Semi-Source Independent Quantum Walk Random Number Generation

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

***Abstract*—Semi-source independent quantum random number generators (SI-QRNG) are cryptographic protocols which attempt to extract random strings from quantum sources where the source is under the control of an adversary (but with known dimension) while the measurement devices are fully characterized. This represents a middle-ground between fully-trusted and full-device independence, allowing for fast bit-generation rates with current-day technology, while also providing a strong security guarantee. In this paper we analyze a SI-QRNG protocol based on quantum walks and develop a proof of security. We derive a novel entropic uncertainty relation for this application which is necessary since standard relations actually fail in this case.**

I. Introduction

Random number generation is an important process for a variety of application domains. Due to the intrinsic randomness of quantum processes, quantum random number generation (QRNG) is an important field of study within quantum information science. By now, cryptographically secure QRNG protocols are well studied under a variety of security models ranging from the "fully trusted device" scenario (whereby all devices used, sources and measurements, are fully characterized) to the "fully device independent" scenario (where all devices used are not trusted) [1], [2]. Clearly from a cryptographic point of view, DI-QRNG protocols are the desirable ideal due to their minimal assumptions needed for security. However, though experimental progress has been rapidly improving, the bit-rates of such protocols cannot compare to other models [3], [4]. As a compromise, the *source independent* (SI) model was introduced in [5] whereby measurement devices are characterized (though not necessarily ideal) whereas the source is under the control of the adversary. One may envision the source being a quantum server, providing a service to users who wish to distill cryptographically secure random strings without trusting the server (e.g., the server may be adversarial). The SI model affords fast experimental bit generation rates [6] (with a recent paper discussing an implementation with a rate over 8Gb/s [7]) along with fascinating potential applications, including the use of sunlight as a source [8]. For a survey of QRNG protocols, the reader is referred to [9]. Note that we are actually considering a semi-source independent model where the dimension of the source is known but no other assumptions are made (this is exactly the model introduced in [5]).

Outside of QRNG's, quantum walks (QW), the quantum analogue of classical random walks, are a highly important process in quantum computation [10], [11], [12], [13] and, recently, in quantum cryptography [14], [15], [16], [17]. Recently, a QW-based random number generation protocol was analyzed in [18], though a rigorous security analysis was not done. In this paper, we revisit that protocol, minimally changing it to be a SI-QRNG protocol, and prove its security. To our knowledge, this is the first SI-QRNG protocol with provable composable security based on quantum walks (we use Renner's framework for composability in quantum cryptography [19]). We note that the security analysis of this protocol is not trivial. Due to certain simplifications we make to allow for an easier potential experimental implementation, prior tools are not immediately applicable (though we do not consider experimental concerns in this work, we keep them in mind when developing the protocol). In this work we develop an alternative entropic uncertainty relation which may also hold applications in other quantum cryptographic protocols.

Naturally, QW's are random processes and, so, at first glance designing and proving secure, a QW-QRNG protocol seems a trivial task. Indeed, the following protocol is a trivial solution to the problem with an "easy" (using modern information theoretic tools) security proof in the SI model: (1) First, a source prepares a state $|\psi_{0,0}\rangle^{\otimes(n+m)}$ where $|\psi_{0,0}\rangle$ is some quantum walker state. While we discuss this in detail later, for now it suffices to consider $|\psi_{0,0}\rangle = W|0,0\rangle$ where W is a unitary operator and $|0,0\rangle$ lives in some Hilbert space of dimension $2P$. This state is sent to Alice. (2) Second, Alice chooses a random subset of size m and measures the systems indexed by this subset in the "quantum walk basis", namely the orthonormal basis $\{W|0,0\rangle, W|0,1\rangle, \cdots, W|1,P-1\rangle\}$. Ideally, this measurement should always produce the zeroth state of this basis. The remaining n walker systems are measured in the computational basis $\{|0,0\rangle, |0,1\rangle, \cdots, |1,P-1\rangle\}$. The first outcome is used to test the fidelity of the received state while the second is used as a raw-random string. This string is then further processed through a privacy amplification process, the output of which is the final cryptographic random string.

Indeed this protocol can be proven secure in a very straightforward manner using entropic uncertainty [20], [21], [22]. However, there are two complications with the protocol itself. First, it would require the ability for Alice to perform a full basis measurement in the quantum-walk basis (namely, she would need to distinguish all states of the form $W|c,x\rangle$). This

might require complex optics to do experimentally. Second, for the randomness generation measurement, she needs to be able to perform a measurement in the full coin and position basis, namely a measurement that can distinguish all states of the form $|c, x\rangle$. Our goal is to analyze a far simpler protocol, building off of the one from [18]. The protocol will only require Alice to be able to distinguish a single walker state, namely $W|0,0\rangle$ from any other; and, second, she need only perform a measurement of the position of the walk for randomness, and she need not also determine the state of the coin itself. The second restriction is identical to the protocol in [18] though, since they did not consider the source independent model, they did not require any other test. We add only this minimal test ability, namely the ability to distinguish a single quantum walk state from the $2P-1$ others in the walk basis, to ensure a cryptographically secure protocol.

Interestingly, standard entropic uncertainty relations of the form [21]:

$$H_{\infty}^{\epsilon}(A|E)+H_{max}^{\epsilon}(A|B) \geq -\log \max_{x,y} ||\sqrt{M_x}\sqrt{N_y}||_{op}^2, \quad (1)$$

where $\{M_x\}$ and $\{N_y\}$ are the two POVMs used in the protocol, are not applicable and can only yield the trivial bound. Thus a new approach is required to analyze this QW-QRNG protocol. We develop the approach in this paper using a technique of quantum sampling as introduced by Bouman and Fehr in [23] and used by us recently to develop novel *sampling-based entropic uncertainty relations* [24], [25]. In fact, our proof is similar, though with suitable modifications needed for this scenario and, since the result does not follow immediately from our previous analysis, it is necessary to state here.

We make two primary contributions in this paper. First, we analyze for the first time, a QW-QRNG protocol introduced in [18] from a cryptographic perspective. We adapt the protocol sufficiently, and minimally, so as to produce a secure system and prove it is secure in the SI model. This represents, to our knowledge, the first QRNG protocol based on quantum walks in the SI model of security and shows even greater application of quantum walks to other cryptographic primitives. Second, we develop a proof of security to handle this scenario when standard approaches are not immediately applicable. Our security method may also be applicable to other protocols of this nature where standard relations such as Equation 1 cannot be used directly. Our proof utilizes the method of quantum sampling by Bouman and Fehr [23], augmented with techniques we developed in [24], [25] for entropic uncertainty, showing even more potential applications of these methods to complex security analyses. We actually think this second contribution the more significant as it shows how this framework of quantum sampling may be used to tackle cryptographic problems that standard methods would fail to analyze successfully, thus opening the door to a potential wider range of applications. Our proof is based on techniques in our prior work in [25] however with suitable modifications to handle the quantum measurements that arise in the protocol. In particular, the main result from [25] cannot be applied directly here. Modifications to the proof are required to handle the measurement scenario we introduce in this paper, and the technique we use may see broad application elsewhere when proving security of protocols for which standard entropic uncertainty relations fail.

II. Notation and Definitions

We now introduce some basic definitions and notation that we will use throughout this paper. By $\mathcal{A}_d$ we mean a d-dimensional alphabet, namely $\mathcal{A}_d = \{0, 1, \cdots, d-1\}$. Given a word $q \in \mathcal{A}_d^N$ and some subset $t \subset \{1, 2, \cdots, N\}$, we write q_t to mean the substring of q indexed by t (i.e., those characters in q indexed by $i \in t$). We write q_{-t} to mean the substring indexed by the complement of t. The *Hamming Weight* of q is denoted $wt(q) = |\{i \ : \ q_i \neq 0\}|$ while the *relative Hamming weight* is denoted $w(q) = wt(q)/|q|$.

A *density operator* is a Hermitian positive semi-definite operator of unit trace acting on some Hilbert space $\mathcal{H}$. Given a pure quantum state $|\psi\rangle \in \mathcal{H}$ we write $[\psi]$ to mean $|\psi\rangle\langle\psi|$.

The Shannon entropy of a random variable X is denoted by $H(X)$ while the d-ary entropy function is denoted $h_d(x)$. This function is defined to be $h_d(x) = x\log_d(d-1) - x\log_d x - (1-x)\log_d(1-x)$. We also define the *extended d-ary entropy function* to be $\bar{H}_d(x)$ which equals $h_d(x)$ for all $x \in [0, 1 - 1/d]$ but is 0 for all $x < 0$ and is 1 for all $x > 1 - 1/d$.

Let ρ_{AE} be a quantum state (density operator) acting on some Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_E$. The *conditional quantum min entropy* [19] is defined to be: $H_{\infty}(A|E)_{\rho} = \sup_{\sigma_E} \max(\lambda \in \mathbb{R} \ : \ 2^{-\lambda} I_A \otimes \sigma_E - \rho_{AE} \geq 0)$, where I_A is the identity operator on $\mathcal{H}_A$. Note that if the E system is trivial and the A portion is classical (namely $\rho_A = \sum_x p_x[\mathbf{x}]$) then it is easy to show that $H_{\infty}(A) = -\log \max_x p_x$. If the E portion is classical, namely $\rho_{AE} = \sum_e p_e \rho_A^e \otimes [\mathbf{e}]$, then it can be shown that:

$$H_{\infty}(A|E)_{\rho} \geq \min_e H_{\infty}(A)_{\rho^e}. \quad (2)$$

Finally, the *smooth conditional min entropy* is defined to be [19]: $H_{\infty}^{\epsilon}(A|E)_{\rho} = \sup_{\sigma \in \Gamma_{\epsilon}(\rho)} H_{\infty}(A|E)_{\sigma}$, with: $\Gamma_{\epsilon}(\rho) = \{\sigma \ : \ ||\sigma - \rho|| \leq \epsilon\}$. Here, $||X||$ is the trace distance of operator X.

Given a classical-quantum state ρ_{AE}, let σ_{KE} be the result of a *privacy amplification* process on the A register of this state. Namely, a process of mapping the A register through a randomly chosen two-universal hash function. If the output of this hash function is ℓ bits long, then it was shown in [19] that:

$$\left|\left|\sigma_{KE} - I_K/2^{\ell} \otimes \sigma_E\right|\right| \leq 2^{-\frac{1}{2}(H_{\infty}^{\epsilon}(A|E)_{\rho} - \ell)} + 2\epsilon. \quad (3)$$

A. Quantum Random Walks

In this work we will consider discrete-time quantum walks on a cycle graph [26]. Such a process involves a Hilbert space $\mathcal{H}_W = \mathcal{H}_C \otimes \mathcal{H}_P$ where $\mathcal{H}_C$ is the two-dimensional *coin space* and $\mathcal{H}_P$ is the P-dimensional *position space*. The walk begins with the walker at some initial position $|c, x\rangle$ (e.g., $|0,0\rangle$) from which a *walk operator* is applied T times.

The walk operator first applies a unitary operator on the coin space (for us, we only consider the Hadamard operator here, though other possibilities exist of course). Following this a *shift operator* is applied S which maps $|0,x\rangle \mapsto |0,x+1\rangle$ and $|1,x\rangle \mapsto |1,x-1\rangle$ where all arithmetic in the position space is done modulo P. Let $W = S \cdot (H \otimes I_P)$ be the walk operator; then, after T steps, the walker evolves to state $W^T |c,x\rangle$. Generally, at this point, a measurement may be done on the position space causing a collapse at one of the P spots.

Later, we will denote by $|w_{c,x}\rangle$ to mean the evolved state $W^T |c,x\rangle$. We will also use $|w_i\rangle$ when appropriate, using the natural relationship of tuples (c,x) to integers i, with $(0,0)$ being the first index $i=0$. Finally, given a walk state $|w_{c,x}\rangle$ we use the notation $Pr_W(|w_{c,x}\rangle \to z)$ to denote the probability that the walker is observed at position z after measurement. Namely, $Pr_W(|w_{c,x}\rangle \to z) = \langle w_{c,x}|I_C \otimes [\mathbf{z}]|w_{c,x}\rangle$. Finally, we denote by γ to be the maximal positional probability of the walk which starts at $|0,0\rangle$, namely:

$$\gamma = \max_z Pr_W(|w_{0,0}\rangle \to z). \tag{4}$$

Obviously, this is a function of the walk parameters (the operation W along with the number of steps T).

B. Quantum Sampling

In [23], Bouman and Fehr discovered a fascinating connection linking classical sampling strategies with quantum ones, even when the quantum state is entangled with an environment system (e.g., an adversary). Here we review some of these concepts, however for more details the reader is referred to [23].

Let $q \in \mathcal{A}_d^N$. A classical sampling strategy is a process of choosing a random subset $t \subset \{1,\cdots,N\}$, observing q_t, and estimating the value of some target value of the *unobserved portion*. Here, as in [23], we consider the target value to be the relative Hamming weight. One sampling strategy we will employ consists of choosing a subset t of size $m \leq N/2$ uniformly at random, observing q_t, and outputting $w(q_t)$ as an estimate of the Hamming weight in the unobserved portion. It was shown in [23] that, for $\delta > 0$:

$$\epsilon_\delta^{cl} := \max_{q \in \mathcal{A}_d^N} Pr(q \notin \mathcal{G}_{t,\delta}) \leq 2\exp\left(\frac{-\delta^2 m(n+m)}{m+n+2}\right), \tag{5}$$

where the probability is over all choices of subsets t and $\mathcal{G}_{t,\delta}$ is the set of all "good" words for which this sampling strategy is guaranteed to produce a δ-close estimate of the Hamming weight of the unobserved portion, namely:

$$\mathcal{G}_{t,\delta} = \{q \in \mathcal{A}_d^N \ : \ |w(q_t) - w(q_{-t})| \leq \delta\}.$$

The value ϵ_δ^{cl} is the error probability of the classical sampling strategy (the "cl" superscript is used to refer to a classical sampling strategy).

The main result from [23] shows how to promote such a classical strategy to a quantum one in a way that the failure probabilities of the quantum strategy are functions of the classical ones. Fix a basis $\{|0\rangle,\cdots,|d-1\rangle\}$ (the exact choice may be arbitrary but then fixed - later when using this result, we will use the walk basis $\{W^T|c,x\rangle\}_{c,x}$). Define:

$$span(\mathcal{G}_{t,\delta}) = span(|i_1 i_2 \cdots i_N\rangle \ : \ |w(i_t) - w(i_{-t})| \leq \delta).$$

This is the quantum analogue of the "good set" of classical words. In particular, note that if given a state $|\phi\rangle_{AE} \in span(\mathcal{G}_{t,\delta}) \otimes \mathcal{H}_E$, then if a measurement in the given basis were performed on those qudits indexed by t leading to outcome $q \in \mathcal{A}_d^m$, it must hold that the remaining state is a superposition of the form: $|\phi_{t,q}\rangle = \sum_{i\in J} \alpha_i |i,E_i\rangle$, where $J \subset \{i \in \mathcal{A}_d^{N-m} \ : \ |w(i) - w(q)| \leq \delta\}$.

The main result from [23], reworded for our application here, was to prove the following theorem:

Theorem 1. (Modified from [23]): Let $\delta > 0$. Given the above classical sampling strategy and an arbitrary quantum state $|\psi\rangle_{AE}$, there exists a collection of "ideal states" $\{|\phi^t\rangle\}_t$, indexed over all possible subsets the sampling strategy may choose, such that each $|\phi^t\rangle \in span(\mathcal{G}_{t,\delta}) \otimes \mathcal{H}_E$ and:

$$\frac{1}{2}\left|\left|\frac{1}{T}\sum_t [\mathbf{t}] \otimes [\psi] - \frac{1}{T}\sum_t [\mathbf{t}] \otimes \left[\phi^{\mathbf{t}}\right]\right|\right| \leq \sqrt{\epsilon_\delta^{cl}}. \tag{6}$$

where $T = \binom{N}{m}$ and the sum is over all subsets of size m.

Note that the result requires a fixed basis of reference (from which to define $\mathcal{G}_{t,\delta}$).

III. The Protocol

We consider a QW-QRNG protocol introduced in [18]. That protocol was not analyzed rigorously from a cryptographic standpoint and, in fact, would not be secure in the SI model. We modify that protocol, adding a minimal testing ability for Alice, and later show it is secure in the SI model of security. The protocol operates as follows:

Public Parameters: The quantum walk setting, namely the dimension of the position space P (defining the overall Hilbert space of one walker $\mathcal{H}_W = \mathcal{H}_C \otimes \mathcal{H}_P$), the walk operator W, and the number of steps to evolve by, T.

Source: A source, potentially adversarial, produces a quantum state $|\psi_0\rangle \in \mathcal{H}_A \otimes \mathcal{H}_E$, where $\mathcal{H}_A \cong \mathcal{H}_W^{\otimes N}$. If the source is honest, the state prepared should be of the form:

$$|\psi_0\rangle = |w_0\rangle^{\otimes N} \otimes |0\rangle_E,$$

namely, N copies of the walker state $|w_0\rangle = |w_{0,0}\rangle = W^T|0,0\rangle$ unentangled with Eve.

User: Alice chooses a random subset t of size m and measures those walker states using POVM $\mathcal{W} = \{[\mathbf{w_0}], I - [\mathbf{w_0}]\} = \{W_0, W_1\}$ resulting in outcome $q \in \{0,1\}^m$ (equivalently, she reverses the quantum walk and observes whether the initial state was $|0,0\rangle$ or anything else). The remaining states she measures using POVM $\mathcal{Z} = \{I_C \otimes [\mathbf{j}]\}_{j=0}^{P-1} = \{Z_0, Z_1, \cdots, Z_{P-1}\}$ resulting in outcome $r \in \mathcal{A}_P^n$, where $n = N - m$.

Postprocessing: Finally, Alice applies privacy amplification to r, producing a final random string of size ℓ. As proven in [27], the hash function used for privacy amplification need only be

chosen randomly once and then reused for each run of the protocol for a QRNG protocol of this nature.

The goal of this protocol is to ensure that, for a given ϵ_{PA} set by the user, after privacy amplification the resulting string is ϵ_{PA} close to an ideal random string, uniformly generated and independent of any adversary system. Using Equation 3, this involves finding a bound on the quantum min-entropy. Note that, for the given POVMs, it is straight-forward to check that $\max_{x,y} ||\sqrt{W_x}\sqrt{Z_y}||_{op}^2 = 1$ and so Equation 1 only yields the trivial bound on the min entropy. Thus an alternative approach is required which we develop in the next section.

A. Security Analysis

To prove security, we require a bound on the quantum min entropy from which, using Equation 3, we may compute the number of random bits ℓ which may be extracted from N quantum walk states (prepared by an adversary). We assume the adversary is allowed to create any initial state, possibly entangled with her ancilla, however as in [5], the dimension of the system sent to Alice is known; in our case it is $(2P)^N$, namely, N quantum walker states, each of dimension $2P$. We do not assume anything else about this state (for instance, each of the N walkers may be in different states). Such a scenario also models natural noise and an honest source - considering an adversarial source is more general. Finally, we assume that Alice's measurement devices are fully characterized.

Theorem 2. Let $\epsilon > 0$. After executing the above QW-QRNG protocol and observing outcome q during the test stage (namely, after measuring using $\mathcal{W}$), it holds that, except with probability at most $\epsilon^{1/3}$ (where the probability here is over the choice of sample subset and observation q), the protocol outputs a final secret string of size:

$$\ell = -\eta_q \log_2 \gamma - n \cdot \frac{\bar{H}_{2P}(w(q)+\delta)}{\log_{2P}(2)} - 2\log_2 \frac{1}{\epsilon} - \log_2 \binom{N}{m},$$

which is $(5\epsilon + 4\epsilon^{1/3})$-close to an ideal random string (i.e., one that is uniformly generated and independent of any adversary system as in Equation 3). Above, $\eta_q = (N-m)(1-w(q)-\delta)$ and:

$$\delta = \sqrt{\frac{(N+2)\ln(2/\epsilon^2)}{m \cdot N}}. \tag{7}$$

Proof. Fix $\epsilon > 0$ and let $|\psi_0\rangle_{AE}$ be the state the adversarial source Eve creates, sending the A portion to Alice. Using Theorem 1 (with respect to the reference basis $\{W^T|0,0\rangle, \cdots, W^T|1,P-1\rangle\}$), there exist ideal states $\{|\phi^t\rangle\}$, indexed over all subsets $t \subset \{1,2,\cdots,N\}$ of size m, such that $|\phi^t\rangle \in \text{span}(|w_{i_1} w_{i_2} \cdots w_{i_N}\rangle : |w(i_t) - w(i_{-t})| \leq \delta) \otimes \mathcal{H}_E$ and Equation 6 holds. (Note we define $|w_0\rangle = |w_{0,0}\rangle = W^T|0,0\rangle$.) From Equation 5, by setting δ as in Equation 7, we have $\sqrt{\epsilon_\delta^{cl}} = \epsilon$.

We now use a two-step proof method we developed in [24], [25] to utilize quantum-sampling for entropic uncertainty relations. Here, we modify the first step of the proof for this cryptographic application, while the second step remains largely the same. The first step is to analyze the security of the ideal state $\sigma_{TAE} = \frac{1}{T}\sum_t [\mathbf{t}] \otimes \left[\phi^{\mathbf{t}}\right]$. Choosing a subset is equivalent to measuring the T register in σ_{TAE} causing the state to collapse to the given ideal state $|\phi^t\rangle$. At this point, a measurement using $\mathcal{W}$ is made on subset t resulting in some outcome q. The post-measurement state, discarding those systems that were measured, is easily seen to be of the form:

$$\phi_q^t = \sum_{k \in \mathcal{A}_{2P-1}^{wt(q)}} p_k \underbrace{P\left(\sum_{i \in J_q^{(k)}} \alpha_i |w_i\rangle |E_i\rangle\right)}_{\sigma_{AE}^{(k)}}.$$

with $P(z) = zz^*$ and $J_q^{(k)} \subset \{i \in \mathcal{A}_P^n : |w(i) - w(q)| \leq \delta\}$. Recall $n = N - m$.

Let us consider one of the $\sigma_{AE}^{(k)}$ states and perform a measurement using POVM $\mathcal{Z}$ on the remaining A portion. To compute this state, we write a single quantum walker $|w_i\rangle \in \mathcal{H}_W$ as: $|w_i\rangle = |0\rangle|\phi(0,i)\rangle + |1\rangle|\phi(1,i)\rangle$, where $|\phi(c,i)\rangle$ are (not necessarily normalized) states in $\mathcal{H}_P$. Using this notation, after some algebra, we find that the post-measurement state, with Alice storing the outcome $z \in \mathcal{A}_P^n$ in a classical register Z and also tracing out the unmeasured coin register is:

$$\sigma_{ZE}^{(k)} = \sum_{z \in \mathcal{A}_P^n} [\mathbf{z}]_Z \sum_{i,j \in J_q^{(k)}} \alpha_i \alpha_j^* \sum_{c \in \{0,1\}^n} x_{z,c,i} x_{z,c,j}^* \otimes |E_i\rangle\langle E_j|$$

where given a string $c \in \{0,1\}^n$, $z \in \mathcal{A}_P^n$, and $i \in J_q^{(k)}$, we define $x_{c,z,i}$ as: $x_{z,c,i} = \prod_\ell \langle z_\ell | \phi(c_\ell | i_\ell)\rangle$. To compute the min-entropy of this state, we will consider the following density operator:

$$\chi_{ZE} = \sum_z [\mathbf{z}] \sum_{i \in J_q^{(k)}} |\alpha_i|^2 \sum_c |x_{c,z,i}|^2 \otimes [\mathbf{E_i}]$$

Using a proof similar to a lemma in [19] which bounds the min-entropy of a superposition based on the min-entropy of a suitable mixed state, we find that:

$$H_\infty(Z|E)_{\sigma^{(k)}} \geq H_\infty(Z|E)_\chi - \log|J_q^{(k)}|.$$

Note that, though the lemma in [19] is not immediately applicable to the above scenario, the proof is, indeed, identical and so we omit the details for space reasons.

Consider the state χ_{ZEI} where we append an auxiliary system spanned by orthonormal basis $|i\rangle$:

$$\chi_{ZEI} = \sum_{i \in J_q^{(k)}} |\alpha_i|^2 \underbrace{\left(\sum_z [\mathbf{z}] \sum_c |x_{c,z,i}|^2\right)}_{\chi^{(i)}} \otimes [\mathbf{E_i}] \otimes [\mathbf{i}]$$

For strings $z \in \mathcal{A}_P^n$ and $i \in \mathcal{A}_{2P}^n$, let $p(z|w_i)$ be the probability that outcome z is observed if measuring the pure, and unentangled state, state $|w_{i_1} w_{i_2} \cdots w_{i_n}\rangle$ using POVM $\mathcal{Z}$. Simple algebra shows that this is in fact $p(z|w_i) = \sum_c |x_{c,z,i}|^2$. Thus $\chi^{(i)} = \sum_z [\mathbf{z}] p(z|w_i)$. From Equation 2 and treating the joint EI register as a single classical register, we have:

$$H_\infty(Z|E)_\chi \geq H_\infty(Z|EI)_\chi \geq \min_i H_\infty(Z)_{\chi^{(i)}}.$$

Fix a particular $i \in J_q^{(k)}$ and let $\eta = n - wt(i)$ (namely, η is the number of zeros in the string i). Then, it is clear that: $p(z|w_i) \leq \max_{x \in \mathcal{A}_P} Pr_W(|w_0\rangle \to x)^\eta = \gamma^\eta$, where γ was defined in Equation 4. Indeed, any other $Pr_W(|w_i\rangle \to z) \leq 1$ and so we may consider only the $|w_0\rangle$ terms as contributing to this upper-bound. From this, it follows that: $H_\infty(Z)_{\chi^{(i)}} = -\log \max_z p(z|w_i) \geq -\log \gamma^{n-wt(i)}$.

Now, since $i \in J_q^{(k)}$, we know that $wt(i) \leq n(w(q) + \delta)$ and so:

$$H_\infty(Z|E)_\chi \geq H_\infty(Z|EI)_\chi \geq \min_i H_\infty(Z)_{\chi^{(i)}}$$
$$\geq -\log \gamma^{n(1-w(q)-\delta)} = -\eta_q \log \gamma.$$

Finally, we note that $|J_q^{(k)}| \leq d^{n\bar{H}_{2P}(w(q)+\delta)}$ (using the well known bound on the volume of a Hamming ball), we have:

$$H_\infty(Z|E)_\sigma \geq \min_k H_\infty(Z|E)_{\sigma^{(k)}}$$
$$\geq -\eta_q \log_2 \gamma - n \cdot \frac{\bar{H}_{2P}(w(q)+\delta)}{\log_{2P}(2)}$$

Of course, this is the ideal state analysis. However, we may use a similar technique that we employed in [24] for translating this ideal analysis to the real case. Indeed, let $\rho_{ZE}^{t,q}$ be the state of the real system, $|\psi\rangle$, conditioned on the protocol sampling subset t and observing outcome q and let $\sigma_{ZE}^{t,q}$ be the same for the ideal state. If we define: $\Delta_{t,q} = \frac{1}{2}\left|\left|\rho_{ZE}^{t,q} - \sigma_{ZE}^{t,q}\right|\right|$, then, treating $\Delta_{t,q}$ as a random variable over the choice of t and outcome q, it can be shown (see the proof of Theorem 2 in [24] for explicit details) that except with probability $\epsilon^{1/3}$, it holds that $\Delta_{t,q} \leq \epsilon + \epsilon^{1/3}$ where the probability is over the choice of t and outcome q. Thus, by switching to smooth min entropy, we have, except with probability at most $\epsilon^{1/3}$ that $H_\infty^{2\epsilon+2\epsilon^{1/3}}(Z|E)_\rho \geq H_\infty(Z|E)_\sigma$. Privacy amplification (Equation 3, setting the right-hand-side of that equation equal to $\epsilon_{PA} = 5\epsilon + 4\epsilon^{1/3}$, namely twice the smoothening parameter plus an additional ϵ), along with the fact that it requires $\log \binom{N}{m}$, random bits to choose a subset of size m, completes the proof. Note that bounding Equation 3 as we do proves composable security [19] □

Evaluation: We evaluate the performance of our protocol under a variety of position dimensions P. Ordinarily, users would run the protocol and observe q directly; however, to simulate its execution, we will assume the noise follows a depolarization channel with parameter Q. We do this only to evaluate our protocol; furthermore, this noise model is a standard one to evaluate on in simulations. From this, after sampling, Alice will have an expected Hamming weight in her test measurement of $w(q) = Q$. In our evaluations, we will set $\epsilon = 10^{-36}$ which will imply a failure probability, and an ϵ_{PA}-secure string, both on the order of 10^{-12}. We also use a sample size that is the square-root of the total number of signals N, namely $m = \sqrt{N}$. Finally, to evaluate our bit-generation rate, we will require γ (Equation 4). Since the walk settings are chosen by the user, we wrote a program that, for fixed dimension P, found the minimum γ value over all time settings $T = 1, 2, \cdots, 5000$. The evaluation of the bit generation rate of this SI-QW-QRNG protocol, using our analysis in Theorem 2, is shown in Figure 1. A comparison to an alternative SI-QRNG protocol from [28] is shown in Figure 2. Note that as the dimension of the walker increases, the bit-generation rates, even under high noise levels, increases. Interestingly, as shown in Figure 2, depending on the walker dimension, the QW based protocol can sometimes outperform the SI-QRNG protocol from [28] (which is based on mutually unbiased measurements of a highly entangled state).

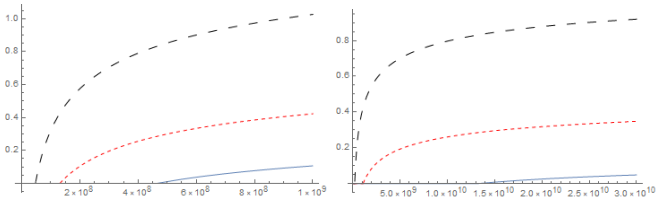

Fig. 1. Random bit generation rates of the QW-QRNG protocol. x-axis: number of signals sent N (from which $m = \sqrt{N}$ are used for sampling); y-axis: random bit-generation rate (namely ℓ/N where ℓ is computed using Theorem 2). Black dashed (top) is $P = 51$; red-dashed (middle) is $P = 11$; blue solid (lowest) is $P = 5$. Left graph is with 15% noise in the source (namely $w(q) = 0.15$); Right graph has 20% noise.

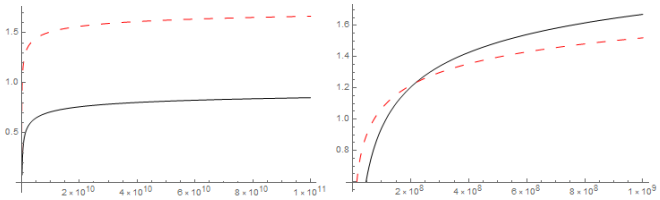

Fig. 2. Comparing the QW-QRNG protocol's bit generation rate (black-solid) with that of the SI-QRNG protocol in [28] (red-dashed). Left: $P = 5$; Right: $P = 51$. In both cases we assume 10% noise in the signal state. For the SI-QRNG protocol's evaluation from [28], we use a dimension of $2P$.

IV. Closing Remarks

In this paper, we modified, minimally, a QRNG protocol from [18], based on quantum walks, to be secure in the semi-source independent (SI) model. Since standard entropic uncertainty relations cannot be directly applied as discussed, we develop an alternative entropic uncertainty relation for this protocol based on our work in [25] but modified to work with this measurement scenario. Our methods may potentially find applications in other difficult to analyze quantum cryptographic protocols. There are important reasons for studying this QW-based protocol. For instance, it is important to harness alternative quantum processes such as quantum-walk states, as it is still unclear what future experimental developments will yield. Second, it is interesting from a theoretical stand-point. Many exciting open problems remain, in particular a more rigorous evaluation of the performance of this QW-QRNG protocol for different walk parameters (such as alternative coin operators) or alternative models (such as history-dependent walks [29], [30], [31], [32]) would be very exciting.

Acknowledgments: WOK would like to acknowledge support from NSF grant number 2006126.

REFERENCES

[1] R. Colbeck and A. Kent, "Private randomness expansion with untrusted devices," *Journal of Physics A: Mathematical and Theoretical*, vol. 44, no. 9, p. 095305, 2011.

[2] S. Pironio and S. Massar, "Security of practical private randomness generation," *Physical Review A*, vol. 87, no. 1, p. 012336, 2013.

[3] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam *et al.*, "Experimentally generated randomness certified by the impossibility of superluminal signals," *Nature*, vol. 556, no. 7700, pp. 223–226, 2018.

[4] Y. Liu, X. Yuan, M.-H. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Y.-H. Li, L.-K. Chen, H. Li *et al.*, "High-speed device-independent quantum random number generation without a detection loophole," *Physical review letters*, vol. 120, no. 1, p. 010503, 2018.

[5] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, "Quantum randomness certified by the uncertainty principle," *Physical Review A*, vol. 90, no. 5, p. 052327, 2014.

[6] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, "Secure heterodyne-based quantum random number generator at 17 gbps," *arXiv preprint arXiv:1801.04139*, 2018.

[7] D. Drahi, N. Walk, M. J. Hoban, A. K. Fedorov, R. Shakhovoy, A. Feimov, Y. Kurochkin, W. S. Kolthammer, J. Nunn, J. Barrett, and I. A. Walmsley, "Certified quantum random numbers from untrusted light," *Phys. Rev. X*, vol. 10, p. 041048, Dec 2020. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevX.10.041048

[8] Y.-H. Li, X. Han, Y. Cao, X. Yuan, Z.-P. Li, J.-Y. Guan, J. Yin, Q. Zhang, X. Ma, C.-Z. Peng *et al.*, "Quantum random number generation with uncharacterized laser and sunlight," *npj Quantum Information*, vol. 5, no. 1, pp. 1–5, 2019.

[9] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Reviews of Modern Physics*, vol. 89, no. 1, p. 015004, 2017.

[10] E. Farhi and S. Gutmann, "Quantum computation and decision trees," *Physical Review A*, vol. 58, no. 2, p. 915, 1998.

[11] A. M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann, and D. A. Spielman, "Exponential algorithmic speedup by a quantum walk," in *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing*, 2003, pp. 59–68.

[12] A. M. Childs, "Universal computation by quantum walk," *Physical review letters*, vol. 102, no. 18, p. 180501, 2009.

[13] N. B. Lovett, S. Cooper, M. Everitt, M. Trevers, and V. Kendon, "Universal quantum computation using the discrete-time quantum walk," *Physical Review A*, vol. 81, no. 4, p. 042330, 2010.

[14] P. P. Rohde, J. F. Fitzsimons, and A. Gilchrist, "Quantum walks with encrypted data," *Physical review letters*, vol. 109, no. 15, p. 150501, 2012.

[15] C. Vlachou, J. Rodrigues, P. Mateus, N. Paunković, and A. Souto, "Quantum walk public-key cryptographic system," *International Journal of Quantum Information*, vol. 13, no. 07, p. 1550050, 2015.

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

[17] S. Srikara and C. Chandrashekar, "Quantum direct communication protocols using discrete-time quantum walk," *Quantum Information Processing*, vol. 19, no. 9, pp. 1–15, 2020.

[18] A. Sarkar and C. Chandrashekar, "Multi-bit quantum random number generation from a single qubit quantum walk," *Scientific reports*, vol. 9, no. 1, pp. 1–11, 2019.

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

[20] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, "The uncertainty principle in the presence of quantum memory," *Nature Physics*, vol. 6, no. 9, pp. 659–662, 2010.

[21] M. Tomamichel and R. Renner, "Uncertainty relation for smooth entropies," *Physical review letters*, vol. 106, no. 11, p. 110506, 2011.

[22] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, "Entropic uncertainty relations and their applications," *Rev. Mod. Phys.*, vol. 89, p. 015002, Feb 2017.

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

[24] W. O. Krawec, "Quantum sampling and entropic uncertainty," *Quantum Information Processing*, vol. 18, no. 12, p. 368, 2019.

[25] ——, "A new high-dimensional quantum entropic uncertainty relation with applications," in *IEEE International Symposium on Information Theory, ISIT 2020*. IEEE, 2020, pp. 1978–1983.

[26] D. Aharonov, A. Ambainis, J. Kempe, and U. Vazirani, "Quantum walks on graphs," in *Proceedings of the thirty-third annual ACM symposium on Theory of computing*, 2001, pp. 50–59.

[27] D. Frauchiger, R. Renner, and M. Troyer, "True randomness from realistic quantum devices," *arXiv preprint arXiv:1311.4547*, 2013.

[28] F. Xu, J. H. Shapiro, and F. N. Wong, "Experimental fast quantum random number generation using high-dimensional entanglement with entropy monitoring," *Optica*, vol. 3, no. 11, pp. 1266–1269, 2016.

[29] P. P. Rohde, G. K. Brennen, and A. Gilchrist, "Quantum walks with memory provided by recycled coins and a memory of the coin-flip history," *Physical Review A*, vol. 87, no. 5, p. 052302, 2013.

[30] M. McGettrick, "One dimensional quantum walks with memory," *Quantum Inf. Comput.*, vol. 10, no. 5, pp. 509–524, 2010.

[31] W. O. Krawec, "History dependent quantum walk on the cycle with an unbalanced coin," *Physica A: Statistical Mechanics and its Applications*, vol. 428, pp. 319–331, 2015.

[32] T. A. Brun, H. A. Carteret, and A. Ambainis, "Quantum walks driven by many coins," *Physical Review A*, vol. 67, no. 5, p. 052317, 2003.