Security analysis of quantum key distribution with small block length and its application to quantum space communications

Charles Ci-Wen Lim,[1, 2, *] Feihu Xu,[3, 4] Jian-Wei Pan,[3, 4] and Artur Ekert[2, 5]

[1] *Department of Electrical & Computer Engineering, National University of Singapore, Singapore*
[2] *Centre for Quantum Technologies, National University of Singapore, Singapore*
[3] *Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, China*
[4] *Shanghai Branch, CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai, China*
[5] *Mathematical Institute, University of Oxford, Oxford, United Kingdom*

The security of real-world quantum key distribution (QKD) critically depends on the number of data points the system can collect in a fixed time interval. To date, state-of-the-art finite-key security analyses require block lengths in the order of 10^4 bits to obtain positive secret keys. This requirement, however, can be very difficult to achieve in practice, especially in the case of entanglement-based satellite QKD systems, where the overall channel loss can go up to 70 dB or more. Here, we provide an improved finite-key security analysis which can reduce the block length requirement by 14% to 17% for standard channel and protocol settings. In practical terms, this reduction could save entanglement-based satellite QKD weeks of measurement time and resources, thereby bringing space-based QKD technology closer to reality. As an application, we use the improved analysis to show that the recently reported Micius QKD satellite is capable of generating positive secret keys with a 10^{-5} security level.

Introduction.—Quantum key distribution (QKD) is arguably the most mature quantum technology today with full-stack systems already being deployed in real-world networks [1–4]. In the research community, the security of real-world QKD systems remains a central programme and much effort have been devoted to understanding the security of side-channels and systems with finite resources. Of particular importance is the non-asymptotic security of QKD—a theoretical programme that analyzes the security of finite-length keys and the security errors of parameter estimation, error correction, and privacy amplification [5].

In fact, the need for finite-key security was recognized long ago [6–8], but it is only in the recent decade that security proof techniques became more accessible. On this note, we refer to those based on entropic uncertainty relations [9], which are known to be pretty efficient in terms of the *block length* [10, 11]. Here, block length is defined as the size of the sifted measurement data before parameter estimation; i.e., $m = n + k$, where n is the *raw key* length and k is the number of bits used for parameter estimation. Previously, one would typically need $m > 10^5$ to get a positive secret key [8]. Now, using the proof techniques based on entropic uncertainty relations, the block length requirement can be reduced to $m > 10^4$, which gives an order of magnitude of saving [10, 11].

For QKD systems deployed in standard optical networks, one can readily obtain their finite-key security since the measurement data size of these systems is typically large enough [4]. However, for QKD systems deployed in challenging environments such as space [12–15], obtaining their finite-key security can be an issue. In particular, owning to high channel loss and environmental

challenges, these systems might not gather enough measurement data in short-time intervals. To overcome this issue, one can either spend more time to gather data (the simplest solution) or upgrade the QKD system's transmitter and receiver to achieve faster data collection rates. These solutions are straightforward for terrestrial-based QKD systems, but the same cannot be said for space-based QKD systems. More specifically, the latter can only communicate with the ground stations over very precise time windows (essentially only over good passes) and upgrading in space may not be realistic with current technology [16]. These limitations hence suggest that space-based QKD is a major scientific challenge. This is especially the case for entanglement-based satellite QKD (EB S-QKD), which is known to be slower than its prepare-and-measure counterpart but offers the attractive possibility of untrusted node operation.

Very recently, it has been reported that the finite-key security of EB S-QKD has been demonstrated for the first time using an improved *Micius* QKD satellite [15]. There, the authors reported a positive key with a security parameter of 10^{-10} based on the security proof technique of Ref [10]. However, the analysis there did not consider the cost of parameter estimation and hence the random sampling bound was not properly applied. As a result, this led to overly-optimistic secret key rates. Using their experimental data ($m \sim 10^3$) and the methods from Refs. [10, 11], we found that one would actually require a larger security parameter of 10^{-5} in order to generate a positive key (see below).

In view of the above, it is thus timely to develop new proof techniques that would further sharpen the finite-key security of QKD systems with small block lengths,

particularly those with block lengths $m \sim 10^3$ to 10^4. To that end, we present here an improved finite-key analysis which can further reduce the block length requirement by 14% to 17%. While the improvement is not dramatic (in the sense by several orders of magnitude), it could already save EB S-QKD many weeks of data collection and resources. Our main theoretical contribution is a new random sampling bound (without replacement), which improves pretty significantly the statistical accuracy of the parameter estimation procedure in the small block length regime. The inequality is presented in Lemma 2 and may be of independent interest to other problems. Using this refined analysis, we show that the improved Micius QKD system [15] is capable of generating positive keys with 10^{-6} security; with the same level of security, no positive keys were found (numerically) with the analysis from Ref. [11].

Entanglement-based QKD.—In order to formally present our results, let us first introduce the BBM92 QKD protocol [17] in consideration. We assume that the QKD users, Alice and Bob, are given a $2m$-partite quantum state ρ_{AB}, which is derived from a larger $(2m+1)$-partite quantum system ABE. Here, the quantum system E is controlled by an adversary, Eve, who is computationally unbounded. We consider a protocol in which the basis choice is uniform and the raw key is randomly sampled from both bases [11]. This protocol is essentially the same as the BBM92 QKD protocol analyzed by Shor and Preskill [18] except that less than half of the sifted data will be used for parameter estimation (via random sampling): n bits for the raw key and $k = m - n$ bits for parameter estimation. Importantly, in sampling from both bases, the errors will be uniformly distributed (and hence symmetrized) between the raw key pair and the random sample used for parameter estimation. This allows us to view the parameter estimation step as a standard random sampling problem, where the goal is to infer the error rate of the raw key pair using the error rate observed in the random sample (drawn without replacement).

The protocol is characterized by the block length, m, and three key distillation subroutines, i.e., parameter estimation, error correction, and privacy amplification, which we denote by pe, ec, and pa, respectively. The parameter estimation subroutine is parameterized by two numbers: $\mathsf{pe} = \{k, \delta\}$, where $k \leq m$ is some positive integer and $\delta \in (0, 1/2)$ is the tolerated error rate. The error correction and privacy amplification subroutines are parameterized by two positive integers and one positive integer, respectively: $\mathsf{ec} = \{t, r\}$ and $\mathsf{pa} = \{\ell\}$. The QKD protocol is described in Protocol. I (with only the details needed to illustrate the main technical results; for a more rigorous description, see Ref. [11]).

Security analysis.—Following standard QKD security definition [19, 20], a QKD protocol is said to be $\varepsilon_{\mathrm{qkd}}$-*secret* if it is ε_1-*correct* and ε_2-*secret*, where $0 < \varepsilon_1 + \varepsilon_2 \leq$

Settings: m, $\mathsf{pe} = \{k, \delta\}$, $\mathsf{ec} = \{t, r\}$ **and** $\mathsf{pa} = \{\ell\}$

1. Measurement. Alice and Bob agree on a random binary string $\Phi \in \{0, 1\}^m$ over an authenticated public channel and measure their respective quantum signals using this string. They then agree on a random sample (drawn without replacement) of size k from the entire measurement data set and store them into two pairs of strings: (X, V) for Alice and (Y, W) for Bob. Here, X and Y are random strings taking values in $\{0, 1\}^n$; thus V and W take values in $\{0, 1\}^k$. Note that $m = n + k$.

2. Parameter estimation using random sampling. Alice publicly sends V to Bob, who then computes the error rate between V and W, i.e., $\bar{Z}_{\mathrm{pe}} := |V \oplus W|/k$. If the error rate exceeds the tolerated error rate δ, they abort the protocol. Otherwise, they proceed to the next step. This decision is stored in a binary-valued flag $F_{\mathrm{pe}} \in \{\checkmark, \varnothing\}$, where $\checkmark$ means successful and $\varnothing$ means abort.

3. Error correction. Alice sends Bob a syndrome T of length r which is computed from her raw key X. Then Bob generates an estimate of Alice's raw key, X', from Y and T. To verify that the correction is successful, Alice computes a hash $H(X)$ (of length t) of X and sends it to Bob, who then compares it with his hash $H(X')$. If the hash values are different (i.e., $H(X) \neq H(X')$), they abort the protocol; this decision is stored in $F_{\mathrm{ec}} \in \{\checkmark, \varnothing\}$.

4. Privacy Amplification. Alice and Bob perform randomness extraction based on two-universal hashing to extract an identical secret key pair, S_A and S_B, each of length ℓ, from X and X', respectively.

Protocol I. BBM92 QKD with random sampling as adapted from Ref. [11].

$\varepsilon_{\mathrm{qkd}}$. The security parameter of the protocol is thus $\varepsilon_{\mathrm{qkd}}$. The correctness criterion captures the maximum probability that Alice's and Bob's output keys are different, and the secrecy criterion looks at how distinguishable Alice's output key is from the ideal output key (i.e., one that is uniformly distributed and independent of Eve's side-information E and all classical messages sent over the public channel). Importantly, this choice of security definition guarantees that the protocol is *universally composable* [19–21]: the pair of secret keys can be safely used in any cryptographic task, e.g., for encrypting messages, that requires a perfectly secret key.

With the definitions and relevant tools in place we are now ready to analyze the finite-key security of Protocol. I. The question which we would like to address here is the following: What is the maximum value of ℓ, the output secret key length, for a desired choice of security parameter $\varepsilon_{\mathrm{qkd}}$ and protocol settings? To answer this question, we first have to identify the mathematical conditions for which the protocol is $\varepsilon_{\mathrm{qkd}}$-secure. These conditions (for the considered BBM92 QKD protocol) are given in Ref. [11, Theorem 2 and Theorem 3], which we

restate in a concise form below:

Theorem 1 (Adapted from Ref. [11]). *For the QKD protocol described above with fixed settings, it is $\varepsilon_{\mathrm{qkd}}$-secure if there exists $\nu \in (0, 1/2 - \delta]$ satisfying*

$$2^{-t} + 2\varepsilon_{\mathrm{pe}}(\nu) + \varepsilon_{\mathrm{pa}}(\nu) \leq \varepsilon_{\mathrm{qkd}}, \tag{1}$$

where the error functions due to privacy amplification and parameter estimation are defined as

$$\varepsilon_{\mathrm{pa}}(\nu) := \frac{1}{2}\sqrt{2^{-n[1-h_2(\delta+\nu)]+r+t+\ell}},$$

$$\varepsilon_{\mathrm{pe}}(\nu) := \exp\left(-\frac{nk^2\nu^2}{m(k+1)}\right),$$

respectively, and with $h_2(x) := -x\log x - (1-x)\log(1-x)$, the binary entropy function.

To illustrate the physical meaning (and importance) of ν, we first recall the parameter estimation step. There, Alice and Bob have to check if $\overline{Z}_{\mathrm{pe}} := |V \oplus W|/k \leq \delta$. If it is true, they proceed to the next step; otherwise they abort the protocol. The whole point of this exercise is to ensure that $\overline{Z}_{\mathrm{key}} := |X \oplus Y|/n$ is very close to δ with very high probability. More formally, what we want is an exponential tail bound on the following event: $\overline{Z}_{\mathrm{pe}} \leq \delta \cap \overline{Z}_{\mathrm{key}} \geq \delta + \nu$. This describes the bad event that the parameter estimation step is successful (i.e., $F_{\mathrm{pe}} = \checkmark$) and that the error rate of the raw key pair exceeds δ by some constant positive term ν. In Refs. [10, 11], it has been shown that the probability of this event, $\mathbb{P}_{\mathrm{pe}} := \Pr\left[\overline{Z}_{\mathrm{pe}} \leq \delta \cap \overline{Z}_{\mathrm{key}} \geq \delta + \nu\right]$, is upper bounded by

$$\mathbb{P}_{\mathrm{pe}} \leq \exp\left(-\frac{2nk^2\nu^2}{m(k+1)}\right) = \varepsilon_{\mathrm{pe}}(\nu)^2, \tag{2}$$

which is based on Serfling's seminal work in probability inequalities for random sampling without replacement [22, Corollary 1.1].

As one can see from the above, the deviation term ν plays an important role in maximizing ℓ: a smaller deviation term ν means a larger secret key. However, ν cannot be arbitrarily small—this would make $\varepsilon_{\mathrm{pe}}(\nu)$ very large (which in turn is constrained by the security parameter, $\varepsilon_{\mathrm{qkd}}$). Evidently, there is a delicate interplay between these error functions and it would pay off very well here if we can further sharpen Eq. (2). In the following, we present a new random sampling probability bound for parameter estimation, which may be of independent interest to other problems as well.

Lemma 2 (New sampling bound). *Let $\overline{Z}_{\mathrm{key}}$ and $\overline{Z}_{\mathrm{pe}}$ be defined as above. Then for any $\nu > \xi > 0$ such that $m(\delta + \xi) \in \mathbb{Z}^+$,*

$$\mathbb{P}_{\mathrm{pe}} \leq \exp\left(-\frac{2mk\xi^2}{n+1}\right) + \exp\left(-2\Gamma_{m(\delta+\xi)}((n\nu')^2 - 1)\right), \tag{3}$$

where $\nu' := \nu - \xi$ and

$$\Gamma_{m(\delta+\xi)} := \frac{1}{m(\delta+\xi)+1} + \frac{1}{m - m(\delta+\xi)+1}.$$

Proof. To start with, let $Z_{\mathrm{blk}} = \sum_{i=1}^m Z_i$ be the total number of errors in the initial block of length m and $\overline{Z}_{\mathrm{blk}} = Z_{\mathrm{blk}}/m$ be the average error. Note that in QKD this information about the total error is not known to the users; we are modeling it here only for technical reasons. With this, we can write $\Pr\left[\overline{Z}_{\mathrm{pe}} \leq \delta \cap \overline{Z}_{\mathrm{key}} \geq \delta + \nu\right]$ as a sum of $\Pr\left[\overline{Z}_{\mathrm{pe}} \leq \delta \cap \overline{Z}_{\mathrm{key}} \geq \delta + \nu \cap \overline{Z}_{\mathrm{blk}} \geq \overline{Z}_{\mathrm{pe}} + \xi\right]$ and $\Pr\left[\overline{Z}_{\mathrm{pe}} \leq \delta \cap \overline{Z}_{\mathrm{key}} \geq \delta + \nu \cap \overline{Z}_{\mathrm{blk}} < \overline{Z}_{\mathrm{pe}} + \xi\right]$ for some $\xi > 0$. The first term can be upper bounded using

$$\Pr\left[\overline{Z}_{\mathrm{pe}} \leq \delta \cap \overline{Z}_{\mathrm{key}} \geq \delta + \nu \cap \overline{Z}_{\mathrm{blk}} \geq \overline{Z}_{\mathrm{pe}} + \xi\right]$$
$$\leq \Pr\left[\overline{Z}_{\mathrm{blk}} \geq \overline{Z}_{\mathrm{pe}} + \xi\right] \leq \exp\left(-\frac{2mk\xi^2}{n+1}\right),$$

where the second inequality is implied from Ref [22, Corollary 1.1] (lower tail instead of upper tail).

For the second term, we have that $\Pr[\overline{Z}_{\mathrm{pe}} \leq \delta \cap \overline{Z}_{\mathrm{key}} \geq \delta + \nu \cap \overline{Z}_{\mathrm{blk}} < \overline{Z}_{\mathrm{pe}} + \xi] \leq \Pr[\overline{Z}_{\mathrm{key}} \geq \delta + \nu \cap \overline{Z}_{\mathrm{blk}} < \delta + \xi]$ as the latter event is implied from the former event, and $\Pr[\overline{Z}_{\mathrm{key}} \geq \delta + \nu \cap \overline{Z}_{\mathrm{blk}} < \delta + \xi] \leq \Pr[\overline{Z}_{\mathrm{key}} \geq \delta + \nu \cap Z_{\mathrm{blk}} < \lceil m(\delta + \xi)\rceil] = \Pr[\overline{Z}_{\mathrm{key}} \geq \delta + \nu \cap Z_{\mathrm{blk}} < m_{\mathrm{err}}]$, where $m_{\mathrm{err}} := \lceil m(\delta + \xi)\rceil$. Generally, we may assume $m_{\mathrm{err}} = m(\delta + \xi)$, i.e., $\delta + \xi$ is chosen such that $m(\delta + \xi)$ is a positive integer.

The above can be further written as $\Pr[\overline{Z}_{\mathrm{key}} \geq \delta + \nu \cap Z_{\mathrm{blk}} < m_{\mathrm{err}}] \leq \sum_{t=0}^{m_{\mathrm{err}}} \Pr[\overline{Z}_{\mathrm{key}} \geq \delta + \nu \cap Z_{\mathrm{blk}} = t] = \sum_{t=0}^{m_{\mathrm{err}}} \Pr[Z_{\mathrm{blk}} = t]\Pr[\overline{Z}_{\mathrm{key}} \geq \delta + \nu | Z_{\mathrm{blk}} = t]$. An upper bound can be obtained by noting that $\sum_{t=0}^{m_{\mathrm{err}}} \Pr[Z_{\mathrm{blk}} = t]\Pr[\overline{Z}_{\mathrm{key}} \geq \delta + \nu | Z_{\mathrm{blk}} = t] \leq \Pr\left[\overline{Z}_{\mathrm{key}} \geq \delta + \nu | Z_{\mathrm{blk}} = m_{\mathrm{err}}\right]$. Notice that the last term is given by the upper tail probability of the hypergeometric distribution given the total number of errors $Z_{\mathrm{blk}} = m_{\mathrm{err}}$ is fixed, i.e., $\Pr[\overline{Z}_{\mathrm{key}} \geq \delta + \nu | Z_{\mathrm{blk}} = m_{\mathrm{err}}] = \Pr[\overline{Z}_{\mathrm{key}} \geq m_{\mathrm{err}}/m + (\nu - \xi)|Z_{\mathrm{blk}} = m_{\mathrm{err}}]$. In the ideal case, the exact value of the upper tail probability can be computed (since the total number of errors is tightly bounded now), but this may introduce numerical inaccuracies due to the discrete nature of the distribution [23, 24]. To that end, we use instead a probability inequality by Hush and Scovel [25], which provides pretty tight exponential bounds for hypergeometric distribution (at least in the settings for which we are interested in). This inequality reads

$$\Pr[\overline{Z}_{\mathrm{key}} \geq m_{\mathrm{err}}/m + (\nu - \xi)|Z_{\mathrm{blk}} = m_{\mathrm{err}}]$$
$$\leq \exp\left(-2\alpha_{m_{\mathrm{err}}}(n^2(\nu - \xi)^2 - 1)\right),$$

where

$$\alpha_{m_{\mathrm{err}}} := \max\left\{\frac{1}{n+1} + \frac{1}{k+1}, \frac{1}{m_{\mathrm{err}}+1} + \frac{1}{m - m_{\mathrm{err}}+1}\right\}.$$

Note that it is important for $\nu > \xi$ since the deviation term must be positive. We can in fact further simplify the bound by picking the right-side-hand term in $\alpha_{m_{err}}$, i.e., $\exp\left(-2\alpha_{m_{err}}(n^2(\nu-\xi)^2-1)\right) \leq \exp\left(-2\Gamma_{m_{err}}(n^2(\nu-\xi)^2-1)\right)$, where $\Gamma_{m_{err}} := 1/(m_{err}+1) + 1/(m-m_{err}+1)$. It can be verified that $\Gamma_{m_{err}}$ decreases with increasing m_{err} and hence

$$\Pr[\overline{Z}_{key} \geq \delta + \nu | Z_{blk} = m_{err}] \leq e^{-2\Gamma_{m_{err}}((n\nu')^2-1)}.$$

where $\nu' := \nu - \xi$ is a positive constant. $\qquad \square$
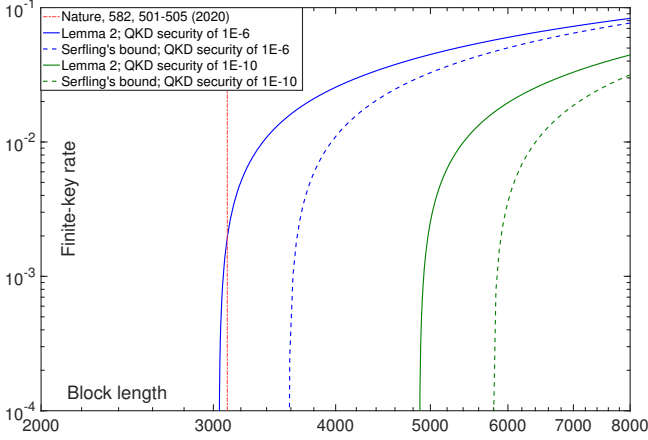
FIG. 1. Numerically optimized finite-key rate ℓ/m vs block length m for $s = 6, 10$. In this simulation, the tolerated error rate is set to $\delta = 4.55\%$ so that the protocol is likely to succeed with high probability. Ref. [15] reported a total error rate of 4.51% and block length $m = 3100$ bits. The (red) vertical line represents the block length obtained in the experiment, which gives a finite-key rate of 1.962×10^{-3} based on $\varepsilon_{qkd} = 10^{-6}$. This suggests that about 6 secret bits can be generated in a single run of the protocol. The numerically optimized parameters are $\vec{x}_{opt} = \{1.962 \times 10^{-3}, 0.5, 0.1141, 0.0693\}$.

Using Lemma. 2, the error function for parameter estimation now reads

$$\varepsilon'_{pe}(\nu, \xi)^2$$
$$= \exp\left(-\frac{2mk\xi^2}{n+1}\right) + \exp\left(-2\Gamma_{m(\delta+\xi)}((n\nu')^2-1)\right).$$

To maximize the secret key length, ℓ, we employ the following program parameterized by a bounded set of four-dimensional real vector, $\vec{x} = (\alpha, \beta, \nu, \xi)$. The block length m, tolerated error rate δ, correctness error $2^{-t} = 10^{-(s+2)}$, and security parameter $\varepsilon_{qkd} = 10^{-s}$ are fixed.

$$\max_{\vec{x} \in \mathbb{R}^4} \quad \ell = \lfloor \alpha m \rfloor$$
$$\text{s.t.} \quad 2^{-t} + 2\varepsilon'_{pe}(\nu, \xi) + \varepsilon_{pa}(\nu) \leq \varepsilon_{qkd},$$
$$\alpha \in [0,1], \beta \in (0, 1/2],$$
$$0 < \xi < \nu < 1/2 - \delta,$$

where $k = \lfloor \beta m \rfloor$ is the number of bits allocated to parameter estimation and $r = 1.19h_2(\delta)$ is the expected error correction leakage. Here, α is the secret key rate, which is defined as the number of secret bits generated divided by the block length, i.e., ℓ/m. For comparison, we also run the same optimization for Theorem. 1, which uses Eq. (2) for parameter estimation. From Figure 1, we observe that the new analysis outperforms the existing analysis for both security levels, $s = 6, 10$: in particular, the minimum block length m has been reduced by about 14% to 17%. However, this improvement is not enough to obtain finite-key security for $\varepsilon_{qkd} = 10^{-10}$ as reported by Ref. [15]; for that, we would need $m > 4800$ (for the new analysis) and $m > 5800$ (for the one based on Eq. (2)). We note that one can still obtain finite-key security using Eq. (2); however the smallest security error that we can find for a positive key is $\varepsilon_{qkd} = 10^{-5}$.

Discussion and conclusion.—In this application study, we find that the improved Micius Satellite (arguably the most advanced QKD technology in space) would have to revise their security parameter from $\varepsilon_{qkd} = 10^{-10}$ to 10^{-6}. This means that the overall security error is four orders of magnitude bigger than reported. This revision immediately raises the following question: Is $\varepsilon_{qkd} = 10^{-6}$ good enough for the space-based QKD? Unfortunately, the answer to this question is not trivial and may entail discussions beyond the scope of this work. For the start, we emphasize that the security statement $\varepsilon_{qkd} \leq 10^{-6}$ does not lend any concrete description to how the QKD system could have gone wrong. It is simply an upper bound on the probability that a bad event happens [20]; note that a QKD system which produces non-identical secret keys with probability 10^{-6} has the same security as one that gives the entire secret key to Eve with probability 10^{-6}. We note that one could also use the adversary's guessing probability as a metric to help determine a *good* value of ε_{qkd}, e.g., see Ref. [26].

Nevertheless, we argue that one can at least refer to *key streaming* for some guidance. In this setting, we consider the use of a QKD system to generate a continuous stream of secret bits, where some portion of the earlier bits are used for authentication in subsequent rounds [19]. By composability, the security of the key stream is then $\varepsilon_{stream} \leq v\varepsilon_{qkd}$, where v is the number of times the users intend to operate the QKD system. With this, we now have a clear connection to how many times the users can operate the QKD system before it needs to be rebooted with a fresh secret key. To appreciate this connection, suppose ε_{stream} has to respect some recommended security level, say 10^{-5}, which is specified by some national standards organization. Then, it is clear that for some fixed ε_{qkd} (determined by the system parameters), the number of times one can operate the QKD system, v, is limited. Applying this example to the improved Micius QKD satellite, we thus have $v \leq 10$, i.e., not more than 10 rounds of QKD operation. This suggests that

the improved Micius QKD satellite may have to be re-booted (with a fresh secret key for authentication) after every 10 QKD cycles, or equivalently, the generation of 60 secret bits.

In conclusion, we have presented an improved finite-key analysis for BBM92 QKD protocol with small block length. While the refined analysis gives pretty good improvements over existing methods, the problem of finite-key security with small block length is still a pressing one. This problem, as we have highlighted above, is especially relevant to long-range QKD systems such as satellite-based QKD, which will most likely form the backbone of the future quantum internet.

---

* charles.lim@nus.edu.sg

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[2] H.-K. Lo, M. Curty, and K. Tamaki, Nat Photon **8**, 595 (2014).

[3] E. Diamanti, H. K. Lo, B. Qi, and Z. Yuan, npj Quantum Information **2** (2016), 10.1038/npjqi.2016.25.

[4] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Rev. Mod. Phys. **92**, 025002 (2020).

[5] R. Renner, International Journal of Quantum Information **6**, 1 (2008).

[6] D. Mayers, J. ACM **48**, 351 (2001).

[7] H. Inamori, N. Lütkenhaus, and D. Mayers, The European Physical Journal D **41**, 599 (2007).

[8] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).

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

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

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

[12] J. Yin *et al.*, Phys. Rev. Lett. **119**, 200501 (2017).

[13] J. Yin *et al.*, Science **356**, 1140 (2017).

[14] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima, Nature Photonics **11**, 502 (2017).

[15] J. Yin *et al.*, Nature **582**, 501 (2020).

[16] R. Bedington, J. M. Arrazola, and A. Ling, npj Quantum Information **3**, 30 (2017).

[17] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[18] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[19] J. Müller-Quade and R. Renner, New Journal of Physics **11**, 085006 (2009), arXiv:1006.2215.

[20] C. Portmann and R. Renner, "Cryptographic security of quantum key distribution," (2014), eprint, arXiv:1409.3525.

[21] M. Ben-Or and D. Mayers, "General security definition and composability for quantum & classical protocols," (2004), eprint, quant-ph/0409062.

[22] R. J. Serfling, Ann. Statist. **2**, 39 (1974).

[23] T. Wu, ACM Trans. Math. Softw. **19**, 33 (1993).

[24] A. Berkopec, Journal of Discrete Algorithms **5**, 341 (2007), 2004 Symposium on String Processing and Information Retrieval.

[25] D. Hush and C. Scovel, Statistics & Probability Letters **75**, 127 (2005).

[26] X.-B. Wang, J.-T. Wang, J.-Q. Qin, C. Jiang, and Z.-W. Yu, npj Quantum Information **6**, 45 (2020).