npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

Tight finite-key analysis for quantum key distribution without monitoring signal disturbance

Hang Liu[1,2,3], Zhen-Qiang Yin[1,2,3]✉, Rong Wang[1,2,3], Ze-Hao Wang[1,2,3], Shuang Wang[1,2,3], Wei Chen[1,2,3], Guang-Can Guo[1,2,3] and Zheng-Fu Han[1,2,3]

Unlike traditional communication, quantum key distribution (QKD) can reach unconditional security and thus attracts intensive studies. Among all existing QKD protocols, round-robin-differential-phase-shift (RRDPS) protocol can be running without monitoring signal disturbance, which significantly simplifies its flow and improves its tolerance of error rate. Although several security proofs of RRDPS have been given, a tight finite-key analysis with a practical phase-randomized source is still missing. In this paper, we propose an improved security proof of RRDPS against the most general coherent attack based on the entropic uncertainty relation. What's more, with the help of Azuma's inequality, our proof can tackle finite-key effects primely. The proposed finite-key analysis keeps the advantages of phase randomization source and indicates experimentally acceptable numbers of pulses are sufficient to approach the asymptotical bound closely. The results shed light on practical QKD without monitoring signal disturbance.

npj Quantum Information (2021)7:95 ; https://doi.org/10.1038/s41534-021-00428-9

INTRODUCTION

As the maturest field of quantum information sciences, quantum key distribution (QKD)[1] is well-known for its information-theoretic security. In QKD, the law of quantum mechanics enables communicators to upper bound the potential information leakage to the eavesdropper (Eve). Since the BB84[1] protocol was proposed, more and more QKD protocols sprang up, such as device-independent (DI)[2] protocol, measurement-device-independent (MDI)[3] protocol and twin-field (TF)[4] protocol. In most of these protocols, estimating Eve's information is dependent on monitoring signal disturbance, e.g., information leakage in BB84 is a function of the error rate of sifted key bits. However, in 2014, Toshihiko Sasaki et al. proposed an exceptional protocol, named round-robin-differential-phase-shift (RRDPS)[5], which can upper bound Eve's information without using any parameter of signal disturbance. After that, the verification of RRDPS has been completed in several experiments[6–9].

In RRDPS, Alice firstly prepares an n-photon L-pulse train as a packet and encodes key bit 0(1) on every pulse by modulating phase 0(π), while these phase information are recorded in Alice's register. Then Alice sends the train to Bob through a quantum channel. Once Bob receives the train which is assumed to be a single-photon quantum state, his local quantum random number generator (QRNG) generates an integer $r \in [1, L-1]$. Bob interferes the a-th and b-th ($b = a + r \le L$) pulses in the train to decode his sifted key bit 0(1) corresponding to phase shift 0(π). After that, Bob announces (a, b) and Alice does xor on key bits on a-th and b-th pulses to get her sifted key bit. In ref. [5], Sasaki et al. proved Eve's information on sifted key bit is no larger than $H_2(\frac{n}{L-1})$, where H_2 is the Shannon entropy $H_2(x) := -x\log x - (1-x)\log(1-x)$. And we subscribe that log represents $\log_2$. It's clear that RRDPS protocol has a high error rate tolerance and doesn't need to monitor bit error rate to estimate information leakage.

Although ref. [5] has beautiful results, the bound for Eve's information is not tight. In 2018, Yin et al. put forward a phase-randomized method to improve it by constructing the optimal collective attack model[10]. Until now, their work has kept the highest secure key rate among all related works. However, their results cannot be directly used in finite-key cases because the collective attack is not equivalent to the most general coherent attack in finite-key cases. In order to remove this restriction, Liu et al. applied the post-selection technique[11] to the results of ref. [10], then completed finite-key analysis[12]. Unfortunately, the results showed that RRDPS needed too many pulses to obtain satisfactory performance. Therefore, finite-key analysis for RRDPS is still an open issue.

RRDPS protocol will never be considered into practice until finding a proper method to reduce finite-size effects and minimize the number of emitted pulses as far as possible. Here we give a tight finite-key analysis for RRDPS with widely used phase-randomized weak coherent source. The essential idea is observing that the randomized phases of each pulse of the train lead the composite system of Alice, Bob and Eve into becoming a mixture state, in which different components may have different information leakage. Next one can apply the entropic uncertainty relation[13] to estimate phase error rates and min-entropies for each mixture components. Moreover, by introducing Azuma's inequality[14], the effects of coherent attacks are well-considered. Note that the entropic uncertainty relation has been applied to BB84[15], MDI[16] and even TF[17] protocol, although not to RRDPS yet, our analysis shows that it's doubtlessly feasible to use this technique in RRDPS. Numerical simulations fully demonstrate that our theoretical model is almost the optimal solution of the finite-key RRDPS with phase-randomized weak coherent source: experimentally acceptable amounts of pulses can help RRDPS behave closely to the asymptotic bounds given in ref. [10].

[1]CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China. [2]CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China. [3]State Key Laboratory of Cryptology, P. O. Box 5159, Beijing 100878, China. ✉email: yinzq@ustc.edu.cn

RESULTS

Definition of protocol

The flow of actual RRDPS protocol has been given in ref. [5]. On the other hand, it's pointed out in ref. [5] that the security of RRDPS protocol is essentially regarded as a virtual protocol. Specifically, since the security proof can be reduced to how to bound Eve's potential information on Alice's key bits, one can just consider the virtual protocol 1 given as below.

Step. 1 Alice prepares $|\Psi\rangle_{\mathrm{B}}$, which is the state of L-pulse train as a packet containing n-photon. Meanwhile, Alice prepares local L-qubit $|+\rangle_{\mathrm{A}_1}=(|0\rangle_{\mathrm{A}_1}+|1\rangle_{\mathrm{A}_1})/\sqrt{2},|+\rangle_{\mathrm{A}_2},\ldots,|+\rangle_{\mathrm{A}_L}$, obtains the encoding state $\sqrt{2^{-L}}\otimes_{i=1}^{L}\sum_{s=0,1}|s\rangle_{\mathrm{A}_i}(-1)^{s\hat{n}_i}|\Psi\rangle_{\mathrm{B}}$, where $\hat{n}_i:=\hat{a}_i^{\dagger}\hat{a}_i$ is the photon number operator for the i-th pulse in $|\Psi\rangle_{\mathrm{B}}$, and then emits B to Bob via an unreliable quantum channel. The first step will be repeated for N_{em} times.

Step. 2 For each B of N_{em} emissions from Alice, Bob receives an L-pulse train (or a packet) B and measures its photon number. Bob just retains the trial that there is only one photon in the train. For each of the retained trials, Bob measures which pulse in the train the single-photon is in. Assuming the single-photon is in the a-th pulse, Bob generates another random number $b\in[1,L]$ and $b\neq a$, then announces (a,b) and the index of this trial through an authenticated classical channel. One may note that in the actual protocol, Bob measures the phase shift between two pulses through a variable-delay interferometer to obtain his sifted key bit. Anyway, the actual protocol is equivalent to the virtual one in the sense of security proof.

Step. 3 Given (a,b) for each of the retained trials, Alice applies a controlled-NOT operation to the corresponding local qubits A_a and A_b, where the former is the control qubit and the latter is the target qubit. Then Alice measures A_a with $\mathbb{Z}$-basis to obtain the sifted key bit for each trial. We denote $\widetilde{\mathbf{Z}}$ as the bit string of the sifted key bits from N retained trials and $|\widetilde{\mathbf{Z}}|=N$.

Step. 4 Alice and Bob evaluate some parameters used in privacy amplification, e.g., Eve's smooth min-entropy on $\widetilde{\mathbf{Z}}$, which is essential for the security proof. Note that the results calculated here can be directly applied in the actual protocol to perform a post-processing step of sifted key bits and generate the final secret key.

Note that in the actual RRDPS protocol, Alice measures each of $|+\rangle_{\mathrm{A}_1}|+\rangle_{\mathrm{A}_2}\ldots|+\rangle_{\mathrm{A}_L}$ with $\mathbb{Z}$-basis at the very beginning of the protocol, and does not perform the controlled-NOT operation. Based on this observation, it's easy to see that the Step. 3 can be replaced by the Step. 3′, say

Step. 3′ Given (a,b) for each trial of the retained trials, Alice applies a controlled-NOT operation to the corresponding local qubits A_a and A_b, where the former is the target qubit and the latter is the control qubit. Then Alice measures A_a with $\mathbb{Z}$-basis to obtain the sifted key bit for each trial. We denote $\widetilde{\mathbf{Z}}$ as the bit string of the sifted key bits from N retained trials and $|\widetilde{\mathbf{Z}}|=N$.

We name the virtual protocol 1 with Step. 3′ instead of Step. 3 as virtual protocol 2. As a matter of fact, the virtual protocols 1 and 2 generates same sifted key bits, and Eve cannot distinguish Alice is performing virtual protocol 1 or virtual protocol 2. Therefore, from the view of security proof, the smooth min-entropy of the actual protocol can be lower bounded by the larger one of min-entropies calculated in virtual protocols 1 and 2. This consideration is the first reason that our analysis can converge to the optimal key rate given in ref. [10]. In the following, we sketch how to estimate these smooth min-entropies.

The bound for smooth min-entropy

Calculating the smooth min-entropies is a complicated problem, especially when the photon-number of $|\Psi\rangle_{\mathrm{B}}$ is large. For the ease of understanding, we only sketch the single-photon case here, while one can refer to Supplementary Note 7: General n photon-number case for the detailed proof for general cases. In single-photon case, we have $|\Psi\rangle_{\mathrm{B}}=\sum_{i=1}^{L}|i\rangle_{\mathrm{B}}$ where $|i\rangle_{\mathrm{B}}$ represents the single-photon is in the i-th pulse. Then the encoding state in step. 1 for each trial can be written in a simple form given by $\sum_{i=1}^{L}|i\rangle_{\mathrm{A}}|i\rangle_{\mathrm{B}}$, where $|i\rangle_{\mathrm{A}}=|+\rangle_{\mathrm{A}_1}|+\rangle_{\mathrm{A}_2}\ldots|-\rangle_{\mathrm{A}_i}\ldots|+\rangle_{\mathrm{A}_L}$, i.e., only the i-th local qubit A_i is in $|-\rangle$ state while all others are in $|+\rangle$ state.

Let's consider Eve launches a coherent attack for the N communication rounds, which results in a tripartite quantum state shared by Alice, Bob and Eve, i.e.,

$$|\Phi\rangle_{\mathrm{ABE}}=\sum_{i^1j^1i^2j^2\ldots i^Nj^N=1}^{L}C_{i^1j^1i^2j^2\ldots i^Nj^N}|i^1i^2\ldots i^N\rangle_{\mathrm{A}}|j^1j^2\ldots j^N\rangle_{\mathrm{B}}\left|e_{i^1j^1i^2j^2\ldots i^Nj^N}\right\rangle_{\mathrm{E}}. \tag{1}$$

Here, the superscripts denote the indices of the retained trials of step. 2 in virtual protocols. $|i^1i^2\ldots i^N\rangle_{\mathrm{A}}\triangleq|i^1\rangle_{\mathrm{A}^1}|i^2\rangle_{\mathrm{A}^2}\ldots|i^N\rangle_{\mathrm{A}^N}$. For example, $|i^1\rangle_{\mathrm{A}^1}=|+\rangle_{\mathrm{A}_1^1}|+\rangle_{\mathrm{A}_2^1}\ldots|-\rangle_{\mathrm{A}_{i^1}^1}\ldots|+\rangle_{\mathrm{A}_L^1}$ represents Alice's local qubits for the first retained trial. Similarly, $|j^1j^2\ldots j^N\rangle_{\mathrm{B}}\triangleq|j^1\rangle_{\mathrm{B}^1}|j^2\rangle_{\mathrm{B}^2}\ldots|j^N\rangle_{\mathrm{B}^N}$ means that in the first retained trial the single photon is in the j^1-th pulse, in the second retained trial the single photon is in the j^2-th pulse, and in the last retained trial the single photon is in the j^N-th pulse. $C_{i^1j^1i^2j^2\ldots i^Nj^N}$ is a complex number.

Since we are interested in the Alice and Bob's local states for the l-th retained trial, the quantum state $|\Phi\rangle_{\mathrm{ABE}}$ can be rewritten as

$$|\Phi\rangle_{\mathrm{ABE}}=\sum_{i^lj^l=1}^{L}\widetilde{C}^{l}_{i^lj^l}|i^l\rangle_{\mathrm{A}^l}|j^l\rangle_{\mathrm{B}^l}, \tag{2}$$

where $\widetilde{C}^{l}_{i^lj^l}:=\sum_{i^1j^1i^2j^2\ldots i^Nj^N/i^lj^l}C_{i^1j^1i^2j^2\ldots i^Nj^N}|i^1i^2\ldots i^N/i^l\rangle_{\mathrm{A}^{\neq l}}|j^1j^2\ldots j^N/j^l\rangle_{\mathrm{B}^{\neq l}}|e_{i^1j^1i^2j^2\ldots i^Nj^N}\rangle_{\mathrm{E}}$.

Moreover, assuming that Bob announces (a,b) in the l-th trial, we obtain the quantum state

$$\begin{aligned}\rho_{\mathrm{ABE}}&=tr_{\mathrm{A}_1^l\mathrm{A}_2^l\ldots\mathrm{A}_L^l/\mathrm{A}_a^l\mathrm{A}_b^l}\mathcal{P}\left\{{}_{\mathrm{B}^l}\langle a|\Phi\rangle_{\mathrm{ABE}}\right\}\\&=\mathcal{P}\left\{\widetilde{C}^{l}_{aa}|-\rangle_{\mathrm{A}_a^l}|+\rangle_{\mathrm{A}_b^l}+\widetilde{C}^{l}_{ba}|+\rangle_{\mathrm{A}_a^l}|-\rangle_{\mathrm{A}_b^l}\right\}+\sum_{i^l\neq a,b}\mathcal{P}\left\{\widetilde{C}^{l}_{i^la}|+\rangle_{\mathrm{A}_a^l}|+\rangle_{\mathrm{A}_b^l}\right\}.\end{aligned} \tag{3}$$

where $\mathcal{P}\{|x\rangle\}:=|x\rangle\langle x|$. Note that $\widetilde{C}^{l}_{i^lj^l}$ is a quantum system of $\mathrm{A}^{\neq l}$, $\mathrm{B}^{\neq l}$ and E. Then, it's very clear that the first part $\mathcal{P}\left\{\widetilde{C}^{l}_{aa}|-\rangle_{\mathrm{A}_a}|+\rangle_{\mathrm{A}_b}+\widetilde{C}^{l}_{ba}|+\rangle_{\mathrm{A}_a}|-\rangle_{\mathrm{A}_b}\right\}$ is coupled with Eve, which means Eve may learn sifted key bit from this mixture component. Conversely, the second part $\sum_{i^l\neq a,b}\mathcal{P}\left\{\widetilde{C}^{l}_{i^la}|+\rangle_{\mathrm{A}_a}|+\rangle_{\mathrm{A}_b}\right\}$ is decoupled with Eve, which will result in perfect secret key evidently. We call the former coupled case and the latter decoupled case, whose probabilities are $P^{l}_{\mathrm{co}}=\frac{\sum_b|\widetilde{C}^{l}_{aa}|^2+|\widetilde{C}^{l}_{ba}|^2}{\sum_b\sum_{i^l}|\widetilde{C}^{l}_{i^la}|^2}$ and $P^{l}_{\mathrm{deco}}=\frac{\sum_b\sum_{i^l\neq a,b}|\widetilde{C}^{l}_{i^la}|^2}{\sum_b\sum_{i^l}|\widetilde{C}^{l}_{i^la}|^2}$ respectively.

To analyze the smooth min-entropy in the coupled case, we refer to the entropic uncertainty relation[13,15,18]. Indeed, a so-called phase error rate e_{ph} can be used to characterize the smooth min-entropy. In ref. [5], e_{ph} is defined as the probability of finding A_b in $|-\rangle$. Differently, we define P^{l}_{a} to be the probability of finding A^{l}_{a} in $|-\rangle$ and P^{l}_{b} the probability of finding A^{l}_{b} in $|-\rangle$, just corresponding to the virtual protocols 1 and 2 respectively. Then it's straightforward to obtain $P^{l}_{a}=\frac{\sum_b|\widetilde{C}^{l}_{aa}|^2}{\sum_b\sum_{i^l}|\widetilde{C}^{l}_{i^la}|^2}$, $P^{l}_{b}=\frac{\sum_b|\widetilde{C}^{l}_{ba}|^2}{\sum_b\sum_{i^l}|\widetilde{C}^{l}_{i^la}|^2}$. For ease of notations, we define variables $x^{l}_{1}=|\widetilde{C}^{l}_{aa}|^2$ and $x^{l}_{2}=\sum_b|\widetilde{C}^{l}_{ba}|^2$, which satisfy $\sum_b|\widetilde{C}^{l}_{aa}|^2=(L-1)x^{l}_{1}$ and $\sum_b\sum_{i^l\neq a,b}|\widetilde{C}^{l}_{i^la}|^2=$

$(L-2)x_2^l$. Here $b \in \{1,2,\ldots,L\}$ and $b \neq a$. Then, $P^l_{\text{deco}} = \frac{(L-2)x_2^l}{(L-1)\sum_{j=1}^2 x_j^l}$, $P^l_{\text{co}} = \frac{(L-1)x_1^l + x_2^l}{(L-1)\sum_{j=1}^2 x_j^l}$, $P^l_a = \frac{(L-1)x_1^l}{(L-1)\sum_{j=1}^2 x_j^l}$ and $P^l_b = \frac{x_2^l}{(L-1)\sum_{j=1}^2 x_j^l}$.

Above formulae of calculating P^l_{deco}, P^l_{co}, P^l_a and P^l_b are just for the l-th bit of $\widetilde{\mathbf{Z}}$. On the other hand, the security proof needs to estimate the upper bound of smooth min-entropy of $\widetilde{\mathbf{Z}}$. We resort to Azuma's inequality to complete estimation. The basic idea is to think of above cases as the flip of coins. Consider N coin tosses, and the results of the l-th coin maybe head or not, which is dependent on previous $l-1$ tosses. We set a random variable $X_i = h_i - \sum_{l=1}^i p^l$, where p^l is the probability of having a head in the l-th round, and h_i is the number of heads. $X_0, X_1, \ldots$ is a martingale, and for two adjacent variables, $|X_k - X_{k-1}| \leq 1, k \in \{1,2,\ldots,i\}$. According to Azuma's inequality, for all $N \geq 0$ and any $\alpha \geq 0$ we can get

$$\Pr\left[\left|\frac{h_N - \sum_{l=1}^N p^l}{N}\right| \geq \alpha\right] \leq 2e^{-N\alpha^2/2}. \tag{4}$$

It's very similar between "coin cases" and our cases, which means in the l-th round, Alice's local qubits A_a and A_b in Step. 3 can be classified into decoupled cases or coupled cases, while coupled ones can be classified into with phase error and no phase error. For every kind of cases, we could construct a martingale, respectively, which justifies the application of Azuma's inequality. The same logic can be seen in ref. [19]. Among the N bits sifted key $\widetilde{\mathbf{Z}}$, we denote $N_{\text{deco}}(N_{\text{co}})$ as the bit number of decoupled(coupled) sifted key $\widetilde{\mathbf{Z}}_{\text{deco}}(\widetilde{\mathbf{Z}}_{\text{co}})$, and e_{ph} as the phase error rate of the N_{co} bits coupled key $\widetilde{\mathbf{Z}}_{\text{co}}$. According to Azuma's inequality, for all $N \geq 0$ we can find

$$\left|N_{\text{deco}} - \sum_{l=1}^N P^l_{\text{deco}}\right| \leq \sqrt{2N\ln\frac{2}{\epsilon^N_{\text{deco}}}} \tag{5}$$

holds with probability at least $1 - 2\epsilon^N_{\text{deco}}$. Similarly,

$$\left|N_{\text{co}} - \sum_{l=1}^N P^l_{\text{co}}\right| \leq \sqrt{2N\ln\frac{2}{\epsilon^N_{\text{co}}}} \tag{6}$$

and

$$\left|e_{\text{ph}} - \frac{\sum_{l=1}^{N_{\text{co}}} P^l}{N_{\text{co}}}\right| \leq \sqrt{\frac{2\ln\frac{2}{\epsilon^{e_{\text{ph}}}_{\text{co}}}}{N_{\text{co}}}} \tag{7}$$

hold with probabilities at least $1 - 2\epsilon^N_{\text{co}}$ and $1 - 2\epsilon^{e_{\text{ph}}}_{\text{co}}$, respectively. Note that, $P^l := \min\{P^l_a, P^l_b\}$.

We further set $\sum_{l=1}^N \frac{x_1^l}{\sum_{j=1}^2 x_j^l} \triangleq c_1$, and $\sum_{l=1}^N \frac{x_2^l}{\sum_{j=1}^2 x_j^l} \triangleq c_2$, where c_1, $c_2 \in [0, N]$, $c_1 + c_2 \leq N$. Then these inequalities could be rewritten by

$$\begin{aligned}
&\left|N_{\text{deco}} - \tfrac{(L-2)c_2}{L-1}\right| \leq \sqrt{2N\ln\tfrac{2}{\epsilon^N_{\text{deco}}}},\\
&\left|N_{\text{co}} - \tfrac{(L-1)c_1+c_2}{L-1}\right| \leq \sqrt{2N\ln\tfrac{2}{\epsilon^N_{\text{co}}}},\\
&e_{\text{ph}} = \min\{e_{\text{pha}}, e_{\text{phb}}\},
\end{aligned} \tag{8}$$

where

$$\begin{aligned}
e_{\text{pha}} &\leq \tfrac{c_1}{N_{\text{co}}} + \sqrt{\tfrac{2\ln\frac{2}{\epsilon^{e_{\text{ph}}}_{\text{co}}}}{N_{\text{co}}}},\\
e_{\text{phb}} &\leq \tfrac{c_2}{(L-1)N_{\text{co}}} + \sqrt{\tfrac{2\ln\frac{2}{\epsilon^{e_{\text{ph}}}_{\text{co}}}}{N_{\text{co}}}}.
\end{aligned} \tag{9}$$

Now, we are ready to calculate Eve's smooth min-entropy $H^\epsilon_{\min}(\widetilde{\mathbf{Z}}|\mathrm{E})$. According to chain rules and entropic uncertainty relation, we have

$$\begin{aligned}
H^\epsilon_{\min}(\widetilde{\mathbf{Z}}|\mathrm{E}) &\geq H^\epsilon_{\min}(\widetilde{\mathbf{Z}}_{\text{deco}}\widetilde{\mathbf{Z}}_{\text{co}}|\mathrm{E})\\
&\geq H^{\epsilon_{\text{deco}}}_{\min}(\widetilde{\mathbf{Z}}_{\text{deco}}|\widetilde{\mathbf{Z}}_{\text{co}}\mathrm{E}) + H^{\epsilon_{\text{co}}}_{\min}(\widetilde{\mathbf{Z}}_{\text{co}}|\mathrm{E}) - \log\tfrac{2}{\epsilon'^2_0}\\
&\geq N_{\text{deco}} + N_{\text{co}} - N_{\text{co}}H_2(e_{\text{ph}}) - \log\tfrac{2}{\epsilon'^2_0},\\
&= N - N_{\text{co}}H_2(e_{\text{ph}}) - \log\tfrac{2}{\epsilon'^2_0},
\end{aligned} \tag{10}$$

where the smooth parameters satisfy $\epsilon = 2\epsilon_{\text{deco}} + \epsilon_{\text{co}} + \epsilon'_0 = 2\epsilon^N_{\text{co}} + 2\epsilon^{e_{\text{ph}}}_{\text{co}} + \epsilon'_0$ and $\epsilon_{\text{deco}} = 0$. Finally, the smooth min-entropy $H^\epsilon_{\min}(\widetilde{\mathbf{Z}}|\mathrm{E})$ depends on N_{co} and e_{ph}, which are further decided by parameters c_1 and c_2. This means that we can optimize these parameters to obtain the maximum of $H^\epsilon_{\min}(\widetilde{\mathbf{Z}}|\mathrm{E})$.

Basically, the derivations of $H^\epsilon_{\min}(\widetilde{\mathbf{Z}}|\mathrm{E})$ for n-photon case is following the same manner and detailed in Supplementary Note 7: General n photon-number case. In short, ρ_{ABE} is a mixture of decoupled component and n different types of coupled components, which implies $H^\epsilon_{\min}(\widetilde{\mathbf{Z}}|\mathrm{E})$ is characterized by the bits of decoupled key N_{deco}, the bits of the i-th type of coupled key $N_{\text{co}i}$ and its corresponding phase error rate $e_{\text{ph}i}$, $1 \leq i \leq n$.

Secret key rate

We have obtained the smooth min-entropy in n photon-number case. However, it's more complex in actual QKD system with phase-randomized weak coherent source, which makes $|\Psi\rangle_B$ to be a mixture of Fock states with Poisson distribution. Similarly, with the idea in ref. [5], we set a threshold value of photon-number as v_{th} and classified $\widetilde{\mathbf{Z}}$ into $\mathbf{Z}_{n\leq v_{\text{th}}}$ and $\mathbf{Z}_{n>v_{\text{th}}}$, where $\mathbf{Z}_{n>v_{\text{th}}}(\mathbf{Z}_{n\leq v_{\text{th}}})$ represents the sifted key bits generated by $|\Psi\rangle_B$ of photon-number (no) larger than v_{th}. Without compromising the security, Eve's smooth min-entropy of $\mathbf{Z}_{n>v_{\text{th}}}$ is treated as 0, while each of $\mathbf{Z}_{n\leq v_{\text{th}}}$ is regarded as the v_{th} photon-number case, whose smooth min-entropy can be solved by the results in the last section.

Accordingly, we present the secret key length ℓ as

$$\ell = \left\lfloor N_{n\leq v_{\text{th}}} - \sum_{i=1}^{v_{\text{th}}} N_{\text{co}i}H_2(e_{\text{ph}i}) - \xi NH_2(e_{\text{bit}}) - \log\frac{2^{v_{\text{th}}+1}}{(\tilde{\epsilon}^2)^{v_{\text{th}}+2}}\right\rfloor. \tag{11}$$

where $N_{n\leq v_{\text{th}}} = |\mathbf{Z}_{n\leq v_{\text{th}}}|$. ξ refers to bit error correction efficiency, and e_{bit} is the bit error rate. Besides, for simplicity, we have set all failure parameters to be the same $\tilde{\epsilon}$. See the Methods for a detailed derivation.

Now we are going to evaluate the performance of RRDPS with a phase randomized weak coherent source in finite regions. We use Mathematica to simulate the final secret key rate per pulse marked as $R = \ell/LN_{\text{em}}$ under different conditions. The detailed formula and the simulation parameters of R can be seen in Methods.

In Fig. 1, we show R versus channel loss at different number of pulses and L, while R versus N_{em} with different L are shown in Fig. 2. The results show that to eliminate finite-key effects, pulse numbers less than 10^{11} are sufficient for typical values of L.

DISCUSSION

From the results of simulations, we can see that the larger the value of L, the more emitted pulses needed. Despite all this, it's evident that our method makes R to be sufficiently close to the asymptotic bound when the number of emitted pulses is achievable in practical high speed QKD systems[20–24].

The protocol most commonly used for comparison is decoy-state[25–27] BB84 protocol. Evidently, if the optical misalignment is large, e.g., $e_{\text{mis}} \geq 0.11$, RRDPS with relevant L always has higher key rate. This is because BB84 can tolerant error rate e_{bit} up to 0.11. Besides, RRDPS protocol does not require monitoring signal disturbance, which obviously reduces finite-size effects and

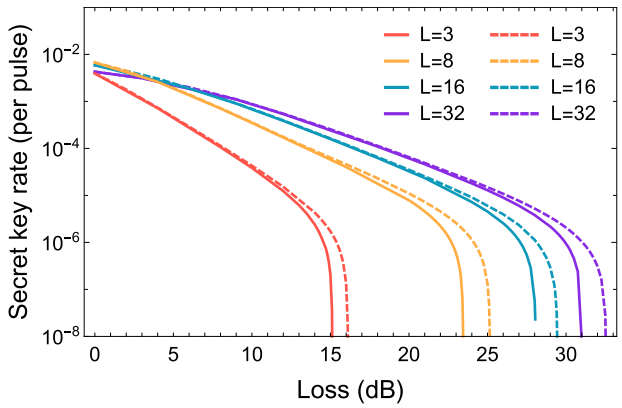

Fig. 1 Secret key rate *R* versus channel loss. The full lines show the secret key rate R versus channel loss for the RRDPS protocol when $N_{\rm em}$ is finite. From left to right, L is 3, 8, 16, 32, and the corresponding total emitted pulses are 2×10^9, 10^{10}, 4×10^{10}, 6×10^{10}, respectively. While the dashed lines represent the asymptotic results correspond to ref. [10]. The total security parameter of final key is $\epsilon_{\rm tot}:=10^{-10}$. Dark counts rate is $d=10^{-6}$ per pulse, and the misalignment of measurement is $e_{\rm mis}=0.015$. The efficiency of error correction ξ is 1.1.

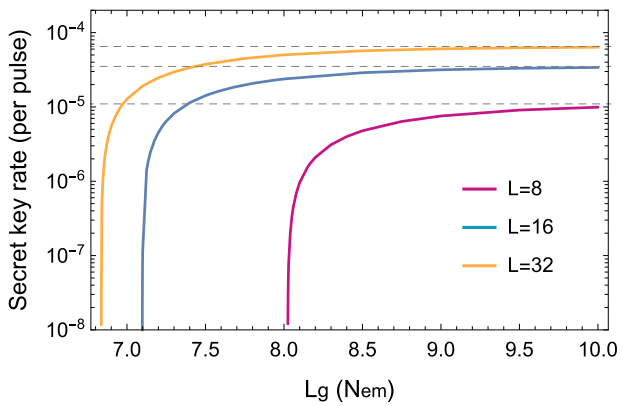

Fig. 2 Secret key rate *R* versus $N_{\rm em}$. The full lines show the secret key rate R versus $N_{\rm em}$ for the RRDPS protocol when $N_{\rm em}$ is finite. These lines from bottom to up with $L=8, 16, 32$. The dashed lines represent the asymptotic results. The total security parameter of the final key is $\epsilon_{\rm tot}:=10^{-10}$. The channel loss is fixed at 20 dB. Dark counts rate is $d=10^{-6}$ per pulse, and the misalignment of measurement is $e_{\rm mis}=0.015$. The efficiency of error correction ξ is 1.1.

simplifies the flow of post-processing. A comparison in finite-key region, especially when pulse number is particularly small, is more meaningful. Before comparison, one should note that Azuma's inequality is used in our proof which makes our proof applicable to arbitrary correlations and sifting[28,29]. Meanwhile, most of works on decoy-state BB84, typically the finite-key analysis in ref. [18], assume independent random variables, and thus only applicable in non-iterative sifting[28,29]. Therefore, in some sense it's not fair to directly compare our results with decoy-state BB84 finite-key analyses. In order to solve this problem, we derive a corollary based on our general theory. Please see Supplementary Method: A corollary of an improved bound on phase error rate for details. This corollary gives a simple but improved (compared with ref. [5]) bound on phase error rate $e_{\rm ph}$, i.e., $e_{\rm ph}\le n/L$. Then we can use Chernoff's inequality instead of Azuma's inequality to obtain a simple finite-key analysis just applicable for independent random variables and non-iterative sifting. With the same channel model and parameters, it's easy to verify that our method exhibits

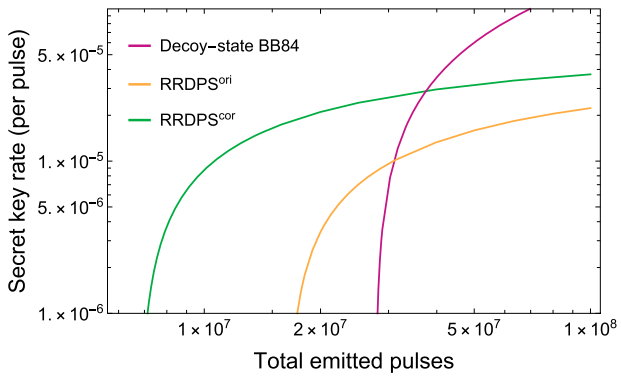

Fig. 3 Comparison with other protocols. The full lines show the secret key rate versus total emitted pulses. The red curve represents the finite-key analysis of decoy-state BB84 protocol in ref. [18]. The yellow curve represents the original finite-key analysis of RRDPS protocol given in ref. [5]. The green curve represents the key rate based on our corollary. We set $L=53$. The total security parameter of the final key is $\epsilon_{\rm tot}:=10^{-10}$. The channel loss is fixed at 20dB, dark counts rate is $d=10^{-6}$ per pulse, and the misalignment of measurement is $e_{\rm mis}=0.015$. The efficiency of error correction ξ is 1.1.

positive key rate when total number of pulses is $10^{6.85}$ with $L=53$, while decoy-state BB84 needs $10^{7.44}$ pulses. Please see Fig. 3 for the complete curves. This implies the advantage of RRDPS over decoy-state BB84 when communication time is very short.

We note that there have been two important related works about finite-key analysis of RRDPS protocol. In ref. [30], the security proof of RRDPS protocol is refined, but their results do not benefit from phase-randomized source thus cannot reach the asymptotic secret key rate given in ref. [10]. Besides, according to ref. [30], they found that their key rate is lower than ref. [5] when pulse number is small. This implies that the key rate based on our corollary is higher than ref. [30] in cases of small pulse number–see Fig. 3. As for ref. [12], it keeps the advantage of phase randomization, but the required number of pulses is too large to meet the practical systems. As far as we know, our results are optimal for RRDPS in finite-key region, which implies that QKD without monitoring signal disturbance can be realized in present QKD systems. Besides, from the view of security proofs, this is a try to apply the uncertainty relation and Azuma's inequality in high-dimensional QKD protocols. This may shed lights on the developments of techniques for security proofs.

METHODS

Calculation for secret key rate

Our analysis is based on the universally composable security theory[31].

In the frame of universally composable security, Alice can extract ℓ bits of the secret key using a random leftover hash function[32] or Trevisan's extractor[33]. The secret key length ℓ is Δ-secret[15],

$$\Delta=\min_{\varepsilon}(2\varepsilon+\frac{1}{2}\sqrt{2^{\ell-H^{\varepsilon}_{\min}(\widetilde{\mathbf{Z}}|\mathrm{E}')}}) \tag{12}$$

where $\widetilde{\mathbf{Z}}$ denotes the sifted key bits, $|\widetilde{\mathbf{Z}}|=N$. E′ is labelled as all information Eve knows about $\widetilde{\mathbf{Z}}$ during the protocol, i.e., Eve's quantum system E, error correction and verification codes announced by Alice.

To justify $\Delta\le2\varepsilon+\bar{\epsilon}$, we can set

$$\ell\le\max_{\varepsilon,\bar{\epsilon}}\lfloor H^{\varepsilon}_{\min}(\widetilde{\mathbf{Z}}|\mathrm{E}')-2\log\frac{1}{2\bar{\epsilon}}\rfloor. \tag{13}$$

Considering the bits announced for error correction and verification[31], we have

$$\ell\le\max_{\varepsilon,\bar{\epsilon}}\lfloor H^{\varepsilon}_{\min}(\widetilde{\mathbf{Z}}|\mathrm{E})-\xi NH_2(e_{\rm bit})-\log\frac{2}{\epsilon_{\rm cor}}-2\log\frac{1}{2\bar{\epsilon}}\rfloor, \tag{14}$$

where ξ is the efficiency of error correction we have mentioned before and ϵ_{cor} is the failure probability of error verification.

Calculating $H_{\min}^{\epsilon}(\widetilde{\mathbf{Z}}|\mathrm{E})$ is essential in our proof. Following a generalized chain rule for smooth min-entropy[34], we have

$$\begin{aligned} H_{\min}^{\epsilon}(\widetilde{\mathbf{Z}}|\mathrm{E}) &\geq H_{\min}^{\epsilon}(\mathbf{Z}_{n\leq v_{\text{th}}}\mathbf{Z}_{n>v_{\text{th}}}|\mathrm{E}) \\ &\geq H_{\min}^{\epsilon_{n>v_{\text{th}}}}(\mathbf{Z}_{n>v_{\text{th}}}|\mathbf{Z}_{n\leq v_{\text{th}}}\mathrm{E}) + H_{\min}^{\epsilon_{n\leq v_{\text{th}}}}(\mathbf{Z}_{n\leq v_{\text{th}}}|\mathrm{E}) - \log\tfrac{2}{\epsilon'^2} \\ &\geq H_{\min}^{\epsilon}(\mathbf{Z}_{n\leq v_{\text{th}}}|\mathrm{E}) - \log\tfrac{2}{\epsilon'^2}, \end{aligned} \tag{15}$$

where $\mathbf{Z}_{n\leq v_{\text{th}}}$ represents the sifted key bits which are generated by $|\Psi\rangle_{\mathrm{B}}$ of photon-number n no larger than v_{th}, $|\mathbf{Z}_{n\leq v_{\text{th}}}| = N_{n\leq v_{\text{th}}}$, and $\mathbf{Z}_{n>v_{\text{th}}}$ represents the sifted key bits are generated by $|\Psi\rangle_{\mathrm{B}}$ of photon-number n larger than v_{th}. For simplicity, we abbreviate $\epsilon_{n\leq v_{\text{th}}}$ to ϵ, and then $H_{\min}^{\epsilon_{n\leq v_{\text{th}}}}(\mathbf{Z}_{n\leq v_{\text{th}}}|\mathrm{E})$ to $H_{\min}^{\epsilon}(\mathbf{Z}_{n\leq v_{\text{th}}}|\mathrm{E})$. Besides, $\varepsilon = \epsilon + \varepsilon'$.

Right now, we are going to calculate $H_{\min}^{\epsilon}(\mathbf{Z}_{n\leq v_{\text{th}}}|\mathrm{E})$. Without compromising security, it is assumed that all bits of $\mathbf{Z}_{n\leq v_{\text{th}}}$ are generated by $|\Psi\rangle_{\mathrm{B}}$ of photon-number v_{th}. As proved in Supplementary Note 7: General n photon-number case, $\mathbf{Z}_{n\leq v_{\text{th}}}$ can be decomposed into decoupled bits $\mathbf{Z}_{\text{deco}}$ and v_{th} different types of coupled bits $\mathbf{Z}_{\text{co}i}(i = 1, 2, \ldots, v_{\text{th}})$. Using v_{th} times of chain rule, we have

$$\begin{aligned} H_{\min}^{\epsilon}(\mathbf{Z}_{n\leq v_{\text{th}}}|\mathrm{E}) &\geq H_{\min}^{\epsilon_{\text{deco}}}(\mathbf{Z}_{\text{deco}}\mathbf{Z}_{\text{co}1}\mathbf{Z}_{\text{co}2}\ldots\mathbf{Z}_{\text{co}v_{\text{th}}}|\mathrm{E}) \\ &\geq H_{\min}^{\epsilon_{\text{deco}}}(\mathbf{Z}_{\text{deco}}|\mathbf{Z}_{\text{co}1}\mathbf{Z}_{\text{co}2}\ldots\mathbf{Z}_{\text{co}v_{\text{th}}}\mathrm{E}) + H_{\min}^{\epsilon_{\text{co}1}}(\mathbf{Z}_{\text{co}1}|\mathbf{Z}_{\text{co}2}\mathbf{Z}_{\text{co}3}\ldots\mathbf{Z}_{\text{co}v_{\text{th}}}\mathrm{E}) \\ &\quad + H_{\min}^{\epsilon_{\text{co}2}}(\mathbf{Z}_{\text{co}2}|\mathbf{Z}_{\text{co}3}\mathbf{Z}_{\text{co}4}\ldots\mathbf{Z}_{\text{co}v_{\text{th}}}\mathrm{E}) + \ldots \\ &\quad + H_{\min}^{\epsilon_{\text{co}(v_{\text{th}}-1)}}(\mathbf{Z}_{\text{co}(v_{\text{th}}-1)}|\mathbf{Z}_{\text{co}v_{\text{th}}}\mathrm{E}) + H_{\min}^{\epsilon_{\text{co}v_{\text{th}}}}(\mathbf{Z}_{\text{co}v_{\text{th}}}|\mathrm{E}) - \left(\sum_{i=0}^{v_{\text{th}}-1}\log\tfrac{2}{\epsilon_i'^2}\right). \end{aligned} \tag{16}$$

Since $\mathbf{Z}_{\text{deco}}$ is completely independent to other quantum systems including Eve's system E,

$$H_{\min}^{\epsilon_{\text{deco}}}(\mathbf{Z}_{\text{deco}}|\mathbf{Z}_{\text{co}1}\mathbf{Z}_{\text{co}2}\ldots\mathbf{Z}_{\text{co}v_{\text{th}}}\mathrm{E}) \geq |\mathbf{Z}_{\text{deco}}| := N_{\text{deco}} \tag{17}$$

always holds with $\epsilon_{\text{deco}} = 0$. And the smooth parameter $\epsilon = 2\left(\sum_{i=1}^{v_{\text{th}}-1}\epsilon_{\text{co}i}\right) + \epsilon_{\text{co}v_{\text{th}}} + \sum_{i=0}^{v_{\text{th}}-1}\epsilon_i'$.

To estimate $H_{\min}^{\epsilon_{\text{co}i}}(\mathbf{Z}_{\text{co}i}|\mathbf{Z}_{\text{coother}}\mathrm{E})$, we can refer to the uncertainty relation, namely,

$$H_{\min}^{\epsilon_{\text{co}i}}(\mathbf{Z}_{\text{co}i}|\mathbf{Z}_{\text{coother}}\mathrm{E}) \geq N_{\text{co}i} - N_{\text{co}i}H_2(e_{\text{ph}i}) \tag{18}$$

where $\mathbf{Z}_{\text{coother}} = \mathbf{Z}_{\text{co}(i+1)}\mathbf{Z}_{\text{co}(i+2)}\ldots\mathbf{Z}_{\text{co}v_{\text{th}}}$, $i \in [1, v_{\text{th}}]$, $|\mathbf{Z}_{\text{co}i}| = N_{\text{co}i}$, and $e_{\text{ph}i}$ denotes the upper bound of phase error rate for $\mathbf{Z}_{\text{co}i}$, i.e., the chance of observing $|-\rangle$ with a hypothetical $\mathbb{X}$-basis instead of $\mathbb{Z}$-basis. Meanwhile, $\epsilon_{\text{co}i}$ is equal to the probability that number of $|-\rangle$ is larger than $N_{\text{co}i}e_{\text{ph}i}$.

The next issue is how to calculate N_{deco}, $N_{\text{co}i}$ and $e_{\text{ph}i}$. We prove that for an l-th retained trial (the event generating the l-th bit of $\mathbf{Z}_{n\leq v_{\text{th}}}$), the probabilities of obtaining decoupled case, i-th coupled case and a corresponding phase error event, all of which can be given by some non-negative real numbers $c_i(i \in [1, v_{\text{th}}+1])$ satisfying $\sum_{i=1}^{v_{\text{th}}+1} c_i = N_{n\leq v_{\text{th}}}$. We point out that the analysis method is similar to the single-photon case above, but more complex. The detailed proof is present in Supplementary Note 7: General n photon-number case.

Similarly, with the help of Azuma's inequality, one can bound N_{deco}, $N_{\text{co}i}$ and $e_{\text{ph}i}$ for the sifted key bit string $\mathbf{Z}_{n\leq v_{\text{th}}}$ in terms of c_i with some failure probabilities. Specifically, with probabilities at least $1 - 2\epsilon_{\text{deco}}^{N_{n\leq v_{\text{th}}}}$, $1 - 2\epsilon_{\text{co}i}^{N_{n\leq v_{\text{th}}}}$ and $1 - 2\epsilon_{\text{co}i}^{e_{\text{ph}}}$ respectively,

$$\begin{aligned} &\left|N_{\text{deco}} - \tfrac{(L-v_{\text{th}}-1)c_{v_{\text{th}}+1}}{L-1}\right| \leq \sqrt{2N_{n\leq v_{\text{th}}}\ln\tfrac{2}{\epsilon_{\text{deco}}^{N_{n\leq v_{\text{th}}}}}}, \\ &\left|N_{\text{co}i} - \tfrac{(L-i)c_i + ic_{i+1}}{L-1}\right| \leq \sqrt{2N_{n\leq v_{\text{th}}}\ln\tfrac{2}{\epsilon_{\text{co}i}^{N_{n\leq v_{\text{th}}}}}}, \\ &e_{\text{ph}i} = \min\left\{e_{\text{ph}ai}, e_{\text{ph}bi}\right\} \end{aligned} \tag{19}$$

hold. Here, if $v_{\text{th}} \in$ odd and $j \in [1, \frac{v_{\text{th}}+1}{2}]$,

$$\begin{aligned} e_{\text{pha}(2j-1)} &\leq \tfrac{[L-(2j-1)]c_{2j-1}}{L-1}/N_{\text{co}(2j-1)} + \sqrt{\tfrac{2\ln\frac{2}{\epsilon_{\text{ph}}^{2}}}{N_{\text{co}(2j-1)}}}; \\ e_{\text{phb}(2j-1)} &\leq \tfrac{(2j-1)c_{2j-1}}{L-1}/N_{\text{co}(2j-1)} + \sqrt{\tfrac{2\ln\frac{2}{\epsilon_{\text{ph}}^{2}}}{N_{\text{co}(2j-1)}}}; \\ e_{\text{pha}(2j)} &= e_{\text{phb}(2j)} \leq \tfrac{(2j)c_{2j+1}}{L-1}/N_{\text{co}(2j)} + \sqrt{\tfrac{2\ln\frac{2}{\epsilon_{\text{ph}}^{2}}}{N_{\text{co}(2j)}}}. \end{aligned} \tag{20}$$

If $v_{\text{th}} \in$ even and $j \in [1, \frac{v_{\text{th}}}{2}]$,

$$\begin{aligned} e_{\text{pha}(2j-1)} &= e_{\text{phb}(2j-1)} \leq \tfrac{(2j-1)c_{2j}}{L-1}/N_{\text{co}(2j-1)} + \sqrt{\tfrac{2\ln\frac{2}{\epsilon_{\text{ph}}^{2}}}{N_{\text{co}(2j-1)}}}; \\ e_{\text{pha}(2j)} &\leq \tfrac{(L-2j)c_{2j}}{L-1}/N_{\text{co}(2j)} + \sqrt{\tfrac{2\ln\frac{2}{\epsilon_{\text{ph}}^{2}}}{N_{\text{co}(2j)}}}; \\ e_{\text{phb}(2j)} &\leq \tfrac{(2j)c_{2j+1}}{L-1}/N_{\text{co}(2j)} + \sqrt{\tfrac{2\ln\frac{2}{\epsilon_{\text{ph}}^{2}}}{N_{\text{co}(2j)}}}. \end{aligned} \tag{21}$$

To summarize the above analysis of $H_{\min}^{\epsilon}(\widetilde{\mathbf{Z}}|\mathrm{E})$, we have

$$\begin{aligned} H_{\min}^{\epsilon}(\widetilde{\mathbf{Z}}|\mathrm{E}) &\geq N_{\text{deco}} + N_{\text{co}1} + N_{\text{co}2} + \ldots + N_{\text{co}v_{\text{th}}} - N_{\text{co}1}H_2(e_{\text{ph}1}) \\ &\quad - N_{\text{co}2}H_2(e_{\text{ph}2}) - \ldots - N_{\text{co}v_{\text{th}}}H_2(e_{\text{ph}v_{\text{th}}}) - \left(\sum_{i=0}^{v_{\text{th}}-1}\log\tfrac{2}{\epsilon_i'^2}\right) - \log\tfrac{2}{\varepsilon'^2} \\ &= N_{n\leq v_{\text{th}}} - \sum_{i=1}^{v_{\text{th}}}N_{\text{co}i}H_2(e_{\text{ph}i}) - \left(\sum_{i=0}^{v_{\text{th}}-1}\log\tfrac{2}{\epsilon_i'^2}\right) - \log\tfrac{2}{\varepsilon'^2}, \end{aligned} \tag{22}$$

where N_{deco}, $N_{\text{co}i}$ and $e_{\text{ph}i}$ can be decided by Eqs. (19)–(21). The smooth parameters satisfy

$$\begin{aligned} \varepsilon &= \epsilon + \varepsilon' = 2\sum_{i=1}^{v_{\text{th}}-1}\epsilon_{\text{co}i} + \epsilon_{\text{co}v_{\text{th}}} + \sum_{i=0}^{v_{\text{th}}-1}\epsilon_i' + \varepsilon' \\ &= 4\sum_{i=1}^{v_{\text{th}}-1}\left(\epsilon_{\text{co}i}^{N_{n\leq v_{\text{th}}}} + \epsilon_{\text{co}i}^{e_{\text{ph}}}\right) + 2\left(\epsilon_{\text{co}v_{\text{th}}}^{N_{n\leq v_{\text{th}}}} + \epsilon_{\text{co}v_{\text{th}}}^{e_{\text{ph}}}\right) + \sum_{i=0}^{v_{\text{th}}-1}\epsilon_i' + \varepsilon' \end{aligned} \tag{23}$$

So far, we've completed the derivation of $H_{\min}^{\epsilon}(\widetilde{\mathbf{Z}}|\mathrm{E})$. By optimizing the parameters c_i, the lower bound of $H_{\min}^{\epsilon}(\widetilde{\mathbf{Z}}|\mathrm{E})$ can be found. In following, $\sum_{i=1}^{v_{\text{th}}}N_{\text{co}i}H_2(e_{\text{ph}i})$ represents its minimum value by optimizing c_i under given smooth parameters. Substituting Eq. (22) to Eq. (14), we have

$$\begin{aligned} \ell &\leq \lfloor N_{n\leq v_{\text{th}}} - \sum_{i=1}^{v_{\text{th}}}N_{\text{co}i}H_2(e_{\text{ph}i}) - (v_{\text{th}}+1)\log\tfrac{2}{\tilde{\epsilon}} - \xi NH_2(e_{\text{bit}}) - \log\tfrac{1}{2\tilde{\epsilon}}\rfloor \\ &= \lfloor N_{n\leq v_{\text{th}}} - \sum_{i=1}^{v_{\text{th}}}N_{\text{co}i}H_2(e_{\text{ph}i}) - \xi NH_2(e_{\text{bit}}) - \log\tfrac{2^{v_{\text{th}}}}{(\tilde{\epsilon})^{2v_{\text{th}}+5}}\rfloor. \end{aligned} \tag{24}$$

where we have set all failure probabilities or smooth parameters in Eq. (22) to be the same one $\tilde{\epsilon}$.

Finally, we can get the secret key rate per pulse $R := \frac{\ell}{LN_{\text{em}}}$,

$$R \leq \frac{1}{L}\left[(Q - e_{\text{src}}^{\text{u}}) - \frac{1}{N_{\text{em}}}\left(\sum_{i=1}^{v_{\text{th}}}N_{\text{co}i}H_2(e_{\text{ph}i})\right) - \xi QH_2(e_{\text{bit}}) - \frac{1}{N_{\text{em}}}\log\frac{2^{v_{\text{th}}}}{(\tilde{\epsilon})^{2v_{\text{th}}+5}}\right]. \tag{25}$$

We use empirical results $N_{\text{deco}} + N_{\text{co}1} + N_{\text{co}2} + \ldots + N_{\text{co}v_{\text{th}}} = N_{n\leq v_{\text{th}}} = (Q - e_{\text{src}}^{\text{u}})N_{\text{em}}$ and the yield per packet $Q = \frac{N}{N_{\text{em}}}$. Besides, considering the fluctuation of photon-number, the upper bound of $e_{\text{src}} := 1 - \sum_{i=0}^{v_{\text{th}}}\mathrm{e}^{-L\mu}(L\mu)^i/i!$ can be given by Chernoff bounds[12,35]: $e_{\text{src}}^{\text{u}} \leq e_{\text{src}} + \sqrt{\frac{3e_{\text{src}}}{N_{\text{em}}}\ln\frac{1}{\epsilon_{\text{PE}}}} = e_{\text{src}} + \sqrt{\frac{3e_{\text{src}}}{N_{\text{em}}}\ln\frac{1}{\tilde{\epsilon}}}$, where μ represents the intensity per pulse of phase-randomized weak coherent source.

The total security parameter[36] of final key is ϵ_{tot},

$$\epsilon_{\text{tot}} = 2\varepsilon + \epsilon_{\text{cor}} + \bar{\epsilon} + \tilde{\epsilon} = (18v_{\text{th}} - 3)\tilde{\epsilon}. \tag{26}$$

Note that for a fixed ϵ_{tot}, one should optimize v_{th} to maximize R.

In the end, we further give the method used in the simulation. The channel efficiency is $\eta = 10^{-\text{loss(dB)}/10}$. We assume that Bob's detectors have dark counts rate of $d = 10^{-6}$ per pulse, and there is a misalignment of measurement, that is $e_{\text{mis}} = 0.015$. Set ξ to be 1.1, $\epsilon_{\text{tot}} = 10^{-10}$. The observed yield Q and error rate e_{bit} are assumed to be always equal to their asymptotic ones respectively, whose expressions can be found in ref. [10]. Then by optimizing the light intensity μ, the threshold photon-number v_{th} and $\{c_i\}$, one can calculate the R under a fixed security parameter ϵ_{tot}.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request

Received: 10 November 2020; Accepted: 19 April 2021;
Published online: 09 June 2021

REFERENCES

1. Bennett, C. H. & Brassard, G. *In Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, IEEE New York 175–179 (Bangalore, India, 1984).
2. Acin, A. et al. Device-Independent Security of Quantum Cryptography against Collective Attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
3. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
4. Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).
5. Sasaki, T., Yamamoto, Y. & Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **509**, 475–478 (2014).
6. Guan, J.-Y. et al. Experimental passive round-robin differential phase-shift quantum key distribution. *Phys. Rev. Lett.* **114**, 180502 (2015).
7. Takesue, H., Sasaki, T., Tamaki, K. & Koashi, M. Experimental quantum key distribution without monitoring signal disturbance. *Nat. Photonics* **9**, 827–831 (2015).
8. Wang, S. et al. Experimental demonstration of a quantum key distribution without signal disturbance monitoring. *Nat. Photonics* **9**, 832–836 (2015).
9. Li, Y.-H. et al. Experimental round-robin differential phase-shift quantum key distribution. *Phys. Rev. A* **93**, 030302 (2016).
10. Yin, Z.-Q. et al. Improved security bound for the round-robin-differential-phase-shift quantum key distribution. *Nat. Commun.* **9**, 457 (2018).
11. Christandl, M., König, R. & Renner, R. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.* **102**, 020504 (2009).
12. Liu, H. et al. Finite-key analysis for round-robin-differential-phase-shift quantum key distribution. *Opt. Express* **28**, 15416–15423 (2020).
13. Tomamichel, M. & Renner, R. Uncertainty relation for smooth entropies. *Phys. Rev. Lett.* **106**, 110506 (2011).
14. Azuma, K. Weighted sums of certain dependent random variables. *Tohoku Math. J.* **19**, 357–367 (1967).
15. Tomamichel, M., Lim, C. C. W., Gisin, N. & Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3**, 634 (2012).
16. Curty, M. et al. Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **5**, 3732 (2014).
17. Currás-Lorenzo, G. et al. Tight finite-key security for twin-field quantum key distribution. *NPJ Quantum Inf.* **7**, 1–9 (2021).
18. Lim, C. C. W., Curty, M., Walenta, N., Xu, F. & Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **89**, 022307 (2014).
19. Boileau, J.-C., Tamaki, K., Batuwantudawe, J., Laflamme, R. & Renes, J. Unconditional Security of a Three State Quantum Key Distribution Protocol. *Phys. Rev. Lett.* **94**, 040503 (2005).
20. Gordon, K. J. et al. Quantum key distribution system clocked at 2 GHz. *Opt. Express* **13**, 3015–3020 (2005).
21. Thew, R. T. et al. Low jitter up-conversion detectors for telecom wavelength GHz QKD. *New J. Phys.* **8**, 32 (2006).
22. Takesue, H. et al. Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. *Nat. Photonics* **1**, 343–348 (2007).
23. Yuan, Z., Dixon, A., Dynes, J., Sharpe, A. & Shields, A. Gigahertz quantum key distribution with InGaAs avalanche photodiodes. *Appl. Phys. Lett.* **92**, 201104 (2008).
24. Sasaki, M. et al. Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **19**, 10387–10409 (2011).
25. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003).
26. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
27. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
28. Pfister, C., Lütkenhaus, N., Wehner, S. & Coles, P. J. Sifting attacks in finite-size quantum key distribution. *New J. Phys.* **18**, 053001 (2016).
29. Tamaki, K. et al. Security of quantum key distribution with iterative sifting. *Quantum Sci. Technol.* **3**, 014002 (2017).
30. Matsuura, T., Sasaki, T. & Koashi, M. Refined security proof of the round-robin differential-phase-shift quantum key distribution and its improved performance in the finite-sized case. *Phys. Rev. A* **99**, 042303 (2019).
31. Renner, R. Security of quantum key distribution. *Int. J. Quantum Inf.* **6**, 1–127 (2008).
32. Tomamichel, M., Renner, R. & Schaffner, C. Leftover Hashing against quantum side information. *IEEE Trans. Inf. Theory* **57**, 5524–5535 (2011).
33. De, A., Portmann, C., Vidick, T. & Renner, R. Trevisan's extractor in the presence of quantum side information. *SIAM J. Comput.* **41**, 915–940 (2012).
34. Vitanov, A., Dupuis, F., Tomamichel, M. & Renner, R. Chain Rules for Smooth Min- and Max-Entropies. *IEEE Trans. Inf. Theory* **59**, 2603–2612 (2013).
35. Chernoff, H. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *Ann. Math. Stat.* **23**, 493–507 (1952).
36. Mueller-Quade, J. & Renner, R. Composability in quantum cryptography. *New J. Phys.* **11**, 085006 (2009).

ACKNOWLEDGEMENTS

This work has been supported by the National Key Research and Development Program of China (Grant No. 2018YFA0306400), the National Natural Science Foundation of China (Grant Nos. 61822115, 61961136004, 61775207, 61627820) and Anhui Initiative in Quantum Information Technologies. The authors acknowledge Dr. Takaya Matsuura in Department of Applied Physics, Graduate School of Engineering, University of Tokyo.

AUTHOR CONTRIBUTIONS

Z.-Q.Y., R.W., S.W., W.C., G.-C.G., Z.-F.H. conceived the basic idea of the security proof. Z.-Q.Y. and H.L. finished the details of the security proof. H.L. designed the simulations. Z.-H.W. designed the simulation for decoy-state BB84. Z.-Q.Y. and H.L. wrote the paper.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-021-00428-9.

Correspondence and requests for materials should be addressed to Z.-Q.Y.

Reprints and permission information is available at http://www.nature.com/reprints

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