



Optimizing the decoy-state BB84 QKD protocol parameters

Thomas Attema^{1,2,3} · Joost W. Bosman³ · Niels M. P. Neumann^{1,3} 

Received: 24 December 2020 / Accepted: 23 March 2021 / Published online: 24 April 2021
© The Author(s) 2021

Abstract

Quantum key distribution (QKD) protocols allow for information theoretically secure distribution of (classical) cryptographic key material. However, due to practical limitations the performance of QKD implementations is somewhat restricted. For this reason, it is crucial to find optimal protocol parameters, while guaranteeing information theoretic security. The performance of a QKD implementation is determined by the tightness of the underlying security analysis. In particular, the security analyses determines the *key-rate*, i.e., the amount of cryptographic key material that can be distributed per time unit. Nowadays, the security analyses of various QKD protocols are well understood. It is known that optimal protocol parameters, such as the number of decoy states and their intensities, can be found by solving a nonlinear optimization problem. The complexity of this optimization problem is typically handled by making a number of heuristic assumptions. For instance, the number of decoy states is restricted to only one or two, with one of the decoy intensities set to a fixed value, and vacuum states are ignored as they are assumed to contribute only marginally to the secure key-rate. These assumptions simplify the optimization problem and reduce the size of search space significantly. However, they also cause the security analysis to be non-tight, and thereby result in sub-optimal performance. In this work, we follow a more rigorous approach using both linear and nonlinear programs describing the optimization problem. Our approach, focusing on the decoy-state BB84 protocol, allows heuristic assumptions to be omitted, and therefore results in a tighter security analysis with better protocol parameters. We show an improved performance for the decoy-state BB84 QKD protocol, demonstrating that the heuristic assumptions typically made are too restrictive. Moreover, our improved optimization frameworks shows that the com-

✉ Niels M. P. Neumann
niels.neumann@tno.nl

Thomas Attema
thomas.attema@tno.nl

¹ CWI, Amsterdam, The Netherlands

² Mathematical Institute, Leiden University, Leiden, The Netherlands

³ TNO, Cyber Security and Robustness, The Hague, The Netherlands

plexity of the performance optimization problem can also be handled without making heuristic assumptions, even with limited computational resources available.

Keywords Quantum key distribution · BB84 · Key rates · Decoy states · Nonlinear optimization

1 Introduction

The goal of a key-distribution protocol is for two parties, Alice and Bob, to agree on a key $k \in \{0, 1\}^n$ over an insecure communication channel, such that even an adversary Eve with full control over this communication channel can only obtain a negligible amount of information about this key k . If Alice and Bob are capable of communicating quantum information, they are able to achieve information-theoretic or unconditional security, i.e., security against adversaries with unlimited computational power.

The use of quantum information to securely distribute symmetric cryptographic keys was first proposed in 1984 by Bennett and Brassard [1], and today most, if not all, quantum key distribution (QKD) protocols can be viewed as adaptations of their original BB84 protocol. Since then, much progress has been made and the first QKD systems are already commercially available. Thereby, QKD has become one of the first applications of quantum mechanics at an individual quanta level [2].

The information-theoretic security of the BB84 protocol against the most general attacks allowed by quantum mechanics was proven in 1996 by Mayers [3]. In general, however, Mayers' security notion does not imply that the derived key can securely be used in other cryptographic protocols [4] and a stronger notion of security following the universal composability framework is required [5]. Informally, universal security is proven by comparing the output of the protocol to the output of an ideal key-distribution protocol, i.e., a perfect key. If these two outputs are indistinguishable, the protocol is said to be universally secure. Fortunately, QKD protocols that satisfy Mayers' weaker notion of security were shown to be universally secure [4].

Practical implementations deviate from the theoretical BB84 protocol, which may render them insecure. As any realistic quantum channel introduces noise by imperfections in the source, channel and detector. These benign losses and errors are indistinguishable from the ones introduced by an adversary. For this reason, the conservative assumption is made that all losses and errors are caused by an adversary. Mayers' proof already considered noisy quantum channels, and shows that the BB84 protocol is information-theoretically secure as long as the noise level is below a certain threshold [3]. In contrast to the ideal BB84 protocol, practical implementations therefore require an error correction procedure. An elaborate review of practical quantum key distribution protocols is given in [6], including different adversary strategies for practical QKD protocol implementations.

One of these adversary strategies relates to the photon source. Some protocols, such as the original BB84 protocol, require information to be encoded in single photons. However, producing single photon pulses is hard in practice. Therefore, typically, the quantum information is encoded in weak laser pulses, where the number of photons in each of these laser pulses follows a Poisson distribution with an tunable mean

μ , called the intensity of the source. As a result, laser pulses can contain multiple photons, which can be exploited via the photon-number-splitting (PNS) attack [7,8]. For this reason we must assume that all key material derived from multi-photon pulses is compromised. Privacy amplification is applied to establish a secret key from such a partially compromised key.

In general, the performance of a QKD implementation can be quantified by the key-rate R , indicating the amount of secure key per sent pulse. For the BB84 protocol, this key-rate depends, apart from the noise and losses, also on the laser source intensity μ . By carefully choosing this tunable μ , the key-rate can be maximized. In fact, the protocol does not require the intensity to be fixed throughout the protocol. On the contrary, it has been shown to be beneficial to randomly vary the intensity μ between pulses, resulting in the so-called decoy-state BB84 protocol with higher achievable key-rates [9–11].

This work focuses on the security analysis of the decoy-state BB84 protocol and the optimization of its protocol parameters. The security analysis is based on the uncertainty relation for smooth entropies [12]. In [13], the uncertainty relation was applied to the analysis of the BB84 protocol implemented with a perfect single photon source. This analysis was extended to the decoy-state BB84 protocol in which weak pulsed laser sources with tunable intensities are applied [14]. The analysis of [14] restricts itself to the case where the intensities are randomly varied between three different levels. The intensities and sample distribution are chosen to optimize the key-rate that is achieved in a specific set-up. This approach can be generalized to arbitrary numbers of intensities resulting in a larger parameter search space over which the key-rate is optimized.

Our main contribution is the formulation of the key-rate optimization problem as linear and nonlinear programs. Analytical lower bounds on the number of multi-photon states can be found [14,15], as the number of photons is assumed to follow a Poisson distribution. Whereas in general these lower bounds are non-tight, the linear programs allow for tight lower bounds, which in turn results in an improved security analysis. Additionally, the linear programs are used to upper bound the number of single-photon errors. Constrained nonlinear optimization techniques [16] are then used to optimize the lower bound on the key-rate.

Due to the larger parameter search space, higher key-rates are found using linear programs, compared to analytical methods. For that reason, linear programs have been used before to optimize the key-rate for the BB84 protocol [17] and measurement-device independent QKD protocols [18]. Both works however still make assumptions, for instance by only including the first laser intensity instead of all or by fixing the probabilities for the bases and intensities.

We formalize the approach and do not make such assumptions. Furthermore, we improve the lower bounds found with the linear programs by including the vacuum and single photon pulses in a single linear program. This opposed to determining lower bounds for the two separately, resulting in conservative and sub-optimal estimates. We furthermore allow for freely varying each of the intensities.

We show that using this formal approach results in an improved obtainable secure key-rate. We furthermore show the effects of using more decoy states and the effects of increasing the number of sent pulses. First, we explain the BB84 protocol in Sect. 2 and

discuss the security and robustness of the protocol from a mathematical perspective in Sect. 3. The same mathematical perspective is used in Sect. 4 to explain how to obtain secure key-material from a BB84 protocol execution. This section also introduces finite key-effects. Afterwards, Sect. 5 explains how to optimize the secure key-rate and how to incorporate the used quantum channel in our model. Results of our model are presented in Sect. 6 and a conclusion is given in Sect. 7.

2 Decoy-state BB84 protocol

In this section, we recall the decoy-state BB84 QKD protocol. Alice and Bob are assumed to have access to a (noisy) quantum channel and an authenticated classical channel. Both channels are insecure and can be fully controlled by the adversary, however, active attacks on the classical channel are assumed to be immediately detected as this channel is authenticated.

In the following, all keys are denoted by an uppercase K and the superscripts refer to the party Alice a or Bob b and type of key: raw r , sifted s or error-corrected e . The decoy-state BB84 protocol now goes as follows.

Preparation: Alice generates a raw key by sampling a uniformly random bit string in $K^{ra} \in \{0, 1\}^N$. Moreover, Alice samples a random basis string $\mathcal{X}^a \in \{X, Z\}^N$, where $P(\mathcal{X}_i^a = X) = p_X$ for all $1 \leq i \leq N$. For all i she encodes bit K_i^{ra} in basis \mathcal{X}_i^a resulting in a sequence of qubits in $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}^N$.

Communication: For all $1 \leq i \leq N$, Alice samples an intensity U_i from a probability distribution $P_{U_i|\mathcal{X}_i^a}$ conditioned on the chosen basis $\mathcal{X}_i^a \in \{X, Z\}$. The distribution $P_{U_i|\mathcal{X}_i^a}$ is independent of the index i and for both bases its support lies in a finite set of intensities $\{\mu_0, \dots, \mu_m\}$. Alice encodes the associated qubit in a laser pulse with intensity U_i and sends this pulse to Bob over the quantum channel.

Measurement: Bob samples a random basis string $\mathcal{X}^b \in \{X, Z\}^N$, where $P(\mathcal{X}_i^b = X) = p_X$ for all $1 \leq i \leq N$ and measures pulse i in basis \mathcal{X}_i^b . If both of Bob's detectors register an event, for example in the case of a multi-photon pulse and a measurement incompatible with Alice's preparation, Bob randomly selects a measurement outcome $K_i^{rb} \in \{0, 1\}$. It can also occur that no detector registers an event, in this case Bob defines the outcome to be \emptyset . As a result Bob obtains his raw key $K^{rb} \in \{0, 1, \emptyset\}^N$. Note that Bob's sifting probability p_X^b is equal to that of Alice p_X^a , i.e., $p_X^a = p_X^b = p_X$. This is not required, but it can be shown that for all protocol instantiations with $p_X^a \neq p_X^b$, there exists a protocol instance with $p_X^a = p_X^b$ with at least the same secure key-rate.

Sifting: Alice and Bob announce their basis choices and Bob announces the pulses for which no detection event took place. The pulses that were prepared and measured in the same basis and for which a detection event occurred, are sifted from the raw keys K^{ra} and K^{rb} and Alice and Bob obtain sifted keys $K^{sa} \in \{0, 1\}^{n_s}$ and $K^{sb} \in \{0, 1\}^{n_s}$, respectively. In addition, we let $K_{\mathcal{X}}^{sa}, K_{\mathcal{X}}^{sb} \in \{0, 1\}^{n_{\mathcal{X}}}$ be the strings containing the bits of K^{sa} and K^{sb} obtained by preparing and measuring in the \mathcal{X} -basis for $\mathcal{X} \in \{X, Z\}$.

Parameter estimation: Alice announces the chosen intensities U , which allows Alice and Bob to compute the amount of detection events

$$n_{\mu_j, \mathcal{X}} = \left| \left\{ i : \mathcal{X}_i^a = \mathcal{X}_i^b = \mathcal{X} \wedge U_i = \mu_j \wedge K_i^{rb} \neq \emptyset \right\} \right|, \tag{1}$$

for all intensities μ_j and for both bases $\mathcal{X} \in \{X, Z\}$. In addition, Alice and Bob reveal the parts of the sifted keys $K_Z^{sa}, K_Z^{sb} \in \{0, 1\}^{n_Z}$. Using this information they can compute the amount of errors in the Z -basis

$$E_{\mu_j, Z} = \left| \left\{ i : \mathcal{X}_i^a = \mathcal{X}_i^b = Z \wedge U_i = \mu_j \wedge (K_Z^{sa})_i \neq (K_Z^{sb})_i \right\} \right|, \tag{2}$$

for all intensities μ_j . Given these values Alice and Bob determine upper-bounds on the number of bits in K_X^{sa} that are associated to multi-photon events and the error-rate $e_{1,Z}$ for single photon pulses in the Z -basis. From these bounds Alice and Bob determine the length ℓ of the secret key that can be extracted after the error reconciliation phase. If $\ell \leq 0$ the protocol aborts. Note that only the Z -events are used to determine ℓ . The X -events will be used in the error reconciliation and privacy amplification phase to construct the final key.

Error reconciliation: Errors in the quantum channel can cause the strings K_X^{sa} and K_X^{sb} to be distinct. For this reason Alice and Bob perform an information reconciliation protocol by which they obtain error-corrected keys $K^{ea}, K^{eb} \in \{0, 1\}^{n_X}$, respectively.

Verification: Alice samples a uniformly random hash function h from a two-universal family of hash functions $\mathcal{F}_e : \{0, 1\}^{n_X} \rightarrow \{0, 1\}^{\lceil -\log_2(\epsilon_{\text{cor}}) \rceil}$ [19]. Here $0 \leq 1 - \epsilon_{\text{cor}} \leq 1$ is a lower bound on the probability that the protocol is correct, i.e., that Alice and Bob will obtain identical keys. Alice applies this hash function to her error-corrected key K^{ea} . She sends the hash-function h and hash-value $h(K^{ea})$ to Bob, who then computes $h(K^{eb})$. If $h(K^{ea}) \neq h(K^{eb})$, the protocol aborts.

Privacy amplification: Alice samples a uniformly random hash function h from a two-universal family \mathcal{F}_p mapping $\{0, 1\}^{n_X}$ to $\{0, 1\}^\ell$ and announces h to Bob, where ℓ has been determined in the parameter estimation phase. Both Alice and Bob compute the secret keys $K^a = h(K^{ea})$ and $K^b = h(K^{eb})$, respectively.

3 Correctness and robustness

In this section, we recall two important (security) properties of QKD protocols. A QKD protocol should be correct and secure against any attack allowed by quantum mechanics. Moreover, the protocol should only abort with a small probability, i.e., it should be robust. In this section we formalize the correctness and robustness properties, following the approach of [20], and show why the decoy-state BB84 protocol admits these properties. The security of the protocol will be analyzed in Sect. 4.

A QKD protocol is ϵ_{cor} -correct if

$$P(K^a \neq K^b) \leq \epsilon_{\text{cor}}, \tag{3}$$

for all possible strategies of an adversary. This property is easily seen to be satisfied if in the verification phase \mathcal{F}_θ is indeed a family of two-universal hash functions mapping $\{0, 1\}^{n_X}$ to $\{0, 1\}^{\lceil -\log_2(\epsilon_{\text{cor}}) \rceil}$. The hash value reveals

$$\left\lceil \log_2 \left(\frac{1}{\epsilon_{\text{cor}}} \right) \right\rceil \leq \log_2 \left(\frac{2}{\epsilon_{\text{cor}}} \right) \tag{4}$$

bits of information to the adversary.

Note that the protocol is allowed to abort, in which case no secure key is exchanged. We denote this event by $K^a = K^b = \perp$. The probability p_{abort} that the protocol aborts in the absence of an adversary, depends on the error reconciliation protocol that is applied. For any security parameter $\delta_{\text{ec}} > 0$, there exist error reconciliation protocols that leak at most

$$n_X (h(e_X) + \delta_{\text{ec}}) \tag{5}$$

bits of information [20], where h is the binary entropy function and e_X is the quantum bit error rate (QBER) of the sifted keys in the X -basis. Moreover,

$$p_{\text{abort}} \leq \text{P} \left(K^{ea} \neq K^{eb} \right) \leq 2 \exp \left(\frac{-n_X \delta_{\text{ec}}^2}{3 \log_2(5)^2} \right), \tag{6}$$

where the last inequality follows from Corollary 6.3.5 of [20]. To achieve an abort probability of at most p_{abort} we therefore take

$$\delta_{\text{ec}}(p_{\text{abort}}, n_X) = \sqrt{\ln \left(\frac{2}{p_{\text{abort}}} \right) \frac{3 \log_2(5)^2}{n_X}}. \tag{7}$$

4 Security of the decoy-state BB84 protocol

In this section, we recall the standard (composable) security definitions for QKD protocols, specifically focusing on the Decoy-State BB84 protocol. In particular, we derive an expression for the length of a key that can securely be generated by running this QKD protocol (Sect. 4.1). This expression contains a number of variables that are unknown to Alice and Bob. In Sect. 4.2, we show how these unknown protocol variables can be bounded by solving certain linear programs.

4.1 Secure key length

To evaluate the security of the protocol let us consider the joint state of the classical random variable $K := K^a$ with support \mathcal{K} and the adversary’s quantum system

$$\rho_{KE} = \sum_{x \in \mathcal{K}} P(K = x) |x\rangle \langle x| \otimes \rho_E^x, \tag{8}$$

where ρ_E^x is the state of the adversary’s system given that $K = x$. Ideally, the classical probability distribution $P(K = x)$ is uniform and the adversary’s state is independent of K . Hence, the joint state of a perfect key and the adversary’s system is given by

$$\frac{1}{|\mathcal{K}|} \sum_{x \in \mathcal{K}} |x\rangle\langle x| \otimes \rho_E. \tag{9}$$

A QKD-protocol is now said to be ϵ_{sec} -secure if

$$\frac{1}{2} \left\| \rho_{KE} - \frac{1}{|\mathcal{K}|} \sum_{x \in \mathcal{K}} |x\rangle\langle x| \otimes \rho_E \right\|_1 \leq \epsilon_{\text{sec}}, \tag{10}$$

where $\|A\|_1 = \text{tr}(\sqrt{A^*A})$ is the trace norm of the complex matrix A .

If a QKD-protocol is ϵ_{sec} -secure the output cannot be distinguished from that of a perfect protocol with probability more than ϵ_{sec} [20]. Moreover, this security definition ensures universal composability, i.e., the key K can safely be used in other cryptographic protocols.

In general, Alice’s bit-string $K^{ea} \in \{0, 1\}^{n_X}$, obtained after the error correction and verification phase, does not satisfy the above security definition. For this reason privacy amplification is applied. From the leftover hash lemma [21] it follows that the QKD protocol is ϵ_{sec} -secure if there exists an $\epsilon \geq 0$ such that

$$\ell = \left\lceil H_{\min}^\epsilon(K^{ea}|E) - 2 \log_2 \left(\frac{1}{2(\epsilon_{\text{sec}} - \epsilon)} \right) \right\rceil, \tag{11}$$

where $H_{\min}^\epsilon(K^{ea}|E)$ is the smooth min-entropy of the random variable K^{ea} conditioned on the adversary’s (quantum) information E . The leftover hash lemma thus gives an expression of the bit-length ℓ of the secure key K in terms of this conditional smooth entropy.

The error corrected key is obtained from the sifted key after performing the error correction and verification phase, which both leak some information to the adversary. If we let E^s be the adversary’s (quantum) information after the sifting phase, it follows from Eqs. (4) and (5) that

$$H_{\min}^\epsilon(K^{ea}|E) \geq H_{\min}^\epsilon(K_X^{sa}|E^s) - n_X (h(E_X) + \delta_{\text{ec}}(p_{\text{abort}}, n_X)) - \log_2 \left(\frac{2}{\epsilon_{\text{cor}}} \right). \tag{12}$$

Now observe that the bits of K_X^{sa} are all derived from vacuum, single-photon or multi-photon pulses. Hence, we can write

$$K_X^{sa} = K_{0,X}^{sa} \otimes K_{1,X}^{sa} \otimes K_{m,X}^{sa}, \tag{13}$$

where $K_{0,X}^{sa}$, $K_{1,X}^{sa}$ and $K_{m,X}^{sa}$ contain the bits associated to the vacuum, single-photon and multi-photon pulses, respectively.

It is impossible for an adversary to obtain information about the bits associated to vacuum pulses, hence for all $\epsilon \geq 0$

$$H_{\min}^{\epsilon}(K_{0,X}^{sa}|E^s) \geq H_{\min}(K_{0,X}^{sa}|E^s) = n_{0,X}, \tag{14}$$

where $n_{0,X}$ is the number of vacuum pulses that were sent. In contrast, the PNS attack allows the adversary to obtain all information about the bits associated to multi-photon pulses. Hence, for all $\epsilon \geq 0$ we must lower bound the associated min-entropy as follows

$$H_{\min}^{\epsilon}(K_{m,X}^{sa}|K_{0,X}^{sa}E^s) \geq 0. \tag{15}$$

Applying the chain rule for smooth min-entropies [22] twice and plugging in Eqs. (14) and (15), we find that for all $\epsilon, \epsilon_1, \epsilon_4, \epsilon_5 \geq 0$ and $\epsilon_2, \epsilon_3 > 0$ such that $2\epsilon_1 + \epsilon_2 + \epsilon_3 + 2\epsilon_4 + \epsilon_5 = \epsilon \leq 1$,

$$\begin{aligned} H_{\min}^{\epsilon}(K_X^{sa}|E^s) &\geq H_{\min}^{\epsilon_5}(K_{0,X}^{sa}|E^s) + H_{\min}^{\epsilon_1}(K_{1,X}^{sa}|\tilde{E}) + H_{\min}^{\epsilon_4}(K_{m,X}^{sa}|K_{0,X}^{sa}E^s) \\ &\quad - \log_2\left(\frac{1}{1-\sqrt{1-\epsilon_2^2}}\right) - \log_2\left(\frac{1}{1-\sqrt{1-\epsilon_3^2}}\right) \\ &\geq n_{0,X} + H_{\min}^{\epsilon_1}(K_{1,X}^{sa}|\tilde{E}) \\ &\quad - \log_2\left(\frac{1}{1-\sqrt{1-\epsilon_2^2}}\right) - \log_2\left(\frac{1}{1-\sqrt{1-\epsilon_3^2}}\right) \\ &\geq n_{0,X} + H_{\min}^{\epsilon_1}(K_{1,X}^{sa}|\tilde{E}) - 2\log_2\left(\frac{2}{\epsilon_2\epsilon_3}\right), \end{aligned} \tag{16}$$

where $\tilde{E} = K_{0,X}^{sa} \otimes K_{m,X}^{sa} \otimes E^s$ and for the third inequality we use that for all $x \leq 1$ it holds that

$$1 - \sqrt{1-x} \geq \frac{x}{2}.$$

See also [14] in which the same lower bound is derived.

Hence, combining Eqs. (11), (12) and (16) gives an achievable secure key-rate in terms of the smooth min-entropy of the $n_{1,X}$ single-photon pulses in the X -basis conditioned on the quantum system \tilde{E} . For these pulses we have the following uncertainty relation [12],

$$H_{\min}^{\epsilon_1}(K_{1,X}^{sa}|\tilde{E}) \geq n_{1,X} - H_{\max}^{\epsilon_1}(L_{1,Z}^{sa}|L_{1,Z}^{sb}), \tag{17}$$

where $L_{1,Z}^{sa}$ and $L_{1,Z}^{sb}$ are the hypothetical sifted keys that would have been obtained if Alice and Bob would have prepared and measured the $K_{1,X}^{sa}$ -pulses in the Z -basis. Informally, this uncertainty relation states that either Eve is uncertain about Alice's key in the X -basis or Alice and Bob observe a high amount of errors in their Z -events.

Let $e_{1,Z}^L$ be the fraction of errors between $L_{1,Z}^{sa}$ and $L_{1,Z}^{sb}$ and let $e_{1,Z}$ be the fraction of errors between $K_{1,Z}^{sa}$ and $K_{1,Z}^{sb}$. The total fraction of single-photon errors that would have been obtained if Alice and Bob had prepared and measured all these pulses in the Z -basis then equals

$$e_{1,Z}^{\text{tot}} = \frac{n_X e_{1,Z}^L + n_Z e_{1,Z}}{n_X + n_Z}. \tag{18}$$

The amount of errors $n_Z e_{1,Z}$ can now be seen to be equal to the number of errors in a subset of size n_Z randomly sampled from a set of size $n_X + n_Z$ containing $(n_X + n_Z)e_{1,Z}^{\text{tot}}$ errors. Hence, $n_Z e_{1,Z}$ follows a hypergeometric distribution and

$$\begin{aligned} P\left(e_{1,Z}^L \geq e_{1,Z} + \delta\right) &= P\left(n_Z e_{1,Z} \leq n_Z e_{1,Z}^{\text{tot}} - \frac{n_X n_Z \delta}{n_X + n_Z}\right), \\ &\leq \exp\left(\frac{-2n_X^2 n_Z \delta^2}{(n_X + n_Z)(n_X + 1)}\right), \end{aligned} \tag{19}$$

where the inequality follows by applying Serfling’s tail bound of the hypergeometric distribution [23]. This upper bound is slightly different from that of [13]. If $n_X \geq n_Z$, then Eq. (19) gives a tighter upper bound than [13], but the difference between the two bounds is negligible. By Eq. (19) the event that an adversary correctly guesses the basis choices is taken into account for example.

If we now take

$$\delta = \delta(n_X, n_Z, \epsilon_1) = \sqrt{\frac{(n_X + n_Z)(n_X + 1)}{2n_X^2 n_Z} \ln\left(\frac{1}{\epsilon_1}\right)}, \tag{20}$$

we find that $P\left(e_{1,Z}^L \geq e_{1,Z} + \delta\right) \leq \epsilon_1$. It now follows that

$$H_{\max}^{\epsilon_1}(L_{1,Z}^{sa}|L_{1,Z}^{sb}) \leq n_{1,X} \bar{h}(e_{1,Z} + \delta(n_X, n_Z, \epsilon_1)), \tag{21}$$

where $\bar{h}(p) = h(\min(p, 1/2))$ for the binary entropy function h (Lemma 3 of [13]). Note that in the asymptotic limit, i.e., $n_X, n_Z \rightarrow \infty$, the term δ vanishes.

Altogether, we thus find that the QKD protocol is ϵ_{sec} -secure if

$$\begin{aligned} \ell = \left[n_{0,X} + n_{1,X} - n_{1,X} \bar{h}(e_{1,Z} + \delta(n_X, n_Z, \epsilon_1)) \right. \\ \left. - n_X (h(e_X) + \delta_{\text{cc}}(p_{\text{abort}}, n_X)) - \log_2\left(\frac{2}{\epsilon_{\text{cor}}(\epsilon_2 \epsilon_3 (\epsilon_{\text{sec}} - \epsilon))^2}\right) \right], \end{aligned} \tag{22}$$

for some $\epsilon_1, \epsilon_2, \epsilon_3 > 0$ and $\epsilon = 2\epsilon_1 + \epsilon_2 + \epsilon_3$. The values $\epsilon, \epsilon_2, \epsilon_3$ can be chosen to maximize the length ℓ of the secure key. Note that this key-length is conditioned

on the fact that the protocol does not abort. The expected key rate of the protocol is therefore given by,

$$R = \frac{1 - p_{\text{abort}}}{N} \left[n_{0,X} + n_{1,X} - n_{1,X} \bar{h}(e_{1,Z} + \delta(n_X, n_Z, \epsilon_1)) - n_X (h(e_X) + \delta_{\text{ec}}(p_{\text{abort}}, n_X)) - \log_2 \left(\frac{2}{\epsilon_{\text{cor}}(\epsilon_2 \epsilon_3 (\epsilon_{\text{sec}} - \epsilon))^2} \right) \right], \tag{23}$$

4.2 Linear programs to bound the unknown parameters

Some of the parameters, such as the amount of successful detection events n_X in the X -basis, in the key rate expression of Eq. (23) can be observed by Alice and Bob during the execution of the QKD protocol. However, Alice and Bob remain oblivious to other parameter values in this expression. For instance, we assume that Alice and Bob can not distinguish between single and multi-photon events. For this reason, they can not determine the number of single photon events $n_{X,1}$ in the X -basis. To this end, Alice and Bob resort to upper and lower bounds for these unknown parameter values. In this section we describe the linear programs that are used to find these bounds.

Let us first consider the different parameters of Eq. (23). The amount of successful detections n_X in the X -basis and the QBER e_X can be observed by Alice and Bob. The QBER e_X can be estimated before running the QKD protocol, hence no key material has to be sacrificed to estimate this value. A different QBER during the QKD protocol, possibly due to adversarial behavior, will not compromise the security, but merely influence the abort probability of the protocol. Note that the adversary, controlling the quantum channel, is always capable of aborting the protocol, i.e., performing a denial-of-service attack. Since Alice and Bob are unable to determine the amount of photons per pulse, the variables $n_{0,X}$, $n_{1,X}$ and $e_{1,X}$ remain unknown. For this reason the observable quantities $n_{\mu_j, \mathcal{X}}$ [Eq. (1)] and $E_{\mu_j, Z}$ [Eq. (2)] for all intensities μ_j and both bases \mathcal{X} are used to upper bound the error rate $e_{1,Z}$ and to lower bound the expression $n_{0,X} + n_{1,X} - n_{1,X} \bar{h}(e_{1,Z} + \delta(n_X, n_Z, \epsilon_1))$. These bounds result in lower bounds on the secure key length ℓ .

Let $n_{l, \mathcal{X}}$ be the amount of l -photon pulses detected by Bob and prepared and measured in the \mathcal{X} -basis. Then, for $0 \leq j \leq m$, it holds that the expected number of \mathcal{X} -pulses sent with intensity μ_j equals

$$\mathbb{E} \left[n_{\mu_j, \mathcal{X}} \right] = \sum_{l=0}^{\infty} p_{\mu_j | l, \mathcal{X}} n_{l, \mathcal{X}}, \tag{24}$$

where $p_{\mu_j | l, \mathcal{X}}$ is the probability that an l -photon pulse is sent with intensity μ_j given that Alice and Bob chose basis \mathcal{X} . Since the amount of photons in a weak laser pulse follows a Poisson distribution, we find by Bayes' rule that,

$$p_{\mu_j | l, \mathcal{X}} = \frac{e^{-\mu_j} \mu_j^l}{l!} \frac{p_{\mu_j | \mathcal{X}}}{p_{l | \mathcal{X}}}, \tag{25}$$

where $p_{\mu_j|\mathcal{X}}$ is the probability that an \mathcal{X} -pulse is sent with intensity μ_j and

$$p_{l|\mathcal{X}} = \sum_{j=0}^m \frac{p_{\mu_j|\mathcal{X}} e^{-\mu_j} \mu_j^l}{l!}, \tag{26}$$

is the probability that an \mathcal{X} -pulse consists of l photons [14,15].

In addition, the number of l -photon pulses in the \mathcal{X} basis $n_{l,\mathcal{X}}$ that result in a detection event is upper bounded by the number of l -photon pulses $N_{l,\mathcal{X}}$ sent by Alice and measured by Bob in the \mathcal{X} -basis. Note that we use an uppercase N to denote the amount of pulses sent by Alice and a lowercase n to denote the number of events detected by Bob. Hence,

$$n_{l,\mathcal{X}} \leq N_{l,\mathcal{X}} \quad \text{and} \quad \mathbb{E}[N_{l,\mathcal{X}}] = p_{l|\mathcal{X}} N_{\mathcal{X}}, \tag{27}$$

for all $l \geq 0$ and for all $\mathcal{X} \in \{X, Z\}$.

Alice and Bob cannot exactly determine the values $n_{l,\mathcal{X}}$, but Eqs. (25) and (27) do supply them with constraints on these values. The variables $n_{\mu_j,\mathcal{X}}$ are measured in the parameter estimation phase. In the asymptotic limit these estimations are equal to their expected values. Hence, neglecting finite key effects, we can find a lower bound $n_{1,Z}^*$ for $n_{1,Z}$ by solving the following linear program over the unknown variables $n_{l,Z}$ for $l \geq 0$.

$$\begin{aligned}
 n_{1,Z}^* = & \min \quad n_{1,Z}, \\
 \text{s.t.} \quad & \forall 0 \leq j \leq m, \forall l \geq 0 \\
 & n_{\mu_j,Z} = e^{-\mu_j} p_{\mu_j|Z} \sum_{l=0}^{\infty} \frac{\mu_j^l}{l!} \frac{n_{l,Z}}{p_{l|Z}}, \\
 & 0 \leq n_{l,Z} \leq p_{l|Z} N_Z.
 \end{aligned}$$

(28)

However, in all practical situations the amount of pulses is finite and the finite key effects cannot be neglected. By Hoeffding’s bounds [24] we find that

$$P\left(\left|n_{\mu_j,\mathcal{X}} - \mathbb{E}\left[n_{\mu_j,\mathcal{X}}\right]\right| \geq \sqrt{-\ln(\epsilon_{\mu_j}^H/2)n_{\mathcal{X}}/2}\right) \leq \epsilon_{\mu_j,\mathcal{X}}^H, \tag{29}$$

for all $0 \leq j \leq m$, $\mathcal{X} \in \{X, Z\}$ and $\epsilon_{\mu_j}^H > 0$. Since the variables $N_{l,\mathcal{X}}$ are sums of Bernoulli random variables we can apply Chernoff’s bounds [25]. In this effort, let us define the following function,

$$f : \mathbb{Z}_{\geq 0} \times [0, 1] \times (0, 1] \rightarrow \mathbb{R}_{\geq 0} \rightarrow, \quad (N, p, \epsilon) \mapsto -\ln(\epsilon) \left(1 + \sqrt{1 - \frac{2pN}{\ln(\epsilon)}}\right). \tag{30}$$

Then by Chernoff’s bound,

$$P\left(N_{l,\mathcal{X}} \geq \mathbb{E}[N_{l,\mathcal{X}}] + f(N_{\mathcal{X}}; p_{l|\mathcal{X}}; \epsilon_{l,\mathcal{X}}^C)\right) \leq \epsilon_{l,\mathcal{X}}^C, \tag{31}$$

for all $l \geq 0$, $\mathcal{X} \in \{X, Z\}$ and $\epsilon_{l,Z}^C > 0$.

Hence, a lower bound $n_{1,Z}^*$ of $n_{1,Z}$, that holds except with probability at most $\sum_{l=0}^\infty \epsilon_{l,Z}^C + \sum_{j=0}^m \epsilon_{\mu_j,Z}^H$, is given by the linear program of Eq. (32).

$$\begin{aligned} n_{1,Z}^* = \quad & \min \quad n_{1,Z}, \\ \text{s.t.} \quad & \forall 0 \leq j \leq m, \forall l \geq 0 \\ & n_{l,z}, \delta_{\mu_j} \in \mathbb{R}, \\ & n_{\mu_j,Z} + \delta_{\mu_j} = e^{-\mu_j} p_{\mu_j|Z} \sum_{l=0}^\infty \frac{\mu_j^l}{l!} \frac{n_{l,Z}}{p_{l|Z}}, \\ & \sum_{j=0}^m \delta_{\mu_j} = 0, \\ & 0 \leq n_{l,Z} \leq \min\left(p_{l|Z} N_Z + f(N_Z; p_{l|Z}; \epsilon_{l,Z}^C), n_Z\right), \\ & |\delta_{\mu_j}| \leq \sqrt{-\ln(\epsilon_{\mu_j,Z}^H/2)n_Z/2}. \end{aligned} \tag{32}$$

Similarly, an upper bound $E_{1,Z}^*$, that holds except with probability at most $\sum_{l=0}^\infty \epsilon_{l,Z}^C + \sum_{j=0}^m \epsilon_{\mu_j,E}^H$, of the number of errors in single-photon Z-pulses $E_{1,Z}$ is found by solving the linear program of Eq. (33).

$$\begin{aligned} E_{1,Z}^* = \quad & \max \quad E_{1,Z} \\ \text{s.t.} \quad & \forall 0 \leq j \leq m, \forall l \geq 0 \\ & E_{l,z}, \delta_{\mu_j} \in \mathbb{R}, \\ & E_{\mu_j,Z} + \delta_{\mu_j} = e^{-\mu_j} p_{\mu_j|Z} \sum_{l=0}^\infty \frac{\mu_j^l}{l!} \frac{E_{l,Z}}{p_{l|Z}}, \\ & \sum_{j=0}^m \delta_{\mu_j} = 0, \\ & 0 \leq E_{l,Z} \leq \min\left(p_{l|Z} N_Z + f(N_Z; p_{l|Z}; \epsilon_{l,Z}^C), E_Z\right), \\ & |\delta_{\mu_j}| \leq \sqrt{-\ln(\epsilon_{\mu_j,E}^H/2)E_Z/2}. \end{aligned} \tag{33}$$

It follows that

$$e_{1,Z} \leq e_{1,Z}^* = \min \left(\frac{E_{1,Z}^*}{n_{1,Z}^*}, \frac{1}{2} \right) \tag{34}$$

except with probability at most

$$\epsilon_e = \sum_{l=0}^{\infty} \epsilon_{l,Z}^C + \sum_{j=0}^m \left(\epsilon_{\mu_j,Z}^H + \epsilon_{\mu_j,E}^H \right). \tag{35}$$

Finally, a lower bound $n_{0,1,X}^*$ of the expression

$$n_{0,X} + n_{1,X} - n_{1,X} \bar{h} \left(e_{1,Z}^* + \delta(n_X, n_Z, \epsilon_1) \right), \tag{36}$$

that holds except with probability at most $\epsilon_X = \sum_{l=0}^{\infty} \epsilon_{l,X}^C + \sum_{j=0}^m \epsilon_{\mu_j,X}^H$, is found by solving the linear program of Eq. (37). The contribution of the vacuum states, $n_{0,X}$, to the secure key-rate can be argued to be marginal. For this reason, the optimization problem of Eq. (37) is often simplified by ignoring the $n_{0,X}$ component in the objective function.

$$\begin{aligned}
 n_{0,1,X}^* = & \min \quad n_{0,X} + n_{1,X} - n_{1,X} h(e_{1,Z}^* + \delta(n_X, n_Z, \epsilon_1)), \\
 \text{s.t.} \quad & \forall 0 \leq j \leq m, \forall l \geq 0 \\
 & n_{l,X}, \delta_{\mu_j} \in \mathbb{R}, \\
 & n_{\mu_j,X} + \delta_{\mu_j} = e^{-\mu_j} p_{\mu_j|X} \sum_{l=0}^{\infty} \frac{\mu_j^l}{l!} \frac{n_{l,X}}{p_{l|X}}, \\
 & \sum_{j=0}^m \delta_{\mu_j} = 0, \\
 & 0 \leq n_{l,X} \leq \min \left(p_{l|X} N_X + f(N_X; p_{l|X}; \epsilon_{l,X}^C), n_X \right), \\
 & |\delta_{\mu_j}| \leq \sqrt{-\ln(\epsilon_{\mu_j,X}^H/2)} n_X/2.
 \end{aligned}$$
(37)

A detail that has been omitted so far is the fact that these linear programs contain an infinite number of variables, which can be dealt with by truncating the infinite sums at M . For the resulting linear programs, with a finite number of variables, we refer to Appendix B. The same truncation applies to the error terms ϵ_X and ϵ_e , i.e.,

$$\begin{aligned}
 \epsilon_X &= \sum_{l=0}^M \epsilon_{l,X}^C + \sum_{j=0}^m \epsilon_{\mu_j,X}^H, \\
 \epsilon_e &= \sum_{l=0}^M \epsilon_{l,Z}^C + \sum_{j=0}^m \left(\epsilon_{\mu_j,Z}^H + \epsilon_{\mu_j,E}^H \right).
 \end{aligned}
 \tag{38}$$

In addition, the truncation introduces two additional error probabilities $\epsilon_{M,X}$ and $\epsilon_{M,Z}$. Altogether it follows, from solving the linear programs of Eqs. (54), (55) and (56) in Appendix B, that the expected key rate equals

$$R = \frac{1 - p_{\text{abort}}}{N} \left[\left(n_{0,1,X}^* - n_X (h(e_X) + \delta_{\text{ec}}(p_{\text{abort}}, n_X)) - \log_2 \left(\frac{2}{\epsilon_{\text{cor}}(\epsilon_2 \epsilon_3 (\epsilon_{\text{sec}} - \epsilon))^2} \right) \right) \right], \tag{39}$$

where $\epsilon_1, \epsilon_2, \epsilon_3 > 0$ are arbitrary values such that $\epsilon = 2\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_e + \epsilon_X + \epsilon_{M,X} + \epsilon_{M,Z}$.

5 Key-rate optimization

The previous section describes how to compute the key-rate for a given execution of the BB84 protocol. Hence, given the protocol parameters, the number of detection events (Eq. 1) and the number of errors (Eq. 2), the secure key-rate R can be computed by solving three linear programs.

Next, our objective is to maximize this key rate R by choosing optimal protocol parameters μ_j and $p_{\mu_j, \mathcal{X}}$ for $1 \leq j \leq m$ and $\mathcal{X} \in \{X, Z\}$. To this end, we model the quantum channel such that the expected number of detection events and errors can be computed as function of the protocol parameters. The physical model is the final step to find the protocol parameter values that optimize secure key-rate R . This optimal key-rate may be found by using the following nonlinear optimization program:

$$\begin{aligned} \max \quad & R, \\ \text{s.t.} \quad & \forall 0 \leq j \leq m, \mathcal{X} \in \{X, Z\} \\ & \sum_{j=0}^m p_{\mu_j, X} + p_{\mu_j, Z} = 1, \\ & \mu_j \geq 0, \\ & 0 \leq p_{\mu_j, \mathcal{X}} \leq 1. \end{aligned} \tag{40}$$

We obtain the solution of this nonlinear optimization program by applying the constrained nonlinear optimization techniques of [16].

5.1 Quantum channel

We consider a QKD system in which Alice encodes qubits in the polarization of photons and transmits them over a fiber optic cable to Bob. The fiber optic cable is assumed to have an attenuation of α dB/km, i.e., a channel efficiency of $\eta_{\text{ch}} = 10^{-\alpha x/10}$ for distance x km [14]. The channel efficiency equals the fraction of photons that arrive at Bob’s detection apparatus, which we assume to be independent of the polarization. In

addition to photon losses on the channel, losses can occur in Bob’s detection apparatus. These losses are captured by the detector efficiency η_d . The efficiency of the system with a quantum channel of length x is therefore given by

$$\eta_{\text{sys}} = \eta_{\text{ch}}\eta_d = 10^{-\alpha x/10}\eta_d. \tag{41}$$

Bob’s detection apparatus has to be capable of detecting individual photons and is therefore very sensitive. In fact, the photon detectors might click even when they are not illuminated. These events are called dark counts and the probability that a detector clicks without being illuminated is called the dark count probability p_{dark} . Recall that Bob’s detection apparatus contains two single photon detectors, one for each measurement outcome. Together with the fact that the number of photons in each intensity μ_j pulse follows a Poisson distribution with mean μ_j , we can derive the following expressing for the gain of μ_j -pulses in this quantum channel,

$$Q_{\mu_j} = 1 - (1 - p_{\text{dark}})^2 e^{-\mu_j \eta_{\text{sys}}}. \tag{42}$$

The gain Q_{μ_j} indicates the fraction of μ_j -pulses that result in a detection event. For a proper derivation of this expression we refer to [14]. From the gain we easily obtain the expected number of detection events as described in the parameter estimation phase [Eq. (1)],

$$n_{\mu_j, \mathcal{X}} = N p_{\mu_j, \mathcal{X}} Q_{\mu_j}. \tag{43}$$

Recall that N is the total number of pulses that is sent and $p_{\mu_j, \mathcal{X}}$ is the probability that Alice chooses basis \mathcal{X} and intensity μ_j .

To model the errors we assume that they are either caused by optical errors in the polarization or by dark counts. Optical errors are modeled by assuming that the polarization of photons is always rotated by an angle $0 \leq \theta \leq \pi/4$. Hence, when Alice sends the qubit $|0\rangle$, Bob receives qubit $\cos(\theta)|0\rangle + \sin(\theta)|1\rangle$. In practice, the polarization error is different per pulse and the angle θ represents an upper bound on the polarization error. Moreover, $\theta = \pi/4$ results in worst-case behavior, explaining why θ ranges from 0 to $\pi/4$.

Dark counts introduce errors since the associated detection events are independent of the polarization chosen by Alice. Hence, any dark-count event results in an error with probability of 1/2. Altogether, the expected number of errors for μ_j -pulses in the \mathcal{X} basis is,

$$E_{\mu_j, \mathcal{X}} = \frac{N p_{\mu_j, \mathcal{X}}}{2} \left(1 + (1 - p_{\text{dark}}) \left(e^{-\mu_j \eta_{\text{sys}} \cos^2 \theta} - e^{-\mu_j \eta_{\text{sys}} \sin^2 \theta} \right) - (1 - p_{\text{dark}})^2 e^{-\mu_j \eta_{\text{sys}}} \right). \tag{44}$$

In this section polarization encoded qubits transmitted over a fiber optic cable were considered. In practice, qubits transmitted over fiber optic cables are often phase encoded [26]. In contrast, polarization encoding is mostly used to transmit over free

space optical communication channels. Considering, these and other quantum channels requires some (minor) modifications to the physical model.

6 Results

In this section we present the results of our key-rate optimization approach. We start by comparing the results from our model to the results presented in [14]. Afterwards, we consider the effects of increasing the number of pulses sent and increasing the number of intensities used. We denote the number intensity settings by m and number of pulses sent by N .

Our experiments comprise three regimes. As baseline regime we compare our approach using the parameter settings from [14]. The baseline considers a finite number of intensities $m = 3$ and ignores finite key effects $N \rightarrow \infty$ as depicted in Fig. 1. Please note that in contrast to [14], we do not fix any of the used intensity settings. The second regime considers a finite number of intensity settings ($m = 3$), and explores the impact of finite key effects by varying the number of pulses $N \in \{10^7, 10^8, 10^9, 10^{10}, 10^{11}\}$. For comparison, we include our result from the baseline regime (where $N \rightarrow \infty$) as depicted in Fig. 2. In the third regime we vary the number of intensity settings, while discarding finite key effects, i.e., $N \rightarrow \infty$. The third regime includes the fully asymptotic case where both $m \rightarrow \infty$ and $N \rightarrow \infty$. This is depicted in Fig. 3.

6.1 Baseline

For the baseline regime we adopt the following parameter settings from [14]:

- We fix the dark count probability $p_{\text{dark}} = 6 \times 10^{-7}$ and the detector efficiency $\eta_d = 0.1$.
- For the misalignment we take $\theta = 0.0707$, with corresponding probability $e_{\text{mis}} = 5 \times 10^{-3}$.

We only compare the results for the asymptotic case, because the results for finite number of pulses are incomparable. In contrast to [14] we fix the number of pulses sent, while in [14] the post-processing block-size is fixed. To keep the same post-processing length a higher number of pulses needs to be emitted for larger distances.

Our results for the asymptotic case are shown in Fig. 1. Both the maximum achievable secure key-rate in terms of the loss in decibel (Fig. 1a) and the optimal intensity settings (Fig. 1b) are presented. The results in [14] are presented as key-rate per distance in kilometers, however, the two are directly related by an attenuation factor of 0.2 dB/km. In order to compute a lower bound for the secure key rate we apply the LP's of Sect. 4.2. However these contain infinite sums and assume finite key sizes. We refer to Appendix C.1 for the LP formulations that discard finite key effects and truncate the infinite sums. Note that the optimal intensities vary for different channel distances and that, in contrast to [14], fixing one of these intensities is sub-optimal. Estimating the leaked information is relatively easy for low losses, and in that case hardly any decoy states are required and the most frequent intensity can be chosen relatively high. For higher losses, more decoy states with higher intensities are required to still obtain a

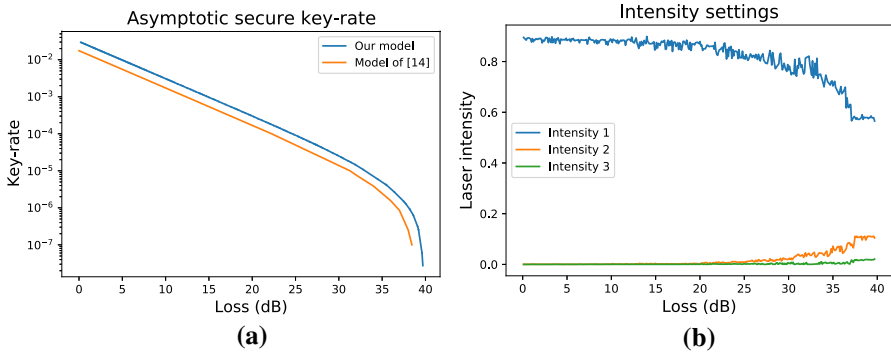


Fig. 1 The maximum achievable secure key-rate using our model compared to the maximum rate using the model of [14]. We discard finite key-effects and for our model, we also present the optimal intensity settings per loss

good estimate on the information leaked to an adversary. This explains the behavior of the three intensities shown.

With our model the maximum achievable key-rate is higher. However, we did not take into account the after-pulse probability. Depending on the magnitude of this error source, the results of our model may be closer to those of [14]. It is expected that the used intensities show a rather smooth evolution with increasing distance, however, different behavior is seen. This might result from the optimization routine where a stopping criteria is met too soon, for instance a maximum number of iterations or a local maxima with zero gradient. This can result in a sub-optimal solution and can be overcome by more strict stopping criteria. Despite these artifacts, the found key-rate is higher than obtained in [14]. Furthermore, secure key material can be extracted for higher losses.

6.2 Finite-key effects

In this regime we consider the effects of increasing the number of sent pulses N on the key-rate while preserving the baseline settings of Sect. 6.1 including $m = 3$. As we include finite key-effects, we have to fix certain cryptographic security parameters. We want to achieve a certain security of our protocol and we want it to be correct with high probability. Therefore, we fix the security and correctness parameters as $\epsilon_{\text{sec}} = \epsilon_{\text{cor}} = 2^{-50}$. Furthermore, we take the abort probability to be $p_{\text{abort}} = 2^{-50}$. Consequently, we fix $\epsilon_{l,X}^C = \epsilon_{l,Z}^C = \epsilon_{\mu_j,X}^H = \epsilon_{\mu_j,X}^H = \epsilon_{\mu_j,E}^H = 2^{-60}$. This gives upper bounds for $\epsilon_e \leq 2^{-54}$ and $\epsilon_X \leq 2^{-55}$ and we set $\epsilon_1 = \epsilon_2 = \epsilon_3 = 2^{-55}$. Combined this gives $\epsilon \leq 2^{-52}$, which matches with our constraint $\epsilon_{\text{sec}} \geq \epsilon$, obtained from Eq. (39). The linear programs given in Sect. 4.2 bound the number of usable pulses and photon errors, but contain an infinite number of variables. We refer to Appendix B for the truncation of the infinite sums of Sect. 4.2.

For the chosen security parameter ϵ_{sec} it is sufficient to upper bound multi photon pulses to at most 20 photons. Indeed, 20 is a sufficiently large upper bound on the

number of photons per pulse: Let X be Poisson distributed with rate μ . According to [27, Corollary 6], the Poisson tail probability may be bounded by

$$P(X \geq x \mid \mu = 1) \leq \min \left(\frac{e^{-D_{\text{KL}}(\mu, x)}}{2}, \frac{e^{-D_{\text{KL}}(\mu, x)}}{\sqrt{2\pi D_{\text{KL}}(\mu, x)}} \right), \quad \text{for } x > \mu, \quad (45)$$

where $D_{\text{KL}}(\mu, x)$ is the Kullback–Leibler divergence between two Poisson distributed random variables with respective means μ and x :

$$D_{\text{KL}}(\mu, x) = \mu - x + x \ln \left(\frac{x}{\mu} \right). \quad (46)$$

Using the bound from Eq. (45), we can show that

$$P(X \geq 20 \mid \mu = 1) < 2^{-63.03} < 2^{-60}. \quad (47)$$

We consider the key-rate for $N = 10^i$ pulses, for $i \in \{7, \dots, 10\}$ and we consider the limit $N \rightarrow \infty$. The results are shown in Fig. 2. The same channel and detector parameters are used as in the baseline. We observe that with increasing number of pulses, the expected secure key-rate indeed increases. Note that already for 10^{10} pulses, our key-rate estimation approaches the asymptotic key-rate quite well. The shown figure is the convex hull of the data points. This to account for instabilities in the optimization. We found that for all considered number of pulses sent, the probability that a pulse was sent in the Z -basis was less than 6%, independent of chosen intensity and the loss of the channel. This corresponds with the asymptotic case where the number of pulses sent in the Z -basis can be assumed to be an arbitrarily small fraction of the number of pulses.

6.3 Asymptotic key rates for different intensity settings

In this experimental regime we vary the number of intensity settings, for $m \in \{2, 3, 4\}$ while preserving the baseline settings of Sect. 6.1 including $N \rightarrow \infty$. We also include the fully asymptotic regime, where $m \rightarrow \infty$, and $N \rightarrow \infty$. We refer to Appendix C.2 for the unknown parameter estimation in this fully asymptotic case. The key-rate results are presented in Fig. 3a and b. We observe that while using only two intensities, the key-rate quickly drops. However, for more than two intensities, the results are very close to each other. Therefore, we focus on regime for 38 dB up to 40.5 dB loss in Fig. 3b. Here we observe that with each additional intensity, more key-material can be extracted. However, we also see that the gains are marginal. Already for three intensities, losses of up to 39.5 dB can be tolerated, with key-rate $\sim 10^{-7}$. Using more intensity settings gives only a minor increase in the maximum losses tolerated and a slightly higher key-rate for the same channel lengths. In the limit $m \rightarrow \infty$, the maximum tolerated loss for safely executing the protocol is bounded by 40.1 dB with a key-rate of about 5×10^{-8} .

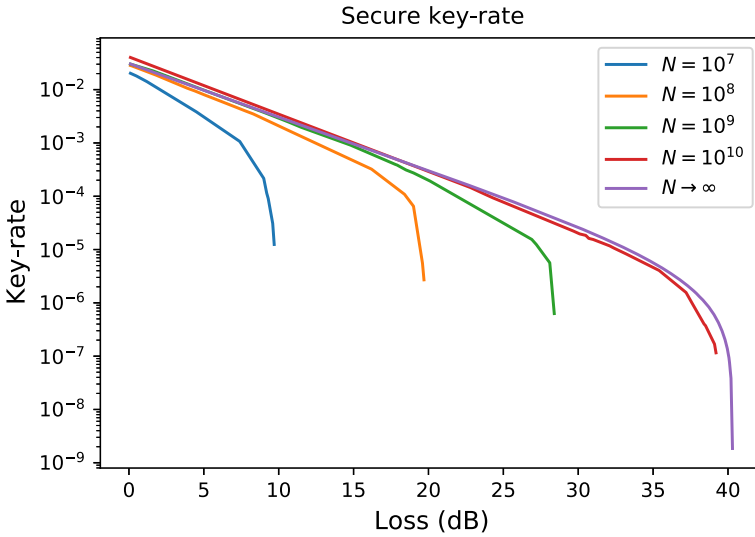


Fig. 2 The secure key-rate obtained in terms of the losses of the quantum channel (dB). For a varying number of pulses

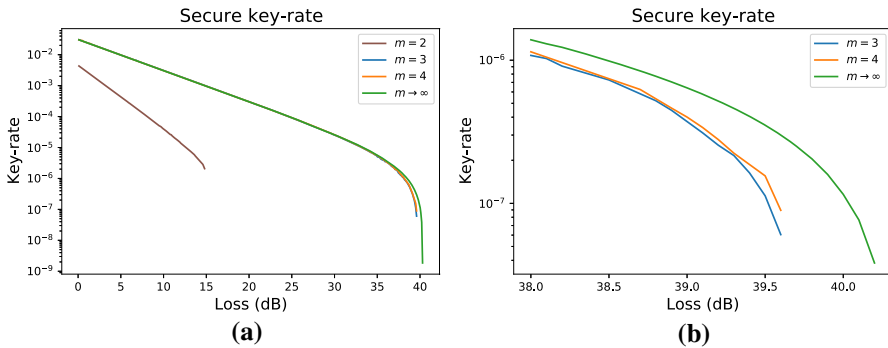


Fig. 3 The secure key-rate obtained in terms of the loss over the quantum channel (dB) for varying number of intensities m

7 Conclusion and discussion

In this work, we presented a key-rate optimization approach for the decoy-state BB84 QKD protocol. Our approach combines several linear and nonlinear programs to derive tighter protocol parameters and better key-rates, compared to previous approaches relying on heuristic assumptions.

Our optimization framework allows the complex optimization problem to be solved, without requiring it to be simplified by means of heuristic assumptions. We compared our model to that of [14] and show that higher key-rates are attained. Furthermore, we show the effect of increasing the number of decoy states and we show that using

three laser intensities is in general sufficient. In this way we validated a heuristic that is commonly used.

Our work is especially relevant to quantum channels with a significant amount of noise. In these cases, the effect of choosing sub-optimal protocol parameters is the largest. Some settings do not even allow any key material to be extracted when sub-optimal protocol parameters are used. In particular, our parameter settings allow for higher losses to be tolerated.

The analysis of this work focused on the BB84 QKD protocol. However, similar analyses can also be applied to other QKD protocols, such as for instance BBM92 or measurement-device independent protocols. The model can also be extended to incorporate more practical disturbances and noise. Furthermore, the model can be used in practical settings to optimize QKD protocol parameters to obtain higher key-rates.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

A Notation

See Table 1.

B Linear programs with finite number of variables

The linear programs given in Sect. 4.2 contain an infinite number of variables. To reduce the number of variables we truncate the infinite sums at M and upper-bound the number of pulses containing more than M photons,

$$m_{M,\mathcal{X}} = \sum_{l=M+1}^{\infty} n_{l,\mathcal{X}}. \quad (48)$$

Namely note that,

$$\begin{aligned} e^{-\mu_j} p_{\mu_j|\mathcal{X}} \sum_{l=0}^M \frac{\mu_j^l}{l!} \frac{n_{l,\mathcal{X}}}{p_{l|\mathcal{X}}} &\leq e^{-\mu_j} p_{\mu_j|\mathcal{X}} \sum_{l=0}^{\infty} \frac{\mu_j^l}{l!} \frac{n_{l,\mathcal{X}}}{p_{l|\mathcal{X}}} \leq m_{M,\mathcal{X}} \\ &+ e^{-\mu_j} p_{\mu_j|\mathcal{X}} \sum_{l=0}^M \frac{\mu_j^l}{l!} \frac{n_{l,\mathcal{X}}}{p_{l|\mathcal{X}}}. \end{aligned} \quad (49)$$

Table 1 Overview of the most important variables

Variable	Domain	Description
N	$\mathbb{Z}_{\geq 0}$	Number of pulses sent by Alice
\mathcal{X}	$\{X, Z\}$	Basis
U	$\{\mu_0, \dots, \mu_m\}$	Intensities
n	$\mathbb{Z}_{\geq 0}$	Number of pulses in which Alice and Bob chose the same basis and Bob registered an detection
E	$\mathbb{Z}_{\geq 0}$	Number of errors
e	$[0, 1/2]$	Error rate
μ	$\mathbb{R}_{\geq 0}$	Pulse intensity (mean photon number)
p	$[0, 1]$	Probability
ℓ	$\mathbb{Z}_{\geq 0}$	Length of the secret key (in bits)
R	$[0, 1]$	Secret key rate
K^r	$\{0, 1\}^N$	Raw key
K^s	$\{0, 1\}^{n_s}$	Sifted key
K^e	$\{0, 1\}^{n_x}$	Error corrected key
K	$\{0, 1\}^\ell$	Secure key

Subscripts are used to condition on events such as basis, intensity or photon number. Superscripts indicate whether the key is Alice’s (a) or Bob’s (b)

Hence, these inequalities allow us to bound the infinite sum by two finite sums.

Let $q_{M,\mathcal{X}}$ be the probability that a \mathcal{X} -pulse contains more than M photons, i.e.

$$q_{M,\mathcal{X}} = \sum_{j=0}^m p_{\mu_j|\mathcal{X}} e^{-\mu_j} \sum_{l=M+1}^{\infty} \frac{\mu_j^l}{l!}. \tag{50}$$

For

$$\Lambda_{M,\mathcal{X}} := q_{M,\mathcal{X}} N_{\mathcal{X}} + f(N_{\mathcal{X}}; q_{M,\mathcal{X}}; \epsilon_{M,\mathcal{X}}), \tag{51}$$

it follows, by Chernoff’s bound, that

$$P(m_{M,\mathcal{X}} \geq \Lambda_{M,\mathcal{X}}) \leq \epsilon_{M,\mathcal{X}}, \tag{52}$$

for all $\epsilon_{M,\mathcal{X}} > 0$. Hence solving the linear programs of Eqs. (54), (55) and (56), that contain a finite number of variables, will allow us to compute the length ℓ^* of the secret key,

$$\ell^* := n_{0,1,X}^* - n_X (h(e_X) + \delta_{ec}(p_{\text{abort}}, n_X)) - \log_2 \left(\frac{2}{\epsilon_{\text{cor}}(\epsilon_2 \epsilon_3 (\epsilon_{\text{sec}} - \epsilon))^2} \right), \tag{53}$$

for some $\epsilon_1, \epsilon_2, \epsilon_3 > 0$ and $\epsilon = 2\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_e + \epsilon_X + \epsilon_{M,X} + \epsilon_{M,Z}$.

$$\begin{aligned}
 n_{1,Z}^* = \min \quad & n_{1,Z}, \\
 \text{s.t.} \quad & \forall 0 \leq j \leq m, \forall 0 \leq l \leq M \\
 & n_{l,Z}, \delta_{\mu_j} \in \mathbb{R}, \\
 & n_{\mu_j,Z} + \delta_{\mu_j} \geq e^{-\mu_j} p_{\mu_j|Z} \sum_{l=0}^M \frac{\mu_j^l}{l!} \frac{n_{l,Z}}{p_{l|Z}}, \\
 & n_{\mu_j,Z} + \delta_{\mu_j} \leq e^{-\mu_j} p_{\mu_j|Z} \sum_{l=0}^M \frac{\mu_j^l}{l!} \frac{n_{l,Z}}{p_{l|Z}} + \Lambda_{M,Z}, \\
 & \sum_{j=0}^m \delta_{\mu_j} = 0, \\
 & 0 \leq n_{l,Z} \leq \min \left(p_{l|Z} N_Z + f(N_Z; p_{l|Z}; \epsilon_{l,Z}^C), n_Z \right), \\
 & |\delta_{\mu_j}| \leq \sqrt{-\ln(\epsilon_{\mu_j,Z}^H/2) n_Z/2}.
 \end{aligned} \tag{54}$$

$$\begin{aligned}
 E_{1,Z}^* = \max \quad & E_{1,Z} \\
 \text{s.t.} \quad & \forall 0 \leq j \leq m, \forall 0 \leq l \leq M \\
 & E_{l,Z}, \delta_{\mu_j} \in \mathbb{R}, \\
 & E_{\mu_j,Z} + \delta_{\mu_j} \geq e^{-\mu_j} p_{\mu_j|Z} \sum_{l=0}^M \frac{\mu_j^l}{l!} \frac{E_{l,Z}}{p_{l|Z}}, \\
 & E_{\mu_j,Z} + \delta_{\mu_j} \leq e^{-\mu_j} p_{\mu_j|Z} \sum_{l=0}^M \frac{\mu_j^l}{l!} \frac{E_{l,Z}}{p_{l|Z}} + \Lambda_{M,Z}, \\
 & \sum_{j=0}^m \delta_{\mu_j} = 0, \\
 & 0 \leq E_{l,Z} \leq \min \left(p_{l|Z} N_Z + f(N_Z; p_{l|Z}; \epsilon_{l,Z}^C), E_Z \right), \\
 & |\delta_{\mu_j}| \leq \sqrt{-\ln(\epsilon_{\mu_j,e}^H/2) E_Z/2},
 \end{aligned} \tag{55}$$

$$\begin{aligned}
 n_{0,1,X}^* = \min & \quad n_{0,X} + n_{1,X} - n_{1,X}h(e_{1,Z}^* + \delta(n_X, n_Z, \epsilon_1)), \\
 \text{s.t.} & \quad \forall 0 \leq j \leq m, \forall 0 \leq l \leq M \\
 & \quad n_{l,X}, \delta_{\mu_j} \in \mathbb{R}, \\
 & \quad n_{\mu_j,X} + \delta_{\mu_j} \geq e^{-\mu_j} p_{\mu_j|X} \sum_{l=0}^M \frac{\mu_j^l}{l!} \frac{n_{l,X}}{p_{l|X}}, \\
 & \quad n_{\mu_j,X} + \delta_{\mu_j} \leq e^{-\mu_j} p_{\mu_j|X} \sum_{l=0}^M \frac{\mu_j^l}{l!} \frac{n_{l,X}}{p_{l|X}} + \Delta_{M,X}, \\
 & \quad \sum_{j=0}^m \delta_{\mu_j} = 0, \\
 & \quad 0 \leq n_{l,X} \leq \min \left(p_{l|Z} N_X + f(N_X; p_{l|X}; \epsilon_{l,X}^C), n_X \right), \\
 & \quad |\delta_{\mu_j}| \leq \sqrt{-\ln(\epsilon_{\mu_j,X}^H/2) n_X/2}.
 \end{aligned}$$

(56)

C Asymptotic case

In the asymptotic limit, i.e. when $N \rightarrow \infty$, the Serfling, Hoeffding and Chernoff terms vanish and the linear programs simplify significantly. In this section the asymptotic linear programs are presented. First, the case with a finite amount of decoy states is presented. Subsequently, we consider the case where the number of decoy intensities m goes to infinity as well. In this case the linear programs can be omitted entirely.

C.1 Finite number of decoy intensities

Let us first define the yields $Y_{l,\mathcal{X}}$ and the gains $Q_{\mu_j,\mathcal{X}}$,

$$\begin{aligned}
 Y_{l,\mathcal{X}} & := \frac{n_{l,\mathcal{X}}}{p_{l|\mathcal{X}} N_{\mathcal{X}}}, \quad \forall l \geq 0, \mathcal{X} \in \{X, Z\}, \\
 Q_{\mu_j,\mathcal{X}} & := \frac{n_{\mu_j,\mathcal{X}}}{p_{\mu_j|\mathcal{X}} N_{\mathcal{X}}}, \quad \forall 0 \leq j \leq m, \mathcal{X} \in \{X, Z\}.
 \end{aligned}$$

In addition, we define the following variables,

$$\begin{aligned}
 \gamma_{l,Z} & := e_{l,Z} Y_{l,Z} = \frac{E_{l,Z} Y_{l,Z}}{n_{l,Z}} = \frac{E_{l,Z}}{p_{l|Z} N_Z}, \quad \forall l \geq 0, \\
 \gamma_{\mu_j,Z} & := e_{\mu_j,Z} Q_{\mu_j,Z} = \frac{E_{\mu_j,Z} Q_{\mu_j,Z}}{n_{\mu_j,Z}} = \frac{E_{\mu_j,Z}}{p_{\mu_j|Z} N_Z}, \quad \forall 0 \leq j \leq m.
 \end{aligned}$$

Substituting the above variables in Eqs. (32), (33) and (37) results in the following linear programs, where $e_{1,Z}^* := \frac{\gamma_{1,Z}^*}{Y_{1,Z}^*}$.

$$\begin{aligned}
 Y_{1,Z}^* = \quad & \min && Y_{1,Z}, \\
 \text{s.t.} &&& \forall 0 \leq j \leq m, \forall l \geq 0 \\
 &&& Q_{\mu_j,Z} = e^{-\mu_j} \sum_{l=0}^{\infty} \frac{\mu_j^l}{l!} Y_{l,Z}, \\
 &&& 0 \leq Y_{l,Z} \leq 1.
 \end{aligned} \tag{59}$$

$$\begin{aligned}
 \gamma_{1,Z}^* = \quad & \max && \gamma_{1,Z} \\
 \text{s.t.} &&& \forall 0 \leq j \leq m, \forall l \geq 0 \\
 &&& \gamma_{\mu_j,Z} = e^{-\mu_j} \sum_{l=0}^{\infty} \frac{\mu_j^l}{l!} \gamma_{l,Z}, \\
 &&& 0 \leq \gamma_{l,Z} \leq 1.
 \end{aligned} \tag{60}$$

$$\begin{aligned}
 Y_{0,1,X}^* = \quad & \min && p_{0|X} Y_{0,X} + p_{1|X} Y_{1,X} (1 - h(e_{1,Z}^*)), \\
 \text{s.t.} &&& \forall 0 \leq j \leq m, \forall l \geq 0 \\
 &&& Q_{\mu_j,X} = e^{-\mu_j} \sum_{l=0}^{\infty} \frac{\mu_j^l}{l!} Y_{l,X}, \\
 &&& 0 \leq Y_{l,X} \leq 1.
 \end{aligned} \tag{61}$$

Solving these linear programs results in a secure key-rate

$$R^* = Y_{0,1,X}^* - Q_X h(e_X). \tag{62}$$

In linear program 61, we have used the fact that the sifting probability p_X can be taken arbitrarily close to 1.

C.2 Infinite number of decoy intensities

If, in addition, we assume an infinite amount of decoy intensities (i.e. $m \rightarrow \infty$) then, for properly chosen intensities, the linear programs can be shown to possess a single feasible solution. Hence, Alice and Bob can in this case compute the exact yields and error rates. The resulting key rate can therefore be computed as follows,

$$R^* = p_{0|X} Y_{0,X} + p_{1|X} Y_{1,X} (1 - h(e_{1,Z})) - Q_X h(e_X). \tag{63}$$

The sifting probabilities $p_{0|X}$ and $p_{1|X}$ depend on the intensities, which are chosen to maximize the key rate.

References

- Bennett, C.H., Brassard, G.: An update on quantum cryptography. In: Blakley, G.R., Chaum, D. (eds.) *Advances in Cryptology, Proceedings of CRYPTO '84*, Santa Barbara, California, USA, August 19–22, 1984, Proceedings, vol. 196 of Lecture Notes in Computer Science, pp. 475–480. Springer (1984)
- Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. *Reviews of Modern Physics* **74**, 145–195 (2002)
- Mayers, D.: Quantum key distribution and string oblivious transfer in noisy channels. In: Koblitz, N. (ed.) *Advances in Cryptology—CRYPTO '96*, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18–22, 1996, Proceedings, vol. 1109 of Lecture Notes in Computer Science, pp. 343–357. Springer, Berlin (1996)
- Ben-Or, M., Horodecki, M., Leung, D.W., Mayers, D., Oppenheim, J.: The universal composable security of quantum key distribution. In: Kilian, J. (ed.) *Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005*, Cambridge, MA, USA, February 10–12, 2005, Proceedings, vol. 3378 of Lecture Notes in Computer Science, pp. 386–406. Springer (2005)
- Canetti, R.: Universally composable security: a new paradigm for cryptographic protocols. In: 42nd Annual Symposium on Foundations of Computer Science, FOCS 2001, 14–17 October 2001, Las Vegas, Nevada, USA, pp. 136–145. IEEE Computer Society (2001)
- Xu, F., Ma, X., Zhang, Q., Lo, H.-K., Pan, J.-W.: Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020)
- Brassard, G., Lütkenhaus, N., Mor, T., Sanders, B.C.: Security aspects of practical quantum cryptography. In: Preneel, B. (ed.) *Advances in Cryptology—EUROCRYPT 2000*, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14–18, 2000, Proceeding, vol. 1807 of Lecture Notes in Computer Science, pp. 289–299. Springer (2000)
- Lütkenhaus, N.: Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **61**, 052304 (2000)
- Hwang, W.-Y.: Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003)
- Lo, H.-K., Ma, X., Chen, K.: Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005)
- Wang, X.-B.: Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005)
- Tomamichel, M., Renner, R.: Uncertainty relation for smooth entropies. *Phys. Rev. Lett.* **106**, 110506 (2011)
- Tomamichel, M., Lim, C.C.W., Gisin, N., Renner, R.: Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3**, 1–6 (2012)
- 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)
- Ma, X., Qi, B., Zhao, Y., Lo, H.-K.: Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326 (2005)
- Conn, A.R., Gould, N.I.M., Toint, P.L.: *Trust Region Methods*. MOS-SIAM Series on Optimization, SIAM, Philadelphia (2000)
- Lucamarini, M., Patel, K.A., Dynes, J.F., Fröhlich, B., Sharpe, A.W., Dixon, A.R., Yuan, Z.L., Pentz, R.V., Shields, A.J.: Efficient decoy-state quantum key distribution with quantified security. *Opt. Express* **21**, 24550–24565 (2013)
- Curty, M., Xu, F., Cui, W., Lim, C.C.W., Tamaki, K., Lo, H.-K.: Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **5**, 1–7 (2014)
- Carter, L., Wegman, M.N.: Universal classes of hash functions. *J. Comput. Syst. Sci.* **18**(2), 143–154 (1979)
- Renner, R.: Security of quantum key distribution. In: Wagner, D. (ed.) *Ausgezeichnete Informatikdissertationen*, vol. D-6 of LNI, pp. 125–134. GI (2005)
- Tomamichel, M., Schaffner, C., Smith, A.D., Renner, R.: Leftover hashing against quantum side information. *IEEE Trans. Inf. Theory* **57**(8), 5524–5535 (2011)

22. Vitanov, A., Dupuis, F., Tomamichel, M., Renner, R.: Chain rules for smooth min- and max-entropies. *IEEE Trans. Inf. Theory* **59**(5), 2603–2612 (2013)
23. Serfling, R.J.: Probability inequalities for the sum in sampling without replacement. *Ann. Stat.* **2**, 39–48 (1974)
24. Hoeffding, W.: Probability inequalities for sums of bounded random variables. *J. Am. Stat. Assoc.* **58**(301), 13–30 (1963)
25. 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)
26. Townsend, P.D., Rarity, J.G., Tapster, P.R.: Single photon interference in 10 km long optical fibre interferometer. *Electron. Lett.* **29**, 634–635 (1993)
27. Short, M.: Improved inequalities for the Poisson and binomial distribution and upper tail quantile functions. *ISRN Probab. Stat.* **2013**, 1–6 (2013)

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