Quantum Random Number Generation with Practical Device Imperfections

Walter O. Krawec[a]

[a]University of Connecticut, Storrs, CT, USA

ABSTRACT

Quantum random number generation (QRNG) is an important cryptographic primitive. Various security models exist from the fully trusted to the fully device independent scenario. Here we look at the middle-ground of semi source independence (where the only thing known about the source is the dimension) and where measurements are not ideal (e.g., there may be loss and detector inefficiencies). We show how to compute optimistic bit generation rates even in this strong security model and our methods may be broadly applicable to other quantum cryptographic protocols in this setting.

1. INTRODUCTION

Quantum random number generators (QRNG) are protocols that distill randomness from a quantum source in a cryptographically secure manner. Various security models exist from the fully-trusted (which leads to systems with weak security guarantees) to the fully device-independent model[1,2] (which leads to systems that are generally very inefficient with today's technology). A middle ground are various semi-device independent (SDI) scenarios[3–8] which provides users with strong security and fast random bit generation rates with today's technology. However, regardless of the security model, ensuring high efficiency is an important challenge that can often be overcome by more optimal security proofs. See[9] for a survey of QRNG protocols.

In this work, we analyze the random bit generation rates for high-dimensional QRNG protocols in a particular SDI scenario. High dimensional states are known to provide several benefits, at least in theory, to quantum cryptographic protocols[10–21] (see also[22] for a survey). Here we consider the case of QRNG protocols where measurement devices are not ideal. In previous work,[23–25] we showed how improvements to bit generation rates of certain Source Independent (SI) QRNG protocols with ideal measurement devices are possible using a new technique we developed which we call sampling-based entropic uncertainty.[24] In this work, we analyze SDI-QRNG protocols in a stronger SDI model and even when the user's measurement devices are not ideal (making our work useful for practical implementations unlike our past work). We show how our sampling-based entropic uncertainty relations can be applied to their security analysis, and can even lead to more optimistic bit generation rates compared to other methods. Our proof techniques, using methods we developed in[25,26] here can also be broadly applied to other cryptographic protocols and also lead to new insights in general quantum information theory.

2. PRELIMINARIES

We begin with some notation and terminology we will use throughout this work. We denote by $\mathcal{A}_d$ to be an alphabet of d characters with a distinguished "0" element. Without loss of generality, we simply assume $\mathcal{A}_d = \{0, 1, \cdots, d-1\}$. Given $q \in \mathcal{A}_d^N$ and a subset $t \subset \{1, \cdots, N\}$, we write q_t to mean the substring of q indexed by t; we write q_{-t} to mean the substring indexed by the complement of t. Finally, we write $w(q)$ to be the relative Hamming weight of q, namely $w(q) = |\{i \ : \ q_i \neq 0\}|/|q|$, where $|q|$ is the number of characters in q.

A quantum state or density operator ρ is a semi-definite Hermitian operator of unit trace. If ρ acts on some bipartite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_E$, we write ρ_{AE}. We also write ρ_E to mean the state resulting from tracing out the A register.

Further author information: (Send correspondence to W.O.K.)
W.O.K.: E-mail: walter.krawec@uconn.edu

By $\mathcal{H}_d$ we mean a Hilbert space of dimension d. Given an orthonormal basis $\mathcal{B} = \{|b_0\rangle, \cdots, |b_{d-1}\rangle\}$ and a word $q \in \mathcal{A}_d^N$, we write $|q\rangle^{\mathcal{B}}$ or $|q^{\mathcal{B}}\rangle$ to mean the state $|b_{q_1}\rangle \otimes |b_{q_2}\rangle \otimes \cdots \otimes |b_{q_N}\rangle$.

Given random variable X, the Shannon entropy is denoted $H(X)$. The d-ary entropy is denote $H_d(x)$ and defined to be:

$$H_d(x) = x \log_d(d-1) - x \log_d x - (1-x)\log_d(1-x). \tag{1}$$

Notice that, when $d = 2$, this becomes the usual binary entropy function.

A very important quantity in quantum cryptography is the *conditional quantum min entropy*[27] defined to be:

$$H_\infty(A|E)_\rho = \sup_{\sigma_E} \max\{\lambda \in \mathbb{R} \ : \ 2^{-\lambda} I_A \otimes \sigma_E - \rho_{AE} \geq 0\}, \tag{2}$$

where the supremum is over all density operators σ_E. Several important properties of min entropy are easily proven, in particular, given $\rho_{AE} = \rho_A \otimes \rho_E$ (i.e., if the A and E systems are independent), then $H_\infty(A|E)_\rho = H_\infty(A)$. Also, it is easy to show that $H_\infty(A) = -\log \max \lambda$, where the maximum is over all eigenvalues λ of ρ_A. Finally, given a state $\rho_{AE} = \sum_a p_a \rho_{AE}^{(a)}$, it can be shown from the definition of min entropy that:

$$H_\infty(A|E) \geq \min_a H_\infty(A|E)_\rho^{(a)}. \tag{3}$$

Smooth entropy is defined to be[27]

$$H_\infty^\epsilon(A|E)_\rho = \sup_\sigma H_\infty(A|E)_\sigma, \tag{4}$$

where the supremum is over all density operators that are ϵ close to ρ in trace distance, namely $||\rho - \sigma|| \leq \epsilon$.

Smooth min entropy is a very important quantity in that it measures how much uniform randomness may be extracted from a quantum state, independent of an adversary. In particular, given a classical-quantum state ρ_{AE}, then, privacy amplification[27] is a process that hashes the A register down to an ℓ bit string. Then, it holds that:[27]

$$\left|\left|\sigma_{KE} - I_K/2^\ell \otimes \sigma_E\right|\right| \leq 2^{-\frac{1}{2}(H_\infty^\epsilon(A|E)_\rho - \ell)} + 2\epsilon. \tag{5}$$

In particular, the amount of min entropy in the state *before* privacy amplification relates directly to the amount of secret randomness that may be extracted from the state. Later, when we analyze QRNG protocols, our main goal will be to bound the quantum min entropy as a function only of observed statistics. In particular, by setting the right-hand side of the above expression to be ϵ_{PA}, one may extract an ℓ bit random string that is ϵ_{PA} close to an ideal uniform and independent random string, with:

$$\ell = H_\infty^\epsilon(A|E)_\rho - 2\log\frac{1}{\epsilon_{PA} - 2\epsilon}. \tag{6}$$

One other important min entropy result we will need later was proven in[28] (using methods in[27]):

LEMMA 2.1. *(From[28]): Given a state* $|\psi\rangle_{AE} = \sum_{i\in J} \alpha_i |i\rangle^X \otimes |E_i\rangle$, *define the mixed state* $\chi = \sum_{i \in J} |\alpha_i|^2 |i\rangle\langle i|^X \otimes |E_i\rangle\langle E_i|$. *Then, if a measurement in the* Z *basis is performed on* $|\psi\rangle$, *the resulting min entropy can be bounded by:*

$$H_\infty(Z|E)_\psi \geq H_\infty(Z|E)_\chi - \log_2 |J|,$$

where $H_\infty(Z|E)_\chi$ *is the min entropy in the mixed state following a measurement in that same basis.*

2.1 Quantum Sampling

Our proof method uses the framework of quantum sampling introduced by Bouman and Fehr in.[28] Here we briefly discuss the main results of this method - for more details see.[28]

A classical sampling strategy consists of a probability distribution over subsets P_T, a guess function $f : \mathcal{A}_d^* \to \mathbb{R}$, and a target function $g : \mathcal{A}_d^* \to \mathbb{R}$. Given a word $q \in \mathcal{A}_d^N$, the strategy consists of sampling t using P_T, observing q_t, and evaluating $f(q_t)$. A good sampling strategy should produce an accurate guess of the value $g(q_{-t})$. In particular, it should hold that, with high probability over the choice of t, that $|f(q_t) - g(q_{-t})| \le \delta$.

More formally, let $\mathcal{G}^t$ be the set of "good" words for a fixed subset t defined as:

$$\mathcal{G}^t = \{q \in \mathcal{A}_d^N \ : \ |f(q_t) - g(q_{-t})| \le \delta\}.$$

Define the error probability to be:

$$\epsilon^{cl} = \max_{q \in \mathcal{A}_d^N} Pr\left(q \notin \mathcal{G}^t\right),$$

where the probability is over the subset choice t. The main result from[28] was to promote this to quantum states as follows. Fix a basis X, then we can define the set of "ideal" quantum states as:

$$\text{span}(\mathcal{G}_t) \otimes \mathcal{H}_E = \text{span}(|q\rangle^X \ : \ q \in \mathcal{G}_t) \otimes \mathcal{H}_E.$$

Notice that, if $|\phi^t\rangle \in \text{span}(\mathcal{G}_t) \otimes \mathcal{H}_E$, then if a measurement of those systems indexed by t were performed, resulting in outcome x, it would hold that the unmeasured portion would collapse to one of the form:

$$|\phi_x^t\rangle = \sum_{i \in J_x} \alpha_i |i\rangle^X \otimes |E_i\rangle,$$

where $J_x = \{i \in \mathcal{A}_d^{N-|t|} \ : \ |g(i) - f(x)| \le \delta\}$. The main result from,[28] then, is:

Theorem 2.2. *(From,[28] though reworded here for our application): Given a sampling strategy as discussed and a quantum state $|\psi\rangle_{AE}$, then there exist ideal states $\{|\phi^t\rangle\}$ such that each $|\phi^t\rangle \in span(\mathcal{G}_t) \otimes \mathcal{H}_E$ and:*

$$\frac{1}{2}\left|\left|\sum_t P_T |t\rangle\langle t| \otimes |\psi\rangle\langle\psi| - \sum_t P_T |t\rangle\langle t| \otimes |\phi^t\rangle\langle\phi^t|\right|\right| \le \sqrt{\epsilon^{cl}}.$$

In particular, quantum states behave "almost like" ideal states (where sampling always works), on average over the subset choice.

One strategy we will use in our work is where the subset is chosen uniformly at random from all subsets of size $m < N/2$ (where N is the number of characters in the word) and where $f(x) = g(x) = w(x)$, the relative Hamming weight. For this strategy, it can be shown (see[28]), that:

$$\epsilon^{cl} \le 2\exp\left(\frac{-\delta^2 m(n+m)}{m+n+2}\right). \tag{7}$$

3. PROTOCOL AND ANALYSIS

The protocol we consider was introduced in[3] and is a high-dimensional semi-source independent protocol. The protocol assumes a source prepares some quantum signal and sends it to Alice. An honest and ideal source should prepare N copies of the state $|0\rangle^X$ for some known orthonormal basis $X = \{|0\rangle^X, \cdots, |d-1\rangle^X, |vac\rangle\}$. Of course, as we are assuming the semi-source independent model, the only assumption made on the source is that its dimension is known. A subset $t \subset \{1, \cdots, N\}$ of size $m < N/2$ is chosen and a measurement of those systems are made in the POVM $\Lambda = \{X_0, X_1, X_{vac}\}$, where:

$$X_i = \eta |i\rangle\langle i|^X, \text{ for } i = 0, \cdots, d-1 \tag{8}$$

$$X_{vac} = I - \sum_i X_i. \tag{9}$$

Here, η is used to represent the detector efficiency (which is one in the ideal case). Unlike our prior work,[25] we assume imperfect measurement detectors with efficiency strictly less than one and potential vacuum signals. Note that in[26] we assumed imperfect detectors but for a QKD application; while we use methods from[26] to derive our key-rate, the application is new and some of the methods are different and thus require restating here. Thus, this measurement results in an outcome $q \in (\mathcal{A}_d \cup \{vac\})^m \cong \mathcal{A}_{d+1}^m$, where we treat symbol d to be the vacuum event. Note that a vacuum may occur if either the signal is an actual vacuum, or one of the other detectors "misses" the signal due to a low efficiency. Note that, in the ideal case, it should hold that $w(q) = 0$; any non-zero Hamming weight will be considered noise.

Following this "test" stage, the remaining $n = N - m$ signals will be subjected to a measurement in an alternative basis $Z = \{|0\rangle^Z, \cdots, |d-1\rangle^Z, |vac\rangle\}$. Ideally, it should hold that these states are mutually unbiased in that $\langle i^Z | j^X \rangle = 1/\sqrt{d}$. Of course the vacuum state lives in both bases and this has inner-product one in both. This results in outcome $r \in \mathcal{A}_{d+1}^N$ (we take vac to be the $d+1$'th symbol). This is then run through a two-universal hash function for privacy amplification purposes to produce a final secret random string of size ℓ.

Note that, to choose random subset t requires $\log \binom{N}{m}$ random bits. Thus, QRNG protocols are really randomness expansion protocols in that they do require some small seed randomness to initialize the system. However, as we will show, this system can produce more random bits than were used so this initial seed may be constantly replenished. Interestingly, the two-universal hash function need only be chosen once and then hard-coded so no additional randomness is needed there.[29]

3.1 Security Analysis

We follow methods we developed in[25, 26] to derive a bound on the quantum min entropy of the system based only on the dimension d and the value q. We do not require a characterization of η or any other assumptions on the source.

The source begins by preparing a quantum state $|\psi\rangle_{AE} \in \mathcal{H}_A \otimes \mathcal{H}_E$ where $\mathcal{H}_A \cong \mathcal{H}_{d+1}^{\otimes N}$ for user chosen $N = n + m$ (with $n > m$). Using Theorem 2.2, along with the sampling strategy analyzed in Equation 7, we know that there exist an ideal state σ_{TAE} of the form:

$$\sigma_{TAE} = \frac{1}{T} \sum_t |t\rangle \langle t| \otimes |\phi^t\rangle \langle \phi^t|,$$

where $T = \binom{N}{m}$ and each $|\phi_t\rangle \in \text{span}(|q\rangle^X \;:\; |w(q_t) - w(q_{-t})| \leq \delta) \otimes \mathcal{H}_E$. By setting:

$$\delta = \sqrt{\frac{(m+n+2)\ln(2/\epsilon^2)}{m(m+n)}},$$

we have (again, using Theorem 2.2 and Equation 7):

$$\frac{1}{2} \left\| \frac{1}{T} \sum_t |t\rangle \langle t| \otimes |\psi\rangle \langle \psi| - \frac{1}{T} \sum_t |t\rangle \langle t| \otimes |\phi^t\rangle \langle \phi^t| \right\| \leq \epsilon.$$

Above, the sum is over all subsets $t \subset \{1, \cdots, N\}$ of size m.

We begin by analyzing the ideal state (where the state of the AE portion depends on the subset choice). The analysis for that may then be promoted, through a probabilistic argument, to the real case (the actual state $|\psi\rangle$ which is independent of the subset choice before sampling).

Consider the ideal state σ. After choosing a subset t, the state collapses to $|\phi^t\rangle$. Then, after observing $q \in \mathcal{A}_{d+1}^m$, it is straight-forward to show that the state must collapse to one of the form:

$$\sigma_{AE}^{(t,q)} = \sum_{x \in J_q} p_x \underbrace{P\left(\sum_{i \in \mathcal{I}_x} \alpha_{i,x} |i\rangle^X \otimes |E_{i,x}\rangle\right)}_{\sigma^x}, \quad (10)$$

where:

$$J_q = \{x_1 \cdots x_m \in \mathcal{A}_{d+1}^m \;:\; x_j = q_j \text{ if } q_j \neq vac\}$$
$$\mathcal{I}_x = \{i \in \mathcal{A}_{d+1}^n \;:\; |w(i) - w(x)| \leq \delta\}.$$

Here, J_q represents the uncertainty on the measured portion of the state due to device imperfections (whenever X_{vac} clicks, the user cannot be certain if it is really due to the underlying signal being $|vac\rangle$ or one of the other states and simply a function of $\eta < 1$). The set $\mathcal{I}_x$ represents the uncertainty in the unmeasured portion which we can bound exactly thanks to Theorem 2.2.

Using Equation 3, we have:

$$H_\infty(A|E)_{\sigma^{(t,q)}} \geq \min_{x \in J_q} H_\infty(A|E)_{\sigma^x}.$$

We now use Lemma 2.1 to bound the min entropy contained in σ^x following a Z basis measurement. Consider the following mixed state:

$$\chi = \sum_{i \in \mathcal{I}_x} |\alpha_{i,x}|^2 \, |i\rangle \langle i|^X \otimes |E_{i,x}\rangle \langle E_{i,x}| \, .$$

Following a Z basis measurement of this state, the outcome is:

$$\chi_Z = \sum_{i \in \mathcal{I}_x} |\alpha_{i,x}|^2 \sum_{z \in \mathcal{A}_{d+1}^n} p(z|i) \, |z\rangle \langle z| \otimes |E_{i,x}\rangle \langle E_{i,x}| \, .$$

Using Equation 3, and noting that, at this point, the E and Z registers are independent (in the mixed state χ_Z), we have:

$$H_\infty(A|E)_\chi \geq -\log \max_{z,i} p(z|i).$$

Note that the maximum above is over all $z \in \mathcal{A}_{d+1}^n$, thus we must also consider the probability of a vacuum event occurring. Thus:

$$p(z|i) = (1)^\nu \cdot \left(\frac{1}{d}\right)^{n-\nu} \tag{11}$$

where ν is the number of vacuum states in $|i\rangle$. Of course, since $i \in \mathcal{I}_x$, we have $\nu \leq n(w(x) + \delta)$ and so:

$$p(z|i) \leq d^{-n(1-w(x)-\delta)}. \tag{12}$$

From Lemma 2.1, we therefore have:

$$H_\infty(A|E)_\sigma \geq \min_x H_\infty(A|E)_{\sigma^x} \geq \min_x \left(n(1 - w(x) - \delta) \log_2 d - \log_2 |\mathcal{I}_x|\right)$$

The minimum above is attained whenever we count a vacuum symbol in q as a non-zero character in x. Thus:

$$H_\infty(A|E)_\sigma \geq n(1 - w(q) - \delta) \log_2 d - n \frac{h_{d+1}(w(q) + \delta)}{\log_d 2}, \tag{13}$$

where, above, we used the well known bound on the volume of a Hamming ball to bound $\mathcal{I}_x$.

Of course, the above was just the ideal state analysis. However, we may use a probabilistic argument, as in,[24–26] to promote this to the real case. Indeed, using methods from,[24–26] it is straight-forward to show that:

$$Pr\left(H_\infty^{4\epsilon+2\epsilon^{1/3}}(A|E)_{\psi(t,q)} \geq n\left((1 - w(q) - \delta) \log_2 d - \frac{h_d(q + \delta)}{\log_d 2}\right)\right) \geq 1 - 2\epsilon^{1/3} \tag{14}$$

where the probability is over all subset choices t and observations q. Combining with Equation 6, we conclude that the number of secret random bits that may be extracted which are $\epsilon_{PA} = 9\epsilon + 4\epsilon^{1/3}$ distant from the ideal random string are:

$$\ell = n\left((1 - w(q) - \delta) \log_2 d - \frac{h_d(w(q) + \delta)}{\log_d 2}\right) - 2 \log \frac{1}{\epsilon}. \tag{15}$$

Note that this expression is very different from the one in[25] where we did not consider loss; it is also different from our expressions in[26] which were QKD specific.

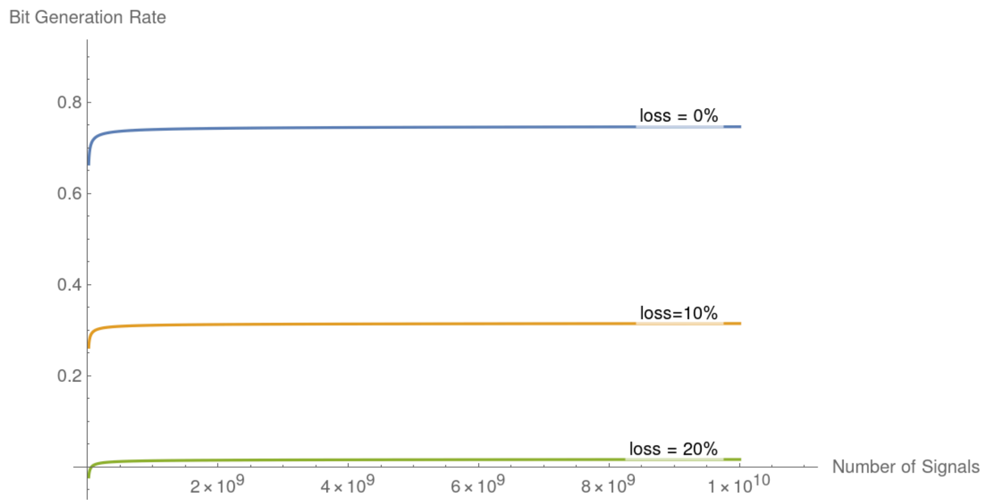

Figure 1. Evaluating our key-rate with imperfect detectors when $d = 2$. Here, we set $Q = 5\%$ and evaluate for various levels of loss ν.

4. EVALUATION

We evaluate our bound assuming a depolarization channel with loss due to fiber and detector inefficiencies. This is an assumption made only in this section in order to evaluate the bound. Our security proof above does not require any such assumption (nor does it require a characterization of the detector efficiencies). Instead, one simply needs to observe q to evaluate the bound above.

First, given a fiber channel of length x km, the probability of loss is $p_l = 1 - 10^{-.15x/10}$. The total probability, then of observing a vacuum on any particular measurement is:

$$\nu = p_l + (1 - p_l)(1 - \eta).$$

If a signal is not lost, it depolarizes with probability Q; in particular:

$$|0\rangle \langle 0|^X \mapsto (1 - Q) |0\rangle \langle 0|^X + Q/dI,$$

thus, we have the expected value of $w(q)$ is: $q = \nu + (1 - \nu)\frac{(d-1)}{d}Q$.

We also compare with our work in[25] for a similar protocol but with perfect detectors; we also compare with the bound produced in[3] (again for ideal detectors). For evaluating our bit rate, we use $m = .07N$ (that is, the sample size is 7% of total signals. We also set $\epsilon = 10^{-36}$ which gives us a failure probability on the order of 10^{-12}.

Evaluating our bound for $d = 2$ and $d = 4$ is shown in Figure 1 and 2. A comparison to our work in[25] for ideal devices is shown in Figure 3 and a comparison to both[25] and[3] can be seen in Figure 4. Interestingly, our bound, even with non-ideal devices, can still outperform alternative methods in[3] using standard entropic uncertainty relations. Our bound does not outperform our work in[25] but this is to be expected as that other work assumed ideal measurement devices and used a sampling-based approach. Note that these are not entirely fair comparisons to our work here as our work here involves a stronger security model where measurement devices are not completely ideal as in that prior work.

5. CLOSING REMARKS

Here we analyzed a high-dimensional QRNG protocol in the semi-source independent security model and where also measurement devices are not ideal. We showed how the framework of quantum sampling[28] and sampling based entropic uncertainty[24] can be used to derive fairly optimistic bit generation rates in this scenario. Our methods may potentially be broadly applied to other quantum cryptographic protocols in this security model.

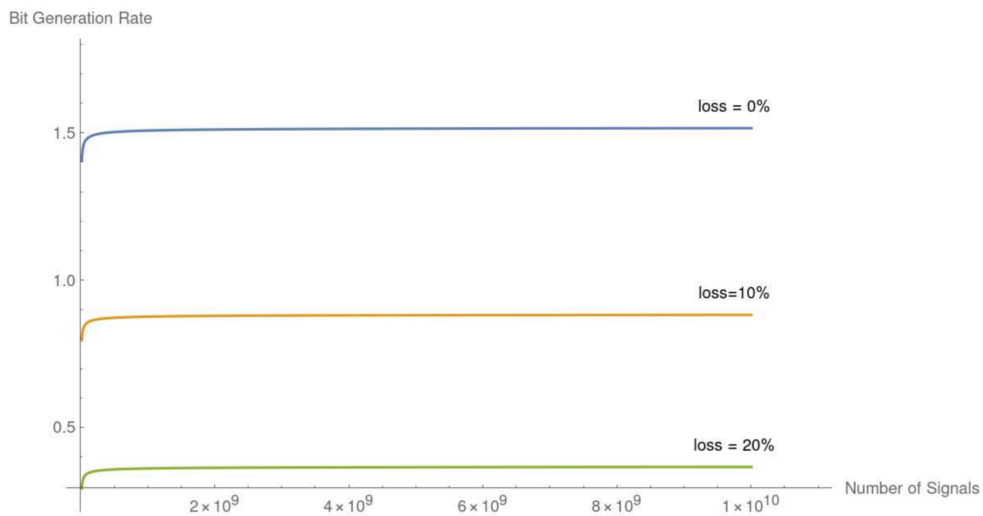

Figure 2. Evaluating our key-rate with imperfect detectors when $d = 4$. Here, we set $Q = 5\%$ and evaluate for various levels of loss ν.

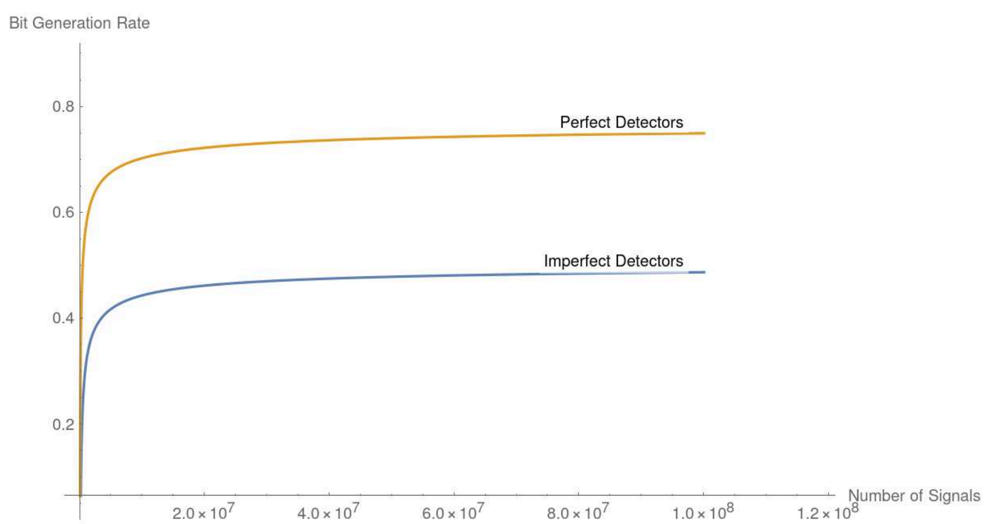

Figure 3. Comparing our bound here assuming non-ideal detectors with that derived in[25] but for ideal detectors when $d = 8$. We note that the old bound from[25] outperforms, however this is to be expected since that work assumed perfect detectors and no loss.

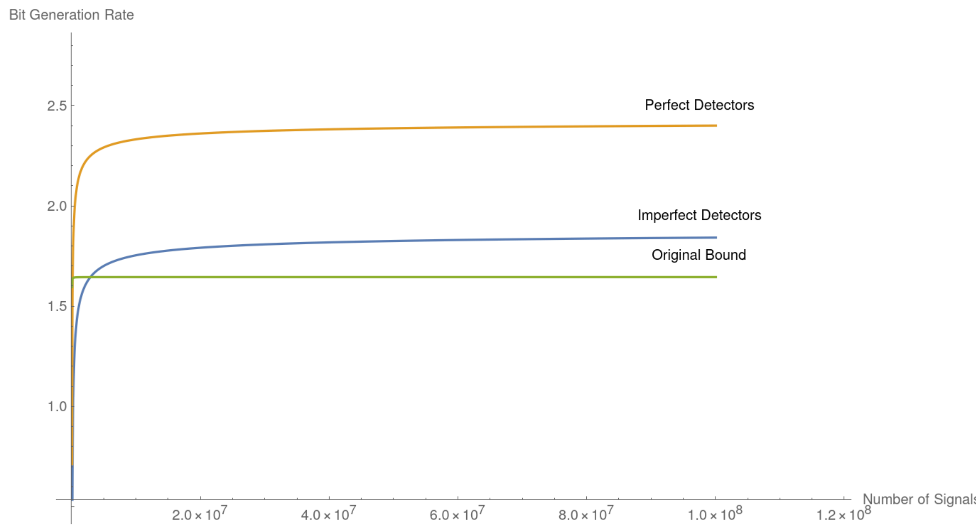

Figure 4. Comparing our bound here assuming non-ideal detectors with that derived in[25] but for ideal detectors when $d = 8$ and also comparing with the original bound from[3] for this protocol (again, assuming ideal detectors and no loss). Interestingly, even with non-ideal devices, our proof method can produce a more optimistic bit generation rate even with non-ideal devices and loss than prior methods.

Acknowledgments

The author would like to acknowledge support from NSF grant number 2006126.

REFERENCES

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

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

[3] Vallone, G., Marangon, D. G., Tomasin, M., and Villoresi, P., "Quantum randomness certified by the uncertainty principle," *Physical Review A* **90**(5), 052327 (2014).

[4] Haw, J.-Y., Assad, S., Lance, A., Ng, N., Sharma, V., Lam, P. K., and Symul, T., "Maximization of extractable randomness in a quantum random-number generator," *Physical Review Applied* **3**(5), 054004 (2015).

[5] Li, Y.-H., Han, X., Cao, Y., Yuan, X., Li, Z.-P., Guan, J.-Y., Yin, J., Zhang, Q., Ma, X., Peng, C.-Z., et al., "Quantum random number generation with uncharacterized laser and sunlight," *npj Quantum Information* **5**(1), 1–5 (2019).

[6] Xu, B., Chen, Z., Li, Z., Yang, J., Su, Q., Huang, W., Zhang, Y., and Guo, H., "High speed continuous variable source-independent quantum random number generation," *Quantum Science and Technology* **4**(2), 025013 (2019).

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

[8] Drahi, D., Walk, N., Hoban, M. J., Fedorov, A. K., Shakhovoy, R., Feimov, A., Kurochkin, Y., Kolthammer, W. S., Nunn, J., Barrett, J., et al., "Certified quantum random numbers from untrusted light," *Physical Review X* **10**(4), 041048 (2020).

[9] Herrero-Collantes, M. and Garcia-Escartin, J. C., "Quantum random number generators," *Reviews of Modern Physics* **89**(1), 015004 (2017).

[10] Bechmann-Pasquinucci, H. and Tittel, W., "Quantum cryptography using larger alphabets," *Physical Review A* **61**(6), 062308 (2000).

[11] Chau, H. F., "Unconditionally secure key distribution in higher dimensions by depolarization," *IEEE Transactions on Information Theory* **51**(4), 1451–1468 (2005).

[12] Sheridan, L. and Scarani, V., "Security proof for quantum key distribution using qudit systems," *Physical Review A* **82**(3), 030301 (2010).

[13] Sasaki, T., Yamamoto, Y., and Koashi, M., "Practical quantum key distribution protocol without monitoring signal disturbance," *Nature* **509**(7501), 475–478 (2014).

[14] Chau, H., "Quantum key distribution using qudits that each encode one bit of raw key," *Physical Review A* **92**(6), 062324 (2015).

[15] Vlachou, C., Krawec, W., Mateus, P., Paunković, N., and Souto, A., "Quantum key distribution with quantum walks," *Quantum Information Processing* **17**(11), 1–37 (2018).

[16] Cerf, N. J., Bourennane, M., Karlsson, A., and Gisin, N., "Security of quantum key distribution using d-level systems," *Physical review letters* **88**(12), 127902 (2002).

[17] Nikolopoulos, G. M. and Alber, G., "Security bound of two-basis quantum-key-distribution protocols using qudits," *Physical Review A* **72**(3), 032320 (2005).

[18] Iqbal, H. and Krawec, W. O., "High-dimensional semiquantum cryptography," *IEEE Transactions on Quantum Engineering* **1**, 1–17 (2020).

[19] Nikolopoulos, G. M., Ranade, K. S., and Alber, G., "Error tolerance of two-basis quantum-key-distribution protocols using qudits and two-way classical communication," *Physical Review A* **73**(3), 032325 (2006).

[20] Yin, Z.-Q., Wang, S., Chen, W., Han, Y.-G., Wang, R., Guo, G.-C., and Han, Z.-F., "Improved security bound for the round-robin-differential-phase-shift quantum key distribution," *Nature communications* **9**(1), 1–8 (2018).

[21] Doda, M., Huber, M., Murta, G., Pivoluska, M., Plesch, M., and Vlachou, C., "Quantum key distribution overcoming extreme noise: simultaneous subspace coding using high-dimensional entanglement," *Physical Review Applied* **15**(3), 034003 (2021).

[22] Cozzolino, D., Da Lio, B., Bacco, D., and Oxenløwe, L. K., "High-dimensional quantum communication: Benefits, progress, and future challenges," *Advanced Quantum Technologies* **2**(12), 1900038 (2019).

[23] Yao, K., Krawec, W. O., and Zhu, J., "Quantum sampling for finite key rates in high dimensional quantum cryptography," *IEEE Transactions on Information Theory* , 1–1 (2022).

[24] Krawec, W. O., "Quantum sampling and entropic uncertainty," *Quantum Information Processing* **18**(12), 1–18 (2019).

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

[26] Krawec, W. O., "Security of a high dimensional two-way quantum key distribution protocol," *arXiv preprint arXiv:2203.02989* (2022).

[27] Renner, R., "Security of quantum key distribution," *International Journal of Quantum Information* **6**(01), 1–127 (2008).

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

[29] Frauchiger, D., Renner, R., and Troyer, M., "True randomness from realistic quantum devices (2013)," *URL http://arxiv. org/abs/1311.4547* .