

Sharp Finite Statistics for Quantum Key Distribution

Vaisakh Mannalath^{*,†}, Víctor Zapatero^{*,‡}, and Marcos Curty^{ib}

Vigo Quantum Communication Center, *University of Vigo*, Vigo E-36310, Spain;
Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, *University of Vigo*,
Vigo E-36310, Spain;
and AtlanTTic Research Center, *University of Vigo*, Vigo E-36310, Spain



(Received 3 October 2024; revised 26 April 2025; accepted 16 June 2025; published 10 July 2025)

The performance of quantum key distribution (QKD) heavily depends on statistical inference. For a broad class of protocols, the central statistical task is a random sampling problem, customarily addressed using a hypergeometric tail bound due to Serfling. Here, we provide an alternative solution for this task of unprecedented tightness among QKD security analyses. As a by-product, confidence intervals for the average of nonidentical Bernoulli parameters follow too. These naturally fit in statistical analyses of decoy-state QKD and also outperform standard tools. Last, we show that, in a vast parameter regime, the use of tail bounds is not enforced because the cumulative mass function of the hypergeometric distribution is accurately computable. This sharply decreases the minimum block sizes necessary for QKD, and reveals the tightness of our analytical bounds when moderate-to-large blocks are considered.

DOI: 10.1103/1735-x48g

Introduction—Quantum key distribution (QKD) is the only approach to key exchange that is provably secure against computationally unbounded adversaries [1]. Today, considerable efforts are being made to boost the performance of practical QKD systems while guaranteeing their physical-layer security [2,3]. Among the multiple facets of this ongoing program, it is of utmost importance to achieve tighter lower bounds on the extractable secret key length, a goal that can be tackled by refining QKD security proofs. These proofs build upon quantum information-theoretic results and strongly rely on statistical inference, which plays a pivotal role to keep the necessary data block sizes to a minimum.

To be precise, establishing the finite-key security of a QKD protocol requires to upper bound the probability of a “failure” happening in its parameter estimation (PE) step. This refers to the event where the protocol does not abort but the adversary obtains nontrivial information about the final key [1]. In BB84-like protocols [4], a very popular proof technique is based on an entropic uncertainty relation (EUR) for smooth entropies [5,6], in which case the simplest formulation of the problem goes as follows. Let

us consider a two-piece experiment where a population of N binary random variables is generated according to an arbitrary probability distribution, and a random sample of size n is drawn from the population afterward. If we denote the frequency of ones in the test (complementary) sample as $\hat{p}$ ($\hat{q}$), the goal is to find a threshold value $q^{\text{th}} \geq p^{\text{th}}$ such that

$$\Pr[\hat{p} \leq p^{\text{th}}, \hat{q} \geq q^{\text{th}}] \leq \epsilon, \quad (1)$$

for arbitrary values of N , n , ϵ and p^{th} . Naturally, an interplay exists between ϵ and q^{th} : fulfilling Eq. (1) with a very small ϵ comes at the price of tolerating larger values of q^{th} . In the context of QKD—in which $\hat{q}$ is often referred to as the phase-error rate—this translates into a direct penalty on the provably secure key length. Notably, the above formulation of the problem shows up exactly in ideal implementations of the BB84 [4] or the BBM92 [7,8] protocols, and we adhere to the latter in the main text for didactic purposes. The detailed protocol description and secret key length formula can be found in Supplemental Material, Sec. I [9]. On the other hand, the popular decoy-state BB84 protocol [27–30], which is implemented in most of today’s commercial QKD setups, is addressed in Supplemental Material, Sec. II [9].

In EUR-based security proofs [8,31], it is commonplace to derive the desired q^{th} by resorting to an exponential tail bound on the hypergeometric (HG) distribution known as Serfling inequality [32]. Recently though, a sharper bound has been derived in [33], combining Serfling inequality with a refined inequality due to Hush and Scovel [34]. Nonetheless, the reported improvement is moderate and

^{*}These authors contributed equally to this work.

[†]Contact author: vmannalath@vqcc.uvigo.es

[‡]Contact author: vzapatero@vqcc.uvigo.es

heavily relies on the use of very large samples for testing, an undesirable feature given the fact that the final key is extracted from the complementary data.

In this Letter, we propose a simpler approach to calculate q^{th} , resorting to a well-known link between random sampling with and without replacement [35]. Remarkably, the bound we obtain outperforms [33] in all the explored parameter regimes relevant for QKD, where one restricts p^{th} to a few percent at most, N to thousands or tens of thousands at least, and ϵ to rather minuscule values (often below 10^{-10}). Furthermore, in the derivation of the bound, confidence intervals (CIs) are obtained for the average parameter of a set of independent Bernoulli trials. These intervals, which provide an additional tool required for current decoy-state QKD security proofs, also outperform the analytical results considered for that purpose so far [30,36]. Last, we show that, contrary to general belief, the cumulative mass function (CMF) of the HG distribution is exactly computable in a vast parameter regime of interest to QKD. Importantly, this enables the calculation of optimal [37–39] confidence upper bounds for the population parameter following the Clopper-Pearson method [40,41]. Applying the latter to the random sampling problem of Eq. (1)—and also to its generalization to decoy-state QKD schemes—we report a dramatic decrease of the minimum block sizes necessary for key extraction. On the other hand, explicit comparison with our simple analytical tools reveals the tightness of the latter for moderate-to-large blocks.

Analytical results—Our analytical results are triggered by two observations. First, the additive Chernoff bound [42] (simply Chernoff bound in what follows), conventionally used in the context of sampling with replacement, also holds for sampling without replacement. This feature, which is a consequence of a general theorem by Hoeffding [35]—see also [43] for a simple proof—has already been exploited in QKD security analyses before [44,45]. Second, Serfling inequality—the standard bound used in sampling without replacement—essentially reduces to Hoeffding inequality [35] for small sampling fractions n/N . Nevertheless, the latter constitutes a loose relaxation of the Chernoff bound, revealing that this bound must certainly be better for small n/N . With this in mind, we derive a tight relaxation of the Chernoff bound and indistinctly use it to obtain one-sided CIs for the population parameters in sampling with and without replacement. Then, we apply these CIs to solve Eq. (1) and its generalization to decoy-state QKD.

Crucially, our relaxation stems from a rational approximation of the Kullback-Leibler divergence, which is based on a logarithmic inequality [46] carefully selected to keep the CIs tight and handy at the same time. Indeed, higher-order rational approximations of the logarithm lead to much more convoluted formulas for the divergence. The reader is referred to Supplemental Material, Sec. III [9] for the

relaxed Chernoff bound, and the corresponding CIs are stated in Proposition 1 and Corollary 1 below.

Proposition 1—Let $\hat{p}$ be the average of n independent Bernoulli variables, with expected value $\mathbb{E}[\hat{p}] = p$, and let $\kappa_{n,\epsilon} = (2/9n) \ln(1/\epsilon)$. Then, for all $\epsilon > 0$, $\Pr[\Gamma_{n,\epsilon}^-(\hat{p}) \geq p] \leq \epsilon$ and $\Pr[\Gamma_{n,\epsilon}^+(\hat{p}) \leq p] \leq \epsilon$, where

$$\Gamma_{n,\epsilon}^-(\hat{p}) = \begin{cases} \gamma_{n,\epsilon}^-(\hat{p}) & \text{if } \hat{p} \in \left[\frac{3\kappa_{n,\epsilon}}{1+\kappa_{n,\epsilon}}, 1\right], \\ -\epsilon & \text{otherwise,} \end{cases} \quad (2)$$

$$\Gamma_{n,\epsilon}^+(\hat{p}) = \begin{cases} \gamma_{n,\epsilon}^+(\hat{p}) & \text{if } \hat{p} \in \left[0, \frac{1-2\kappa_{n,\epsilon}}{1+\kappa_{n,\epsilon}}\right], \\ 1 + \epsilon & \text{otherwise,} \end{cases} \quad (3)$$

and

$$\gamma_{n,\epsilon}^{\pm}(x) = \frac{1}{1 + 4\kappa_{n,\epsilon}} \left[3\kappa_{n,\epsilon} + (1 - 2\kappa_{n,\epsilon})x \pm 3\sqrt{\kappa_{n,\epsilon}(\kappa_{n,\epsilon} + x - x^2)} \right]. \quad (4)$$

A proof of this claim is given in Supplemental Material, Sec. III [9]. Also, the simpler claims $\Pr[\max\{0, \gamma_{n,\epsilon}^-(\hat{p})\} > p] \leq \epsilon$ and $\Pr[\min\{1, \gamma_{n,\epsilon}^+(\hat{p})\} < p] \leq \epsilon$ follow identically [47].

Since Proposition 1 is solely derived from the Chernoff bound, it automatically extends to a HG random variable [35,43]. The upper extension goes as follows.

Corollary 1—Let $\hat{X} \sim \text{Hypergeometric}(N, K, n)$ and $\hat{p} = \hat{X}/n$, such that $\mathbb{E}[\hat{p}] = p$ with $p = K/N$. Then, for all $\epsilon > 0$, $\Pr[\Gamma_{n,\epsilon}^+(\hat{p}) \leq p] \leq \epsilon$, where $\Gamma_{n,\epsilon}^+(x)$ is defined in Proposition 1.

This result readily implies the following proposition.

Proposition 2—A test sample of size n is drawn at random from a binary population with N elements. Let $\hat{p}$ ($\hat{q}$) denote the frequency of ones in the test (complementary) sample. For all $\epsilon > 0$,

$$\Pr[\hat{q} \geq q_{N,n,\epsilon}^{\text{th}}(\hat{p})] \leq \epsilon \quad (5)$$

for

$$q_{N,n,\epsilon}^{\text{th}}(x) = \frac{N\Gamma_{n,\epsilon}^+(x) - nx}{N - n}, \quad (6)$$

where $\Gamma_{n,\epsilon}^+(x)$ is defined in Proposition 1.

Proof—Let $\hat{X}$ be the number of ones in the test sample, such that $\hat{p} = \hat{X}/n$. If we denote by p the fraction of ones in the population, $\hat{X} \sim \text{Hypergeometric}(N, Np, n)$ and the claim follows directly from Corollary 1 by substituting $p = n\hat{p}/N + (N - n)\hat{q}/N$ and rearranging terms. ■

As shown next, Proposition 2 allows us to obtain a threshold value q^{th} fulfilling Eq. (1), which provides the

so-called failure probability estimation of the BBM92 protocol.

Proposition 3—Consider the two-piece experiment presented in the Introduction. Then, for all $\epsilon > 0$ and $p^{\text{th}} < 1/2$,

$$\Pr[\hat{p} \leq p^{\text{th}}, \hat{q} \geq q_{N,n,\epsilon}^{\text{th}}(p^{\text{th}})] \leq \epsilon \quad (7)$$

for the threshold function $q_{N,n,\epsilon}^{\text{th}}(x)$ defined in Eq. (6), given that the latter is locally nondecreasing at p^{th} .

Proof—Let $\hat{T}$ denote the frequency of ones occurring in the population. Then,

$$\begin{aligned} \Pr[\hat{p} \leq p^{\text{th}}, \hat{q} \geq q_{N,n,\epsilon}^{\text{th}}(p^{\text{th}})] &\leq \Pr[\hat{q} \geq q_{N,n,\epsilon}^{\text{th}}(\hat{p})] \\ &\leq \sum_p \Pr[\hat{T} = p] \Pr[\hat{q} \geq q_{N,n,\epsilon}^{\text{th}}(\hat{p}) | \hat{T} = p] \leq \epsilon. \end{aligned} \quad (8)$$

In the first inequality we use the fact that $\{\hat{p} \leq p^{\text{th}}, \hat{q} \geq q_{N,n,\epsilon}^{\text{th}}(p^{\text{th}})\} \Rightarrow \{\hat{q} \geq q_{N,n,\epsilon}^{\text{th}}(\hat{p})\}$. This is so because $q_{N,n,\epsilon}^{\text{th}}(x)$ is nondecreasing for $x \in [0, p^{\text{th}}]$ if it is nondecreasing at $x = p^{\text{th}}$, and the latter is guaranteed by assumption. The averaging over $\hat{T}$ in the second inequality is a purely *ad hoc* step to enable the use of Proposition 2, which presumes a fixed ratio of ones in the population. The third inequality follows from Proposition 2.

A relevant observation is that the condition on the slope at p^{th} , which is equivalent to $\Gamma_{n,\epsilon}^{+'}(p^{\text{th}}) \geq n/N$ [$\Gamma_{n,\epsilon}^{+'}(p^{\text{th}})$ denoting the derivative of $\Gamma_{n,\epsilon}^{+}(x)$ with respect to x evaluated in p^{th}], is unrestrictive for all practical purposes [48].

On another note, the reader is referred to Supplemental Material, Sec. II [9] for the failure probability estimation of a decoy-state QKD protocol, which relies not only on Proposition 2 but also on Proposition 1.

Numerical results—Certainly, tighter results can be obtained by resorting to numerical methods. For instance, using Stirling's formula and the Gaussian cumulative density function, the authors of [44] construct a HG tail inequality that outperforms our relaxed Chernoff bound in certain regimes, but does not enable a closed formula for the related CI. Alternatively, one could use the exact Chernoff bound rather than a relaxation. Note, however, that if one is willing to use numerical techniques, tail inequalities may become superfluous, because numerically computing the CMF of the HG distribution is often feasible in QKD applications. Crucially, this enables the calculation of optimal one-sided CIs [37,39] using the well-known Clopper-Pearson method based on pivoting the CMF [40]. In particular, for our purposes, one can replace $\Gamma_{n,\epsilon}^{+}(\hat{p})$ in Corollary 1 by the tighter statistic $\mathcal{CP}_{N,n,\epsilon}^{+}(\hat{p})$, defined via [37–39]

$$\mathcal{CP}_{N,n,\epsilon}^{+}(x) = \min \{p \geq x | \Pr[\hat{p} \leq x | p] \leq \epsilon\} \quad (9)$$

if the target set of the minimization is nonempty, and via $\mathcal{CP}_{N,n,\epsilon}^{+}(x) = (N+1)/N$ otherwise [49], where we recall that p takes discrete values in the set $\{0, 1/N, 2/N, \dots, 1\}$ [50]. Remarkably, accurate determination of the CMF is required in order to compute $\mathcal{CP}_{N,n,\epsilon}^{+}(\hat{p})$, with a numerical precision beyond ϵ according to Eq. (9) [51]. Indeed, for a broad range of settings of interest to QKD, this is a manageable task with existing software.

Importantly, since $\mathcal{CP}_{N,n,\epsilon}^{+}(\hat{p})$ fulfills Corollary 1, Proposition 2 also holds replacing Eq. (6) by

$$q_{N,n,\epsilon}^{\text{th}}(x) = \frac{N\mathcal{CP}_{N,n,\epsilon}^{+}(x) - nx}{N - n}, \quad (10)$$

and monotonicity arguments allow to further establish Proposition 3 with this alternative threshold function.

In Fig. 1 we compare various candidate threshold values q^{th} satisfying Eq. (1): Eqs. (6) and (10), and the thresholds derived in [33] and [8]. For illustration purposes, we consider typical QKD inputs, $p^{\text{th}} \leq 4\%$, $N = 10^5$, $n = 10^4$, and $\epsilon = 10^{-9}$, and remark that the improvement of our tools—Eqs. (6) and (10)—prevails in all the explored parameter regimes relevant for QKD.

Additionally, in Supplemental Material, Sec. IV [9] we include optimal one-sided CIs for the average of independent Bernoulli parameters [52,53], potentially replacing $\Gamma_{n,\epsilon}^{\pm}(\hat{p})$ (Proposition 1) in the failure probability estimation of decoy-state QKD schemes. These CIs are related to the Clopper-Pearson CIs for binomial proportions, which in fact have been used in the context of QKD security before (see, e.g., [54,55]).

QKD simulations—Next, we show the impact that the proposed tools have in the finite-key performance of QKD.

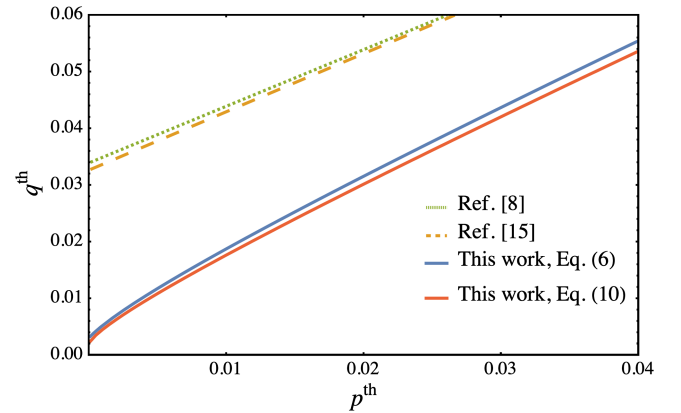


FIG. 1. Threshold value q^{th} satisfying Eq. (1), for $p^{\text{th}} \leq 4\%$, $N = 10^5$, $n = 10^4$, and $\epsilon = 10^{-9}$. The solid red (blue) line corresponds to our numerical (analytical) tool, based on the exact cumulative mass function of the hypergeometric distribution (our relaxed additive Chernoff bound [42]). The dashed orange line uses the result in [33], which combines Serfling [32] and Hush and Scovel [34] inequalities, and the dotted green line uses the result in [8], based on Serfling inequality alone.

Let us consider the ideal BBM92 protocol first. Consistently with [8,33], we evaluate a simplified scenario in which Alice and Bob share a $2N$ -partite quantum state as a protocol input. Then, they jointly select between two binary and complementary quantum measurements uniformly at random on a round-by-round basis, each of them extracting a raw data block of N bits. These blocks are randomly split into a fixed-length test (sifted-key) string of n ($N - n$) bits. That is to say, both the key and the test string are randomly sampled from the two bases. In the simulations, we set the tolerated quantum bit error rate (QBER) to $p^{\text{th}} = 4.55\%$ for ease of comparison with [33], where this choice is motivated by the results of the Micius experiment [56]. Also, an error correction leakage of $\lambda_{\text{EC}} = 1.19(N - n)h(p^{\text{th}})$ bits is assumed, $h(x)$ denoting the binary entropy of x . The correctness parameter, ϵ_{cor} , and the privacy amplification error, ϵ_{PA} , are both set to 10^{-8} for illustration purposes, and the failure probability bound is set to $\epsilon_{\text{PE}} = 4 \times 10^{-16}$. Altogether, these settings lead to an overall secrecy parameter of $\epsilon_{\text{sec}} = 5 \times 10^{-8}$ (see Supplemental Material, Sec. I [9]).

With these inputs, in Fig. 2(a) we plot the extractable key length divided by the data block size for blocks up to $N = 10^6$ bits, optimizing the sampling fraction n/N . In addition, we superpose an inset of the minimum block-size regime, showing that our analytical tool (solid blue line) reduces the minimum block size with respect to [33] (dashed orange line) by more than 16%, while our numerical tool (solid red line) attains a reduction beyond 40%. Furthermore, the tool of [33] would roughly require a 3-orders-of-magnitude larger ϵ_{PE} for a nonzero key with the block size collected in the Micius experiment [56] (dotted black vertical line in the inset). Notably as well, both of our tools perform very similarly—and significantly above [8,33]—for noncritical block sizes.

Let us now assess the more practical decoy-state BB84 protocol. We consider a scheme with three common intensities per basis, μ (signal), ν (decoy), and ω (vacuum), and employ the Z (X) basis for key extraction (PE) with a fixed-size data block of N_Z (N_X) bits drawn at random from the corresponding data pool. Again, in the simulations we contemplate blocks up to $N = N_Z + N_X = 10^6$ bits, and superpose an inset of the minimum block-size regime. Naturally, we set $N_Z = q_Z^2 / (q_Z^2 + q_X^2)N$, where q_Z (q_X) denotes the Z (X) basis probability, common to both parties. Also, we fix $\omega = 10^{-4}$ to account for the finite extinction ratio of the intensity modulator [57]. The settings μ and ν , together with their respective probabilities, p_μ and p_ν , and the test basis probability, q_X , are tuned to optimize the key length per block, l/N . For simplicity, in order to select the acceptance thresholds of the PE tests [58], the average behavior of a typical fiber and detector model is considered (see Supplemental Material, Sec. II [9] for the details). We assume an overall system loss of 30 dB, a dark

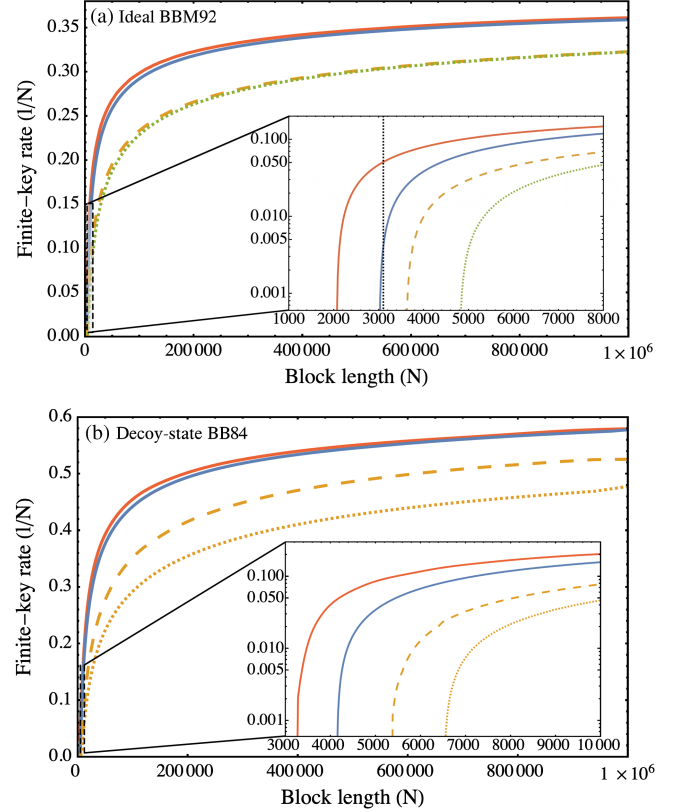


FIG. 2. Finite secret key rate versus data block size. (a) Ideal BBM92 protocol. The dotted green line uses the result in [8], the dashed orange line uses the result in [33], and the solid blue line uses Proposition 3 in this Letter, originating from our relaxed additive Chernoff bound. Last, the solid red line corresponds to the numerical upgrade of Proposition 3, which replaces the threshold function of Eq. (6)—relaxed-Chernoff—by that of Eq. (10)—Clopper-Pearson. The dotted black vertical line in the inset indicates the block size gathered in the Micius experiment [56], $N = 3100$ bits. (b) Decoy-state BB84 protocol. Both orange lines use the random sampling tool of [33], but the dotted (dashed) line relies on Hoeffding’s inequality [35] (the tighter multiplicative Chernoff bound deployed in [36]) for the extra confidence intervals for Bernoulli trials required by the decoy-state method. The solid blue line uses the random sampling tool of Proposition 2 and the extra confidence intervals of Proposition 1, both based on our relaxed Chernoff bound. Finally, the solid red line uses our numerical upgrades of these two propositions, deploying optimal confidence intervals in both cases [37,52]. The protocol inputs and experimental settings considered in the simulations are listed in the main text.

count probability of $p_d = 6 \times 10^{-7}$ [59], and a misalignment error rate of $e_{\text{mis}} = 5 \times 10^{-3}$ [30]. As in the BBM92 protocol, the error correction leakage is set to $\lambda_{\text{EC}} = 1.19N_Z h(\theta^{\text{th}})$, θ^{th} denoting the correctable QBER of a key block [60]. Last, we set again the overall failure probability to $\epsilon_{\text{PE}} = 4 \times 10^{-16}$, and assume a common value for each individual error term contributing to it [61]. Similarly, we take $\epsilon_{\text{cor}} = \epsilon_{\text{PA}} = \delta = 10^{-8}$, where $\delta > 0$ is an intrinsic variable of the security analysis (see

Supplemental Material, Sec. II [9]). Overall, this leads to $\epsilon_{\text{sec}} = 7 \times 10^{-8}$.

The results are shown in Fig. 2(b). Unlike the BBM92 protocol, the security of the decoy-state scheme does not rely on the random sampling tool alone, but also on CIs for the average parameter of a set of Bernoulli trials. In fact, such CIs are repeatedly used in the decoy-state analysis, and thus they have a critical impact in the performance. The reader is referred to the caption for the specifications of the different lines in Fig. 2(b). Overall, our analytical tools reduce the minimum block size by more than 22% compared to previous approaches, and the reduction exceeds 38% with the numerical tools. Once more, our analytical and numerical solutions perform very similarly in noncritical regimes, with a strong edge over existing approaches.

On top of all the above results, in Supplemental Material, Secs. V and VI [9] we survey analytical HG bounds available in the literature, and derive two tools that perform better than our Chernoff-based confidence upper bound (Corollary 1) for small blocks. Particularly, in this regime, we obtain a performance comparable to the numerical one by reproducing our analytical method but with Hush and Scovel inequality.

Conclusions—The performance of QKD is deeply affected by finite statistics. In satellite QKD [56,62–64], the data collection per satellite overpass is limited, and sharp statistics may entail an enormous saving of time and resources. Moreover, one could envision future applications requiring short keys on demand for daily transactions with high security standards. For these, a poor statistical analysis would result in an unbearable penalty.

In this Letter, we have developed statistical tools of unprecedented tightness among QKD security proofs [5]. Although we devise the tools for the BBM92 and the decoy-state BB84 protocols, they are of use in, e.g., measurement-device-independent QKD [57,65] and twin-field QKD [66,67] as well. Technically, the key enablers of our main analytical results are a classical link between random sampling with and without replacement [35], and a careful relaxation of the long-known additive Chernoff bound [42]. Arguably, the tools might be of interest beyond the realm of QKD, in applications such as quality control tests, clinical trials, or hypothesis testing in general. To support this claim, in Supplemental Material, Secs. V and VI [9] we thoroughly compare our relaxed Chernoff bound with existing hypergeometric bounds suited to the same purpose. What is more, for Hush and Scovel inequality and a tight Bernstein-type [68] inequality due to Greene and Wellner [69], we further reproduce our analytical method and obtain new analytical tools that outperform our Chernoff-based confidence bound if small enough block sizes are considered.

On top of it, we have put forward the possibility of replacing tail inequalities—the cornerstone of statistical

analyses in QKD today—by exact computational methods in statistical inference. Remarkably, our results reveal the game-changing potential of such methods to achieve QKD with minimum block sizes, and reinforce the tightness of our simpler analytical tools when moderate-to-large blocks are considered.

Acknowledgments—We acknowledge discussions with Jay Bartroff, Davide Rusca, and Jean-Daniel Bancal, and useful feedback from Jon Wellner. This work was supported by the Galician Regional Government (consolidation of Research Units: AtlantTIC), the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through Grant No. PID2020-118178RB-C21, MICIN with funding from the European Union NextGenerationEU (PRTR-C17.I1) and the Galician Regional Government with own funding through the “Planes Complementarios de I+D+I con las Comunidades Autónomas” in Quantum Communication, the European Union’s Horizon Europe Framework Programme under the Marie Skłodowska-Curie Grant No. 101072637 (Project QSI) and the project Quantum Secure Networks Partnership (QSNP) (Grant No. 101114043). M. C. acknowledges support from a “Salvador de Madariaga” grant from the Spanish Ministry of Science, Innovation and Universities (Grant No. PRX22/00192).

-
- [1] C. Portmann and R. Renner, Security in quantum cryptography, *Rev. Mod. Phys.* **94**, 025008 (2022).
 - [2] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, *Rev. Mod. Phys.* **92**, 025002 (2020).
 - [3] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, *Nat. Photonics* **8**, 595 (2014).
 - [4] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the 1984 IEEE International Conference on Computers, Systems & Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
 - [5] M. Tomamichel and R. Renner, Uncertainty relation for smooth entropies, *Phys. Rev. Lett.* **106**, 110506 (2011).
 - [6] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, Entropic uncertainty relations and their applications, *Rev. Mod. Phys.* **89**, 015002 (2017).
 - [7] C. H. Bennett, G. Brassard, and M. D. Mermin, Quantum cryptography without Bell’s theorem, *Phys. Rev. Lett.* **68**, 557 (1992).
 - [8] M. Tomamichel and A. Leverrier, A largely self-contained and complete security proof for quantum key distribution, *Quantum* **1**, 14 (2017).
 - [9] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/1735-x48g> for a collection of appendices of this Letter, which includes Refs. [10–26].
 - [10] M. Tomamichel *et al.*, Leftover hashing against quantum side information, *IEEE Trans. Inf. Theory* **57**, 5524 (2011).

- [11] V. Zapatero and M. Curty, Finite-key security of passive quantum key distribution, *Phys. Rev. Appl.* **21**, 014018 (2024).
- [12] A. Vitanov *et al.*, Chain rules for smooth min-and max-entropies, *IEEE Trans. Inf. Theory* **59**, 2603 (2013).
- [13] C. Bonferroni, Teoria statistica delle classi e calcolo delle probabilit , Pubbl. Ist. Super. Sci. Economiche Commerciali Firenze **8**, 3 (1936).
- [14] V. Zapatero and M. Curty, Secure quantum key distribution with a subset of malicious devices, *npj Quantum Inf.* **7**, 26 (2021).
- [15] J. Neyman, On the problem of confidence intervals, *Ann. Math. Stat.* **6**, 111 (1936).
- [16] J. Neyman, Outline of a theory of statistical estimation based on the classical theory of probability, *Phil. Trans. R. Soc. A* **236**, 333 (1937).
- [17] J. D. Bancal, K. Redeker, P. Sekatski, W. Rosenfeld, and N. Sangouard, Self-testing with finite statistics enabling the certification of a quantum network link, *Quantum* **5**, 401 (2021).
- [18] S. Holmes, Stein’s method for birth and death chains, in *Stein’s Method: Expository Lectures and Applications*, Institute of Mathematical Statistics Lecture Notes—Monograph Series (Institute of Mathematical Statistics, Beachwood, Ohio, USA, 2004), Vol. 46, pp. 45–67, [10.1214/lnms/1196283792](https://doi.org/10.1214/lnms/1196283792).
- [19] E. Greene, Finite sampling exponential bounds, Doctoral dissertation, University of Washington, 2016.
- [20] G. Bennett, Probability inequalities for the sum of independent random variables, *J. Am. Stat. Assoc.* **57**, 33 (1962).
- [21] R. Bardenet and O. A. Maillard, Concentration inequalities for sampling without replacement, *Bernoulli* **21**, 1361 (2015).
- [22] L. Goldstein and  .  slak, Concentration inequalities via zero bias couplings, *Stat. Probab. Lett.* **86**, 17 (2014).
- [23] S. Chatterjee, Stein’s method for concentration inequalities, *Probab. Theory Relat. Fields* **138**, 305 (2007).
- [24] https://ahlenotes.wordpress.com/2015/12/08/hypergeometric_tail/.
- [25] S. Hui and C. J. Park, The representation of hypergeometric random variables using independent Bernoulli random variables, *Commun. Stat.* **43**, 4103 (2014).
- [26] J. Pitman, Probabilistic bounds on the coefficients of polynomials with only real zeros, *J. Comb. Theory Ser. A* **77**, 279 (1997).
- [27] W. Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, *Phys. Rev. Lett.* **91**, 057901 (2003).
- [28] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [29] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, *Phys. Rev. Lett.* **94**, 230503 (2005).
- [30] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, *Phys. Rev. A* **89**, 022307 (2014).
- [31] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, *Nat. Commun.* **3**, 1 (2012).
- [32] R. J. Serfling, Probability inequalities for the sum in sampling without replacement, *Ann. Stat.* **2**, 39 (1974).
- [33] C. C.-W. Lim, F. Xu, J.-W. Pan, and A. Ekert, Security analysis of quantum key distribution with small block length and its application to quantum space communications, *Phys. Rev. Lett.* **126**, 100501 (2021).
- [34] D. Hush and C. Scovel, Concentration of the hypergeometric distribution, *Stat. Probab. Lett.* **75**, 127 (2005).
- [35] W. Hoeffding, Probability inequalities for sums of bounded random variables, *J. Am. Stat. Assoc.* **58**, 13 (1963).
- [36] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, Improved key-rate bounds for practical decoy-state quantum-key-distribution systems, *Phys. Rev. A* **95**, 012333 (2017).
- [37] J. P. Buonaccorsi, A note on confidence intervals for proportions in finite populations, *Am. Stat.* **41**, 215 (1987).
- [38] T. Wright, *Exact Confidence Bounds when Sampling from Small Finite Universes: An Easy Reference Based on the Hypergeometric Distribution* (Springer Science & Business Media, New York, NY, 2012), Vol. 66, [10.1007/978-1-4612-3140-0](https://doi.org/10.1007/978-1-4612-3140-0).
- [39] W. Wang, Exact optimal confidence intervals for hypergeometric parameters, *J. Am. Stat. Assoc.* **110**, 1491 (2015).
- [40] C. J. Clopper and E. S. Pearson, The use of confidence or fiducial limits illustrated in the case of the binomial, *Biometrika* **26**, 404 (1934).
- [41] In a QKD security proof, any confidence interval must guarantee that its coverage is above its nominal value, a property known as *exactness* in the literature of statistical inference. As shown in [39], in the hypergeometric setting, the exact one-sided intervals that arise from the Clopper-Pearson method are length minimizing and thus optimal. Conversely, any tighter one-sided interval is necessarily not exact and thus unsuitable for QKD.
- [42] H. Chernoff, A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations, *Ann. Math. Stat.* **23**, 493 (1952).
- [43] V. Chv tal, The tail of the hypergeometric distribution, *Discrete Math.* **25**, 285 (1979).
- [44] M. Hayashi and T. Tsurumaru, Concise and tight security analysis of the Bennett–Brassard 1984 protocol with finite key lengths, *New J. Phys.* **14**, 093014 (2012).
- [45] M. Hayashi and R. Nakayama, Security analysis of the decoy method with the Bennett–Brassard 1984 protocol for finite key lengths, *New J. Phys.* **16**, 063009 (2014).
- [46] F. Tops e, Some bounds for the logarithmic function, in *Inequality Theory and Applications* (Nova Publishers, New York, 2007), Vol. 4, p. 137, ISBN: 13978-1-59454-874-1.
- [47] In this Letter, we contemplate the equality sign following the criterion of [8]. With this criterion, “0” and “1” do not provide trivial confidence bounds on the population parameter, forcing us to take the looser values given in Eqs. (2) and (3).
- [48] For instance, it is straightforward to show that setting $\epsilon > \exp\{-[9(N - n)n/4(2n + N)]\}$ suffices to assure that $\Gamma_{n,\epsilon}^+(p^{\text{th}}) \geq n/N$ for all $p^{\text{th}} < 1/2$. This condition on ϵ is unrestrictive for all practical purposes.
- [49] The statistic $\mathcal{CP}_{N,n,\epsilon}^+(\hat{p})$ we introduce here does not exactly match—but is trivially determined by—the one presented in [37,38]. Precisely, they are related by a “one-unit shift.” The discrepancy arises because we contemplate the equality sign in the bounds, requesting $\Pr[\mathcal{CP}_{N,n,\epsilon}^+(\hat{p}) \leq p] \leq \epsilon$ rather than $\Pr[\mathcal{CP}_{N,n,\epsilon}^+(\hat{p}) < p] \leq \epsilon$.

- [50] One can speedup the computation of $\mathcal{CP}_{N,n,\epsilon}^+(x)$ by exploring the complementary set of potential p 's (namely, $\{p \geq x | \Pr[\hat{p} \leq x | p] > \epsilon\}$), by carefully selecting the starting p for the iterations (e.g., based on existing analytical bounds), or by applying a binary search or an interpolation algorithm.
- [51] Precisely, computing the CMF to a precision beyond the $\lceil \log_{10}(\epsilon^{-1}) \rceil$ th digit suffices.
- [52] J.D. Bancal and P. Sekatski, Simple Buehler-optimal confidence intervals on the average success probability of independent Bernoulli trials, [arXiv:2212.12558](#).
- [53] L. Mattner and C. Tasto, Confidence intervals for average success probabilities, [arXiv:1403.0229](#).
- [54] M. Lucamarini *et al.*, Efficient decoy-state quantum key distribution with quantified security, *Opt. Express* **21**, 24550 (2013).
- [55] M. Lucamarini, J. F. Dynes, B. Fröhlich, Z. Yuan, and A. J. Shields, Security bounds for efficient decoy-state quantum key distribution, *IEEE J. Sel. Top. Quantum Electron.* **21**, 197 (2015).
- [56] J. Yin *et al.*, Entanglement-based secure quantum cryptography over 1,120 kilometres, *Nature (London)* **582**, 501 (2020).
- [57] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, *Nat. Commun.* **5**, 3732 (2014).
- [58] A novelty of our protocol with respect to [30] is that, in the PE step, the parties evaluate suitable decoy-state bounds for the single-photon security parameters (e.g., the number of single-photon counts and their phase-error rate). If these bounds do not fulfill predetermined acceptance thresholds, the protocol aborts. Otherwise, a fixed-length output key matching the acceptance thresholds is extracted. Furthermore, a finer-grained PE test is devised when considering the tool of [33], in order to adapt this tool to the decoy-state setting [9].
- [59] N. Walenta *et al.*, Sine gating detector with simple filtering for low-noise infra-red single photon detection at room temperature, *J. Appl. Phys.* **112**, 063106 (2012).
- [60] Note that we use different variables for the correctable QBER in the BBM92 and the BB84 protocols, respectively given by p^{th} and θ^{th} . For consistency, θ^{th} is set to the expected QBER of the considered channel model.
- [61] The total number of error terms contributing to ϵ_{PE} varies depending on the random sampling tool under consideration [9].
- [62] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. Oi, Finite key effects in satellite quantum key distribution, *npj Quantum Inf.* **8**, 18 (2022).
- [63] T. Roger *et al.*, Real-time gigahertz free-space quantum key distribution within an emulated satellite overpass, *Sci. Adv.* **9**, eadj5873 (2023).
- [64] R. Bedington, J. M. Arrazola, and A. Ling, Progress in satellite quantum key distribution, *npj Quantum Inf.* **3**, 30 (2017).
- [65] J.-Y. Liu, X. Ma, H.-J. Ding, C.-H. Zhang, X.-Y. Zhou, and Q. Wang, Experimental demonstration of five-intensity measurement-device-independent quantum key distribution over 442 km, *Phys. Rev. A* **108**, 022605 (2023).
- [66] G. Currás-Lorenzo, A. Navarrete, K. Azuma, G. Kato, M. Curty, and M. Razavi, Tight finite-key security for twin-field quantum key distribution, *npj Quantum Inf.* **7**, 22 (2021).
- [67] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang *et al.*, Experimental twin-field quantum key distribution over 1000 km fiber distance, *Phys. Rev. Lett.* **130**, 210801 (2023).
- [68] S. Bernstein, On a modification of Chebyshev's inequality and of the error formula of Laplace, *Ann. Sci. Inst. Sav. Ukraine Sect. Math* **1**, 38 (1924).
- [69] E. Greene and J. A. Wellner, Exponential bounds for the hypergeometric distribution, *Bernoulli* **23**, 1911 (2017).