One-Shot Min-Entropy Calculation of Classical-Quantum States and Its Application to Quantum Cryptography

Rong Wang[*] and H. F. Chau[†]

Department of Physics, University of Hong Kong, Hong Kong SAR, China

(Received 16 July 2024; revised 3 May 2025; accepted 9 June 2025; published 8 July 2025)

In quantum Shannon theory, various kinds of quantum entropies are used to characterize the capacities of noisy physical systems. Among them, min-entropy and its smooth version attract wide interest especially in the field of quantum cryptography as they can be used to bound the information obtained by an adversary. However, calculating the exact value or nontrivial bounds of min-entropy are extremely difficult because the composite system dimension may scale exponentially with the dimension of its subsystem. Here, we develop a one-shot lower bound calculation technique for the min-entropy of a classical-quantum state that is applicable to both finite and infinite dimensional reduced quantum states. Moreover, we show our technique is of practical interest in at least three situations. First, it offers an alternative tight finite-data analysis for the BB84 quantum key distribution scheme. Second, it gives the best finite-key bound known to date for a variant of device independent quantum key distribution protocol. Third, it provides a security proof for a novel source-independent continuous-variable quantum random number generation protocol. These results show the effectiveness and wide applicability of our approach.

DOI: 10.1103/ynm5-k1vq

Introduction—Quantum Shannon theory [1] is an active subfield of quantum information processing whose aim is to quantitatively characterize the ultimate capacity of noisy physical systems. Under the independent and identically distributed (i.i.d.) assumption and in the asymptotic limit (that is, when there are infinitely many copies of the state), the relevant entropy measures are the von Neumann entropy and its variations. The situation is different in the nonasymptotic or non-i.i.d. setting. Here, more general entropy measures have to be used [2]. One of them is the quantum conditional min-entropy, which we shall simply call min-entropy throughout this Letter, together with its smooth version. For example, if an adversary tries to guess a string of random variable conditioned on some accessible quantum states, then the supremum possible correctly guessing probability is the min-entropy of the random variable conditioned on the quantum states [2]. Clearly, this adversarial setting is important as it includes important primitives such as quantum key distribution (QKD) [3] and quantum random number generation (QRNG) [4].

The min-entropy of raw data conditioned on adversary's state plays an important role in the information security analysis of quantum cryptography. In fact, by the quantum leftover hashing lemma [5,6], the smooth min-entropy [5] determines the length of distillable key. To calculate the lower bound of smooth min-entropy of the large composite system shared by the users and Eve, the usual way is to reduce it to i.i.d. states and then sum up their von Neumann entropies via de Finetti representation theorem [7], post-selection technique [8], quantum asymptotic equipartition property [9], or entropy accumulation theorem [10,11]. However, these approaches cannot provide a tight length of final key when comparing to one-shot calculations using uncertainty relations for smooth entropies [12–15]. Since these entropic uncertainty relations stem from the fact that the result of incompatible measurements are impossible to predict [16], their applications in quantum cryptography are limited as they require characterized measurements [12–14]. Therefore, it is instructive to find other one-shot approaches that are irrelevant to incompatible measurements.

In this Letter, we propose an alternative one-shot approach to min-entropy lower bound calculation, which can be extended naturally to the case of smooth min-entropy. In essence, given a classical-quantum (CQ) state whose quantum subsystem may be finite- or infinite-dimensional, we develop a technique to calculate the lower bound of min-entropy of its classical random variable conditioned on its quantum subsystem. Unlike the entropic uncertainty relation mentioned above, our approach can directly calculate the lower bound of min-entropy once the density matrix of a CQ state is given. Concretely, we can always assume that the classical variable of a CQ state is uniformly distributed in an adversarial setting. If not, we

[*] Contact author: ericrongwang19@gmail.com

[†] Contact author: hfchau@hku.hk

apply Weyl operators to transform the distribution to a uniform one. Clearly, this transformation does not decrease the adversary's information gain. By working on the CQ state whose classical random variable is uniformly distributed, the min-entropy can be written in terms of the eigenvalues of the adversary's state. In this way, we reduce the complicated problem of min-entropy calculation to a simple problem of solving eigenvalues.

To illustrate the effectiveness of our one-shot min-entropy approach in solving a wide range of quantum cryptographic problems, we consider the following three applications. First, we reproduce the best known provably secure key rate of the BB84 QKD protocol. Next, we report the best provably secure key rate for a variation of device-independent (DI) QKD protocol under the assumption of independent measurement. Finally, we show the security of a novel source-independent continuous-variable (SI-CV) QRNG protocol against general attacks.

Definitions—Here we describe the task of min-entropy calculation in a quantum cryptographic setting. Alice holds a classical random variable X that may take on values in the finite set $\{0, 1, \ldots, d-1\}$, while Eve holds her system E. Given a CQ state like

$$\tau_{XE} = \sum_{x=0}^{d-1} p_x |x\rangle\langle x| \otimes \tau_x, \tag{1}$$

where p_x is its probability distribution of X, τ_x is Eve's state when X takes the value x, Eve wants to maximize her chance of correctly guessing X with the help of the quantum state in her system E. This optimized guessing probability is given by

$$p_{\mathrm{guess}}(X|E)_{\tau_{XE}} \coloneqq \sup_{\{M_x\}} \sum_{x=0}^{d-1} p_x \mathrm{Tr}(M_x \tau_x), \tag{2}$$

where the supremum is over all possible positive operator-valued measures (POVMs) $\{M_x\}$ on Eve's system.

The optimized guessing probability is related to the min-entropy of τ_{XE}. Given ρ_{AB}, recall that the min-entropy is defined by [2,5,17–19]

$$H_{\min}(A|B)_{\rho_{AB}} \coloneqq \sup_{\sigma_B}\{\lambda \in \mathbb{R} : 2^{-\lambda} I_A \otimes \sigma_B \geq \rho_{AB}\}, \tag{3}$$

where the supremum is over all normalized states σ_B within subsystem B, and I_A is the identity matrix of subsystem A. (Throughout this Letter, the symbol of the identity matrix of any subsystem is similarly defined.) From the operational meaning of min-entropy [2], the guessing probability is determined by the min-entropy of X conditioned on E, that is,

$$p_{\mathrm{guess}}(X|E)_{\tau_{XE}} = 2^{-H_{\min}(X|E)_{\tau_{XE}}}. \tag{4}$$

Results—In the cryptographic setting, the task is to bound $p_{\mathrm{guess}}(X|E)$ or equivalently $H_{\min}(X|E)_{\tau_{XE}}$. This can be done via Lemma 1, Theorem 1 and Corollary 1 below whose proofs can be found in Sec. I of Supplemental Material (SM) [20].

Lemma 1—For any state τ_{XE} shared between Alice and Eve, there exists a corresponding

$$\rho_{XE} = \frac{1}{d}\sum_{x=0}^{d-1} |x\rangle\langle x| \otimes |\Psi_x\rangle\langle\Psi_x| \tag{5}$$

with

$$H_{\min}(X|E)_{\rho_{XE}} \leq H_{\min}(X|E)_{\tau_{XE}}. \tag{6}$$

Here, $|\Psi_x\rangle$ is Eve's pure state when X takes the value x. Moreover, we can write $|\Psi_x\rangle$ as

$$|\Psi_x\rangle = \sum_{y=0}^{d-1} \omega^{xy}\sqrt{\lambda_y}|e_y\rangle, \tag{7}$$

where ω is a primitive dth root of unity, λ_y's are the eigenvalues of Eve's state. In other words,

$$\rho_E = \mathrm{Tr}_X[\rho_{XE}] = \frac{1}{d}\sum_{x=0}^{d-1} |\Psi_x\rangle\langle\Psi_x| = \sum_{y=0}^{d-1} \lambda_y |e_y\rangle\langle e_y|, \tag{8}$$

with $\sum_{y=0}^{d-1} \lambda_y = 1$, and $\{|e_y\rangle\}$ is an orthonormal eigenbasis of subsystem E.

Theorem 1—The min-entropy of the state ρ_{XE} given by Eq. (5) in Lemma 1 equals

$$H_{\min}(X|E)_{\rho_{XE}} = \log d - \log\left(\sum_{y=0}^{d-1}\sqrt{\lambda_y}\right)^2. \tag{9}$$

Hence,

$$H_{\min}(X|E)_{\tau_{XE}} \geq \log d - \log\left(\sum_{y=0}^{d-1}\sqrt{\lambda_y}\right)^2. \tag{10}$$

Corollary 1—For the state ρ_{XE} given by Eq. (5) in Lemma 1 and its min-entropy expressed in Eq. (9) in Theorem 1, the guessing probability $p_{\mathrm{guess}}(X|E)_{\rho_{XE}}$ can be attained by the POVM $\{M_x\}_{x=0}^{d-1}$, where

$$M_x = P\left\{\frac{1}{\sqrt{d}}\sum_{y=0}^{d-1}\omega^{xy}|e_y\rangle\right\}. \tag{11}$$

Applications—We use three examples to illustrate the effectiveness of our approach in solving quantum cryptographic problems. The first one is the entanglement-based (EB) version of the BB84 QKD scheme. This example helps us to understand how our technique work in the security proof against general attack. From the quantum leftover hashing lemma [6], the extracted secure key length is determined by the smooth min-entropy of raw key conditioned on Eve's quantum side information.

Therefore, the core issue is to express this smooth min-entropy in terms of the observable statistics. To this end, we first express n pair of qubit (shared by Alice and Bob before measurements) with some parameters, and Eve naturally holds the purification. We then apply our technique to calculate the smooth min-entropy (for the n-partite CQ state shared by Alice and Eve after Alice's measurements) using these parameters. In this way, we write the min-entropy in terms of observable statistics. Within the framework of universal composable security [5,21,22], this gives a way to prove the unconditional security against general attack for the BB84 protocol. The final key length obtained turns out to be the same as the best one-shot result known to date [13,14]. Details are reported in §II.A of SM [20].

Entropic uncertainty relations may be ineffective when comes to security involving uncharacterized or imperfect measurements. To show the effectiveness of our one-shot min-entropy approach in such scenarios, we consider in our second example the security analysis of a QKD protocol with uncharacterized measurements. We pick the protocol introduced in Ref. [24], whose methods are listed in Procedure I, in our illustration. It is a variant of DI QKD [25–27] with assumption of independent measurements. This independence condition may be justifiable in several implementations and is necessarily satisfied when the raw key is generated by N separate pairs of devices [24]. For more practical implementation, in which the raw key is generated by repeatedly performing measurements in sequence on a single pair of devices, this assumption means that the device outputs do not depend on any internal memory storing the quantum states and measurement results obtained in previous rounds [24]. Thus, it is not secure against memory attack [28]. By applying our approach with a new technique for classical data estimation, Theorem 1 below offers an almost tight finite-size key rate which deviates from the asymptotic result only by terms that are caused by the unavoidable statistical fluctuations in parameter estimations. Actually, the obtained key rate is better than all other known proofs to date. The proof of Theorem 1 can be found in §II.B of SM [20].

Procedure I: The DI QKD Protocol With Causally Independent Measurements.

1. *State preparation and distribution:* Eve prepares an N-pair qubit state. She sends half of each pair to Alice and the other half to Bob.
2. *Measurement:* for each qubit pair sent by Eve, both Alice and Bob randomly and separately choose either the key generation mode or the testing mode. If the testing mode is selected, Alice (Bob) uniformly at random chooses $\kappa_a = 0, 1$ ($\kappa_b = 0, 1$), where $\kappa_a \in \{0, 1\}$ and $\kappa_b \in \{0, 1, 2\}$, whereas if the key generation mode is picked, Alice (Bob) sets $\kappa_a = 0$ ($\kappa_b = 2$). They separately measure their share of the qubit pair according to the mode they have selected. [See the discussion near Eq. (63) in SM [20] for their measurements used.] They jot down their measurement result as the bits x and y, respectively.
3. *Sifting:* Alice (Bob) publicly announces her (his) mode. And they keep the mode-matched data. Denote the number of testing rounds by $4k$ with each combination $(\kappa_a, \kappa_b) \in \{00, 01, 10, 11\}$ by k. Further denote the number of key generation mode by $4n$. Clearly, $4n + 4k = N$. (We may assume for simplicity that n and k are large positive integers.)
4. *Parameter estimation:* Alice and Bob calculate the winning probability of the CHSH game using their measurement results from the testing mode. That is to say, they compute the chance that $x \oplus y = \kappa_a \cdot \kappa_b$ [23]. They abort the protocol if the winning frequency is lower than predefined threshold.
5. *Classical postprocessing:* for the remaining $4n$ bits of data from key generation mode, Alice and Bob execute an information reconciliation scheme that leaks at most

   $\mathrm{leak}_{\mathrm{EC}} + \lceil \log_2(1/\varepsilon_{\mathrm{cor}}) \rceil$ bits if the protocol is $\varepsilon_{\mathrm{cor}}$-correct.

   Then they apply a random two-universal hash function to the resultant error-corrected bits to extract ℓ bits of secret key.

Procedure II: The SI-CV QRNG Protocol.

1. *Sending untrusted states:* Eve prepares an N-partite optical quantum state and sends them to Alice one by one.
2. *Measurement:* for each photon sent by Eve, Alice randomly chooses either the randomness generation mode or the testing mode. Denote the number of photons used in the randomness generation mode and testing mode by n and k, respectively. Clearly, $n + k = N$. We fix k so that $N \gg k$. If randomness generation mode chosen, Alice performs an heterodyne measurement on the received optical pulse to obtain the phase $\theta \in [0, 2\pi)$ and amplitude $\mu \in [0, +\infty)$. If testing mode chosen, Alice performs a single photon measurement on the received optical pulse. She records the frequency of detection Q, namely, the number of detection events divided by k.
3. *Parameter estimation:* Alice continues the protocol only if Q is smaller than the predefined threshold.
4. *Discretization:* Alice maps the continuous number $\theta \in [0, 2\pi)$ to a discrete number $x \in \{0, 1, 2, 3\}$. Specifically, $x = 0$ when $\theta \in [0, \pi/2)$, $x = 1$ when $\theta \in [\pi/2, \pi)$, $x = 2$ when $\theta \in [\pi, 3\pi/2)$, and $x = 3$ when $\theta \in [3\pi/2, 2\pi)$. In this way, the sequence of continuously distributed θ's is mapped to the raw sequence of discrete random variables.
5. *Randomness extraction:* Alice applies a random two-universal hash function to the raw sequence of x to extract final secret ℓ-bit random numbers.

Theorem 2—If the final key length ℓ obeys

$$\ell \leq 4n\left[1 - h\left(\frac{1 - \sqrt{16\hat{\omega}_S(\hat{\omega}_S - 1) + 3}}{2}\right)\right] - \mathrm{leak}_{\mathrm{EC}} - \log\frac{2}{\varepsilon_{\mathrm{sec}}^2\varepsilon_{\mathrm{cor}}} \qquad (12)$$

where

$$\hat{\omega}_S = \omega - \sqrt{\frac{2}{k}\ln\frac{\sqrt{6}}{\varepsilon_t}} - \sqrt{\frac{(n+k)(4k+1)}{16nk^2}\ln\frac{1}{\varepsilon_g}} \tag{13}$$

and the classical information of the error correction leaked to Eve is at most $\mathrm{leak}_{\mathrm{EC}} + \log_2(1/\varepsilon_{\mathrm{cor}})$, then this protocol is $\varepsilon_{\mathrm{sec}}$-secret. Here ϵ_t and ϵ_g are defined by Eqs. (83) and (84) in SM [20] and are related to the failure probabilities due to statistical fluctuations in the parameter estimation step.

To demonstrate the power of our approach in infinite dimensional systems, we report as our last example a novel SI-CV QRNG protocol that uses more commonly available and cheaper threshold detectors rather than photon number resolving ones (see Procedure II) [29–33] and apply our method to prove its security against general attacks. Here we assume that the optical source is untrusted, but the measurement devices are trusted and perfect. Inspired by the number–phase uncertainty relation [34] of electromagnetic field, the randomness stems from the fact that the more certain the photon number is, the more uncertain the phase will be. Naively, if we ensure that the standard deviation of the photon number of an incoming light is sufficiently small, then the phase of this light must be close to a uniform i.i.d. distribution. In this way, we do not need to trust the incoming light as long as we could test both of phase and photon number. The problem of this approach is that it is not clear how to define a general quantum phase operator (see §2.7 in Ref. [34] for discussion). Fortunately, we may substitute the quantum phase operator by heterodyne detection. That is, a threshold detection is designed to test how close the untrusted optical source is to the vacuum state; and an heterodyne detection is designed to generate randomness if the source is sufficiently close enough to the vacuum state. Our security proof goes as follows. We first express the CQ state shared by the user and eavesdropper with some parameters, and then apply our technique to calculate its smooth min-entropy. By linking the observable statistics to these parameters, we obtain the final secure random number. Our result is stated in Theorem 2 below whose proof is reported in §II.C of SM [20]. In contrast, it is unclear whether entropic uncertainty relations could be applied to analyze the security of this QRNG protocol because it is not straightforward to calculate the overlap (which quantifies how much incompatible between two measurements).

Theorem 3—If the final key length is given by

$$\ell \le n[2 - H(\hat{Q})] - \log\frac{1}{\varepsilon_{\mathrm{sec}}^2}, \tag{14}$$

then this protocol is $\varepsilon_{\mathrm{sec}}$-secret. Here $H(\hat{Q}) \coloneqq -\hat{Q}\log\hat{Q} - (1-\hat{Q})\log[(1-\hat{Q})/3]$ is the Shannon entropy of a random variable with four possible states following the probability distribution $\{\hat{Q}, (1-\hat{Q})/3, (1-\hat{Q})/3, (1-\hat{Q})/3\}$ and $\hat{Q}$ is the upper bound of detection frequency Q by concentration inequality.

Summary—We develop a powerful technique to calculate nontrivial lower bound on min-entropy as well as its smoothed version for a given classical-quantum state by reducing the computation to a problem of eigenvalues of the adversary state. This eases the lower bound computation. Using three examples, we demonstrate the usefulness of our one-shot min-entropy calculation technique in computing the upper bound on the information obtained by an adversary in both discrete and continuous variable finite-data size problems in quantum key distribution and quantum random number generation.

Acknowledgments—We thank Chao Wang for the discussion of experimental feasibility of our proposed SI-CV QRNG protocol. This work is supported by RGC Grant No. 17303323 of the HKSAR Government.

[1] M. M. Wilde, *Quantum Information Theory* (Cambridge University Press, Cambridge, England, 2013).

[2] R. Konig, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).

[3] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[4] M. Herrero-Collantes and J. C. Garcia-Escartin, Rev. Mod. Phys. **89**, 015004 (2017).

[5] R. Renner, Int. J. Quantum. Inform. **06**, 1 (2008).

[6] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, IEEE Trans. Inf. Theory **57**, 5524 (2011).

[7] R. Renner, Nat. Phys. **3**, 645 (2007).

[8] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. **102**, 020504 (2009).

[9] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theory **55**, 5840 (2009).

[10] F. Dupuis, O. Fawzi, and R. Renner, Commun. Math. Phys. **379**, 867 (2020).

[11] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Nat. Commun. **9**, 1 (2018).

[12] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).

[13] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 634 (2012).

[14] M. Tomamichel and A. Leverrier, Quantum **1**, 14 (2017).

[15] R. Wang, Z.-Q. Yin, H. Liu, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. Res. **3**, 023019 (2021).

[16] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, Rev. Mod. Phys. **89**, 015002 (2017).

[17] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theory **56**, 4674 (2010).

[18] F. Furrer, J. Åberg, and R. Renner, Commun. Math. Phys. **306**, 165 (2011).

[19] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, J. Math. Phys. (N.Y.) **54**, 122203 (2013).

[20] See Supplemental Material at http://link.aps.org/supplemental/10.1103/ynm5-k1vq for the detail procedures and proofs.

[21] J. Müller-Quade and R. Renner, New J. Phys. **11**, 085006 (2009).

[22] C. Portmann and R. Renner, Rev. Mod. Phys. **94**, 025008 (2022).

[23] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[24] L. Masanes, S. Pironio, and A. Acín, Nat. Commun. **2**, 238 (2011).

[25] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[26] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[27] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).

[28] J. Barrett, R. Colbeck, and A. Kent, Phys. Rev. Lett. **110**, 010503 (2013).

[29] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, Phys. Rev. A **90**, 052327 (2014).

[30] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Phys. Rev. X **6**, 011020 (2016).

[31] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, npj Quantum Inf. **2**, 16021 (2016).

[32] D. G. Marangon, G. Vallone, and P. Villoresi, Phys. Rev. Lett. **118**, 060503 (2017).

[33] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, Nat. Commun. **9**, 5365 (2018).

[34] C. C. Gerry and P. L. Knight, *Introductory Quantum Optics* (Cambridge University Press, Cambridge, England, 2023).