- -

Concise security bounds for practical decoy-state quantum key distribution

- -

Lim, Ci Wen; Curty, Marcos; Walenta, Nino; Xu, Feihu; Zbinden, Hugo

Concise security bounds for practical decoy-state quantum key distribution

Charles Ci Wen Lim,[1,*] Marcos Curty,[2] Nino Walenta,[1] Feihu Xu,[3] and Hugo Zbinden[1]

[1]*Group of Applied Physics, University of Geneva, Switzerland*

[2]*EI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Spain*

[3]*Center for Quantum Information and Quantum Control, Department of Physics and Department of Electrical & Computer Engineering, University of Toronto, Canada*

Due to its ability to tolerate high channel loss, decoy-state quantum key distribution (QKD) has been one of the main focuses within the QKD community. Notably, several experimental groups have demonstrated that it is secure and feasible under real-world conditions. Crucially, however, the security and feasibility claims made by most of these experiments were obtained under the assumption that the eavesdropper is restricted to particular types of attacks or that the finite-key effects are neglected. Unfortunately, such assumptions are not possible to guarantee in practice. In this work, we provide concise and tight finite-key security bounds for practical decoy-state QKD that are valid against general attacks.

I. INTRODUCTION

In 1984, Bennett and Brassard proposed a quantum key distribution (QKD) scheme in which a cryptographic key can be securely distributed between two remote parties, Alice and Bob, in an untrusted environment [1]. Since then, this proposal (traditionally referred to as the BB84 protocol) has received considerable attention, and significant progress has been made in both theory and practice [2].

In actuality, implementations of the BB84 protocol differ in some important aspects from the original theoretical proposal. This is particularly the case in the choice of the quantum information carrier, where a weak pulsed laser source is used in place of an ideal single-photon source (which is not yet available). However, pulsed laser sources have a critical drawback in that a non-negligible fraction of the emitted laser pulses contain more than one photon—which an adversary, Eve, can exploit via the so-called photon-number-splitting (PNS) attack [3]. In fact, this attack has been shown to be extremely powerful, especially when the loss in the quantum channel connecting Alice and Bob is high.

To tackle the PNS attack in the presence of high channel loss, most BB84 implementations (e.g., see Refs. [4–14]) adopt the decoy-state method [15–17]. The basic idea is conceptually very simple, and more importantly, it requires minimal modification to existing BB84 implementations. Specifically, instead of preparing phase-randomized laser pulses of the same mean photon-number, Alice varies randomly and independently the mean photon number of each laser pulse she sends to Bob. Crucially, by using the fact that the variation of the mean photon number is inaccessible to Eve, it is possible to detect the presence of photon-number-dependent loss in the quantum channel, i.e., by analyzing the data shared between Alice and Bob. As a result, photon-number-dependent type of attacks are circumvented, and the secret key rates and the tolerance to the channel loss are significantly improved.

The security of decoy-state QKD has been obtained in the asymptotic regime [16,17], i.e., in the limit of infinitely long keys. In the case of finite-length keys, several attempts have

been made (e.g., see Refs. [18–23]), but most (if not all) of these results assume that Eve is restricted to particular types of attacks. Very recently, finite-key security bounds against general attacks have been derived by Hayashi and Nakayama [24], although the security analysis is rather involved.

In this work, we provide concise and tight finite-key security bounds for a practical decoy-state QKD protocol that are directly applicable to most current decoy-state QKD implementations. The security analysis is based on a combination of a recent security proof technique [25,26] and a finite-size analysis for the decoy-state method, which allows us to greatly simplify the security analysis. As a result, we are able to derive tight finite-key security bounds that are valid against general attacks. Moreover, these bounds can be straightforwardly computed with just five concise formulas [see Eqs. (1)–(5)], which experimentalists can readily use for their implementations. In addition, we evaluate the performance of our security bounds by applying them to a realistic fiber-based system model. The evaluation shows that our security bounds are relatively tight, in the sense that for realistic postprocessing block sizes, the achievable secret key rates are comparable to those obtained in the asymptotic regime. In fact, for small postprocessing block sizes (of the order of 10^4 bits), we observe that secret keys can be securely distributed over a fiber length of up to 135 km.

II. PROTOCOL DESCRIPTION

We consider an asymmetric coding BB84 protocol [27], i.e., the bases X and Z are chosen with probabilities that are biased. Specifically, the bases X and Z are selected with probabilities q_x and $1 - q_x$, respectively, and the secret key is extracted from the events whereby Alice and Bob both choose the X basis. In addition, the protocol is based on the transmission of phase-randomized laser pulses, and uses two-decoy settings. The intensity of each laser pulse is randomly set to one of the three intensities μ_1, μ_2, and μ_3, and the intensities satisfy $\mu_1 > \mu_2 + \mu_3$ and $\mu_2 > \mu_3 \geqslant 0$. Note, however, that our analysis can also be straightforwardly generalized to any number of intensity levels. Next, we provide a detailed description of the protocol.

1. Preparation. Alice chooses a bit value uniformly at random and records the value in y_i. Then, she selects a basis choice

*Corresponding author: charles.lim.geneva@gmail.com

$a_i \in \{X, Z\}$ with probabilities q_X and $1 - q_X$, respectively, and an intensity choice $k_i \in \mathcal{K} := \{\mu_1, \mu_2, \mu_3\}$ with probabilities p_{μ_1}, p_{μ_2}, and $p_{\mu_3} = 1 - p_{\mu_1} - p_{\mu_2}$, respectively. Finally, she prepares a (weak) laser pulse based on the chosen values and sends it to Bob via the quantum channel.

2. Measurement. Bob chooses a basis $b_i \in \{X, Z\}$ with probabilities q_X and $1 - q_X$, respectively. Then, he performs a measurement in basis b_i and records the outcome in y_i'. In practice, the measurement device is usually implemented with two single-photon detectors. In this case, there are four possible outcomes $\{0, 1, \emptyset, \perp\}$ where 0 and 1 are the bit values, and $\emptyset$ and $\perp$ are the no detection and double detection events, respectively. For the first three outcomes, Bob assigns what he observes to y_i', and for the last outcome $\perp$ he assigns a random bit value to y_i'.

3. Basis reconciliation. Alice and Bob announce their basis and intensity choices over an authenticated public channel and identify the following sets: $\mathcal{X}_k := \{i : a_i = b_i = X \wedge k_i = k \wedge y_i' \neq \emptyset\}$ and $\mathcal{Z}_k := \{i : a_i = b_i = Z \wedge k_i = k \wedge y_i' \neq \emptyset\}$ for all $k \in \mathcal{K}$. Then, they check for $|\mathcal{X}_k| \geqslant n_{X,k}$ and $|\mathcal{Z}_k| \geqslant n_{Z,k}$ for all values of k. They repeat steps 1–3 until these conditions are satisfied. We denote as N the number of laser pulses sent by Alice until the conditions are fulfilled.

4. Generation of raw key and error estimation. First, a raw key pair $(\mathbf{X}_A, \mathbf{X}_B)$ is generated by choosing a random sample of size $n_X = \sum_{k \in \mathcal{K}} n_{X,k}$ of $\mathcal{X} = \cup_{k \in \mathcal{K}} \mathcal{X}_k$, where n_X is the postprocessing block size. Note that we use all intensity levels for the key generation, while existing decoy-state QKD protocols typically use only one intensity level. Second, they announce the sets $\mathcal{Z}_k$ and compute the corresponding number of bit errors, $m_{Z,k}$. Third, they calculate the number of vacuum events $s_{X,0}$ [Eq. (2)] and the number of single-photon events $s_{X,1}$ [Eq. (3)] in $(\mathbf{X}_A, \mathbf{X}_B)$. Also, they calculate the number of *phase errors* $c_{X,1}$ [Eq. (5)] in the single-photon events. Finally, they check that the phase error rate ϕ_X is less than ϕ_{tol} where ϕ_{tol} is a predetermined phase error rate, $\phi_X := c_{X,1}/s_{X,1} < \phi_{tol}$. If this condition is not met, they abort the protocol, otherwise they proceed to step 5.

5. Postprocessing. First, Alice and Bob perform an error-correction step that reveals at most λ_{EC} bits of information. In this step, we assume that they try to correct for an error rate that is predetermined. Next, to ensure that they share a pair of identical keys, they perform an error-verification step using two-universal hash functions that publishes $\lceil \log_2 1/\varepsilon_{hash} \rceil$ bits of information [28]. Here, ε_{hash} is the probability that a pair of nonidentical keys passes the error-verification step. Finally, conditioned on passing this last step, they perform privacy amplification on their keys to extract a secret key pair $(\mathbf{S}_A, \mathbf{S}_B)$ where $|\mathbf{S}_A| = |\mathbf{S}_B| = \ell$ bits.

III. SECURITY BOUNDS

Before we state the security bounds for our protocol, it is instructive to spell out the security criteria that we are using. For some small protocol errors, $\varepsilon_{cor}, \varepsilon_{sec} > 0$, we say that our protocol is $\varepsilon_{cor} + \varepsilon_{sec}$ secure if it is ε_{cor} correct and ε_{sec} secret. The former is satisfied if $\Pr[\mathbf{S}_A \neq \mathbf{S}_B] \leqslant \varepsilon_{cor}$, i.e., the secret keys are identical except with a small probability ε_{cor}. The latter is satisfied if $(1 - p_{abort}) \|\rho_{AE} - U_A \otimes \rho_E\|_1/2 \leqslant \varepsilon_{sec}$

where ρ_{AE} is the classical-quantum state describing the joint state of $\mathbf{S}_A$ and $\mathbf{E}$, U_A is the uniform mixture of all possible values of $\mathbf{S}_A$, and p_{abort} is the probability that the protocol aborts. Importantly, this secrecy criterion guarantees that the protocol is universally composable: the pair of secret keys can be safely used in any cryptographic task, e.g., for encrypting messages, that requires a perfectly secure key [29].

In the following, we present only the necessary formulas to compute the security bounds; the full security analysis is deferred to Appendixes A and B.

The correctness of the protocol is guaranteed by the error-verification step. This step ensures that Bob's corrected key is identical to Alice's key with probability at least $1 - \varepsilon_{hash}$, which implies that the final secret keys $(\mathbf{S}_A, \mathbf{S}_B)$ are identical with probability at least $1 - \varepsilon_{hash}$. Therefore, the correctness of the protocol is $\varepsilon_{cor} = \varepsilon_{hash}$.

Conditioned on passing the checks in the error-estimation and error-verification steps, a ε_{sec}-secret key of length

$$\ell = \left\lfloor s_{X,0} + s_{X,1} - s_{X,1} h(\phi_X) \right. $$
$$\left. - \lambda_{EC} - 6 \log_2 \frac{21}{\varepsilon_{sec}} - \log_2 \frac{2}{\varepsilon_{cor}} \right\rfloor \quad (1)$$

can be extracted, where $h(x) := -x \log_2 x - (1 - x) \log_2(1 - x)$ is the binary entropy function. Recall that $s_{X,0}$, $s_{X,1}$, and $\phi_X = c_{X,1}/s_{X,1}$ are the number of vacuum events, the number of single-photon events, and the phase error rate associated with the single-photons events in $\mathbf{X}_A$, respectively. Next, we show how to calculate them in two steps.

First, we extend the decoy-state analysis proposed in Ref. [30] to the case of finite sample sizes. Accordingly, the number of vacuum events in $\mathbf{X}_A$ satisfies

$$s_{X,0} \geqslant \tau_0 \frac{\mu_2 n_{X,\mu_3}^- - \mu_3 n_{X,\mu_2}^+}{\mu_2 - \mu_3}, \quad (2)$$

where $\tau_n := \sum_{k \in \mathcal{K}} e^{-k} k^n p_k/n!$ is the probability that Alice sends a n-photon state, and

$$n_{X,k}^\pm := \frac{e^k}{p_k} \left[n_{X,k} \pm \sqrt{\frac{n_X}{2} \ln \frac{21}{\varepsilon_{sec}}} \right], \quad \forall k \in \mathcal{K}.$$

The number of single-photon events in $\mathbf{X}_A$ is

$$s_{X,1} \geqslant \frac{\tau_1 \mu_1 \left[n_{X,\mu_2}^- - n_{X,\mu_3}^+ - \frac{\mu_2^2 - \mu_3^2}{\mu_1^2} \left(n_{X,\mu_1}^+ - \frac{s_{X,0}}{\tau_0} \right) \right]}{\mu_1(\mu_2 - \mu_3) - \mu_2^2 + \mu_3^2}. \quad (3)$$

We also calculate the number of vacuum events, $s_{Z,0}$, and the number of single-photon events, $s_{Z,1}$, for $\mathcal{Z} = \cup_{k \in \mathcal{K}} \mathcal{Z}_k$, i.e., by using Eqs. (2) and (3) with statistics from the basis Z. In addition, the number of bit errors $v_{Z,1}$ associated with the single-photon events in $\mathcal{Z}$ is also required. It is given by

$$v_{Z,1} \leqslant \tau_1 \frac{m_{Z,\mu_2}^+ - m_{Z,\mu_3}^-}{\mu_2 - \mu_3}, \quad (4)$$

where

$$m_{Z,k}^\pm := \frac{e^k}{p_k} \left[m_{Z,k} \pm \sqrt{\frac{m_Z}{2} \ln \frac{21}{\varepsilon_{sec}}} \right], \quad \forall k \in \mathcal{K},$$

and $m_Z = \sum_{k \in \mathcal{K}} m_{Z,k}$.

Second, the formula for the phase error rate of the single-photon events in $\mathbf{X}_A$ is [31]

$$\phi_{\mathsf{X}} := \frac{c_{\mathsf{X},1}}{s_{\mathsf{X},1}} \leqslant \frac{v_{\mathsf{Z},1}}{s_{\mathsf{Z},1}} + \gamma\left(\varepsilon_{\sec}, \frac{v_{\mathsf{Z},1}}{s_{\mathsf{Z},1}}, s_{\mathsf{Z},1}, s_{\mathsf{X},1}\right), \qquad (5)$$

where

$$\gamma(a,b,c,d) := \sqrt{\frac{(c+d)(1-b)b}{cd\log 2}\log_2\left(\frac{c+d}{cd(1-b)b}\frac{21^2}{a^2}\right)}.$$

IV. EVALUATION

We consider a fiber-based QKD system model that borrows parameters from recent decoy-state QKD and single-photon detector experiments. In particular, we assume that Alice can set the intensity of each laser pulse to one of the three predetermined intensity levels, μ_1, μ_2, and $\mu_3 = 2 \times 10^{-4}$ [32]. Bob uses an active measurement setup with two single-photon detectors (InGaAs APDs): they have a detection efficiency of $\eta_{\text{Bob}} = 10\%$, a dark count probability of $p_{\text{dc}} = 6 \times 10^{-7}$, and an after-pulse probability of $p_{\text{ap}} = 4 \times 10^{-2}$ [33]. The measurement has four possible outcomes $\{0, 1, \emptyset, \perp\}$ which correspond to bit values 0, 1, no detection, and double detection.

The system model is applied to two types of channel architectures, namely one that uses a dedicated optical fiber for the quantum channel and one that uses dense wavelength division multiplexing (DWDM) to put the quantum channel together with the classical channels into one optical fiber (e.g., see Refs. [34–36]). In both cases, we assume that the fibers have an attenuation coefficient of 0.2 dB/km. That is, their transmittance is $\eta_{\text{ch}} = 10^{-0.2L/10}$, where L (km) is the fiber length.

The considered channel architectures, however, do not have the same channel error model. For the dedicated fiber, the probability of having a bit error for intensity k is $e_k = p_{\text{dc}} + e_{\text{mis}}[1 - \exp(-\eta_{\text{ch}}k)] + p_{\text{ap}}D_k/2$, where e_{mis} is the error rate due to optical errors. Here, the expected detection rate (excluding after-pulse contributions) is $D_k = 1 - (1 - 2p_{\text{dc}})\exp(-\eta_{\text{sys}}k)$, where $\eta_{\text{sys}} = \eta_{\text{ch}}\eta_{\text{Bob}}$. The expected detection rate (including after-pulse contributions) is thus $R_k = D_k(1 + p_{\text{pa}})$. The channel error model for the DWDM architecture is more involved due to additional noise contributions from Raman scattering and cross talks between channels. We refer to Ref. [35] for details about it.

The parameter λ_{EC} is set to a simple function $f_{\text{EC}}h(e_{\text{obs}})$ where f_{EC} is the error-correction efficiency and e_{obs} is the average of the observed error rates in basis X (we note that very recently, a more accurate theoretical model of λ_{EC} has been derived in Ref. [37]). In practice, however, λ_{EC} should be set to the size of the information exchanged during the error-correction step. Regarding the secrecy, we set $\varepsilon_{\sec}$ to be proportional to the secret key length, that is, $\varepsilon_{\sec} = \kappa\ell$ where κ is a security constant; this security constant can be seen as the secrecy leakage per generated bit.

For the evaluation, we numerically optimize the secret key rate $R := \ell/N$ over the free parameters $\{q_{\mathsf{x}}, p_{\mu_1}, p_{\mu_2}, \mu_1, \mu_2\}$ given that the set $\{\kappa, \varepsilon_{\text{cor}}, e_{\text{mis}}, f_{\text{EC}}, L, n_{\mathsf{X}}\}$ is fixed. Specifically, we fix $\kappa = 10^{-15}$, $\varepsilon_{\text{cor}} = 10^{-15}$, $e_{\text{mis}} = 5 \times 10^{-3}$, and $f_{\text{EC}} = 1.16$, and generate curves (see Fig. 1) for a range of realistic
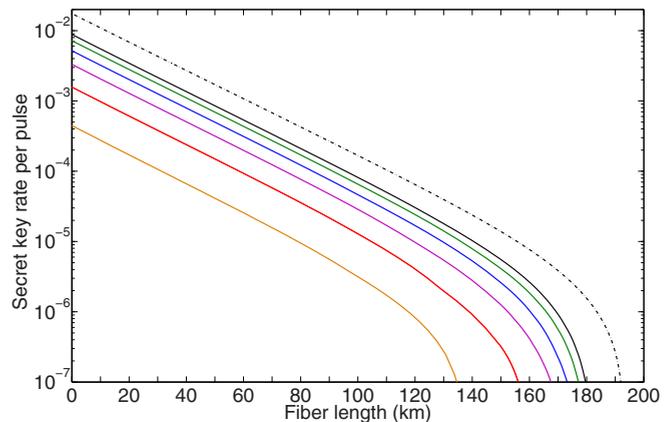

FIG. 1. (Color online) Secret key rate vs fiber length (dedicated fiber). Numerically optimized secret key rates (in logarithmic scale) are obtained for a fixed postprocessing block size $n_{\mathsf{X}} = 10^s$ with $s = 4, 5, \ldots, 9$ (from left to right). The dashed curve corresponds to the asymptotic secret key rate, i.e., in the limit of infinitely large keys; however, here we still assume that the number of intensity levels is 3. The number of laser pulses sent by Alice can be approximated with the secret key rate and the block size, i.e., $N \leqslant n_{\mathsf{X}}/R$.

postprocessing block sizes, i.e., $n_{\mathsf{X}} = 10^s$ with $s = 4, 5, \ldots, 9$. From Fig. 1, we see that the security performances corresponding to block sizes 10^7, 10^8, and 10^9 have only slight differences. For example, at a fiber length of 100 km, the secret key rate obtained with $n_{\mathsf{X}} = 10^9$ is about 1.75 times the one based on $n_{\mathsf{X}} = 10^7$. This suggests that it may not be necessary to go to large block sizes (where computational resources are high) to gain significant improvements. On the other hand, for block sizes 10^4, 10^5, and 10^6, there is a distinct advantage in terms of the secret key rate and fiber length for larger block sizes. This is expected since smaller block sizes correspond to larger statistical fluctuations in the estimation process. Interestingly, we see that even if we use a block size of 10^4, cryptographic keys can still be distributed over a fiber length of 135 km. The same trend is observed for the DWMD channel architecture (see Fig. 2).

V. CONCLUDING REMARKS

Although our security bounds are rather general and can be applied to a wide class of implementations, some assumptions are still needed. In particular, we require that the probability of having a detection in Bob's measurement device is independent of his basis choice. This assumption is normally satisfied when the detectors are operating according to specification. However, if the detectors are not implemented correctly, then there may be serious security consequences, e.g., see Ref. [39]; see also Ref. [40] for the corresponding countermeasures. Alternatively, one can adopt the recently proposed measurement-device-independent QKD (mdiQKD) [41] to remove all detector side channels. We note, however, that the implementation of mdiQKD is more complex than the one of decoy-state QKD, and the achievable finite-key secret key rates are typically lower [42].

In summary, we have provided tight finite-key security bounds for a practical decoy-state QKD protocol that can be
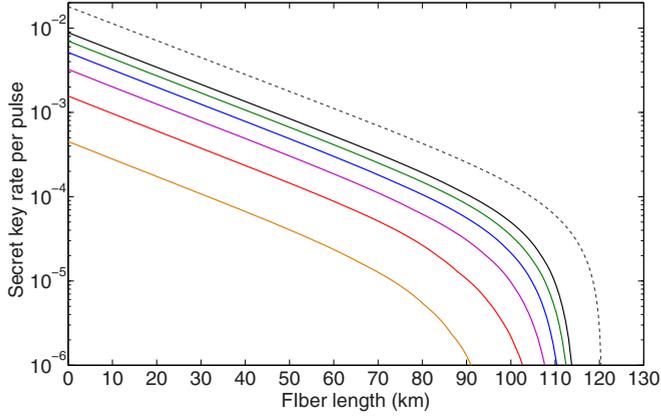
FIG. 2. (Color online) Secret key rate vs fiber length (DWDM). We consider a (4+1) DWDM channel architecture [35] that puts four classical channels and one quantum channel into an optical fiber. In the simulation, we take that each classical channel has a power of −34 dBm at the receiver [38]. Numerically optimized secret key rates (in logarithmic scale) are obtained for a fixed postprocessing block size $n_X = 10^s$ with $s = 4, 5, \ldots, 9$ (from left to right). The dashed curve corresponds to the asymptotic secret key rate, i.e., in the limit of infinitely long keys.

applied to existing QKD implementations. More importantly, these bounds are secure against general attacks, and can be easily computed by referring to just five concise formulas, i.e., Eqs. (1)–(5). On the application side, we also see that secret keys can be securely distributed over large distances with rather small postprocessing block sizes. Accordingly, this allows existing QKD implementations to speed up their key-distillation processes.

ACKNOWLEDGMENTS

APPENDIX A: DECOY-STATE ANALYSIS

Here, we provide the details for the security bounds presented in the main text. The security analysis is a combination of a proof technique based on entropic uncertainty relations [26] and a finite-size analysis for the two-decoy-state method. In the following, we first present the details for the decoy-state analysis.

Recall that our two-decoy-state method consists in Alice setting the intensity of each laser pulse to one of the three intensity levels, μ_1, μ_2, and μ_3, where $\mu_1 > \mu_2 + \mu_3$ and $\mu_2 > \mu_3 \geqslant 0$. Crucially, from the perspective of the eavesdropper, the final prepared state (i.e., with the encoded bit value) appears the same to her regardless of the choice of intensity level (or equivalently, the average photon number). Therefore, one can imagine an equivalent *counterfactual*

protocol: one in which Alice has the ability to send n-photon states, and she only decides on the choice of the average photon number after Bob has a detection. In the following, we provide the analysis for the X basis; the same analysis applies to the Z basis.

Consider the case whereby Alice encodes the states in the X basis and let $s_{X,n}$ be the number of detections observed by Bob given that Alice sent n-photon states. Note that $\sum_{n=0}^{\infty} s_{X,n} = n_X$ is the total number of detections given that Alice sent states prepared in the X basis. In the asymptotic limit, we expect $n_{X,k}$ events from n_X events to be assigned to the intensity k, that is,

$$n_{X,k} \to n^*_{X,k} = \sum_{n=0}^{\infty} p_{k|n} s_{X,n}, \quad \forall k \in \mathcal{K} = \{\mu_1, \mu_2, \mu_3\},$$

where $p_{k|n}$ is the conditional probability of choosing the intensity k given that Alice prepared a n-photon state. For finite sample sizes, using Hoeffding's inequality for independent events [43], we have that $n_{X,k}$ satisfies

$$|n^*_{X,k} - n_{X,k}| \leqslant \delta(n_X, \varepsilon_1), \tag{A1}$$

with probability at least $1 - 2\varepsilon_1$, where $\delta(n_X, \varepsilon_1) := \sqrt{n_X/2\ln(1/\varepsilon_1)}$. Note that the deviation term $\delta(n_X, \varepsilon_1)$ is the same for all values of k. Basically, Eq. (A1) allows us to establish a relation between the asymptotic values and the observed statistics (i.e., n_{X,μ_1}, n_{X,μ_2}, and n_{X,μ_3}). Moreover, the same relation can also be made for the expected number of errors and the observed number of errors. Let $v_{X,n}$ be the number of errors associated with $s_{X,n}$, then in the asymptotic limit, we expect $m_{X,k}$ errors from m_X errors to be assigned to the intensity k, i.e.,

$$m_{X,k} \to m^*_{X,k} = \sum_{n=0}^{\infty} p_{k|n} v_{X,n}, \quad \forall k \in \mathcal{K} = \{\mu_1, \mu_2, \mu_3\}.$$

Using Hoeffding's inequality [43], we thus have for all values of k,

$$|m^*_{X,k} - m_{X,k}| \leqslant \delta(m_X, \varepsilon_2), \tag{A2}$$

which holds with probability at least $1 - 2\varepsilon_2$.

For the moment, we keep these relations aside; they will be needed later when we apply the decoy-state analysis (to be detailed below) to the observed statistics.

1. Lower-bound on the number of vacuum events

An analytical lower-bound on $s_{X,0}$ can be established by exploiting the *structure* of the conditional probabilities $p_{k|n}$. First of all, we note that with Bayes' rule, for all k, we have

$$p_{k|n} = \frac{p_k}{\tau_n} p_{n|k} = \frac{p_k}{\tau_n} \frac{e^{-k} k^n}{n!}, \tag{A3}$$

where $\tau_n := \sum_{k \in \mathcal{K}} p_k e^{-k} k^n / n!$ is the probability that Alice prepares a n-photon state. Using this and following an approach proposed by [30], we have that

$$\frac{\mu_2 e^{\mu_3} n^*_{X,\mu_3}}{p_{\mu_3}} - \frac{\mu_3 e^{\mu_2} n^*_{X,\mu_2}}{p_{\mu_2}}$$

$$= \frac{(\mu_2 - \mu_3) s_{X,0}}{\tau_0} - \mu_2 \mu_3 \sum_{n=2}^{\infty} \frac{(\mu_2^{n-1} - \mu_3^{n-1}) s_{X,n}}{n! \tau_n},$$

where the second term on the right-hand side is non-negative for $\mu_2 > \mu_3$. Rewriting the above expression for $s_{\mathsf{X},0}$ gives

$$s_{\mathsf{X},0} \geqslant \frac{\tau_0}{(\mu_2 - \mu_3)} \left(\frac{\mu_2 e^{\mu_3} n^*_{\mathsf{X},\mu_3}}{p_{\mu_3}} - \frac{\mu_3 e^{\mu_2} n^*_{\mathsf{X},\mu_2}}{p_{\mu_2}} \right). \quad \text{(A4)}$$

Note that this lower bound is tight when $\mu_3 \to 0$.

2. Lower bound on the number of single-photon events

The lower bound for the number of single-photon events is slightly more involved, but it can be demonstrated in three concise steps.

First, note that

$$\frac{e^{\mu_2} n^*_{\mathsf{X},\mu_2}}{p_{\mu_2}} - \frac{e^{\mu_3} n^*_{\mathsf{X},\mu_3}}{p_{\mu_3}}$$

$$= \frac{(\mu_2 - \mu_3)s_{\mathsf{X},1}}{\tau_1} + \sum_{n=2}^{\infty} \frac{(\mu_2^n - \mu_3^n)s_{\mathsf{X},n}}{n!\tau_n}$$

$$\leqslant \frac{(\mu_2 - \mu_3)s_{\mathsf{X},1}}{\tau_1} + \frac{\mu_2^2 - \mu_3^2}{\mu_1^2} \sum_{n=2}^{\infty} \frac{\mu_1^n s_{\mathsf{X},n}}{n!\tau_n},$$

where the inequality is due to

$$\mu_2^n - \mu_3^n = \frac{(\mu_2^2 - \mu_3^2)}{(\mu_2 + \mu_3)} \sum_{i=0}^{n-1} \mu_2^{n-i-1} \mu_3^i$$

$$\leqslant (\mu_2^2 - \mu_3^2)(\mu_2 + \mu_3)^{n-2} \leqslant (\mu_2^2 - \mu_3^2)\mu_1^{n-2},$$

for $n \geqslant 2$ and $\mu_2 + \mu_3 \leqslant \mu_1$. Note that we used $\sum_{i=0}^{n-1} \mu_2^{n-i-1} \mu_3^i \leqslant (\mu_2 + \mu_3)^{n-1}$ for $n \geqslant 2$.

Second, using the fact that the sum of multiphoton events is given by

$$\sum_{n=2}^{\infty} \frac{\mu_1^n s_{\mathsf{X},n}}{n!\tau_n} = \frac{e^{\mu_1} n^*_{\mathsf{X},\mu_1}}{p_{\mu_1}} - \frac{s_{\mathsf{X},0}}{\tau_0} - \frac{\mu_1 s_{\mathsf{X},1}}{\tau_1},$$

we further get

$$\frac{e^{\mu_2} n^*_{\mathsf{X},\mu_2}}{p_{\mu_2}} - \frac{e^{\mu_3} n^*_{\mathsf{X},\mu_3}}{p_{\mu_3}} \leqslant \frac{(\mu_2 - \mu_3)s_{\mathsf{X},1}}{\tau_1}$$

$$+ \frac{\mu_2^2 - \mu_3^2}{\mu_1^2} \left(\frac{e^{\mu_1} n^*_{\mathsf{X},\mu_1}}{p_{\mu_1}} - \frac{s_{\mathsf{X},0}}{\tau_0} - \frac{\mu_1 s_{\mathsf{X},1}}{\tau_1} \right).$$

Finally, solving for $s_{\mathsf{X},1}$ gives

$$s_{\mathsf{X},1} \geqslant \frac{\mu_1 \tau_1}{\mu_1(\mu_2 - \mu_3) - (\mu_2^2 - \mu_3^2)} \left[\frac{e^{\mu_2} n^*_{\mathsf{X},\mu_2}}{p_{\mu_2}} \right.$$

$$\left. - \frac{e^{\mu_3} n^*_{\mathsf{X},\mu_3}}{p_{\mu_3}} + \frac{\mu_2^2 - \mu_3^2}{\mu_1^2} \left(\frac{s_{\mathsf{X},0}}{\tau_0} - \frac{e^{\mu_1} n^*_{\mathsf{X},\mu_1}}{p_{\mu_1}} \right) \right]. \quad \text{(A5)}$$

3. Upper bound on the number of single-photon errors

An upperbound on the number of single-photon errors can be obtained with just m^*_{X,μ_2} and m^*_{X,μ_3}; i.e., by taking $e^{\mu_2} m^*_{\mathsf{X},\mu_2}/p_{\mu_2} - e^{\mu_3} m^*_{\mathsf{X},\mu_3}/p_{\mu_3}$, it is easy to show that

$$v_{\mathsf{X},1} \leqslant \frac{\tau_1}{\mu_2 - \mu_3} \left(\frac{e^{\mu_2} m^*_{\mathsf{X},\mu_2}}{p_{\mu_2}} - \frac{e^{\mu_3} m^*_{\mathsf{X},\mu_3}}{p_{\mu_3}} \right). \quad \text{(A6)}$$

4. Finite-size decoy-state analysis

The bounds given above are still not applicable to the observed statistics since Eqs. (A4)–(A6) involve terms that are valid only in the asymptotic limit, i.e., $\{n^*_{\mathsf{X},k}\}_{k\in\mathcal{K}}$ and $\{m^*_{\mathsf{X},k}\}_{k\in\mathcal{K}}$. However, this is easily resolved by using Eqs. (A1) and (A2). Specifically, let

$$n^*_{\mathsf{X},k} \leqslant n_{\mathsf{X},k} + \delta(n_{\mathsf{X}}, \varepsilon_1) =: \tilde{n}^+_{\mathsf{X},k}, \quad \text{(A7)}$$

$$n^*_{\mathsf{X},k} \geqslant n_{\mathsf{X},k} - \delta(n_{\mathsf{X}}, \varepsilon_1) =: \tilde{n}^-_{\mathsf{X},k}, \quad \text{(A8)}$$

and

$$m^*_{\mathsf{X},k} \leqslant m_{\mathsf{X},k} + \delta(m_{\mathsf{X}}, \varepsilon_2) =: \tilde{m}^+_{\mathsf{X},k}, \quad \text{(A9)}$$

$$m^*_{\mathsf{X},k} \geqslant m_{\mathsf{X},k} - \delta(m_{\mathsf{X}}, \varepsilon_2) =: \tilde{m}^-_{\mathsf{X},k} \quad \text{(A10)}$$

for all values of k. Putting them into Eqs. (A4)–(A6), we thus have the formulas as stated in the main text.

APPENDIX B: SECRECY ANALYSIS

The secrecy analysis roughly follows along the lines of Ref. [26], i.e., we use a certain family of entropic uncertainty relations to establish bounds on the smooth min-entropy of the raw key conditioned on Eve's information.

To start with, let system $\mathbf{E}'$ be the information that Eve gathers on $\mathbf{X}_A$, i.e., the raw key of Alice, up to the error-verification step. By applying privacy amplification with two-universal hashing [29], a ε_{sec}-secret key of length ℓ can be extracted from $\mathbf{X}_A$. Specifically, the secret key is ε_{sec} secret if ℓ is chosen such that

$$\ell = \left\lfloor H^\nu_{\min}(\mathbf{X}_A|\mathbf{E}') - 2\log_2 \frac{1}{2\bar{\nu}} \right\rfloor, \quad \text{(B1)}$$

for $\nu + \bar{\nu} \leqslant \varepsilon_{\text{sec}}$ where $\nu, \bar{\nu}$ are chosen to be proportional to $\varepsilon_{\text{sec}}/(1 - p_{\text{abort}})$. Here, $H^\nu_{\min}(\mathbf{X}_A|\mathbf{E}')$ is the conditional smooth min-entropy, which quantifies the amount of uncertainty system $\mathbf{E}'$ has on $\mathbf{X}_A$. In fact, this quantity is the heart of our security analysis. In the following, we show how to bound $H^\nu_{\min}(\mathbf{X}_A|\mathbf{E}')$ using statistics obtained in the protocol.

First, using a chain-rule inequality for smooth entropies, and the fact that λ_{EC} bits and $\log_2 2/\varepsilon_{\text{cor}}$ bits of information were published during the error-correction and error-verification steps, respectively, we get $H^\nu_{\min}(\mathbf{X}_A|\mathbf{E}') \geqslant H^\nu_{\min}(\mathbf{X}_A|\mathbf{E}) - \lambda_{\text{EC}} - \log_2 2/\varepsilon_{\text{cor}}$, where system $\mathbf{E}$ is the remaining (possibly quantum) information Eve has on $\mathbf{X}_A$. In general, λ_{EC} should be determined by the amount of leakage the actual protocol reveals during the error-correction step.

Second, we decompose $\mathbf{X}_A$ into $\mathbf{X}_A^{\text{v}} \mathbf{X}_A^{\text{s}} \mathbf{X}_A^{\text{m}}$, which are the corresponding bit strings due to the vacuum, single-photon, and multiphoton events. Note that this decomposition is known to Eve, i.e., the decomposition information is included inside system $\mathbf{E}$. By using a generalized chain-rule result from Ref. [44], we have that

$$H^\nu_{\min}(\mathbf{X}_A|\mathbf{E}) \geqslant H^{\alpha_1}_{\min}(\mathbf{X}_A^{\text{s}}|\mathbf{X}_A^{\text{v}} \mathbf{X}_A^{\text{m}} \mathbf{E})$$

$$+ H^{\alpha_3 + 2\alpha_4 + \alpha_5}_{\min}(\mathbf{X}_A^{\text{v}} \mathbf{X}_A^{\text{m}}|\mathbf{E}) - 2\log_2 \frac{1}{\alpha_2} - 1,$$

for $\nu = 2\alpha_1 + \alpha_2 + (\alpha_3 + 2\alpha_4 + \alpha_5)$ where $\alpha_i > 0$ for all i. Next, we use the same chain rule again on the second term on the right-hand side to get

$$H_{\min}^{\alpha_3 + 2\alpha_4 + \alpha_5}\left(\mathbf{X}_A^v \mathbf{X}_A^m | \mathbf{E}\right)$$

$$\geqslant H_{\min}^{\alpha_4}\left(\mathbf{X}_A^m | \mathbf{X}_A^v \mathbf{E}\right) + H_{\min}^{\alpha_5}\left(\mathbf{X}_A^v | \mathbf{E}\right) - 2\log_2 \frac{1}{\alpha_3} - 1$$

$$\geqslant s_{X,0} - 2\log_2 \frac{1}{\alpha_3} - 1.$$

To get the second inequality, we used $H_{\min}^{\alpha_4}(\mathbf{X}_A^m | \mathbf{X}_A^v \mathbf{E}) \geqslant 0$ and $H_{\min}^{\alpha_5}(\mathbf{X}_A^v | \mathbf{E}) \geqslant H_{\min}(\mathbf{X}_A^v | \mathbf{E}) = H_{\min}(\mathbf{X}_A^v) = \log_2 2^{s_{X,0}} = s_{X,0}$. The former is given by the fact that all multiphoton events are taken to be insecure, i.e., due to the photon-number-splitting attack. The latter is based on the assumption that vacuum contributions contain zero information about the chosen bit values and the bits are uniformly distributed.

Third, we provide a bound on the remaining smooth min-entropy quantity which is now restricted to the single-photon events, i.e., via the uncertainty relation for smooth entropies [25]. Under the assumption that Alice prepares the states using mutually unbiased bases (i.e., X is the computational basis and Z is the Hadamard basis), we can further bound this quantity with the max-entropy between Alice and Bob, which is directly given by the amount of correlation between them [26]. More precisely, we have

$$H_{\min}^{\alpha_1}\left(\mathbf{X}_A^s | \mathbf{X}_A^v \mathbf{X}_A^m \mathbf{E}\right) \geqslant s_{X,1} - H_{\max}^{\alpha_1}\left(\mathbf{Z}_A^s | \mathbf{Z}_B^s\right)$$

$$\geqslant s_{X,1}\left[1 - h\left(\frac{c_{X,1}}{s_{X,1}}\right)\right],$$

where the first inequality is given by the uncertainty relation [25] and the smooth max-entropy $H_{\max}^{\alpha_1}(\mathbf{Z}_A^s | \mathbf{Z}_B^s)$ is a measure of correlations between $\mathbf{Z}_A^s$ and $\mathbf{Z}_B^s$. Here, $\mathbf{Z}_A^s$ and $\mathbf{Z}_B^s$ are

the bit strings Alice and Bob would have obtained if they had measured in the basis Z instead. The second inequality is achieved by using $H_{\max}^{\alpha_1}(\mathbf{Z}_A^s | \mathbf{Z}_B^s) \leqslant s_{X,1} h(c_{X,1}/s_{X,1})$ (see [26, Lemma 3]), where $c_{X,1}$ is the number of phase errors in the single-photon events. Here, the number of phase errors $c_{X,1}$ has to be estimated via a random-sampling theory (without replacement) as these errors are not directly observed in the protocol. More concretely, by using a random sampling without replacement result given in Ref. [31] which is based on an approximation technique for the hypergeometric distribution, we have with probability at least $1 - \alpha_1$,

$$\frac{c_{X,1}}{s_{X,1}} \leqslant \frac{v_{Z,1}}{s_{Z,1}} + \gamma\left(\alpha_1, \frac{v_{Z,1}}{s_{Z,1}}, s_{Z,1}, s_{X,1}\right), \qquad (B2)$$

where

$$\gamma(a,b,c,d) := \sqrt{\frac{(c+d)(1-b)b}{cd\log 2} \log_2\left(\frac{c+d}{cd(1-b)b} \frac{1}{a^2}\right)}.$$

Fourth, putting everything together, we arrive at a secret key length of

$$\ell = \left\lfloor s_{X,0} + s_{X,1}\left[1 - h\left(\frac{c_{X,1}}{s_{X,1}}\right)\right] - \lambda_{EC} - \log_2 \frac{2}{\varepsilon_{cor}\beta}\right\rfloor,$$
$$(B3)$$

where $\beta := (\alpha_2 \alpha_3 \bar{\nu})^2$. Note that $s_{X,0}$, $s_{X,1}$, $s_{Z,0}$, $s_{Z,1}$, $v_{Z,1}$ are to be bounded by Eqs. (A4)–(A6) using the relations given by Eqs. (A7)–(A10).

Finally, after composing the error terms due to finite-sample sizes and setting $\alpha_4 = \alpha_5 = 0$, the secrecy is

$$\varepsilon_{sec} = 2[2\alpha_1 + \alpha_2 + \alpha_3] + \bar{\nu} + 10\varepsilon_1 + 2\varepsilon_2. \qquad (B4)$$

To get the secrecy given in the main text we set each error term to a common value ε, thus $\varepsilon_{sec} = 21\varepsilon$.

---

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

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002); V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *ibid.* **81**, 1301 (2009).

[3] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995); G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[4] Y. Zhao, B. Qi, X. Ma, H. K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).

[5] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Phys. Rev. Lett. **98**, 010503 (2007).

[6] C. Z. Peng, J. Zhang, D. Yang, W. B. Gao, H. X. Ma, H. Yin, H. P. Zeng, T. Yang, X. B. Wang, and J. W. Pan, Phys. Rev. Lett. **98**, 010505 (2007).

[7] Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **90**, 011118 (2007).

[8] A. R. Dixon *et al.*, Opt. Express **16**, 18790 (2008).

[9] A. Tanaka *et al.*, Opt. Express **16**, 11354 (2008).

[10] D. Rosenberg *et al.*, New J. Phys. **11**, 045009 (2009).

[11] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **96**, 161102 (2010).

[12] Y. Liu *et al.*, Opt. Express **18**, 8587 (2010).

[13] M. Sasaki *et al.*, Opt. Express **19**, 10387 (2011).

[14] J. Y. Wang *et al.*, Nat. Photon. **7**, 387 (2013).

[15] W. Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[16] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[17] X. B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[18] M. Hayashi, Phys. Rev. A **76**, 012329 (2007); J. Hasegawa, M. Hayashi, T. Hiroshima, and A. Tomita, arXiv:0707.3541.

[19] R. Cai and V. Scarani, New J. Phys. **11**, 045024 (2009).

[20] T. T. Song, J. Zhang, S. J. Qin, and Q. Y. Wen, Quantum Inf. Comput. **11**, 374 (2011).

[21] R. D. Somma and R. J. Hughes, Phys. Rev. A **87**, 062330 (2013).

[22] Z. Wei, W. Wang, Z. Zhang, M. Gao, Z. Ma, and X. Ma, Sci. Rep. **3**, 2453 (2013).

[23] M. Lucamarini *et al.*, Opt. Express **21**, 24550 (2013).

[24] M. Hayashi and R. Nakayama, arXiv:1302.4139v4.

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

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

[27] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptol. **18**, 133 (2005).

[28] M. N. Wegman and J. L. Carter, J. Comput. Syst. Sci. **22**, 265 (1981).

[29] R. Renner, arXiv:quant-ph/0512258.

[30] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

[31] C. H. F. Fung, X. Ma, and H. F. Chau, Phys. Rev. A **81**, 012318 (2010).

[32] B. Fröhlich *et al.*, Nature (London) **501**, 69 (2013).

[33] N. Walenta *et al.*, J. Appl. Phys. **112**, 063106 (2012).

[34] N. A. Peters *et al.*, New J. Phys. **11**, 045012 (2009).

[35] P. Eraerds *et al.*, New J. Phys. **12**, 063027 (2010).

[36] K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, Phys. Rev. X **2**, 041010 (2012).

[37] M. Tomamichel, J. Martinez-Mateo, C. Pacher, and D. Elkouss, arXiv:1401.5194.

[38] We remark that −34 dBm is achievable with commercial devices, e.g., see OptiCin SFP-DWDM-15xx.xx-28. Note that in Ref. [35], they worked with a receiver sensitivity of −28 dBm.

[39] L. Lydersen *et al.*, Nat. Photon. **4**, 686 (2010).

[40] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Appl. Phys. Lett. **98**, 231104 (2011); M. Legré and G. Robordy, intl. patent. appl. WO 2012/046135 A2 (filed in 2010).

[41] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[42] M. Curty *et al.*, arXiv:1307.1081.

[43] W. Hoeffding, J. Amer. Stat. Assoc. **58**, 13 (1963).

[44] A. Vitanov, F. Dupuis, M. Tomamichel, and R. Renner, IEEE Trans. Inf. Theor. **59**, 2603 (2013).