Quantum Information Processing (2019) 18:368
https://doi.org/10.1007/s11128-019-2481-5

Quantum sampling and entropic uncertainty

Walter O. Krawec[1]

Received: 5 May 2019 / Accepted: 18 October 2019 / Published online: 29 October 2019

Abstract

In this paper, we show an interesting connection between a quantum sampling technique and quantum uncertainty. Namely, we use the quantum sampling technique, introduced by Bouman and Fehr, to derive a novel entropic uncertainty relation based on smooth min- entropy, the binary Shannon entropy of an observed outcome, and the probability of failure of a classical sampling strategy. We then show two applications of our new relation. First, we use it to develop a simple proof of a version of the Maassen and Uffink uncertainty relation. Second, we show how it may be applied to quantum random number generation.

Keywords Quantum information · Entropic uncertainty · Quantum sampling · Quantum cryptography

1 Introduction

In this paper, we revisit a famous entropic uncertainty relation proven by Maassen and Uffink [1] (which followed a conjecture by Kraus [2] and was also an improvement of an entropic uncertainty relation first proposed by Deutsch [3]). Given a quantum system ρ and two projective measurements (PMs) $\{M_x\}$ and $\{N_x\}$ (where $M_x = |\mu_x\rangle\langle\mu_x|$ and $N_y = |\nu_y\rangle\langle\nu_y|$ for some orthonormal bases $\{|\mu_x\rangle\}$ and $\{|\nu_y\rangle\}$), then one cannot necessarily be certain of the outcome of both measurements. More specifically, the relation states:

$$H(M) + H(N) \geq -\log_2 c, \tag{1}$$

where c is a function of the two measurements, namely:

$$c = \max_{x,y} |\langle\mu_x|\nu_y\rangle|^2. \tag{2}$$

✉ Walter O. Krawec
walter.krawec@uconn.edu

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

This relation, and numerous others like it ([4–7] just to list a very few), is not only interesting in and of themselves, but also has numerous other applications throughout quantum information science and quantum cryptography. For a general survey of entropic uncertainty relations, the reader is referred to [8–10].

In this paper, using a quantum sampling technique introduced in [11], we derive a novel entropic uncertainty relation based on smooth *quantum* min-entropy with a direct connection to *classical* sampling strategies. We use this to derive a novel, and in our opinion simpler, proof of Eq. 1 for projective measurements over two-dimensional systems. We also show how our new bound can be applied to cryptographic applications. To our knowledge, this sampling technique has not seen application to more broad areas of quantum information before our paper.

Our new entropic uncertainty bound utilizes smooth min-entropy and has a direct connection to sampling strategies. It is also applicable for states which are not necessarily i.i.d.; that is, our result is applicable to arbitrary states and we do *not* need to assume the given state is i.i.d. This is very useful for cryptographic applications as non-i.i.d. states arise when an adversary has the ability to perform an arbitrary general attack on a quantum state; thus, the ability for our bound to handle such arbitrary systems means it can be used to prove security for some protocols against general coherent attacks. This new relation, informally, states that, except with small probability (determined by the user and the dimension of the system), measuring a portion of a system in one basis resulting in outcome q implies the smooth min-entropy in the remaining portion, after measuring in a second basis, can be lower-bounded by the binary Shannon entropy of the Hamming weight of q and the maximal overlap of the two basis measurements, up to some error induced by the sampling technique. This new relation, which to our knowledge has not been discovered before, may hold interesting applications in quantum cryptography as we discuss later. Furthermore, the techniques we used to derive and prove this new relation may be useful in further extending the quantum sampling technique to other application domains.

There are several contributions in this work. First, we discover a novel entropic uncertainty bound (involving smooth min-entropy and applicable to arbitrary, non-i.i.d. states) directly related to sampling strategies and which may have interesting applications to quantum cryptography and information theory. We show a rather interesting connection between quantum sampling and quantum uncertainty and use this to derive a much simpler proof of a particular case of Eq. 1. We also discuss how our methods can be used to analyze certain cryptographic protocols, in particular, quantum random number generators. Finally, the techniques we use in this paper may find application to other areas of quantum information science and may eventually lead to better bounds for quantum cryptography in the finite-key setting.

1.1 Notation and definitions

Let $\mathcal{A}$ be a finite alphabet of size d. Then if $q \in \mathcal{A}^n$ and $\tau = \{\tau_1, \dots, \tau_k\} \subset \{1, \dots, n\}$, we write q_τ to mean the sub-string of q indexed by τ, namely $q_\tau = (q_{\tau_1}, \dots, q_{\tau_k})$. We write $q_{-\tau}$ to mean the sub-string of q indexed by the complement of τ.

If $\mathcal{A} = \{0, 1\}$, the *Hamming weight* of the string q is defined to be the number of nonzero elements in q. For arbitrary $\mathcal{A}$ and for any $a \in \mathcal{A}$, we define the *relative a-Hamming weight*, which we denote by $w_a(q)$, to be the number of letters in q *not equal to a* and that quantity divided by the length of q. Namely: $w_a(q) = |\{i \mid q_i \neq a\}|/|q|$, where $|q|$ denotes the length of the string q.

A *density operator* acting on Hilbert space $\mathcal{H}$ is a Hermitian positive semi-definite operator of unit trace. Given $|\psi\rangle \in \mathcal{H}$ we write $[\psi]$ to mean $|\psi\rangle\langle\psi|$. We define a *Projective Measurement* or PM over a d-dimensional Hilbert space $\mathcal{H}$ to be a set of projectors $N = \{[\phi_\mathbf{1}], \dots, [\phi_\mathbf{d}]\}$, where $\{|\phi_i\rangle\}_{i=1}^{d}$ form an orthonormal basis of $\mathcal{H}$. It is not difficult to see that we may treat a measurement outcome of $|\phi_{j_1}\rangle \otimes \cdots \otimes |\phi_{j_n}\rangle$ as the classical string $j = j_1 \cdots j_n$. We often write $\mathcal{H}_d$ to mean a d-dimensional Hilbert space.

We denote $H(X)$ to be the Shannon entropy of random variable X. If ρ is a density operator acting on Hilbert space $\mathcal{H}$ and if N is a PM over $\mathcal{H}$, we write $H(N)_\rho$ to mean the Shannon entropy of the random variable induced by measuring ρ using PM N. Similarly, if $|\psi\rangle$ is a pure state in $\mathcal{H}$, we write $H(N)_\psi$ to mean the entropy of the result of measuring $[\psi]$ using PM N. For technical reasons later, we define an *extended binary entropy function*, denoted $\bar{H}(x)$ which is defined to be $H(x, 1-x)$ if $x \in [0, 1/2]$; otherwise, if $x < 0$, $\bar{H}(x) = 0$ and if $x > 1/2$, then $\bar{H}(x) = 1$.

Given a density operator ρ_{AE}, acting on some Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, the conditional quantum min- entropy [12], denoted $H_\infty(A|E)_\rho$, is defined to be:

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

Here, I_A is the identity operator on $\mathcal{H}_A$ and the notation $X \geq 0$, for some operator X, implies that X is positive semi-definite.

To attempt to gain some insight into what, exactly, the above definition means, first consider the case where the E system is trivial. In this case, we may write $H_\infty(A)_\rho$ and it holds that:

$$H_\infty(A)_\rho = -\log \lambda_{\max}(\rho),$$

where $\lambda_{\max}(\rho)$ is the maximal eigenvalue of ρ (note that all logarithms in this paper are base 2 unless otherwise stated). For classical states, this has a very clear meaning. Let $\rho_A = \sum_i p_i\, [\mathbf{i}]$ for some orthonormal basis $\{|i\rangle\}$. Then, $H_\infty(A)_\rho$ is simply $-\log \max_i p_i$. A comparison to von Neumann entropy for the two-dimensional case is shown in Fig. 1.

The more general, conditional min-entropy is more difficult to understand conceptually using only Eq. 3. Instead, it is more intuitive to think of min-entropy in terms of guessing probabilities (*at least, for classical-quantum (cq) states*). If we have a cq-state of the form $\rho_{AE} = \sum_i p_i\, [\mathbf{i}] \otimes \rho_E^{(i)}$, then it was shown in [13] that:

$$H_\infty(A|E)_\rho = -\log P_{\text{guess}}(\rho_{AE}),$$

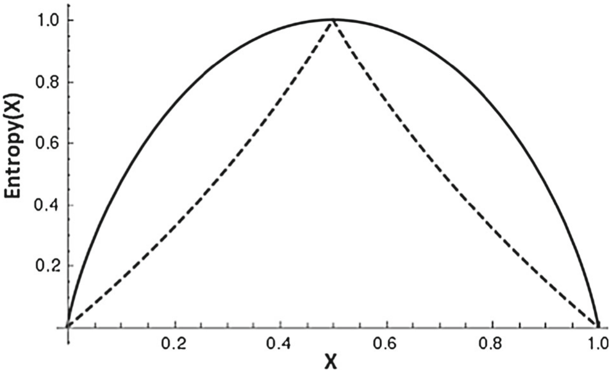

Fig. 1 Comparing Shannon entropy (solid) with min-entropy of a classical state (dashed) in the two-dimensional case

where:

$$P_{\text{guess}}(\rho_{AE}) = \max_{\{\mathcal{M}_i\}} \sum_i p_i tr(\mathcal{M}_i \rho_E^{(i)}),$$

and the maximum is over all POVM operators on $\mathcal{H}_E$. Thus, for cq-states at least, one can think of min-entropy in terms of "guessing games." This will not be important to our discussion, however, it helps to give a clearer picture of what, exactly, min-entropy is measuring.

Quantum min-entropy has many applications in quantum cryptography, especially in finite-key scenarios. In particular, given a cq-state ρ_{AE} (perhaps derived from some quantum cryptographic protocol), where the A register is correlated with the E register in some way. One may apply *privacy amplification* to attempt to establish a uniform random string independent of E's quantum register. Let $\sigma_{KE'}$ be the resulting cq-state after processing ρ_{AE} through privacy amplification (essentially, *publicly* choosing a random two-universal hash function, and applying it to the A register). The K register is of size ℓ bits, and the E' register contains E's original information plus the hash function used. In [12], it was shown that:

$$\left|\left|\sigma_{KE'} - I_K/2^\ell \otimes \sigma_{E'}\right|\right| \leq 2^{-\frac{1}{2}(H_\infty(A|E)_\rho - \ell)}. \tag{4}$$

Thus, deriving bounds on min-entropy is highly useful as they lead directly to bounds on how large a random string may be distilled from a given cq-state (they also may be used for quantum key distribution, though there one must also take into account the information leaked during error correction). We will return to this in a later section.

For notation, if N is a PM on $\mathcal{H}$ and ρ is a density operator on $\mathcal{H}^{\otimes n}$, then we use $H_\infty(N)_\rho$ to mean the min-entropy of the resulting state following the measurement of each of the n sub-spaces ρ acts on using PM N. If $p(j)$ is the probability of observing outcome $j = j_1 \cdots j_n$ (i.e., after measuring, one observes the quantum state $|\phi_{j_1}\rangle \otimes \cdots \otimes |\phi_{j_n}\rangle$), it is not difficult to see that: $H_\infty(N)_\rho = -\log \max_j p(j)$.

Given a density operator ρ_{AC} acting on $\mathcal{H}_A \otimes \mathcal{H}_C$, where the C portion is *classical* (namely, we may write $\rho_{AC} = \sum_c p_c \sigma_A^{(c)} \otimes [\mathbf{c}]$, where $\{|c\rangle\}$ is an orthonormal basis of $\mathcal{H}_C$ and each $\sigma_A^{(c)}$ is an arbitrary density operator acting on $\mathcal{H}_A$) then the conditional min-entropy $H_\infty(A|C)_\rho$ is:

$$H_\infty(A|C)_\rho \geq \inf_c H_\infty(A)_{\sigma^{(c)}}, \tag{5}$$

The above can be proven from Lemma 3.1.8 in [12] and the definition of conditional min- entropy.

Finally, the ϵ-*smooth min-entropy*, denoted $H_\infty^\epsilon(\rho)$ is defined to be:

$$H_\infty^\epsilon(\rho) = \sup_{\sigma \in \Gamma_\epsilon(\rho)} H_\infty(\sigma), \tag{6}$$

where $\Gamma_\epsilon(\rho)$ is the set of all density operators ϵ close to ρ as measured by the trace distance; i.e.,

$$\Gamma_\epsilon(\rho) = \{\sigma \mid ||\sigma - \rho|| \leq \epsilon\}, \tag{7}$$

and $||A||$ is the *trace distance* of A. We define $H_\infty^\epsilon(N)_\rho$ similarly to $H_\infty(N)_\rho$ described earlier whenever N is a PM. The conditional smooth entropy, $H_\infty^\epsilon(A|B)$ is defined similarly. Note that there is a version of privacy amplification (Eq. 4) for smooth min-entropy, proven in [12], which we will use later:

$$\left|\left|\sigma_{KE'} - I_K/2^\ell \otimes \sigma_{E'}\right|\right| \leq 2^{-\frac{1}{2}(H_\infty^\epsilon(A|E)_\rho - \ell)} + 2\epsilon. \tag{8}$$

An important result, which we will use later, was proven in [11] (based on a Lemma in [12]) and allows one to compute the min-entropy of a superposition of states:

Lemma 1 (From [11]) *Let $\mathcal{H}$ be a d-dimensional Hilbert space with orthonormal basis $\{|i\rangle\}_{i=1}^d$ and let $\mathcal{H}_E$ be an arbitrary finite dimensional Hilbert space. Then, for any pure state $|\psi\rangle = \sum_{i \in J} \alpha_i |i\rangle \otimes |\phi_i\rangle_E \in \mathcal{H} \otimes \mathcal{H}_E$, if we define:*

$$\rho = \sum_{i \in J} |\alpha_i|^2 \, [\mathbf{i}] \otimes [\phi_{\mathbf{i}}]_E \, ,$$

it holds that for any PM N on $\mathcal{H}$:

$$H_\infty(N|E)_\psi \geq H_\infty(N|E)_\rho - \log_2 |J|. \tag{9}$$

The above lemma will allow us to bound the min-entropy of a *superposition* of states, by computing, instead, the min- entropy in a suitable *mixed* state.

2 Quantum sampling

Since our proof relies on the quantum sampling technique introduced in [11], we now review this subject here. All information in this section is derived from [11] (we make only a few changes in notation and some generality) and is meant only as a review of this material for completeness.

Let $\mathcal{A}$ be a finite alphabet of size d, and let $a \in \mathcal{A}$, and $k \in \mathbb{N}$. We assume d, a, and k are arbitrary, but fixed. A sampling strategy is a pair $\Sigma = (P_T^k, \mathcal{F}_a^k)$ where P_T^k is a distribution over all subsets of $\{1, \dots, n\}$ of size k and $\mathcal{F}_a^k$ is a function which, given a subset of a sample $q \in \mathcal{A}^n$ (i.e., given q_τ), will output a guess of the value $w_a(q_{-\tau})$. That is, given a randomly chosen sample q_τ (where τ was drawn according to P_T^k), $\mathcal{F}_a^k$ will estimate the value of w_a in *the remaining portion* of q. When it is clear, we will often forgo writing the superscript, and simply write $\mathcal{F}_a$.

Define $B_{\tau,a}^\delta(\Sigma)$ to be the set of all words in $\mathcal{A}^n$ such that the estimate provided by $\mathcal{F}_a$ is δ close to the actual value given a fixed subset $\tau \subset \{1, \dots, n\}$ of size k. That is, let:

$$B_{\tau,a}^\delta(\Sigma) = \{q \in \mathcal{A}^n \mid |\mathcal{F}_a(q_\tau) - w_a(q_{-\tau})| \le \delta\}.$$

Informally, if we have a fixed subset τ with $|\tau| = k$, then the set $B_{\tau,a}^\delta(\Sigma)$ defines the set of all "good" strings; i.e., strings for which the sampling strategy Σ provides an accurate estimate of w_a, up to an error of δ assuming τ was the chosen subset.

From this, the *error probability of* Σ is defined to be:

$$\epsilon_\delta^{\text{cl}} = \max_{q \in \mathcal{A}^n} Pr(q \notin B_{T,a}^\delta(\Sigma)). \tag{10}$$

where the probability is over all subsets τ chosen according to P_T^k (i.e., we treat $B_{T,a}^\delta$ as a random variable induced by choosing subsets τ according to P_T^k). From this definition, it is clear that for any word $q \in \mathcal{A}^n$, the estimated value of w_a, given by the sampling strategy Σ, is δ close to the real value in the remainder of the string (i.e., in the portion of the string that was not used in the test set τ), except with probability $\epsilon_\delta^{\text{cl}}$. Note the superscript "cl" is used to show this is the error probability of a *classical* sampling strategy.

One important sampling strategy we will make use of is the following: Let P_T^k be the uniform distribution over all subsets $\tau \subset \{1, \dots, N\}$ with $|\tau| = k$; i.e., $Pr(P_T^k = \tau) = 1/\binom{N}{k}$. Then, given a string $q \in \mathcal{A}^N$, the function $\mathcal{F}$ is defined simply to be: $\mathcal{F}_a(q_\tau) = w_a(q_\tau)$. That is, the sampling strategy is to choose a random subset, uniformly at random, evaluate w_a on that subset, and output, as an estimate of the value $w_a(q_{-\tau})$, the value $w_a(q_\tau)$. The following Lemma was proven in [11] (see Appendix B in the extended, online version, of that reference):

Lemma 2 (From [11]) *Let $\delta > 0$ be given and Σ be as described above in the text. If $|\tau| = k \le N/2$ then for any d and a, it holds that:*

$$\epsilon_\delta^{\text{cl}} \le 2\exp\left(-\frac{\delta^2 kN}{N+2}\right). \tag{11}$$

These notions can be extended to the quantum domain [11]. Consider an orthonormal basis $\{|a\rangle \mid a \in \mathcal{A}\}$ and let $\mathcal{H}_A$ be the d-dimensional Hilbert space spanned by this basis. Let U be a unitary operator acting on $\mathcal{H}_A$. Then, we may define an orthonormal basis:

$$\mathcal{B} = \{U^{\otimes n}|b_1 \cdots b_n\rangle = U|b_1\rangle \otimes \cdots \otimes U|b_n\rangle \mid b_i \in \mathcal{A}\},$$

of the Hilbert space $\mathcal{H}_A^{\otimes n}$. Then, given a state $|\psi\rangle \in \mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_E$, it is said to have relative a-Hamming weight β *in* A *with respect to basis* $\mathcal{B}$, if we can write $|\psi\rangle = U^{\otimes n}|b_1 \cdots b_n\rangle \otimes |\phi\rangle_E$ with $w_a(b) = \beta$. Note that we are allowed an additional, arbitrary, system in some Hilbert space $\mathcal{H}_E$ (this may be the trivial space if it is not needed). Also, notice that this definition is dependent on the choice of basis.

By abusing notation slightly, we may also define $\text{span}(B^{\delta}_{\tau,a})$ to be:

$$\text{span}\left(\{U^{\otimes n}|q\rangle \mid q \in \mathcal{A}^n \text{ and } |w_a(q_\tau) - w_a(q_{-\tau})| \leq \delta\}\right)$$

Note that if $|\psi\rangle \in \text{span}(B^{\delta}_{t,a}) \otimes \mathcal{H}_E$ then, if sampling is done by measuring in the $\mathcal{B}$ basis on subset τ, it is guaranteed that the state collapses to a superposition of states which are δ close to the observed a-Hamming weight (with respect to basis $\mathcal{B}$). Also note we will drop the δ superscript when the context is clear.

Using the above definitions, the main result from [11] is as follows.

Theorem 1 (From [11], though reworded for our application in this paper and our specific sampling strategy) *Let $k \leq n/2$ be given and consider sampling strategy Σ as described above. Then, for every pure state $|\psi\rangle \in \mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_E$, there exists a collection of "ideal states" $\{|\phi^\tau\rangle\}$ where the index is over all subsets τ of size k and each $|\phi^\tau\rangle \in$ span $(B^{\delta}_{\tau,a}) \otimes \mathcal{H}_E$ such that:*

$$\left\| \frac{1}{T}\sum_{\tau} [\tau] \otimes [\psi] - \frac{1}{T}\sum_{\tau} [\tau] \otimes \left[\phi^\tau\right] \right\| \leq \sqrt{\epsilon_\delta^{\text{cl}}},$$

where $T = \binom{n}{k}$ and the sum is over all subsets of size k. Note that we prepend an auxiliary system spanned by orthonormal basis $\{|\tau\rangle\}$ for all appropriate subsets τ.

The above result states that, on average over the choice of subset τ, the real system $|\psi\rangle$ is ϵ-close to an ideal state, where the ideal state is defined to be one where the sampling strategy always works (i.e., where, after sampling, regardless of the subset choice, the state collapses to one which is a superposition of states δ close to the estimate). Furthermore, ϵ can be computed from the classical error probability.

3 Main result

We are now in a position to state, and prove, our new entropic uncertainty relation.

Theorem 2 *Let $\hat{\epsilon} \geq \epsilon > 0$, $a \in \{0, 1\}$, $0 < \beta < 1/2$, and ρ a density operator acting on Hilbert space $\mathcal{H}_2^{\otimes(m+n)}$ with $m \leq n$ be given. Also, let $M = \{[\mu_{\mathbf{0}}], [\mu_{\mathbf{1}}]\}$ and $N = \{[\nu_{\mathbf{0}}], [\nu_{\mathbf{1}}]\}$, be two projective measurements. If a subset t of size m of ρ*

is measured using M resulting in outcome q, we denote by $\rho(t,q)$ to be the post-measurement state (this is well defined given ρ). Then, it holds that:

$$Pr\left[H_\infty^{2\epsilon+2\epsilon^\beta}(N)_{\rho(t,q)} + n\bar{H}(w_a(q)+\delta) \geq -n\log c)\right] \geq 1-\hat{\epsilon}^{1-2\beta}$$

where the probability is over all choice of subsets and resulting measurement outcomes. Above, c is defined in Eq. 2 and:

$$\delta = \sqrt{\frac{(m+n+2)\ln(2/\epsilon^2)}{m(m+n)}}. \tag{12}$$

Proof We first consider the case when ρ is pure; that is, $\rho = [\psi]$ for some $|\psi\rangle \in \mathcal{H}_2^{\otimes(m+n)}$. Then, applying Theorem 1 to ρ, using the sampling strategy described in the previous section for a sample subset size of m, it follows that there exists an "ideal" state σ of the form: $\sigma = \frac{1}{T}\sum_t [\mathbf{t}] \otimes \left[\phi^{\mathbf{t}}\right]$, where T is the number of possible subsets (i.e., $T = \binom{n+m}{m}$); the summation is over all possible subsets t of $\{1,\ldots,n+m\}$ which are of size m (we expand the underlying Hilbert space to include this auxiliary subspace $\mathcal{H}_T$ spanned by orthonormal basis $\{|t\rangle \mid t \subset \{1,\ldots,n+m\}, |t| = m\}$; and, finally, each $|\phi^t\rangle \in \text{span}\,(B_{t,a}^\delta)$. This ideal state satisfies the following:

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

Given δ as in Eq. 12, and also given Lemma 2, it holds that $\sqrt{\epsilon_\delta^{\text{cl}}} = \epsilon$.

Consider the following experiment: First, run the sampling strategy, choosing a random subset t (which is chosen by measuring the auxiliary $\mathcal{H}_T$ subspace) and performing a measurement in the M basis resulting in outcome q (note that q depends on the subset chosen and the intrinsic randomness of the measurement itself). Let $\rho(t,q)$ be the post-measurement state if this experiment is performed on the true state $\rho = [\psi]$. Likewise, let $\sigma(t,q)$ be the post-measurement state if this experiment is performed on the ideal state σ. Both post-measurement states are well defined given both t and q (though, of course, the post-measurement state may be a superposition, they are, however, exactly defined pure states, conditioning on the outcome of t and q).

We first show:

$$H_\infty(N)_{\sigma(t,q)} \geq -n\log c - n\bar{H}(w_a(q)+\delta). \tag{13}$$

That is, with certainty, for any subset t and observed value q, Eq. 13 holds in the *ideal case*.

Let t be the chosen subset, thus the measurement in basis M is performed on the pure state $|\phi^t\rangle$. Since $|\phi^t\rangle \in \text{span}\,(B_{t,a}^\delta)$, it follows that the post-measurement state, after observing value q, collapses to a superposition of the form:

$$|\phi'\rangle = \sum_{i \in J} \alpha_i |\mu_{i_1}, \ldots, \mu_{i_n}\rangle, \tag{14}$$

where $J \subset I = \{i \in \{0,1\}^n \mid |w_a(i) - w_a(q)| \leq \delta\}$ and normalization requires $\sum_i |\alpha_i|^2 = 1$. Of course $\sigma(t, q) = \left[\phi'\right]$.

Now, consider the mixed state:

$$\chi = \sum_{i \in J} |\alpha_i|^2 \left[\mu_{\mathbf{i_1}} \ldots, \mu_{\mathbf{i_n}}\right].$$

By applying Lemma 1, we have:

$$H_\infty(N)_{\sigma(t,q)} = H_\infty(N)_{\phi'} \geq H_\infty(N)_\chi - \log|J|. \tag{15}$$

We now compute $H_\infty(N)_\chi$. Let χ_N be the result of measuring χ using PM N. It is not difficult to see that this state is simply:

$$\begin{aligned} \chi_N &= \sum_{i \in J} |\alpha_i|^2 \left(\sum_{j \in \{0,1\}^n} p(j|i) \left[\nu_{\mathbf{j_1}}, \ldots, \nu_{\mathbf{j_n}}\right] \right) \\ &= \sum_{j \in \{0,1\}^n} p(j) \left[\nu_{\mathbf{j_1}}, \ldots, \nu_{\mathbf{j_n}}\right], \end{aligned}$$

where we define $p(j|i) = p(j_1 \cdots j_n | i_1 \cdots i_n)$ to be the probability of observing $|\nu_{j_1} \cdots \nu_{j_n}\rangle$ if given an input state of $|\mu_{i_1} \cdots \mu_{i_n}\rangle$. We define $p(j) = \sum_{i \in J} |\alpha_i|^2 p(j|i)$. It is straight-forward to compute $p(j|i)$:

$$p(j|i) = p(j_1 \cdots j_n | i_1 \cdots i_n) = \prod_{l=1}^n |\langle \nu_{j_l} | \mu_{i_l} \rangle|^2 \tag{16}$$

Since χ_N is a classical system, we have:

$$H_\infty(N)_\chi = -\log \max_j p(j) = -\log \max_j \left[\sum_{i \in J} |\alpha_i|^2 p(j|i) \right].$$

Let $p^* = \max_{i,j} p(j|i)$ (where the maximum is over all $i \in J$ and $j \in \{0,1\}^n$). Then, it is clear that:

$$\max_j p(j) = \max_j \left[\sum_{i \in J} |\alpha_i|^2 p(j|i) \right] \leq p^*,$$

(recall that $\sum_i |\alpha_i|^2 = 1$) and thus:

$$H_\infty(N)_\chi = -\log \max_j p(j) \geq -\log p^*.$$

Finally, we compute a bound on p^* as:

$$p^* = \max_{\substack{j\in\{0,1\}^n \\ i\in J}} \prod_{l=1}^n |\langle \nu_{j_l}|\mu_{i_l}\rangle|^2 \leq c^n,$$

where $c = \max_{x,y} |\langle \nu_x|\mu_y\rangle|^2$. Thus:

$$H_\infty(N)_\chi \geq -\log p^* \geq -n\log c. \tag{17}$$

It is clear that $J \subset \{i \in \{0,1\}^n \mid w_a(i) \leq w_a(q) + \delta\}$ and so using the well-known bound on the volume of a Hamming ball we have $|J| \leq 2^{n\bar{H}(w_a(q)+\delta)}$ (note we are using our "extended" version $\bar{H}$ here to avoid the issue when $w_a(q)+\delta > 1/2$; indeed, if that is the case then $\bar{H}(\cdot) = 1$ and so the bound holds trivially), we may combine this with Eqs. 15 and 17 to derive:

$$H_\infty(N)_{\sigma(t,q)} \geq -n\log c - n\bar{H}(w_a(q) + \delta).$$

Of course, the above analysis only considered the ideal state from which we are guaranteed that the sampling strategy was successful. We now consider the "real" state $\rho = [\psi]$.

Consider the real state $\frac{1}{T}\sum_t [\mathbf{t}] \otimes [\psi]$. The process of choosing a subset t, measuring, and observing q (resulting in post-measurement state $\rho(t,q)$) may be described, entirely, by the mixed state: $\rho_{\text{TQR}} = \frac{1}{T}\sum_t [\mathbf{t}] \sum_q p(q|t) \left[\mathbf{q}\right] \otimes \rho(t,q)$, where $p(q|t)$ is the probability of observing outcome q given subset t was sampled; here we use "R" to denote the "remainder"—that is the portion of the state not yet measured. Likewise, the ideal state, after performing this experiment, may be written as the mixed state: $\sigma_{\text{TQR}} = \frac{1}{T}\sum_t [\mathbf{t}] \sum_q \tilde{p}(q|t) \left[\mathbf{q}\right] \otimes \sigma(t,q)$. Since quantum operations cannot increase trace distance, we have $||\rho_{\text{TQR}} - \sigma_{\text{TQR}}|| \leq \epsilon$. By basic properties of trace distance:

$$\epsilon \geq \frac{1}{T}\sum_t \sum_q ||p(q|t)\rho(t,q) - \tilde{p}(q|t)\sigma(t,q)||. \tag{18}$$

Of course, it holds that $\frac{1}{T}\sum_t \sum_q |p(q|t) - \tilde{p}(q|t)| \leq \epsilon$ (this follows by tracing out the unmeasured portion "R" of ρ_{TQR} and σ_{TQR} and again realizing that quantum operations, such as partial trace, do not increase trace distance). Let $\tilde{p}(q|t) = p(q|t) + \epsilon_{q,t}$ where $\epsilon_{q,t}$ may be positive or negative. Then, the above inequality of course implies $\frac{1}{T}\sum_t \sum_q |\epsilon_{q,t}| \leq \epsilon$.

Returning to Eq. 18 we then find:

$$\begin{aligned}\epsilon &\geq \frac{1}{T}\sum_t\sum_q ||p(q|t)(\rho(t,q)-\sigma(t,q))-\epsilon_{q,t}\sigma(t,q)||\\ &\geq \sum_t\sum_q p(q\wedge t)2\cdot\Delta_{q,t}-\epsilon,\end{aligned} \tag{19}$$

where we define $\Delta_{q,t}=\frac{1}{2}||\rho(t,q)-\sigma(t,q)||\leq 1$. Note that, above, we made use of the reverse triangle inequality and the fact that $||\sigma(t,q)||=tr\sigma(t,q)=1$ since $\sigma(t,q)$ is a positive operator of unit trace. We also used the fact that $p(q\wedge t)=p(q|t)p(t)=p(q|t)\cdot\frac{1}{T}$ (here, $p(q\wedge t)$ is the probability of sampling subset t and observing q). Of course, the above implies:

$$\sum_{t,q}p(q\wedge t)\Delta_{q,t}\leq\epsilon. \tag{20}$$

Now, let us consider $\Delta_{q,t}$ as a random variable over the choice of all subsets t and measurement outcomes on that subset q. The expected value is easily seen to be $\mathbb{E}(\Delta_{q,t})=\mu\leq\epsilon$. We also compute the variance V^2:

$$\begin{aligned}V^2&=\sum_{q,t}p(q\wedge t)\Delta_{q,t}^2-\mu^2\leq\sum_{q,t}p(q\wedge t)\Delta_{q,t}-\mu^2\\ &=\mu(1-\mu)\leq\mu\leq\epsilon,\end{aligned}$$

where, above, we used the fact that $\Delta_{q,t}\leq 1$ and so $\Delta_{q,t}^2\leq\Delta_{q,t}$.

Now, by Chebyshev's inequality, we have:

$$Pr\left(|\Delta_{q,t}-\mu|\geq\epsilon^\beta\right)\leq\frac{V^2}{\epsilon^{2\beta}}\leq\epsilon^{1-2\beta}\leq\hat{\epsilon}^{1-2\beta}, \tag{21}$$

(the last inequality follows since $\beta<1/2$); note that this probability is over all subsets t and measurement outcomes q. Thus, except with probability at most $\hat{\epsilon}^{1-2\beta}$, after choosing t and observing q, it holds that $|\Delta_{q,t}-\mu|\leq\epsilon^\beta$ which, of course, implies:

$$\frac{1}{2}||\rho(t,q)-\sigma(t,q)||=\Delta_{t,q}\leq\mu+\epsilon^\beta\leq\epsilon+\epsilon^\beta.$$

Since, in this case we have $\sigma(t,q)\in\Gamma_{2\epsilon+2\epsilon^\beta}(\rho(t,q))$, it holds:

$$H_\infty^{2\epsilon+2\epsilon^\beta}(N)_{\rho(t,q)}\geq H_\infty(N)_{\sigma(t,q)}\geq -n\log c-\bar{H}(w_a(q)+\delta),$$

completing the proof when the case ρ is pure.

Now consider the case when ρ is not pure. In this case, let $|\psi\rangle_{HC}$ be a purification of ρ, where the H portion is the original $\mathcal{H}_2^{\otimes(m+n)}$ space and the C portion lives in an extra Hilbert space ($\mathcal{H}_C$) needed to purify ρ. As before, using quantum sampling, there exists an ideal state σ where, now, each of the $|\phi^t\rangle \in \text{span}\ (B^{\delta}_{t,a}) \otimes \mathcal{H}_C$.

Let us consider running the same experiment as before on this ideal state (where, now, the experiment consists only of measuring the H portion, not the C portion). Let t be the chosen subset and q the observed value. Then, in the ideal case, the state collapses to a pure state of the form:

$$|\phi'\rangle_{HC} = \sum_{i\in J} \alpha_i |\mu_{i_1}, \ldots, \mu_{i_n}\rangle \otimes |C_i\rangle,$$

where J is defined as before and the states $|C_i\rangle$ are arbitrary (not necessarily orthogonal) states in $\mathcal{H}_C$. Let $\chi_{HC} = \sum_{i\in J} |\alpha_i|^2 \left[\mu_{\mathbf{i_1}}, \cdots, \mu_{\mathbf{i_n}}\right] \otimes [\mathbf{C_i}]$. From Lemma 1, we have:

$$H_\infty(N|C)_{\phi'} \geq H_\infty(N|C)_\chi - \log|J|.$$

We add an additional system I spanned by orthonormal basis $\{|I_i\rangle\}_{i\in J}$ and define the following state:

$$\chi_{HCI} = \sum_{i\in J} |\alpha_i|^2 \left[\mu_{\mathbf{i_1}}, \ldots, \mu_{\mathbf{i_n}}\right] \otimes [\mathbf{C_i}] \otimes [\mathbf{I_i}]$$

Measuring this state using PM N yields:

$$\chi_{NCI} = \sum_{i\in J} |\alpha_i|^2 [\mathbf{I_i}] \otimes [\mathbf{C_i}] \otimes \sum_{j\in\{0,1\}^n} p(j|i) \left[\nu_{\mathbf{j_1}}, \ldots, \nu_{\mathbf{j_n}}\right],$$

where $p(j|i)$ is defined as before in Eq. 16 (also, note that we permuted the ordering of the sub-spaces above only for clarity). Define the states $\chi_{N,i}$ as:

$$\chi_{N,i} = \sum_{j\in\{0,1\}^n} p(j|i) \left[\nu_{\mathbf{j_1}}, \ldots, \nu_{\mathbf{j_n}}\right].$$

from which we may write $\chi_{NCI} = \sum_{i\in J} |\alpha_i|^2 [\mathbf{I_i}, \mathbf{C_i}] \otimes \chi_{N,i}$.

Thinking of the CI system jointly, the above state is classical on this joint CI system; thus, from Eq. 5, we have:

$$\begin{aligned} H_\infty(N|CI)_\chi &\geq \inf_{i\in J} H_\infty(N)_{\chi_{N,i}} \\ &= \inf_i (-\log \max_j p(j|i)) \\ &\geq -\log p^* \geq -n \log c. \end{aligned}$$

Finally, from the strong subadditivity of min-entropy [12]:

$$\begin{aligned}H_\infty(N)_{\phi'} &\geq H(N|C)_{\phi'} \geq H_\infty(N|C)_\chi - \log|J|\\ &\geq H_\infty(N|CI)_\chi - \log|J|\\ &\geq -n\log c - \log|J|\\ &\geq -n\log c - n\bar{H}(w_a(q)+\delta),\end{aligned}$$

The above analysis only utilized the ideal state from which sampling is guaranteed to succeed. However, the analysis of the real state follows identically as earlier (when we considered an initial pure state), thus completing the proof. □

4 Applications

Our Theorem 2 gives us an interesting entropic uncertainty bound in terms of smooth entropy and also in terms of the success of a classical sampling strategy. Beyond its independent interest, we show two applications of our new entropic uncertainty result. First, it gives us a new proof of the Maassen and Uffink entropy relation. Second, we can apply it to the analysis of source-independent quantum random number generation protocols against adversarial, but memoryless, sources.

4.1 Application one: Maassen and Uffink entropic uncertainty

As a simple corollary, our Theorem 2 gives us the usual Maassen and Uffink entropic relation.

Corollary 1 *Let M and N be two PMs and ρ a qubit density operator. Then, except with arbitrarily small probability, it holds that:*

$$H(M)_\rho + H(N)_\rho \geq -\log c.$$

Proof Let ρ be a density operator on $\mathcal{H}_2$ and consider the state $\rho' = \rho^{\otimes 2n}$. Let $a = \max_x tr([\mu_{\mathbf{x}}]\cdot\rho)$; in particular, if measuring ρ using M the probability of observing $|\mu_a\rangle$ is no less than $1/2$. Note that this "a" need not be known to users making the measurement, however it clearly exists. Since ρ' is i.i.d., for any subset t of size n and any measurement outcome q on that subset, the post-measurement state is simply $\rho^{\otimes n}$.

Fix $\hat{\epsilon} > 0$ and $0 < \beta < 1/2$. Then, *for any* n and $\epsilon \leq \hat{\epsilon}$, Theorem 2 implies that, except with probability at most $\hat{\epsilon}^{1-2\beta}$, the following inequality holds:

$$\frac{1}{n}H_\infty^{2\epsilon+2\epsilon^\beta}(N)_{\rho^{\otimes n}} + \bar{H}(w_a(q)+\delta) \geq -\log c, \tag{22}$$

where q is the observed value after measuring using M and:

$$\delta = \sqrt{\frac{(n+1)\ln(2/\epsilon^2)}{n^2}}.$$

(We used $m = n$ when applying the theorem.) By the asymptotic equipartition property [14], we have $\lim_{\epsilon\to 0}\lim_{n\to\infty}\frac{1}{n}H_\infty^{2\epsilon+2\epsilon^\beta}(N)_{\rho^{\otimes n}} = H(N)_\rho$. By the law of large numbers, we have $\lim_{n\to\infty} w_a(q) = p_{1-a}$. Note that by definition of a, we have $p_{1-a} \leq 1/2$ thus allowing us to replace $\bar{H}(\cdot)$ with $H(p_{1-a}, p_a) = H(M)_\rho$. Finally, $\delta \to 0$ as $n \to \infty$. Given fixed $\hat{\epsilon}$ the above holds; of course $\hat{\epsilon}$ may be made arbitrarily small, thus yielding the result. □

4.2 Second application: random number generation

We show in this section an interesting application of our new entropic uncertainty relation derived in Theorem 2 to quantum random number generation in the source-independent model. The goal of a quantum random number generator (QRNG) is to utilize quantum physical properties (e.g., random measurement outcomes) to produce true randomness useful for numerous other tasks (including for cryptography). Several security models exist ranging from the very weak fully-trusted scenario to the very strong device independent (DI) model [15,16] (which, though having strong security guarantees, is slow to implement in practice [17,18]). In between is the *source-independent* (SI) model whereby only the source is untrusted, but the measurement devices are characterized [19–22]. See [23] for a general survey of QRNGs and their security models.

We show that our new entropic uncertainty relation, proven in Theorem 2, has applications to this cryptographic protocol. This is only preliminary work to show the potential usefulness of quantum sampling applied to broader quantum information science and cryptography and, so, the model we consider is a memoryless adversarial source. This source, controlled by an adversary, prepares a general N qubit state and sends it to user A. An honest source should prepare the state $|+\rangle^{\otimes N}$ but an adversarial source may prepare anything—we do not require any assumptions on the overall structure of this state beyond that it consists of N qubits and it may even be non-i.i.d. This user chooses a random sample of size m (this requires some initial private randomness, thus the QRNG must actually extend this initial seed randomness and it's usage must be taken into account) and measures in a test basis (for our sake, we use the $X = \{|+\rangle, |-\rangle\}$ basis) observing outcome q (as a bitstring—if there is no noise and the source is honest, $q = 0^m$). The remaining $n = N - m$ qubits are measured in the $Z = \{|0\rangle, |1\rangle\}$ basis. Following this, privacy amplification may be run to distill an ℓ-bit random string. Using privacy amplification (see Eq. 8 but the E system is trivial here as we consider a memoryless adversary), we have:

$$\left|\left|\rho_R - I_R/2^\ell\right|\right| \leq 2\epsilon' + 2^{-\frac{1}{2}(H_\infty^{\epsilon'}(A)-\ell)} = \epsilon_{\text{PA}}. \tag{23}$$

Above, ρ_A is the state of the n measurement results in the Z basis *before* privacy amplification and ρ_R is the state after privacy amplification (transforming the A register of size n to the R register of size ℓ). Thus, if we want the trace distance to be no greater than a given ϵ_{PA} (giving us an ϵ_{PA}-random string), we have:

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

(Note we require $\epsilon_{\text{PA}} > 2\epsilon'$, where ϵ' is whatever smoothening parameter is used.) Interestingly, while the choice of the random hash function used for privacy amplification must be random, it was proven in [24] that once chosen it can be fixed and so we do not need to use additional randomness to choose a hash function (it could be chosen randomly once and then hard-coded into A's device—see [24] for more details).

If the adversary prepares N qubit states, unentangled with any quantum memory, then we may immediately use our Theorem 2 to compute ℓ. Indeed, let $\epsilon > 0$ and $\beta \in (0, 1/2)$ be given. Let $\epsilon_{\text{PA}} = 5\epsilon + 4\epsilon^\beta$. Then, using the Z and X basis, where $c = 1/2$, we have, except with a failure probability of $\epsilon^{1-2\beta}$, after privacy amplification the size of the final random string is:

$$\ell_{\text{QRNG}} = n(1 - \bar{H}(w(q) + \delta))) - \log\frac{1}{\epsilon}.$$

where q is the observed bit string on the m test qubits (measured in the X basis), and where δ is given in Eq. 12. Note that the choice of β factors into ϵ_{PA} (which determines how close the output is to uniform randomness) and the failure probability of the entire protocol. Of course both terms may be made arbitrarily small, but note that, for *fixed* ϵ, as β decreases, the failure probability decreases, while ϵ_{PA} increases. This choice of β is something users may optimize over.

Of course, we must also take into account the randomness used to choose a random subset of size m. This requires $\log\binom{N}{m}$ bits. Thus, the total size of the final random string, after sacrificing these initial seed bits, is:

$$\ell_{\text{QRNG}} = n(1 - \bar{H}(w(q) + \delta))) - \log\frac{1}{\epsilon} - \log\binom{N}{m}. \tag{24}$$

The random bit generation rate is simply $\ell_{\text{QRNG}}/N = \ell_{\text{QRNG}}/(n+m)$.

We set $\epsilon = 10^{-36}$ and $\beta = .33$. (We did not optimize β and so a better choice can lead to more optimistic settings for our bound.) With these settings, the protocol fails with probability less than $\epsilon^{1-2\beta} = 10^{-12}$ while $\epsilon_{\text{PA}} < 5 \times 10^{-12}$. A graph of the random generation rate of this protocol using our new entropic uncertainty bound is shown in Fig. 2.

Note that, in the original quantum sampling paper [11], their method was applied to the security proof of BB84 [25]. However, their proof relied on many internal symmetries within BB84 which we did not need for our proof here—instead, our entropic uncertainty bound applied immediately to the QRNG protocol without requiring any

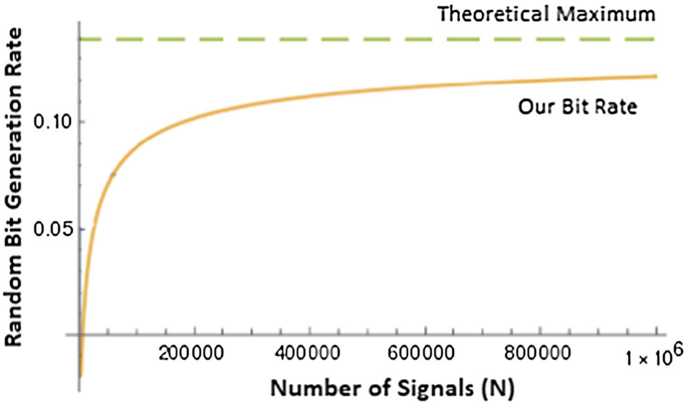

Fig. 2 Showing the random bit generation rate, we derived using our entropic uncertainty relation (solid line), namely ℓ_{QRNG}/N as the number of signals $N = n + m$ increases. We assume a high source noise level of 20% here (namely, $w(q) = .2$). We use $m = 0.07n$ in this graph and $\beta = .33$. Neither settings were optimized, so the result could potentially be improved further. Also showing the theoretical, asymptotic upper bound (dashed line) for this same noise level. We note that, as N increases beyond the plotted 10^6, our lower-bound numerically tends to approach the theoretical maximum

additional reductions. We believe that with further refinements to our method, along with an extension to adversaries with quantum memories, this technique of utilizing quantum sampling, *augmented with the analysis framework we introduced in our proof of Theorem* 2, can lead to a powerful mechanism for proving security of cryptographic protocols in finite-key settings.

5 Closing remarks

In this paper, we showed an interesting connection between quantum sampling and quantum uncertainty. We used the quantum sampling technique introduced in [11] to derive and prove a new entropic uncertainty relation based on smooth min-entropy, the Shannon entropy of an observed outcome, and the probability of failure of a classical sampling strategy. Our result is applicable to arbitrary, finite, states that are not necessarily i.i.d. From this, we were able to derive an alternative, and simple, proof for the Maassen and Uffink bound first proven in [1]. We also showed how our result can be used to derive bit generation rates for quantum random number generators where the source is controlled by a memoryless adversary. To our knowledge, this is the first time quantum sampling has been extended to general quantum information theory and our method of proving Theorem 2 may hold broad application in future research. Note that, though we only proved the qubit case of the Maassen and Uffink entropic uncertainty relation, we strongly suspect this technique can be used to prove the higher dimensional case also. It would also be interesting to see if quantum sampling can yield a simple proof for the conditional version of the uncertainty relation, namely $H(M|B) + H(N|E) \geq -\log c$ [8,26]. We are currently investigating this, also, as future work. Finally, investigating our method's application to other cryptographic protocols is another interesting line of investigation.

Acknowledgements The author would like to thank the anonymous reviewers for their comments which have greatly improved the presentation of this paper. The author would also like to acknowledge support from National Science Foundation Grant Number 1812070.

References

1. Maassen, H., Uffink, J.B.M.: Generalized entropic uncertainty relations. Phys. Rev. Lett. **60**, 1103–1106 (1988)
2. Kraus, K.: Complementary observables and uncertainty relations. Phys. Rev. D **35**, 3070–3075 (1987)
3. Deutsch, D.: Uncertainty in quantum measurements. Phys. Rev. Lett. **50**, 631–633 (1983)
4. Bialynicki-Birula, I.: Formulation of the uncertainty relations in terms of the rényi entropies. Phys. Rev. A **74**, 052101 (2006)
5. Berta, M., Christandl, M., Colbeck, R., Renes, J.M., Renner, R.: The uncertainty principle in the presence of quantum memory. Nat. Phys. **6**(9), 659 (2010)
6. Pramanik, T., Chowdhury, P., Majumdar, A.S.: Fine-grained lower limit of entropic uncertainty in the presence of quantum memory. Phys. Rev. Lett. **110**(2), 020402 (2013)
7. Adabi, F., Salimi, S., Haseli, S.: Tightening the entropic uncertainty bound in the presence of quantum memory. Phys. Rev. A **93**(6), 062123 (2016)
8. Coles, P.J., Berta, M., Tomamichel, M., Wehner, S.: Entropic uncertainty relations and their applications. Rev. Mod. Phys. **89**, 015002 (2017)
9. Bialynicki-Birula, I., Rudnicki, L.: Entropic uncertainty relations in quantum physics. In: Sen, K.D. (ed.) Statistical Complexity, pp. 1–34. Springer, New York (2011)
10. Wehner, S., Winter, A.: Entropic uncertainty relations—a survey. New J Phys. **12**(2), 025009 (2010)
11. Bouman, N.J., Fehr, S.: Sampling in a quantum population, and applications. In: Annual Cryptology Conference, pp. 724–741. Springer, New York (2010)
12. Renner, R. Security of Quantum Key Distribution. Ph.D. thesis, Citeseer (2005)
13. Konig, R., Renner, R., Schaffner, C.: The operational meaning of min- and max-entropy. IEEE Trans. Inf. Theory **55**(9), 4337–4347 (2009)
14. Tomamichel, M., Colbeck, R., Renner, R.: A fully quantum asymptotic equipartition property. IEEE Trans. Inf. Theory **55**(12), 5840–5847 (2009)
15. Colbeck, R., Kent, A.: Private randomness expansion with untrusted devices. J. Phys. A: Math. Theor. **44**(9), 095305 (2011)
16. Pironio, S., Massar, S.: Security of practical private randomness generation. Phys. Rev. A **87**(1), 012336 (2013)
17. Bierhorst, P., Knill, E., Glancy, S., Zhang, Y., Mink, A., Jordan, S., Rommal, A., Liu, Y.K., Christensen, B., Nam, S.W., et al.: Experimentally generated randomness certified by the impossibility of superluminal signals. Nature **556**(7700), 223 (2018)
18. Liu, Y., Yuan, X., Li, M.-H., Zhang, W., Zhao, Q., Zhong, J., Cao, Y., Li, Y.-H., Chen, L.-K., Li, H., Peng, T., Chen, Y.-A., Peng, C.-Z., Shi, S.-C., Wang, Z., You, L., Ma, X., Fan, J., Zhang, Q., Pan, J.-W.: High-speed device-independent quantum random number generation without a detection loophole. Phys. Rev. Lett. **120**, 010503 (2018)
19. Vallone, G., Marangon, D.G., Tomasin, M., Villoresi, P.: Quantum randomness certified by the uncertainty principle. Phys. Rev. A **90**, 052327 (2014)
20. Haw, J.Y., Assad, S.M., Lance, A.M., Ng, N.H.Y., Sharma, V., Lam, P.K., Symul, T.: Maximization of extractable randomness in a quantum random-number generator. Phys. Rev. Appl. **3**, 054004 (2015)
21. Bingjie, X., Chen, Z., Li, Z., Yang, J., Qi, S., Huang, W., Zhang, Y., Guo, H.: High speed continuous variable source-independent quantum random number generation. Quantum Sci. Technol. **4**(2), 025013 (2019)
22. Avesani, M., Marangon, D.G., Vallone, G., Villoresi, P.: Secure heterodyne-based quantum random number generator at 17 Gbps (2018). arXiv preprint arXiv:1801.04139
23. Herrero-Collantes, M., Garcia-Escartin, J.C.: Quantum random number generators. Rev. Mod. Phys. **89**(1), 015004 (2017)

24. Frauchiger, D., Renner, R., Troyer, M.: True randomness from realistic quantum devices (2013). arXiv preprint arXiv:1311.4547
25. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, New York, vol. 175 (1984)
26. Tomamichel, M., Renner, R.: Uncertainty relation for smooth entropies. Phys. Rev. Lett. **106**(11), 110506 (2011)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.