Entropic Uncertainty for Biased Measurements

Walter O. Krawec
University of Connecticut
Storrs CT, USA
walter.krawec@uconn.edu

***Abstract*—Entropic Uncertainty relations are powerful tools, especially in quantum cryptography. They typically bound the amount of uncertainty a third-party adversary may hold on a measurement outcome as a result of the measurement overlap. However, when the two measurement bases are biased towards one another, standard entropic uncertainty relations do not always provide optimal lower bounds on the entropy. Here, we derive a new entropic uncertainty relation, for certain quantum states, which can provide a significantly higher bound even if the two measurement bases are no longer mutually unbiased. We evaluate our bound on two different quantum cryptographic protocols, including BB84 with faulty/biased measurement devices, and show that our new bound can produce substantially higher key-rates under several scenarios when compared with prior work using standard entropic uncertainty relations.**

I. Introduction

Quantum entropic uncertainty relations are a powerful tool in quantum information theory and quantum cryptography. Such relations typically bound the amount of uncertainty in the outcome of two different measurements as a function only of the measurements themselves. For instance, the famous Maassen and Uffink inequality [**?**] states that if a quantum state is measured in one of two bases Z or X, then $H(Z)+H(X) \geq c$, where $H(Z)$ is the entropy in the Z basis outcome (similar for $H(X)$), and c is a function of the "measurement overlaps" between the X and Z bases and is maximal whenever Z and X are mutually unbiased bases. By now there are a large variety of different entropic uncertainty relations [**?**], [**?**], [**?**], [**?**]; see [**?**] for a general survey.

One very useful entropic uncertainty relation was introduced in [**?**] which bounds the quantum min entropy - a quantity we define formally later, but denote by $H_\infty(A|E)$. Min entropy is a very useful resource to measure as it is directly related to how many uniform random secret bits may be extracted from a quantum state [**?**]. In a little detail, let's assume ρ_{ABE} is a quantum state where the A and B registers consist of n qubits each and let $Z = \{|0\rangle, |1\rangle\}$ be the standard computational basis for qubits and $X = \{|x_0\rangle, |x_1\rangle\}$ be some other basis with $|x_0\rangle = \sqrt{1/2+b}$ and $|x_1\rangle = \sqrt{1/2-b}$ for some "bias" parameter $b \in [0, .5]$ (e.g., this may be the Hadamard basis if $b = 0$). Note the results will be symmetric if we have $b \in [-.5, 0]$. Assume a measurement is made on the A system in either the Z basis (resulting in some random variable A_Z) or the X basis (yielding random variable A_X); similar for the B system. Then, the relation defined in [**?**] roughly states (when restricted to basis measurements of this form), that:

$$H_\infty(A_Z|E) + H_{max}(A_X|B_X) \geq -n \cdot \log_2\left(\frac{1}{2} + b\right). \quad (1)$$

Note that the lower-bound is maximal when $b = 0$ and one gets $H_\infty(A_Z|E)+H_{max}(A_X|B_X) \geq n$. This relation is used many times in various quantum cryptographic proofs of security as it allows one to bound the quantum min entropy between Alice and an adversary system Eve, simply as a function of the measurements performed and $H_{max}(A_X|B_X)$, the latter of which may be easily bounded through standard classical sampling arguments and is generally a function of the "error" induced in the quantum communication line.

The above expression, as stated, is not only highly useful, but also widely applied. However, when $b \neq 0$, it is not difficult to see that the lower bound on $H_\infty(A|E)$ begins to drop rapidly. In this work, we derive a new entropic uncertainty relation for cases when there is non-zero bias in the measurement bases. Our new relation, though stated formally in Theorem 2, roughly takes the form:

$$H_\infty(A_Z|E) + n \cdot h\left(Q_X + 4b^2 + \epsilon\right) \geq n, \quad (2)$$

where $h(x)$ is the binary entropy, Q_X is the relative number of errors in Alice and Bob's X basis measurement, and ϵ is a function of the number of qubits that were measured in the X basis (and which goes to zero in the asymptotic limit). Note, the above is only true if $Q_X + 4b^2 + \epsilon < 1/2$ which can be checked by the users of the protocol before continuing. This already puts an upper-bound on b of $\sqrt{1/8} \approx 0.3535$ (unlike Equation 1 which has an upper bound of $b < 1/2$). Thus, when there is bias but no noise ($Q_X = 0$ and $H_{max}(A_X|B_X) = 0$), our result performs worse; however, importantly, when there is both noise and bias, our bound often outperforms Equation 1, sometimes substantially so as our later evaluations show. Thus, it can be immediately applied to cryptographic proofs of protocols where measurements are biased and there is noise in the channel (either natural noise or adversarial noise) and used to show that higher bit generation rates are possible under these circumstances. *We comment that our proof in this paper requires* a particular (though arguably minimal, and even enforceable by the users, as we comment later) assumption on the quantum state under investigation. However, this assumption is only needed in one part of the proof and we suspect our methods can be suitably extended to work, with the same result, even without this assumption. However, this we leave as future work.

Our relation is a so-called *sampling-based entropic uncertainty relation*, which is a class of entropic uncertainty relations introduced in [**?**], [**?**]. These relations utilize a quantum sampling framework of Bouman and Fehr introduced in [**?**] for their proof. Such relations, though still relatively new, have shown to hold numerous benefits in several applications including higher bit generation rates for random number generation [**?**] (only shown there for un-biased measurements) along with new applications and easier proofs for high-dimensional systems [**?**]. They have been shown to be useful in proving security of quantum cryptographic protocols where standard relations such as Equation 1 actually fail (i.e., prior relations show a trivial bound of 0 whereas sampling based entropic uncertainty methods show a positive bound) [**?**], [**?**].

In this work, we use the sampling-based approach to derive a novel entropic uncertainty relation for cases where user measurements are biased. This can occur due to faulty measurement devices for example or, perhaps, "cheaper" measurement devices are used which cannot perform an exact measurement in a mutually unbiased basis. It is also interesting from a theoretical point of view as we prove, here, that better bounds on min entropy are possible even if the two measurement bases are "close" to one another. Finally, it shows even more advantages to the sampling-based approach to entropic uncertainty and we suspect our proof methods here may be highly beneficial to other scenarios where measurement or source devices are imperfect.

We note that, while the main contribution of this paper is our new entropic uncertainty bound, we also make other contributions along the way. We prove an interesting result (Lemma 3), that may be independently useful, which bounds the min entropy of a particular superposition state. We also prove that higher bit generation rates are possible for BB84 with faulty source and measurement devices and higher bit generation rates are possible for a particular quantum random number generation (QRNG) protocol. Finally, our main results can be easily incorporated into other quantum cryptographic protocols.

II. Preliminaries

We begin by introducing some notation that we use throughout this paper. We denote by $\mathcal{A}_d$ to be a d-character alphabet; without loss of generality we simply assume $\mathcal{A}_d = \{0, 1, \cdots, d-1\}$. 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, that is $q_t = q_{t_1} q_{t_2} \cdots q_{t_{|t|}}$. We write q_{-t} to mean the substring of q indexed by the complement of t. Finally, for $i = 1, 2, \cdots, n$, we write q_i to mean the i'th character of q.

Let $a, b \in \mathcal{A}_d^n$. We write $\#_i(a)$ to be the number of times the character i appears in a. Formally $\#_i(a) = |\{\ell \ : \ a_\ell = i\}|$. We extend this to multiple counts in the obvious way, for example $\#_{i,j}(a)$ is the number of times the character i and j appear in a, or $\#_{i,j}(a) = |\{\ell \ : \ a_\ell = i \text{ or } a_\ell = j\}|$. For a bit string $x \in \{0, 1\}$, we denote by $w(x)$ to be the relative Hamming weight, namely $w(x) = \#_1(x)/|x|$. Finally, we denote by $\Delta_H(a, b)$ to be the Hamming distance of words a and b, namely: $\Delta_H(a, b) = |\{\ell \ : \ a_\ell \neq b_\ell\}|$.

Given a random variable X, we denote by $H(X)$ to be the Shannon entropy of X. If X takes outcome x_i with probability p_i, then $H(X) = -\sum_i p_i \log_2 p_i$. Note that all logarithms in this paper are base two unless otherwise specified. If X is a two outcome random variable taking x_1 with probability p, then we use $h(p)$ to denote the binary entropy and $H(X) = h(p) = -p \log p - (1-p) \log(1-p)$. We also define the bounded binary entropy function $\hat{h}(x)$, where $\hat{h}(x) = h(x)$ whenever $x < 1/2$ and $\hat{h}(x) = 1$ otherwise.

A density operator ρ is a Hermitian positive semi-definite operator of unit trace acting on some Hilbert space $\mathcal{H}$. If ρ_{AE} acts on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_E$, we write ρ_A to mean the state resulting from tracing out the E system, namely $\rho_A = tr_E \rho_{AE}$. This is similar for multiple systems. Given a pure state $|\psi\rangle$ we write $[\psi]$ to mean $[\psi] = |\psi\rangle\langle\psi|$. We also define $P(|z\rangle)$ to be $P(|z\rangle) = [\mathbf{z}]$. Given an orthonormal basis $\mathcal{B} = \{|v_0\rangle, \cdots, |v_{d-1}\rangle\}$, we write $|i\rangle^{\mathcal{B}}$ to mean $|v_i\rangle$. Given $i \in \mathcal{A}_d^n$, we write $|i\rangle^{\mathcal{B}}$ to mean $|v_{i_1}, \cdots, v_{i_n}\rangle$, namely the word i represented in the $\mathcal{B}$ basis. If the basis is not specified, then it is assumed to be the computational basis $\{|0\rangle, \cdots, |d-1\rangle\}$. Finally, we use $|\phi_i\rangle$ to denote the Bell states:

$$|\phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\phi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\phi_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \qquad |\phi_3\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Given ρ_A we write $H(A)_\rho$ to mean the von Neumann entropy of ρ_A, namely $H(A)_\rho = -tr(\rho_A \log \rho_A)$. Given ρ_{AE}, we write $H(A|E)_\rho$ to be the conditional von Neumann entropy, namely $H(A|E)_\rho = H(AE)_\rho - H(E)_\rho$. We write $H_\infty(A|E)_\rho$ to be the *conditional quantum min entropy* defined to be [**?**]:

$$H_\infty(A|E)_\rho = \sup_{\sigma_E} \max \left\{ \lambda \in \mathbb{R} \ : \ 2^{-\lambda} I_A \otimes \sigma_E - \rho_{AE} \geq 0 \right\}, \tag{3}$$

where $A \geq 0$ is used to denote that A is positive semi-definite. The *smooth conditional min entropy* is denoted $H_\infty^\epsilon(A|E)_\rho$ and is defined to be: $H_\infty^\epsilon(A|E)_\rho = \sup_{\sigma_{AE}} H_\infty(A|E)_\sigma$, where the supremum is over all density operators σ_{AE} such that $||\sigma_{AE} - \rho_{AE}|| \leq \epsilon$. Here we use $||A||$ to mean the *trace distance* of operator A.

Quantum min entropy is a very important quantity to measure in quantum cryptography as it relates directly to how many uniform random secret bits may be extracted from a quantum state [**?**]. In detail, assume ρ_{AE} is a *classical-quantum state* (or cq-state). That is, the A register is classical while the E portion is potentially quantum, thus $\rho_{AE} = \sum_a p(a)[\mathbf{a}] \otimes \rho_E^a$. Assume the A register is N-bits in size (i.e., $a \in \{0, 1\}^N$ in the sum). Then *privacy amplification* is a process of picking a random two-universal hash function $f : \{0, 1\}^N \to \{0, 1\}^\ell$ and disclosing the choice to Eve, then hashing the A register to $f(A)$ yielding cq-state $\sigma_{KE'}$. The state $\sigma_{KE'}$ satisfies the following inequality as proven in [?]:

$$||\sigma_{KE'} - \mathcal{U}_\ell \otimes \sigma_{E'}|| \leq 2^{-\frac{1}{2}(H_\infty^\epsilon(A|E)_\rho - \ell)} + 2\epsilon, \qquad (4)$$

where $\mathcal{U}_\ell = I/2^\ell$ is a uniform random string of size ℓ-bits independent of Eve. Thus, to determine how large ℓ can be, one requires a bound on the quantum min entropy *before* privacy amplification.

A. Properties of Quantum Min Entropy

Min entropy has several properties that we will utilize later. In particular, given a cqc-state or qqc-state of the form $\rho_{AEC} = \sum_c p(c)[\mathbf{c}] \otimes \rho_{AE}^{(c)}$, then:

$$H_\infty(A|E)_\rho \geq H_\infty(A|EC)_\rho \geq \min_c H_\infty(A|E)_{\rho^{(c)}}. \qquad (5)$$

The above is easily shown using the definition of min entropy. Informally it says that, conditioning on certain events C happening, the min entropy is the "worst-case" min entropy of each individual sub-event.

The following lemma from [?] lets us bound the min entropy in a superposition as a function of the min entropy of a mixed state, assuming the superposition does not have "too many" terms:

Lemma 1. (From [?], based on a lemma in [?]): Given two orthonormal bases Z and X of some Hilbert space $\mathcal{H}_A$, let $|\psi\rangle_{AE}$ be some pure state of the form $|\psi\rangle_{AE} = \sum_{i\in J} \alpha_i |i\rangle^Z \otimes |E_i\rangle$ where the $|E_i\rangle$ states are arbitrary, but normalized. Then, if we define the mixed state $\rho_{AE} = \sum_{i \in J} |\alpha_i|^2 [\mathbf{i}]^Z \otimes [\mathbf{E_i}]$, it holds that:

$$H_\infty(X|E)_\psi \geq H_\infty(X|E)_\rho - \log_2 |J|,$$

where the X registers, above, are produced by measuring the A register (originally written in the Z basis above), in the X basis.

The next lemma we need is from [?] and shows how one may compute the min entropy in a state that is initially close to another (in trace distance) but after conditioning on an outcome (after which, the states may no longer be close and, thus, smooth min entropy by itself cannot be used):

Lemma 2. (From [?]): Let ρ, σ, and τ, be three quantum states with ρ and σ acting on the same Hilbert space (τ may be arbitrary or trivial). Also, let $\mathcal{F}$ be a CPTP map with the property that:

$$\mathcal{F}(\tau \otimes \rho) = \sum_x p(x)[\mathbf{x}] \otimes \rho_{AE}^{(x)}$$
$$\mathcal{F}(\tau \otimes \sigma) = \sum_x q(x)[\mathbf{x}] \otimes \sigma_{AE}^{(x)}.$$

Then, if $\frac{1}{2}||\rho - \sigma|| \leq \epsilon$, it holds that:

$$Pr\left(H_\infty^{4\epsilon+3\epsilon^{1/3}}(A|E)_{\rho^{(x)}} \geq H_\infty(A|E)_{\sigma^{(x)}}\right) \geq 1 - 2\epsilon^{1/3},$$

where the probability is over the random outcome X in the above states.

Finally, we prove the following lemma below in this work which may be of independent interest. It bounds the min entropy of a quantum state that is a superposition of Bell states on which we have some, but not all, information on (and, thus, Lemma 1 could not be used directly as that lemma requires full information on the superposition size which our lemma below does not require):

Lemma 3. Given $|\psi\rangle = \sum_{i\in J} \alpha_i |\phi_i\rangle |E_i\rangle$, where $J = \left\{i \in \mathcal{A}_4^n \ :\ \frac{1}{n}\#_{1,3}(i) \leq Q\right\}$, let ρ_{AE} be the result of measuring the first particle of each Bell pair in the Z basis (resulting in register A) and tracing out the second particle of each Bell pair. Then it holds that:

$$H_\infty(A|E)_\rho \geq n\left(1 - \hat{h}\left(Q\right)\right). \qquad (6)$$

Proof. We may rewrite $|\psi\rangle$ by permuting subspaces such that the second particle of each Bell pair is "pushed" to the left-most subspace while the first particle of each pair is pushed to the middle register (the right-most register will remain E). Noting that $|\phi_0\rangle$ and $|\phi_2\rangle$ are of the form $\frac{1}{\sqrt{2}}(|+,+\rangle \pm |-,-\rangle)$ while $|\phi_1\rangle$ and $|\phi_3\rangle$ are of the form $\frac{1}{\sqrt{2}}(|+,-\rangle \pm |-,+\rangle)$, the state, after this permutation of subspaces, can be written in the form:

$$|\psi\rangle \cong \sum_{b\in\{0,1\}^n} \beta_b |b\rangle^X \otimes \sum_{\substack{a\in\{0,1\}^n \\ \frac{1}{n}\Delta_H(a,b)\leq Q}} \beta_{a|b} |a\rangle^X |E_{a|b}\rangle. \qquad (7)$$

Above, X is the usual Hadamard basis. From this, we trace out the left-most register (which was originally the second particle of each Bell pair) - this, of course, is equivalent to first measuring the system and then tracing it out - yielding the state:

$$\rho_{RE} = \sum_b |\beta_b|^2 \underbrace{P\left(\sum_{\substack{a\in\{0,1\}^n \\ \frac{1}{n}\Delta_H(a,b)\leq Q}} \beta_{a|b} |a\rangle^X |E_{a|b}\rangle\right)}_{\rho_{RE}^b}, \qquad (8)$$

where, recall, $P(|z\rangle) = [\mathbf{z}]$.

The R system is now measured in the Z basis yielding $\sum_b |\beta_b|^2 \rho_{AE}^b$. From Equation 5, we have $H_\infty(A|E)_\rho \geq \min_b H_\infty(A|E)_{\rho^b}$. From Lemma 1, we have:

$$H_\infty(A|E)_{\rho^b} \geq n - \log\left|\left\{a \in \{0,1\}^n \ :\ \frac{1}{n}\Delta_H(a,b) \leq Q\right\}\right|.$$

Noting that, for any b, the size of the set $\left\{a \in \{0,1\}^n \ :\ \frac{1}{n}\Delta_H(a,b) \leq Q\right\}$ can be bounded using the well-known bound on the size of a Hamming ball, namely

$$\left|\left\{a \in \{0,1\}^n \ :\ \frac{1}{n}\Delta_H(a,b) \leq Q\right\}\right| \leq 2^{n\hat{h}(Q)},$$

completes the proof. □

B. Quantum Sampling

Our new entropic uncertainty relation is a so-called *sampling based entropic uncertainty relation* [**?**] which relies, for its proof, on the quantum sampling framework introduced by Bouman and Fehr in [**?**]. Since we use this framework to prove our main result, we highlight some of the main concepts here. For more information, the reader is referred to the original sampling paper [**?**] from which all information in this section is derived.

A *classical sampling strategy* over $\mathcal{A}_d^N$ is a triple (P_T, g, r), where P_T is a probability distribution over subsets of $\{1, 2, \cdots, N\}$; g is a "guess function," $g : \mathcal{A}_d^* \to \mathbb{R}$; and r is a "target function," $r : \mathcal{A}_d^* \to \mathbb{R}$. Given a word $q \in \mathcal{A}_d^N$, the strategy will first sample t according to P_T, observe q_t and compute $g(q_t)$ (or, equivalently, simply observe $g(q_t)$), and use this as a guess for the value of $r(q_{-t})$. That is, given an observed portion of q, the strategy should use that to guess at the target value of an *unobserved* portion of the string.

Let $\delta > 0$, then we define the set of *ideal words* to be:

$$\mathcal{G}_t = \{q \in \mathcal{A}_d^N \ : \ g(q_t) \sim_\delta r(q_{-t})\},$$

where we write $x \sim_\delta y$ to mean $|x - y| \leq \delta$. Then, the *error probability* of the sampling strategy is defined to be:

$$\epsilon^{cl} = \max_{q \in \mathcal{A}_d^N} Pr\left(q \notin \mathcal{G}_t\right), \tag{9}$$

where the above probability is over the choice of subset t. It is clear from this definition that, for any $q \in \mathcal{A}_d^N$, the probability that the given sampling strategy fails to give a δ-close guess of the target value is at most ϵ^{cl}. Note that the "cl" superscript is used here as a reminder that this is the classical failure probability.

A sampling strategy as above may be promoted to a quantum one. Let B be a d-dimensional orthonormal basis and let $|\psi\rangle_{AE}$ be some quantum state where the A portion lives in a d^N dimensional Hilbert space. Note that the state $|\psi\rangle$ may be arbitrary. Then the sampling strategy will first choose a subset t according to P_T, and then measure those systems in A indexed by t using basis B to produce outcome $q_t \in \mathcal{A}_d^{|t|}$. The unmeasured portion collapses to some state $|\psi_q^t\rangle$. Bouman and Fehr's main result is to give a rigorous analysis of this post measured state.

Formally, we define a space of *ideal states for subset t with respect to basis B* (or simply *ideal states* when the context is clear) as follows:

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

Note that the definition depends on the chosen basis B. An "ideal state for subset t" (with respect to basis B) is one that lives in this space. In general, if a B basis measurement is performed on subset t of an ideal state, yielding outcome q, then it is guaranteed that the post-measured state is of the form:

$$|\psi_q^t\rangle = \sum_{i \in J_q} \alpha_i |i\rangle^B \otimes |E_i\rangle,$$

where $J_q = \{i \in \mathcal{A}_d^{N-|t|} \ : \ g(q) \sim_\delta r(i)\}$. Bouman and Fehr's main result is stated in the Theorem below:

Theorem 1. (From [**?**], though we reword it here for our application): Given a classical sampling strategy with error probability ϵ^{cl} for a given $\delta > 0$, it holds that for any $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_E$ (where $\mathcal{H}_A$ is a d^N dimensional Hilbert space) and any d-dimensional orthonormal basis B, that there exists a collection of ideal states $\{|\phi^t\rangle\}$, indexed by every possible subset choice t, such that $|\phi^t\rangle$ are ideal states for subset t with respect to basis B, and it holds that:

$$\frac{1}{2}\left|\left|\sum_t P_T(t)[\mathbf{t}] \otimes \left([\psi] - [\phi^{\mathbf{t}}]\right)\right|\right| \leq \sqrt{\epsilon^{cl}}. \tag{10}$$

The proof of the above theorem is actually by construction where the ideal states are defined by projecting onto the ideal subspace and a subspace orthogonal to it. In particular, given a fixed t and an input state $|\psi\rangle = \sum_i |i\rangle^B \otimes |E_i\rangle$, then the ideal states are defined by:

$$\begin{aligned}|\psi\rangle &= \langle\phi^t|\psi\rangle\,|\phi^t\rangle + \langle\bar{\phi}^t|\psi\rangle\,|\bar{\phi}^t\rangle \\ &= \alpha \sum_{i \in \mathcal{G}_t} |i\rangle^B \otimes |E_i\rangle + \beta \sum_{i \notin \mathcal{G}_t} |i\rangle^B \otimes |E_i\rangle.\end{aligned}$$

Thus, given some property of Eve's ancilla in the real state, those properties may translate also to the ideal system, a point that will be important in the proof of our main theorem.

We comment on a few things. First, Theorem 1 let's us promote classical sampling strategies to quantum ones where the error (in terms, now, of trace distance) only increases quadratically. Second, one doesn't actually have to perform the sampling strategy in the given basis - the above states exist regardless. Thus, one may use the existence of these states but actually perform different measurements on them, yet still be able to say something about the post-measured state. We will use this later in our proof. Finally, though our wording of Theorem 1 is different from how it was worded originally in [**?**], their original proof is by construction and readily leads to the above statement as shown in [**?**].

Before leaving this section, we discuss a basic sampling strategy for bit strings (i.e., $d = 2$). Let P_T be the uniform distribution on subsets of size m (with $m < N/2$) and let $g(x) = r(x) = w(x)$. From this, it is clear that the set of ideal words is:

$$\mathcal{G}_t = \left\{q \in \{0,1\}^N \ : \ w(q_t) \sim_\delta w(q_{-t})\right\}, \tag{11}$$

where $n = N - m$. Thus, this strategy observes the relative number of 1's in the given string q_t and uses this as a guess as to the number of 1's in the unobserved portion q_{-t}. Then, it was proven in [**?**], that the error probability of this strategy may be bounded by:

$$\epsilon_0^{cl} \leq 2\exp\left(-\delta^2 \frac{mN}{N+2}\right). \tag{12}$$

The above equation will be useful later.

III. New Entropic Uncertainty Relation

We now prove our main result. Consider the following experiment. Let ρ_{ABE} be a quantum state where the A and B registers each consist of N qubits. Also consider two bases Z and $\mathcal{X}_\alpha$, where $\mathcal{X}_\alpha$ is defined to be spanned by the states $|x_0\rangle = \alpha|0\rangle + \sqrt{1-\alpha^2}|1\rangle$ and $|x_1\rangle = \sqrt{1-\alpha^2}|0\rangle - \alpha|1\rangle$ where $\alpha = \sqrt{\frac{1}{2}+b}$ for some bias parameter $b \in [-.5, .5]$ (our methods can be extended to arbitrary complex amplitudes α, however we restrict to real values for this work as the presentation is simpler and, already, this gives an interesting result as shown later in our evaluations). Note that, when $b = 0$, the $\mathcal{X}_\alpha$ basis is the usual Hadamard basis. When $b = \pm 1/2$, the $\mathcal{X}_\alpha$ basis is no different from the Z basis. We assume b is known or can be bounded by the parties running the experiment.

Given ρ_{ABE}, Alice and Bob will choose a random subset t of size $m < N/2$ and measure their qubits, indexed by t, in basis $\mathcal{X}_\alpha$. Let $q \in \{0,1\}^m$ be the result of XOR'ing their measurement results (i.e., $q_i = 0$ if the i'th measurement yielded equal outcomes in the $\mathcal{X}_\alpha$ basis and it is 1 otherwise). This causes the remaining $n = N - m$ qubits to collapse to some state $\rho_{ABE}^{(t,q)}$. Next, the remaining n qubits are measured in the Z basis. Our main result is stated in Theorem 2 below, provides a bound on the min entropy in this Z basis measurement as a function of the bias parameter b, and the Shannon entropy of the observed parity value q.

Our proof assumes the states under investigation have a specific form on the adversary/environment system as defined below in Definition III.1. This assumption is needed in only one part of our proof, though removing the assumption does seem to greatly complicate the proof. We suspect this assumption is not actually required, though a full proof remains elusive. That being said, the assumption below is, in a way, minimal and, in fact, most quantum states investigated in security proofs satisfy it. Thus, while we have to make this assumption on the given quantum state, it is not very problematic towards applications, including cryptographic ones. In fact, this assumption may even be enforced if one utilizes mismatched measurements [**?**], [**?**], [**?**], [**?**] (see also methods in [**?**]).

Definition III.1. Let $|\psi\rangle_{ABE}$ be a quantum state with the A and B portions consisting of N qubits each. Without loss of generality, we may write $|\psi\rangle_{ABE} = \sum_{i\in\mathcal{A}_4^N} \alpha_i |\phi_i\rangle |E_i\rangle$, where $|\phi_i\rangle$ is the Bell basis defined earlier. We say $|\psi\rangle_{ABE}$ is *produced by a depolarizing source* if it holds that $\langle E_i|E_j\rangle = 0$ whenever $i \neq j$.

Note that a depolarizing channel produces a state according to Definition III.1. A state produced by a depolarizing source also produces, in a way, "symmetric" (though potentially still biased based on the measurements' biases) measurement results and so can even be enforced as mentioned earlier (using, potentially, mismatched measurements if measurements are biased [**?**]).

To prove our main result, we'll need the following classical sampling strategy: Given a word $q \in \mathcal{A}_4^{n+m}$, choose a subset $t \subset \{1, \cdots, n+m\}$ of size $|t| = m$ uniformly at random. The guess function is the relative number of 1's and 3's in the observed portion, namely $f(q_t) = \frac{1}{m}\#_{1,3}(q_t)$. The target function is the relative number of 1's and 3's in the unobserved portion, $r(q_{-t}) = \frac{1}{n}\#_{1,3}(q_{-t})$. This induces the set of ideal words:

$$\mathcal{G}_t = \left\{ i \in \mathcal{A}_4^{n+m} \ : \ \frac{1}{m}\#_{1,3}(i_t) \sim_\delta \frac{1}{n}\#_{1,3}(i_{-t}) \right\}. \quad (13)$$

The classical error probability of this sampling strategy is analyzed in the following Lemma:

Lemma 4. Given $\delta > 0$ and $m < n$, the classical error probability ϵ^{cl} of the sampling strategy described above is bounded by:

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

Proof. We prove this by, essentially, reducing to the sampling strategy described at the end of Section II-B and bounded by Equation 12. Let $\widetilde{\mathcal{G}}_t$ be the set of ideal words for the earlier defined sampling strategy (see Equation 11). Let $q \in \mathcal{A}_4^N$ (with $N = n+m$) and consider a fixed subset t of size $m < N/2$. Then, define the word $\widetilde{q} \in \{0,1\}^N$ where $\widetilde{q}_i = 0$ if $q_i = 0$ or 2 and $\widetilde{q}_i = 1$ otherwise. Thus, $w(\widetilde{q}_t) = \frac{1}{m}\#_{1,3}(q_t)$ and, similarly, for the complement of t. In particular, for any t, it holds that $q \notin \mathcal{G}_t \iff \widetilde{q} \notin \widetilde{\mathcal{G}}_t$. From this, we conclude:

$$Pr(q \notin \mathcal{G}_t) = Pr\left(\widetilde{q} \notin \widetilde{\mathcal{G}}_t\right) \leq \max_{i\in\{0,1\}^N} Pr\left(i \notin \widetilde{\mathcal{G}}_t\right) \leq \epsilon_0^{cl},$$

where ϵ_0^{cl} was defined in Equation 12. Since the above is true for any q, the proof is complete. □

We now have all the tools we need to state and prove our main result:

Theorem 2. Let $\epsilon > 0$, $\alpha = \sqrt{1/2+b}$ for some $b \in [-.5, .5]$, and let $|\psi\rangle_{ABE}$ be a state prepared by a depolarizing source (according to Definition III.1) where the A and B registers each consist of N qubits. Assume a random subset is chosen t of size m and a measurement in the $\mathcal{X}_\alpha$ basis is performed in the A and B registers, indexed by t and resulting in outcomes $q_A, q_B \in \{0,1\}^m$. The remaining qubits in the A and B portions are measured in the Z basis resulting in state $\rho_{ABE}^{(t,q)}$ (which depends on $q = q_A \oplus q_B$ and t). Then, except with probability $\epsilon_{fail} = (16\epsilon)^{1/3}$, it holds that:

$$Pr\left(H_\infty^{8\epsilon+3(2\epsilon)^{1/3}}(A|E)_{\rho^{(t,q)}} \geq n(1 - \hat{h}(w(q)+\nu+\delta))\right), \quad (14)$$

where $\hat{h}(x)$ is the bounded binary entropy function and:

$$\delta = \sqrt{\frac{(m+n+2)}{m(m+n)}\ln\frac{2}{\epsilon^2}} \quad (15)$$

and

$$\nu = 4b^2 + \frac{1}{\sqrt{m}}\ln\frac{1}{2\epsilon} \quad (16)$$

The probability is over the choice of subset and the measurement outcome $q = q_A \oplus q_B$.

Proof. Let $\epsilon > 0$ be given and set δ as in Equation 15. From Theorem 1, and using the sampling strategy described earlier in this section and analyzed in Lemma 4, there exist ideal states $\{|\phi^t\rangle_{ABE}\}$, with respect to the Bell basis, such that $|\phi^t\rangle \in \text{span}\,(\mathcal{G}_t) \otimes \mathcal{H}_E$ where:

$$\text{span}\,(\mathcal{G}_t) = \text{span}\left\{|\phi_q\rangle \ : \ \frac{1}{m}\#_{1,3}(q_t) \sim_\delta \frac{1}{n}\#_{1,3}(q_{-t})\right\}$$

and:

$$\left|\left|\sum_t P_T(t)[\mathbf{t}] \otimes ([\psi] - [\phi^{\mathbf{t}}])\right|\right| \le \sqrt{\epsilon^{cl}} \le \epsilon,$$

where the latter inequality follows from Lemma 4 and our choice of δ.

Note that, since these states are constructed by projecting $|\psi\rangle$ into the subspace of ideal states, it is not difficult to see that, since $|\psi\rangle$ is produced by a depolarizing source, each $|\phi^t\rangle$ is also. (See the discussion under Theorem 1.)

We first analyze the ideal states and show the min entropy there is high, based on the observed $\mathcal{X}_\alpha$ basis noise.

By permuting subspaces so that those systems indexed by t are the left-most system, we may write:

$$|\phi^t\rangle \cong \sum_{i \in \mathcal{A}_4^m} \alpha_i |\phi_i\rangle \otimes \underbrace{\sum_{\ell \in J_i} \beta_{\ell|i} |\phi_\ell\rangle |E_{i,j}\rangle}_{|\mu_i\rangle}, \qquad (17)$$

with:

$$J_i = \left\{\ell \in \mathcal{A}_4^n \ : \ \frac{1}{n}\#_{1,3}(\ell) \sim_\delta \frac{1}{m}\#_{1,3}(i)\right\}.$$

Note that we are permuting subspaces only for clarity in presentation, this is not a required step of the protocol. Now, if we were able to make a Bell basis measurement on subset t, observing, say, outcome $x \in \mathcal{A}_d^m$, we would know, for certain, that the post measured state must have collapsed to $|\phi_x^t\rangle = \sum_y \beta_y |\phi_x\rangle |E_x\rangle$ where the number of 1's and 3's in y is δ-close to the number of 1's and 3's in the observed x. However, we can only measure in the $\mathcal{X}_\alpha$ basis leading to outcomes q_A and q_B. The idea is that, based on α, the observed string cannot be too different from the underlying state in the original Bell basis. To prove this formally, we now consider the following two-qubit basis based on $\mathcal{X}_\alpha$ (which we call the $\mathcal{X}_\alpha$-Bell basis):

$$|\phi_0^X\rangle = \frac{1}{\sqrt{2}}|x_0, x_0\rangle + \frac{1}{\sqrt{2}}|x_1, x_1\rangle$$
$$|\phi_1^X\rangle = \frac{1}{\sqrt{2}}|x_0, x_1\rangle + \frac{1}{\sqrt{2}}|x_1, x_0\rangle$$
$$|\phi_2^X\rangle = \frac{1}{\sqrt{2}}|x_0, x_0\rangle - \frac{1}{\sqrt{2}}|x_1, x_1\rangle$$
$$|\phi_3^X\rangle = \frac{1}{\sqrt{2}}|x_0, x_1\rangle - \frac{1}{\sqrt{2}}|x_1, x_0\rangle$$

Note that if $\alpha = 1/\sqrt{2}$ (thus $\mathcal{X}_\alpha$ basis is the Hadamard basis), then it holds $|\phi_i^X\rangle = |\phi_i\rangle$ for $i = 0, 1, 2, 3$.

Changing basis of those systems indexed by t in Equation 17, we have:

$$|\phi^t\rangle \cong \sum_{i \in \mathcal{A}_4^m} \alpha_i \left(\sum_{j \in \mathcal{A}_4^m} \langle \phi_j^X | \phi_i \rangle |\phi_j^X\rangle\right) \otimes |\mu_i\rangle$$
$$= \sum_{j \in \mathcal{A}_4^m} |\phi_j^X\rangle \otimes \left(\sum_{i \in \mathcal{A}_4^m} \alpha_i \langle \phi_j^X | \phi_i \rangle |\mu_i\rangle\right). \qquad (18)$$

A measurement is now performed on the A and B registers, indexed by t, in the $\mathcal{X}_\alpha$ basis. However, the important factor will be the number of errors in the measurements. Thus, we equivalently consider Alice and Bob measuring in the following two-outcome POVM: $X_0 = [\mathbf{x_0}, \mathbf{x_0}] + [\mathbf{x_1}, \mathbf{x_1}]$ and $X_1 = [\mathbf{x_0}, \mathbf{x_1}] + [\mathbf{x_1}, \mathbf{x_0}]$. Thus, X_1 represents an outcome where Alice and Bob get different measurement outcomes after measuring in basis $\mathcal{X}_\alpha$. Note that an outcome of X_1 can only occur if the underlying state is $|\phi_1^X\rangle$ or $|\phi_3^X\rangle$. Of course, if $\alpha = 1/\sqrt{2}$ and $\mathcal{X}_\alpha$ is the Hadamard basis, this gives us an exact count of the number of 1's and 3's in the state i (needed to bound the entropy in $|\mu_i\rangle$). However, we actually only count the number of 1's and 3's in j - from this, we will need to determine a good bound for the number of 1's and 3's in i. Intuitively, this should follow since, for α close to $1/\sqrt{2}$, the $\mathcal{X}_\alpha$-Bell states are almost the Bell states and, so, any entropy equation should behave similarly in both bases for small bias parameter b. We prove this rigorously below.

For a fixed $j \in \mathcal{A}_4^m$, and user-defined $\nu \ge 0$, let's define "good" and "bad" states as follows:

$$G_j = \{i \in \mathcal{A}_4^m \ : \ \Delta_H(i, j) \le m\nu\}$$
$$B_j = \{i \in \mathcal{A}_4^m \ : \ \Delta_H(i, j) > m\nu\}.$$

Note that ν will control how likely we are to get a "good" state as larger ν means more states are considered good - though this will lead to additional uncertainty in i as we also want to control how far i is from j. We will show later that ν may be made a function of ϵ. Given this, we may rewrite Equation 18 as follows: $|\phi^t\rangle \cong$

$$\sum_{j \in \mathcal{A}_4^m} |\phi_j^X\rangle \otimes \left(\sum_{i \in G_j} \alpha_i \langle \phi_j^X | \phi_i \rangle |\mu_i\rangle + \sum_{i \in B_j} \alpha_i \langle \phi_j^X | \phi_i \rangle |\mu_i\rangle\right) \qquad (19)$$

Let $|g_j\rangle = \sum_{i \in G_j} \alpha_i \langle \phi_j^X | \phi_i \rangle |\mu_i\rangle$ and $|b_j\rangle = \sum_{i \in B_j} \alpha_i \langle \phi_j^X | \phi_i \rangle |\mu_i\rangle$ and so $|\phi^t\rangle \cong \sum_j |\phi_j^X\rangle \otimes (|g_j\rangle + |b_j\rangle)$.

We now consider an "ideal-ideal" state $|\widetilde{\phi^t}\rangle$ defined as:

$$|\widetilde{\phi^t}\rangle = \frac{1}{\sqrt{M}} \sum_{j \in \mathcal{A}_4^m} |\phi_j^X\rangle \otimes |g_j\rangle, \qquad (20)$$

where $M = \sum_j \langle g_j | g_j \rangle$. By basic properties of trace distance, we have:

$$\frac{1}{2}\left|\left|[\phi^{\mathbf{t}}] - [\widetilde{\phi^{\mathbf{t}}}]\right|\right| = \sqrt{1 - |\langle \phi^t | \widetilde{\phi^t} \rangle|^2}. \qquad (21)$$

Since all states are prepared by a depolarizing source, we have:

$$\begin{aligned}1 - |\langle \phi^t | \widetilde{\phi}^t \rangle|^2 &= 1 - \left| \frac{1}{\sqrt{M}} \sum_j \left(\langle g_j | g_j \rangle + \langle g_j | b_j \rangle \right) \right|^2 \\ &= 1 - \frac{1}{M} \left(\sum_j \langle g_j | g_j \rangle \right)^2 = 1 - M.\end{aligned}$$

We claim that $1-M$ may be bounded above by an arbitrarily small value if user parameters are set appropriately. Note that $1-M = \sum_j \langle b_j|b_j\rangle$. This follows from the fact that Equation 19 is normalized and so:

$$1 = \sum_j (\langle g_j|g_j\rangle + \langle b_j|b_j\rangle) \Longrightarrow \sum_j \langle b_j|b_j\rangle = 1-M.$$

Now, since the state is produced by a depolarizing source, we find:

$$\begin{aligned}\sum_{j\in\mathcal{A}_4^m} \langle b_j|b_j\rangle &= \sum_{j\in\mathcal{A}_4^m} \left(\sum_{i\in B_j} |\alpha_i|^2 |\langle \phi_j^X|\phi_i\rangle|^2 \right) \\ &= \sum_{i\in\mathcal{A}_4^m} |\alpha_i|^2 \sum_{j\in B_i} |\langle \phi_j^X|\phi_i\rangle|^2. \qquad (22)\end{aligned}$$

For a fixed $i \in \mathcal{A}_4^m$, let's focus on $\sum_{j\in B_i} |\langle \phi_j^X|\phi_i\rangle|^2$. The following identities can be easily shown for any $\alpha \in [0,1]$:

$$\begin{aligned}&|\phi_0^X\rangle = |\phi_0\rangle\,, && |\phi_3^X\rangle = |\phi_3\rangle\,,\\ &|\phi_1^X\rangle = \sqrt{p}\,|\phi_2\rangle + \sqrt{q}\,|\phi_1\rangle\,, &&\\ &|\phi_2^X\rangle = \sqrt{q}\,|\phi_2\rangle - \sqrt{p}\,|\phi_1\rangle &&\end{aligned}$$

where:

$$\sqrt{p} = \beta^2 - \alpha^2 = 2b, \qquad \sqrt{q} = 2\alpha\beta$$

From this, we see that, given a fixed $i \in \mathcal{A}_4^m$, and a particular $j \in B_i$, then if there exists even a single index $\ell \in \{1,2,\cdots,m\}$ such that $i_\ell = 0$ and $j_\ell \neq 0$ or $i_\ell = 3$ and $j_\ell \neq 3$, then the entire inner product $\langle \phi_j^X|\phi_i\rangle = 0$. Since we want to upper-bound Equation 22, the only way that expression can have non-zero terms is if, for a given i, $j_\ell = 0$ whenever $i_\ell = 0$ and $j_\ell = 3$ whenever $i_\ell = 3$. If $i_\ell = 1$ or 2, then j_ℓ may be either 1 or 2. Of course, since we are summing over "bad" states, there must be at least $m\nu$ differences in j.

Considering any fixed i, if $\#_{1,2}(i) \leq m\nu$, it is clear that $\sum_{j\in B_i} |\langle \phi_j^X|\phi_i\rangle|^2 = 0$ since at least one index in each $j \in B_i$ must differ on an index where $i_\ell = 0$ or 3. The only time the sum over j can be non-zero is if i satisfies $\#_{1,2}(i) = k > m\nu$. For any such i, there exists a $j \in B_i$ such that $\Delta_H(i,j) = d$ with $m\nu < d \leq k$ and where $j = i$ everywhere except on d indices where i happens to be 1 (j will be a 2 on such an index) or 2 (j will be a 1 on such an index). This would lead to a value of $|\langle \phi_j^X|\phi_i\rangle|^2 = p^d q^{k-d} = p^d(1-p)^{k-d}$, where we note that $q = 1-p$. The p^d term comes from changing the d indices (flipping a 1 to a 2 and a 2 to a 1) while the q^{k-d} term comes from leaving the remaining 1's and 2's in i the same in j. Of course the rest of i are 0's and 3's which are kept the same in j. Since there are $\binom{k}{d}$ such strings j, it follows that for any i with $\#_{1,2}(i) = k > m\nu$, that $\sum_{j\in B_i} |\langle \phi_j^X|\phi_i\rangle|^2 = \sum_{d=m\nu}^{k} \binom{k}{d} p^d (1-p)^{k-d}$.

Continuing this logic, we can write Equation 22 in the following way:

$$\begin{aligned}1 - M &= \sum_{i\in\mathcal{A}_4^m} |\alpha_i|^2 \sum_{j\in B_i} |\langle \phi_j^X|\phi_i\rangle|^2 \\ &\leq \sum_{k=m\nu}^{m} \widetilde{p}(k) \sum_{d=m\nu}^{k} \binom{k}{d} p^d (1-p)^{k-d}, \qquad (23)\end{aligned}$$

where:

$$\widetilde{p}(k) = \sum_{i\,:\,\#_{1,2}(i)=k} |\alpha_i|^2.$$

Note that, if $m\nu$ is not an integer, we take the floor value and thus the reason for the inequality above. Note also that $\sum_{k=0}^{m} \widetilde{p}(k) = \sum_{i\in\mathcal{A}_4^m} |\alpha_i|^2 = 1$. Thus:

$$\begin{aligned}1 - M &\leq \max_{k\leq m} \left(\sum_{d=m\nu}^{k} \binom{k}{d} p^d (1-p)^{k-d} \right) \\ &\leq \sum_{d=m\nu}^{m} \binom{m}{d} p^d (1-p)^{m-d}. \qquad (24)\end{aligned}$$

This can be considered the tail of the CDF of a binomial distribution with parameter p and m trials. By Hoeffding's inequality, we may derive the following bound, for $\nu \geq p$:

$$1 - M \leq \exp\left(-2m(\nu-p)^2\right). \qquad (25)$$

By setting $\nu = p + \frac{1}{\sqrt{m}} \ln\frac{1}{2\epsilon}$, it holds that $\sqrt{1-M} \leq \epsilon$ and thus we have:

$$\frac{1}{2}\left|\left| \left[\phi^{\mathbf{t}}\right] - \left[\widetilde{\phi}^{\mathbf{t}}\right] \right|\right| \leq \sqrt{1-M} \leq \epsilon.$$

Of course, this is true for any subset t in the ideal system $|\phi^t\rangle$ and, so, by the triangle inequality, along with elementary properties of trace distance, we have:

$$\frac{1}{2}\left|\left| \sum_t P_T(t)[\mathbf{t}] \otimes \left([\psi] - \left[\widetilde{\phi}^{\mathbf{t}}\right] \right) \right|\right| \leq 2\epsilon. \qquad (26)$$

Thus, since the given input state $|\psi\rangle$ is actually 2ϵ close to these "ideal-ideal" states, we may analyze the entropy there and use Lemma 2 to promote the analysis to the real state.

Define $\sigma_{TQ} = \sum_t P_T(t)[\mathbf{t}] \otimes \left[\widetilde{\phi}^{\mathbf{t}}\right]$ and we analyze the min entropy in this state, following the conclusion of the measurements and sampling. Sampling on such a state implies measuring the subset register T causing the state to collapse to $|\widetilde{\phi}^t\rangle$. After measuring those systems indexed by t in the POVM X_0 and X_1 defined above, observing $q \in \{0,1\}^m$, then tracing out the measured portion, the state collapses to $|\widetilde{\phi}_q^t\rangle$ which may be written in the form:

$$|\widetilde{\phi}^t\rangle = \sum_{\substack{j\in\mathcal{A}_4^m \\ \#_{1,3}(j)=\#_1(q)}} p_j P\left(\sum_{i\in G_j} \beta_{i|j}\,|\mu_i\rangle \right). \qquad (27)$$

The above can be seen easily from Equation 20 and simply re-parameterizing. Note that whenever an observation of X_1 is observed, the underlying index of j may be either a 1 or a 3 and, thus, the state collapses to some j where we have a bound on the number of 1's and 3's based on the observed q. Let $Q = \#_1(q)$. Continuing our derivation, we may write the above state in the following form:

$$
\begin{aligned}
|\widetilde{\phi}^t\rangle &= \sum_{\substack{j\in\mathcal{A}_4^m\\ \#_{1,3}(j)=Q}} p_j P\left(\sum_{i\in G_j}\beta_{i|j}\,|\mu_i\rangle\right)\\
&= \sum_{\substack{j\in\mathcal{A}_4^m\\ \#_{1,3}(j)=Q}} p_j P\left(\sum_{\substack{i\in\mathcal{A}_4^m\\ \Delta_H(i,j)\leq m\nu}}\beta_{i|j}\right.\\
&\left.\times\left[\sum_{\substack{\ell\in\mathcal{A}_4^n\\ \frac{1}{n}\#_{1,3}(\ell)\sim_\delta\frac{1}{m}\#_{1,3}(i)}}\gamma_{\ell|i,j}\,|\phi_\ell\rangle\,|E_{\ell|i,j}\rangle\right]\right)\\
&= \sum_{\substack{j\in\mathcal{A}_4^m\\ \#_{1,3}(j)=Q}} p_j P\left(\sum_{\substack{\ell\in\mathcal{A}_4^m\\ \frac{1}{n}\#_{1,3}(\ell)\leq w(q)+\nu+\delta}}\widetilde{\gamma}_{\ell|j}\,|\phi_\ell\rangle\,|\widetilde{E}_{\ell|j}\rangle\right).
\end{aligned}
\tag{28}
$$

Above, for the last equality, we simply re-parameterized and changed the order of the summation. Note that some of the $\widetilde{\gamma}_{\ell|j}$ values may be zero. We did this so that we can easily use Equation 5 along with Lemma 3 to find the following lower-bound: $H_\infty(A|E)_{\widetilde{\phi}_q^t} \geq 1 - \hat{h}(w(q)+\nu+\delta)$, where the A register is used to store a Z basis measurement of the first particle of each Bell pair in the above state (the second particle is traced out).

Of course, this is only the ideal state. However, Equation 26, along with Lemma 2, finishes the proof. In particular, the X random variable for Lemma 2 is the subset choice t and measurement outcome q while the CPTP map $\mathcal{F}$ is the choice of subset and the measurement in POVM $\{X_0, X_1\}$.

□

Corollary III.1. Let ρ_{ABE} be a quantum state where the A and B registers hold a single qubit. Let $\alpha = \sqrt{1/2+b}$ for some $b \in [-.5, .5]$ and let Q_X be the random variable induced by performing an $\mathcal{X}_\alpha$ basis measurement on the A and B qubit and XOR'ing the outcome. Let Q_X^b be the random variable which takes the value 1 with probability $\min(1/2, Pr(Q_X = 1) + 4b^2)$. Then it follows that:

$$H(A_Z|E)_\rho + H\left(Q_X^b\right) \geq 1. \tag{29}$$

where A_Z is the random variable induced by Alice's Z basis measurement on her particle in ρ_{ABE}.

Proof. This follows immediately from Theorem 2 and by the asymptotic equipartition property [**?**] and the law of large numbers. □

A. Comparison to Standard Entropic Uncertainty in the Asymptotic Limit

In the next section, we apply our new entropic uncertainty bound to two particular cryptographic applications, each of which were proven in previous work, using standard entropic uncertainty relations for quantum min entropy and we compare the resulting bit generation rates for various bias parameters and noise levels in the channel. However, before this, we show here a comparison in the asymptotic case to the following standard entropic uncertainty inequality proven in [**?**] (written in a form, here, for the particular scenario and measurements we're interested in):

$$H(A_Z|E) + H(A_X|B_X) \geq -\log_2\left(\frac{1}{2}+b\right), \tag{30}$$

for $b \geq 0$. Such a comparison gives a general notion of the improvement that is possible using our new result, since the asymptotic case will always provide an upper-bound.

For this comparison, we assume the state is produced by a depolarization channel (which is easily confirmed to satisfy Definition III.1), and thus have $H(A_X|B_X) = h(q)$, where q will denote the error rate in the channel. Comparing with Equation 29, of course when $b = 0$, the two identities agree exactly, as expected.

The comparison for $b \geq 0$ is shown in Figure 1. There are several interesting observations to make here; in particular, we note that, in many settings, our entropic uncertainty relation produces a strictly better bound on the entropy. However, this is not always the case. In particular, when the noise and bias are both small, standard entropic uncertainty produces a better result. However, in all other tests we performed when the noise is larger and there is bias, our result produces a strictly better bound on the entropy. Since both our new result and standard results are both lower-bounds, one may, in practice, simply take the maximum of the two and, thus, our work can only benefit future analyses requiring bounds on quantum entropy with biased measurements.

IV. Applications

We now apply our main theorem to two different cryptographic applications. The first is a quantum random number generator (QRNG) with a faulty and uncharacterized source. The second is a QKD protocol where Alice and Bob are not able to measure in mutually unbiased bases, as is typically required by BB84 style protocols to maximize key generation rates. In both instances we show there are several cases where our new result significantly outperforms prior work using standard entropic uncertainty relations.

Quantum Random Number Generation: We first consider a *source independent* (SI) QRNG protocol whereby the measurement devices are fully characterized, but the source is unknown, as introduced in [**?**]. The goal of a QRNG

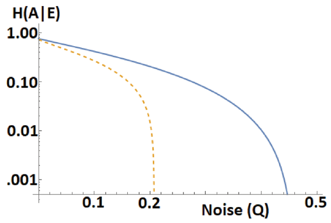

Fig. 1. Comparing our new entropic uncertainty relation (Solid lines, Equation 29) to standard entropic uncertainty relations in the asymptotic limit (Dashed lines, Equation 30). Since these are lower-bounds, higher is better here. Left: Here we fix the bias at $b = .1$ and vary the noise parameter q (x-axis) from 0 to 50%. Right: Here, we fix the noise at 0% (Blue and Yellow) and 20% (Green and Red) as the bias (x-axis) varies from $b = 0$ to $b = 0.5$. Note that our new result produces the same or better results in most settings. However, when there is no noise, our result tends to perform worse, except for a certain range of bias $b < .2$ as shown in the Right figure (Blue and Yellow comparison). See text for additional discussion.

protocol is to distill a cryptographically secure random bit string from a quantum source. SI security models offer a nice "middle ground" between fully trusted devices (which have weak security guarantees) and fully device independent models, which offer strong security guarantees [**?**], [**?**] but have low bit generation rates with today's technology [**?**], [**?**]. SI-QRNG protocols have been demonstrated experimentally to have high bit generation rates reaching in the Gbps range [**?**], [**?**]. For a general survey of QRNG protocols, the reader is referred to [**?**].

Typically SI-QRNG protocols operate by having the uncharacterized source prepare quantum signals and sending them to a user. The user measures some of the signals in one basis to determine the fidelity of the signal. The remaining signals are measured in an alternative basis leading to a *raw random string*. The raw random string may not be truly uniform random and so needs to be further processed through privacy amplification. If one can bound the quantum min entropy of the raw random string, Equation 4 may be used to determine the number of bits that may be extracted from the source, even if the source happens to be adversarial.

We analyze the SI-QRNG protocol introduced in [**?**]. In this protocol, the source should prepare N copies of the Bell state $|\phi_0\rangle$ and send both particles to Alice. Alice chooses a random subset and measures both particles in the $\mathcal{X}_\alpha$ basis (denoting by q as the outcome of the parity of these measurements; namely $q_i = 0$ if on the i'th test, Alice observed the same outcome, either $|x_0\rangle$ or $|x_1\rangle$, in both particles). For the remaining Bell pairs, Alice measures the first particle in the Z basis, discarding the second particle. Let $\alpha = \sqrt{\frac{1}{2} + b}$ with $b \geq 0$ (the case when $b < 0$ turns out to be symmetric with the equations we use). Using a standard entropic uncertainty relation from [**?**], the authors of [**?**] were able to derive the following bound on the bit generation rate:

$$r_{other} = \frac{1}{N}\left(-n\log\left(\frac{1}{2}+b\right) - n\log_2\gamma(w(q)+\delta')\right), \tag{31}$$

where: $\gamma(x) = \left(x+\sqrt{1+x^2}\right)\left(\frac{x}{\sqrt{1+x^2}-1}\right)^x$, and $\delta' = 2\sqrt{\frac{N^2}{n^2 m}\ln\frac{4}{\epsilon'}}$. Of course, the original work in [**?**] only considered the case when $b = 0$, however since their proof relies on the standard entropic uncertainty relation from [**?**], it is not difficult to see it can be applied to any b.

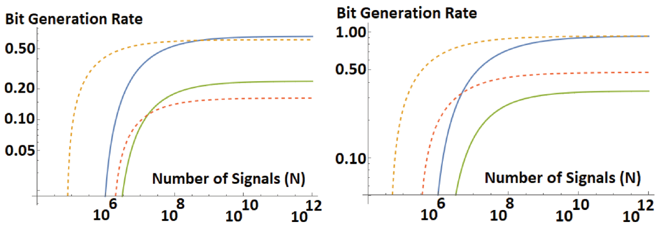

Fig. 2. Evaluating and comparing the QRNG bit generation rates with biased measurements using our new result (Solid lines, Equation 32) and prior work using standard entropic uncertainty (Dashed lines, Equation 31) as the number of signals N (the x-axes) increases. Left: Assuming 5% noise (thus, $w(q) = .05$), Right: Assuming no noise ($w(q) = 0$). Blue: Our new result with no bias; Yellow: prior work with no bias; Green: Our new result with $b = 0.2$; Red: Prior work with $b = 0.2$. We note that when there is some noise, our result clearly produces higher bit generation rates in all comparable cases as long as the number of signals is large enough. When there is no noise, our result produces lower rates. As the number of signals increases, our result converges to prior work when $b = 0$, but produces worse results when $b = 0.2$ in the no noise case (right); however in the noisy case (left), our result surpasses prior work as the number of signals increases. See text for more discussion.

Using our Theorem 2, along with Equation 4, we can, instead, derive the following bit generation rate:

$$r_{ours} = \frac{1}{N}\left(n(1-\hat{h}(w(q)+\nu+\delta)) + 2\log\frac{1}{\epsilon}\right). \tag{32}$$

In our evaluations, we set a sampling size of 7% (thus $m = 0.07N$) and we set $\epsilon' = 10^{-12}$ (for r_{other}) and $\epsilon = 10^{-36}$ (for r_{ours}). This implies a failure probability and a security level on the order of 10^{-12} for both equations to make a fair comparison. Note that in our bound, we require a much smaller ϵ to guarantee the same level of security as other work - this is a disadvantage to our approach caused by the use of Lemma 2. However, we will see that even with this disadvantage, our result still produces higher rates in many scenarios.

Figures 2 and 3 compare the bit generation rates of this protocol using our new result (solid lines) and prior work using standard entropic uncertainty (dashed lines). We note several things. First, our new bound produces higher bit generation rates in many of the tested scenarios. There are times, however, when prior work surpasses ours - in particular when the noise is low, however this was also observed in the previous section. We conjecture that our methods may be improved in the low noise case, however we leave that as interesting future work. Regardless, our work provides substantially improved results in many cases and, since these are all lower bounds, users of these protocols with biased measurements may simply take the max of both our work and prior work to derive the actual bit generation rate.

Quantum Key Distribution: Next, we consider QKD. Here, we derive a key-rate expression for standard BB84 [**?**] where, however, instead of using the Z and Hadamard bases as usual, Alice and Bob measure in either the Z or the $\mathcal{X}_\alpha$

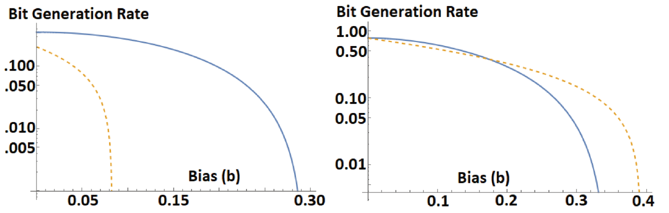

Fig. 3. Evaluating and comparing the QRNG bit generation rates with biased measurements using our new result (Solid lines, Equation 32) and prior work using standard entropic uncertainty (Dashed lines, Equation 31) as the bias parameter b (the x-axes) increases. We fix $N = 10^{10}$ for these evaluations. Left: Assuming a high level of noise at 15% (thus, $w(q) = .15$), Right: Assuming a low level of noise at 2% ($w(q) = 0.02$). Blue: Our new result; Yellow: prior work. Here, again, we see that at high noise our new rate produces substantially higher bit generation rates and has a higher tolerance to biased measurements, whereas at lower levels of noise, standard entropic uncertainty produces a better result in most cases (except for a low level of bias $b < .2$).

basis. Equivalently, Alice sends states in either the Z or $\mathcal{X}_\alpha$ basis while Bob measures in either basis. Using results from [**?**], which depend on standard entropic uncertainty relations, the following key-rate for this protocol was derived:

$$r_{old} = \frac{1}{N}\left(n(c - h(w(q) + \mu)) - \lambda_{EC} - \log_2 \frac{2}{\hat{\epsilon}^2}\right), \quad (33)$$

where λ_{EC} is the amount of information leaked during error correction, $c = -\log_2\left(\frac{1}{2} + b\right)$ and: $\mu = \sqrt{\frac{N(m+1)}{nm^2}\ln\frac{2}{\hat{\epsilon}}}$. The above equations were derived using an entropic uncertainty relation from [**?**].

On the other hand, our new relation in Theorem 2 can be used to immediately find the following key-rate for the protocol:

$$r_{new} = \frac{1}{N}\left(n(1 - \hat{h}(w(q) + \nu + \delta)) - \lambda_{EC} - \log_2 \frac{1}{\epsilon}\right). \quad (34)$$

Note we are ignoring an additional leakage of $\log \frac{1}{\epsilon_{cor}}$ *in both key-rate expressions* caused by a final correctness check - however such a leakage would apply equally to both key-rate expressions and, since we are only interested in a direct comparison, this (small) leakage will not affect the results presented here.

We set the failure rate and security level, along with the sampling rate, similar to the QRNG case. Finally, we use $\lambda_{EC} = 1.2h(w(q) + \delta)$ for our new work and $\lambda_{EC} = 1.2h(w(q) + \mu)$ for previous work (r_{old}); note that δ is usually larger than μ so this is actually to the advantage of prior work (as is setting ϵ so small to produce the same failure rate as prior work - this will actually benefit prior work in our comparison). Despite this, our new result shows significant improvement over prior work in several, though not all, settings as shown in Figures 4 and 5. As shown in Figure 4, in the no noise and no bias case, prior work surpasses our work. However, as the bias increases, our new bound surpasses prior work. Figure 5 again shows previous trends in that our bound is best when there is both bias and significant noise.

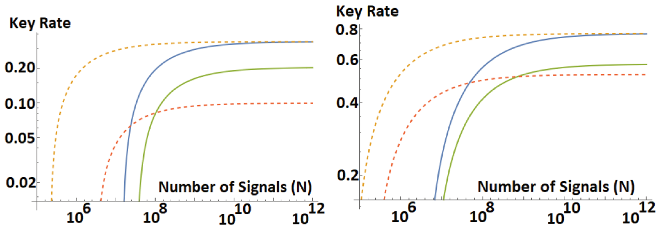

Fig. 4. Evaluating and comparing the QKD key generation rates with biased measurements using our new result (Solid lines, Equation 34) and prior work using standard entropic uncertainty (Dashed lines, Equation 33) as the number of signals N (the x-axes) increases. Left: Assuming 5% noise (thus, $w(q) = .05$), Right: Assuming 1% noise ($w(q) = 0.01$). Blue Solid: Our new result with $b = 0$; Yellow Dashed: prior work with $b = 0$; Green Solid: Our result with $b = 0.1$; Red Dashed: Prior work with $b = 0.1$.

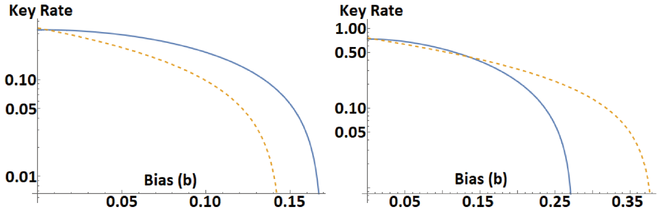

Fig. 5. Evaluating and comparing the QKD key generation rates with biased measurements using our new result (Solid lines, Equation 34) and prior work using standard entropic uncertainty (Dashed lines, Equation 33) as the bias parameter b (the x-axes) increases. We fix $N = 10^{10}$ for these evaluations. Left: Assuming 5% noise (thus, $w(q) = .05$), Right: Assuming a lower level of noise at 1% ($w(q) = 0.01$). Blue solid: Our new result; Yellow dashed: prior work.

V. Closing Remarks

In this work, we derived a new entropic uncertainty relation for biased measurements. We applied our result to QRNG and QKD protocols and compared to prior work. We also compared our relation in the asymptotic scenario to standard entropic uncertainty relations. Our evaluations and comparisons showed that there are several cases where our new relation surpassed prior work, sometimes substantially so. Our result seems best when there is both noise in the channel and bias in the measurements. When the noise is very low or non-existent, prior work produced better results. However, since our result, along with prior work, all produce lower-bounds on the min-entropy, users may simply evaluate both and take the maximum.

Many interesting open questions remain. Most important would be to remove the need for Definition III.1. We suspect our method does not actually need this assumption on the state. It is only used in one part of the proof, to more easily bound the trace distance of two particular states, and we suspect other methods may be used for this. Nonetheless, even with this assumption, our result is still highly practical to quantum cryptography. Other open questions include extending this work to higher dimensions beyond qubits, and dealing with other imperfect measurements beyond bias.

Acknowledgments: The author would like to acknowledge support from the NSF under grant number 2143644.