the SQRNG protocol secure.

We first assume collective attacks for the SQRNG protocol (and thus, by condition (3) of Theorem 1 also for the e-QRNG protocol state); namely, the state $|\psi\rangle$ may be described as a product state $|\psi\rangle = |\mu\rangle^{\otimes N}$ with the probability of accepting any particular signal state $|\mu\rangle$ is $1/2$ (i.e., the probability of Alice observing a $|+\rangle$ in $|\mu\rangle$ is $1/2$) .

Now, let's consider an individual signal state $|\mu\rangle$. We may write this in the most general way as follows:

$$
|\mu\rangle = \sum_{a,c\in\{0,1\}} |a,c\rangle_{AC} \otimes |e_{a,c}\rangle_E , \tag{6}
$$

where the $|e_{a,c}\rangle$ states are arbitrary (not necessarily normalized nor orthogonal) states in Eve's ancilla. Note that, when $c = 0$ in the summation we actually mean a state of $|+\rangle$ while $c = 1$ implies $|-\rangle$. Our goal now is to compute a bound on $S(A|E)_\mu$ since this will give us our bit-rate according to Equation 2. Our bound, of course, must be a function only of those statistics which may be observed by the users in the event the protocol does not abort.

First, consider $P^{AC}_{a,c} = Pr(A = a \wedge C = c)$. From Equation 6, this is easily seen to be $P^{AC}_{a,c} = \langle e_{a,c}|e_{a,c}\rangle$. Ideally, this should be $1/4$, though we do not assume anything about these values in our proof only that they may be observed. Next, consider the $P_{+|acc} = Pr(C = \text{“}+\text{”}|\text{accept})$. Changing basis, we have:

$$
|\mu\rangle = \frac{1}{\sqrt{2}} |+\rangle_A \otimes \left(\sum_c |c\rangle \left(|e_{0,c}\rangle + |e_{1,c}\rangle\right) \right) + \frac{1}{\sqrt{2}} |-\rangle (\cdots)
$$

Since by Theorem 1 we know the probability of accepting (i.e., measuring a $|+\rangle$) is $1/2$ for each signal state independently, the conditional state collapses to:

$$
|+\rangle_A \otimes \left[|0\rangle_C \left(|e_{0,0}\rangle + |e_{1,0}\rangle\right) + |1\rangle_C \left(|e_{0,1}\rangle + |e_{1,1}\rangle\right) \right] ,
$$

from which it is clear that $P_{+|acc} = \langle e_{0,0}|e_{0,0}\rangle + \langle e_{1,0}|e_{1,0}\rangle + 2Re\,\langle e_{0,0}|e_{1,0}\rangle$. Similarly, we may define $P_{-|acc}$ and find it to be $P_{-|acc} = \langle e_{0,1}|e_{0,1}\rangle + \langle e_{1,1}|e_{1,1}\rangle + 2Re\,\langle e_{0,1}|e_{1,1}\rangle$. Note that these probabilities coincide directly with the probability the server sends the message "+"/"−" conditioned on Alice choosing `Reflect` in the SQRNG case.

We are now in a position to compute the bit generation rate. From Equation 6, the system, conditioning on Alice actually

distilling a random bit (namely she measures the A register of $|\mu\rangle$ in the Z basis) is easily found to be:

$$\rho_{ACE} = [\mathbf{0}]_A \otimes \left(\sum_c [\mathbf{c}, \mathbf{e_{0,c}}] \right) + [\mathbf{0}]_A \otimes \left(\sum_c [\mathbf{c}, \mathbf{e_{1,c}}] \right) \quad (7)$$

Of course, Eve has access to the C and and E registers (since the trusted server makes its measurement results public); thus to compute the bit generation rate, we need to bound $S(A|CE)$. Using Theorem 1 from [49], along with our analysis above of Eve's inner-products, we have the following lower-bound:

$$S(A|CE) \geq \left(P_{0,0}^{AC} + P_{1,0}^{AC}\right) \cdot \left(h\left[\frac{P_{0,0}^{AC}}{P_{0,0}^{AC} + P_{1,0}^{AC}} \right] - h\left[\lambda_0\right] \right) \quad (8)$$

$$+ \left(P_{0,1}^{AC} + P_{1,1}^{AC}\right) \cdot \left(h\left[\frac{P_{0,1}^{AC}}{P_{0,1}^{AC} + P_{1,1}^{AC}} \right] - h\left[\lambda_1\right] \right),$$

where:

$$\lambda_c = \frac{1}{2}\left(1 + \frac{\sqrt{(P_{0,c}^{AC} - P_{1,c}^{AC})^2 + 4Re^2\left\langle e_{0,c}|e_{1,c}\right\rangle}}{P_{0,c}^{AC} + P_{0,c}^{AC}} \right). \quad (9)$$

The inner products needed to compute λ_c may be determined from $P_{c|acc}$. For instance, $2Re\left\langle e_{0,0}|e_{1,0}\right\rangle = P_{+|acc} - P_{0,0}^{AC} - P_{1,0}^{AC}$. This gives us everything we need to compute the quantum entropy of the e-QRNG state conditioned on the protocol not aborting. Since the state for the entanglement based protocol conditioned on not aborting is identical to that of the SQRNG protocol of the given, but arbitrary, attack and, furthermore, since all observable statistics in that case are also identical, the computed bit generation rate applies to the SQRNG protocol as desired.

The above rate applies to collective attacks against the SQRNG protocol in the asymptotic scenario. However, for general attacks, the constructed e-QRNG state may be made permutation invariant in the usual way [39] and then, de Finetti style arguments [50] may be used to promote the above analysis to general attacks.

V. Evaluation

To evaluate the bit generation rate of our SQRNG protocol, one only needs to observe those probability values appearing in the entropy expression Equation 8. For the purposes of this paper, we simulate observable probability values assuming the source noise is modeled by a depolarization channel acting independently on each qubit and that the server is honest. Note that this assumption is only used in this section to determine values for those probability values appearing in our bit generation expression above. That is, this assumption is *only used here for evaluation purposes and is not a required assumption in our security proof above.* Normally, one would simply observe the actual probability values; however since we are performing a theoretical analysis and not an experiment, we must simulate "reasonable" values for these probabilities. Depolarization channels are the most common ones evaluated theoretically.

Such a channel takes a qubit quantum state ρ and maps it to $\mathcal{D}_{\mathcal{Q}} : \rho \mapsto (1-2Q)\rho + Q \cdot I$, where I is the identity operator (an equally mixed state of $|+\rangle$ and $|-\rangle$). Of course, since we have a two-way channel, we will need to worry about the noise and behavior of the channel in both directions. For this, we consider two scenarios: *independent* channels and *dependent* ones. The distinction only matters when Alice chooses `Reflect` since, then, it is possible that noise in the reverse channel depends on noise in the forward one. When Alice chooses `Measure-Resend`, the qubit is measured so any channel dependence is broken. More formally, we parameterize the noise in the forward and reverse channels by Q. But in the event Alice chooses `Reflect`, the joint forward/reverse channel is modeled as a depolarization channel with parameter Q_{FR}. For independent channels, the noise in the reverse channel acts independently of the forward for reflection events and, so, we set $Q_{FR} = 2Q(1-Q)$. In the case of dependent channels, the noise in the reverse channel can depend on the forward and so we set $Q_{FR} = Q$. Note that this behavior often appears in fiber implementations where any phase noise picked up in the forward direction is "undone" in the reverse channel assuming the photon is reflected back [51], [52].

From this parameterization, we may determine values for the needed probability values. In particular, we will assume the state arriving at Alice's lab is of the form $\mathcal{D}_Q([+])$. From this, it is clear that the probability of Alice measuring either a $|0\rangle$ or $|1\rangle$ is $1/2$. Conditioned on such a measurement, a qubit returns to the server; the state, then, arriving at the server will be $\mathcal{D}_Q([\mathbf{a}])$, where $a \in \{0,1\}$ is Alice's measurement outcome. Since we are simulating an honest server in this section and a noisy channel, the probability that the server sends the message "+" is also $1/2$. Thus, we find $P_{a,c}^{AC} = 1/4$ for all a, c.

Next, consider the case of a reflection. In this case, the state returning to the server is of the form $\mathcal{D}_{Q_{FR}}([+])$. From this, we see that $P_{+|acc} = (1 - Q_{FR})$. Note that $P_{+|acc}$ is technically defined only for the e-QRNG protocol, however from Theorem 1 it exactly coincides with the probability that the (potentially adversarial) server sends the message "+" conditioned on Alice choosing `Reflect` in the SQRNG case. This gives us everything we need to compute Equation 8. In fact, under these conditions, our entropy bound simplifies significantly to:

$$S(A|CE) \geq 1 - h\left(1 - Q_{FR}\right). \quad (10)$$

This can be seen by noting that all $P_{a,c}^{AC}$ are $1/4$ and that $\lambda_0 = \lambda_1 = 1 - Q_{FR}$ since $4Re^2\left\langle e_{0,0}|e_{1,0}\right\rangle = (1 - Q_{FR} - 1/2)^2$ and $4Re^2\left\langle e_{0,1}|e_{1,1}\right\rangle = (-Q_{FR} + 1/2)^2$. A graph of the resulting bit generation rate is shown in Figure 3. Rather interestingly, in the event of a dependent channel, the SQRNG protocol matches the bit-generation rate of the fully-quantum QRNG protocol introduced in [5], at least in the asymptotic ideal qubit scenario.

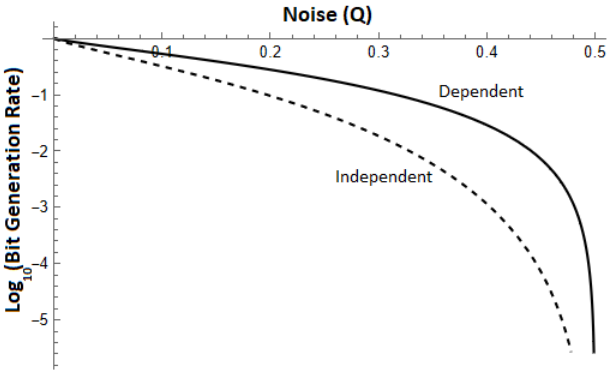

Fig. 3. Showing the bit-generation rate of our SQRNG protocol under depolarization noise. Both the dependent and independent channel cases are plotted.

VI. Closing Remarks

We developed a novel, and to our knowledge the first, semi-quantum random number generation protocol. We also derived a rigorous information theoretic proof of security for the protocol, by reducing it to an entanglement-based protocol and deriving a bound on its random bit generation rate. Our evaluations showed that the bit-generation rate can match that of other fully-quantum QRNG protocols, at least in the asymptotic ideal-qubit scenario. Combined with recent research in semi-quantum key distribution, which shows that the asymptotic behavior of SQKD protocols can match BB84 [38], our work in this paper shows similarly optimistic results for the QRNG case.

Many interesting future problems remain open. Of great importance would be to study SQRNG protocols under more practical considerations. Here certain practical device attacks are problematic such as the photon-tagging attack [43], [44]. However, mirror style devices may mitigate this [36]. Adapting mirror-style devices to the SQRNG case would be an interesting problem. Also of importance would be deriving a bound on the random bit generation rate in the finite signal setting (as opposed to the asymptotic case considered here). Our reduction Theorem 1 applies here, however when analyzing the finite key scenario, one requires bounds on the quantum min entropy which is harder to derive. Thus, we leave this as an open problem, though our reduction in Theorem 1 should prove a valuable tool in that investigation.

Acknowledgment

WOK would like to acknowledge support from the NSF under grant number 2413644.

References

[1] Roger Colbeck and Adrian Kent. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and Theoretical*, 44(9):095305, 2011.

[2] Stefano Pironio and Serge Massar. Security of practical private randomness generation. *Physical Review A*, 87(1):012336, 2013.

[3] Yang Liu, Xiao Yuan, Ming-Han Li, Weijun Zhang, Qi Zhao, Jiaqiang Zhong, Yuan Cao, Yu-Huai Li, Luo-Kan Chen, Hao Li, et al. High-speed device-independent quantum random number generation without a detection loophole. *Physical review letters*, 120(1):010503, 2018.

[4] Peter Bierhorst, Emanuel Knill, Scott Glancy, Yanbao Zhang, Alan Mink, Stephen Jordan, Andrea Rommal, Yi-Kai Liu, Bradley Christensen, Sae Woo Nam, et al. Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature*, 556(7700):223–226, 2018.

[5] Giuseppe Vallone, Davide G Marangon, Marco Tomasin, and Paolo Villoresi. Quantum randomness certified by the uncertainty principle. *Physical Review A*, 90(5):052327, 2014.

[6] Jing-Yan Haw, SM Assad, AM Lance, NHY Ng, V Sharma, Ping Koy Lam, and Thomas Symul. Maximization of extractable randomness in a quantum random-number generator. *Physical Review Applied*, 3(5):054004, 2015.

[7] Bingjie Xu, Ziyang Chen, Zhengyu Li, Jie Yang, Qi Su, Wei Huang, Yichen Zhang, and Hong Guo. High speed continuous variable source-independent quantum random number generation. *Quantum Science and Technology*, 4(2):025013, 2019.

[8] Marco Avesani, Davide G Marangon, Giuseppe Vallone, and Paolo Villoresi. Source-device-independent heterodyne-based quantum random number generator at 17 gbps. *Nature communications*, 9(1):1–7, 2018.

[9] David Drahi, Nathan Walk, Matty J Hoban, Aleksey K Fedorov, Roman Shakhovoy, Akky Feimov, Yury Kurochkin, W Steven Kolthammer, Joshua Nunn, Jonathan Barrett, et al. Certified quantum random numbers from untrusted light. *Physical Review X*, 10(4):041048, 2020.

[10] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. Quantum random number generators. *Reviews of Modern Physics*, 89(1):015004, 2017.

[11] 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.

[12] Stefano Pirandola, Ulrik L Andersen, Leonardo Banchi, Mario Berta, Darius Bunandar, Roger Colbeck, Dirk Englund, Tobias Gehring, Cosmo Lupo, Carlo Ottaviani, et al. Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4):1012–1236, 2020.

[13] Omar Amer, Vaibhav Garg, and Walter O Krawec. An introduction to practical quantum key distribution. *IEEE Aerospace and Electronic Systems Magazine*, 36(3):30–55, 2021.

[14] Michel Boyer, Dan Kenigsberg, and Tal Mor. Quantum key distribution with classical bob. *Phys. Rev. Lett.*, 99:140501, Oct 2007.

[15] Michel Boyer, Ran Gelles, Dan Kenigsberg, and Tal Mor. Semiquantum key distribution. *Phys. Rev. A*, 79:032341, Mar 2009.

[16] Xiangfu Zou, Daowen Qiu, Lvzhou Li, Lihua Wu, and Lvjun Li. Semiquantum-key distribution using less than four quantum states. *Physical Review A*, 79(5):052312, 2009.

[17] Walter O Krawec. Restricted attacks on semi-quantum key distribution protocols. *Quantum Information Processing*, 13(11):2417–2436, 2014.

[18] Omar Amer and Walter O Krawec. Semiquantum key distribution with high quantum noise tolerance. *Physical Review A*, 100(2):022319, 2019.

[19] 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 Journal of Theoretical Physics*, 56(8):2659–2670, 2017.

[20] Walter O Krawec. Mediated semiquantum key distribution. *Physical Review A*, 91(3):032323, 2015.

[21] 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.

[22] Chrysoula Vlachou, Walter Krawec, Paulo Mateus, Nikola Paunković, and André Souto. Quantum key distribution with quantum walks. *Quantum Information Processing*, 17(11):1–37, 2018.

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

[24] Qin Li, Wai Hong Chan, and Dong-Yang Long. Semiquantum secret sharing using entangled states. *Physical Review A*, 82(2):022303, 2010.

[25] Jason Lin, Chun-Wei Yang, Chia-Wei Tsai, and Tzonelih Hwang. Intercept-resend attacks on semi-quantum secret sharing and the improvements. *International Journal of Theoretical Physics*, 52(1):156–162, 2013.

[26] Jian Wang, Sheng Zhang, Quan Zhang, and Chao-Jing Tang. Semi-quantum secret sharing using two-particle entangled state. *International Journal of Quantum Information*, 10(05):1250050, 2012.

[27] XiangFu Zou and DaoWen Qiu. Three-step semiquantum secure direct communication protocol. *Science China Physics, Mechanics & Astronomy*, 57(9):1696–1702, 2014.

[28] 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):1–8, 2018.

[29] 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.

[30] 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.

[31] Zhenbang Rong, Daowen Qiu, Paulo Mateus, and Xiangfu Zou. Mediated semi-quantum secure direct communication. *Quantum Information Processing*, 20(2):1–13, 2021.

[32] 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.

[33] Ye Chongqiang, Li Jian, Chen Xiubo, and Tian Yuan. Efficient semi-quantum private comparison without using entanglement resource and pre-shared key. *Quantum Information Processing*, 20(8):1–19, 2021.

[34] 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.

[35] Nan-Run Zhou, Kong-Ni Zhu, Wei Bi, and Li-Hua Gong. Semi-quantum identification. *Quantum Information Processing*, 18(6):1–17, 2019.

[36] Michel Boyer, Matty Katz, Rotem Liss, and Tal Mor. Experimentally feasible protocol for semiquantum key distribution. *Physical Review A*, 96(6):062335, 2017.

[37] Francesco Massa, Preeti Yadav, Amir Moqanaki, Walter O Krawec, Paulo Mateus, Nikola Paunković, André Souto, and Philip Walther. Experimental semi-quantum key distribution with classical users. *Quantum*, 6:819, 2022.

[38] Hasan Iqbal and Walter O Krawec. Semi-quantum cryptography. *Quantum Information Processing*, 19(3):1–52, 2020.

[39] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008.

[40] Marco Tomamichel, Roger Colbeck, and Renato Renner. A fully quantum asymptotic equipartition property. *IEEE Transactions on information theory*, 55(12):5840–5847, 2009.

[41] 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.

[42] Daniela Frauchiger, Renato Renner, and Matthias Troyer. True randomness from realistic quantum devices. *arXiv preprint arXiv:1311.4547*, 2013.

[43] Yong-gang Tan, Hua Lu, and Qing-yu Cai. Comment on "quantum key distribution with classical bob". *Phys. Rev. Lett.*, 102:098901, Mar 2009.

[44] Michel Boyer, Dan Kenigsberg, and Tal Mor. Boyer, kenigsberg, and mor reply:. *Phys. Rev. Lett.*, 102:098902, Mar 2009.

[45] E Brian Davies and John T Lewis. An operational approach to quantum probability. *Communications in Mathematical Physics*, 17(3):239–260, 1970.

[46] Walter O Krawec. Practical security of semi-quantum key distribution. In *Quantum Information Science, Sensing, and Computation X*, volume 10660, pages 33–45. SPIE, 2018.

[47] Julia Guskind and Walter O Krawec. Mediated semi-quantum key distribution with improved efficiency. *Quantum Science and Technology*, 7(3):035019, 2022.

[48] Mark M Wilde. From classical to quantum shannon theory. *arXiv preprint arXiv:1106.1445*, 2011.

[49] Walter O. Krawec. Quantum key distribution with mismatched measurements over arbitrary channels. *Quantum Information and Computation*, 17(3 and 4):209–241, 2017.

[50] Robert König and Renato Renner. A de finetti representation for finite symmetric quantum states. *Journal of Mathematical physics*, 46(12):122108, 2005.

[51] Marco Lucamarini and Stefano Mancini. Quantum key distribution using a two-way quantum channel. *Theoretical Computer Science*, 560:46–61, 2014.

[52] Normand J Beaudry, Marco Lucamarini, Stefano Mancini, and Renato Renner. Security of two-way quantum key distribution. *Physical Review A*, 88(6):062302, 2013.