Security bounds for efficient decoy-state quantum key distribution

Marco Lucamarini, James F. Dynes, Bernd Fröhlich, Zhiliang Yuan, and Andrew J. Shields

Abstract—Information-theoretical security of quantum key distribution (QKD) has been convincingly proven in recent years and remarkable experiments have shown the potential of QKD for real-world applications. Due to its unique capability of combining high key rate and security in a realistic finite-size scenario, the efficient version of the BB84 QKD protocol endowed with decoy states has been subject of intensive research. Its recent experimental implementation finally demonstrated a secure key rate beyond 1 Mbps over a 50 km optical fiber. However the achieved rate holds under the restrictive assumption that the eavesdropper performs collective attacks. Here, we review the protocol and generalize its security. We exploit a map by Ahrens to rigorously upper bound the Hypergeometric distribution resulting from a general eavesdropping. Despite the extended applicability of the new protocol, its key rate is only marginally smaller than its predecessor in all cases of practical interest.

I. INTRODUCTION

Quantum key distribution (QKD) [1], [2] in two decades has progressed considerably and reached a maturity suitable for real-world use. Fundamental achievements have been obtained in QKD theory and experiments [3]-[12]. On the theoretical side, security proofs have been extended beyond the “asymptotic scenario”, accounting for the fact that real data samples are always finite and subject to statistical fluctuations [13]-[19]. This led to an operational definition of the security of QKD, aimed at quantifying through an ε-value the deviation of a real system from an ideal one. On the experimental side, QKD systems capable of achieving ε-values as small as 10^{-10} have been developed [20]-[24].

In order to bring QKD technology closer to real-world deployment, it is necessary to further reconcile the requirements of the theory with those of a real-world implementation, such as high key rate generation and low manufacturing costs. Therefore QKD protocols are continuously refined to approach the desired levels of efficiency and security.

Here, we review and extend a version of the efficient BB84 protocol [25]-[27] endowed with decoy states [28]-[31], recently introduced and experimentally realized in [24], which provides a key rate beyond 1 Mbps over a 50 km optical fiber with an ε-value of 10^{-10}. This key rate was obtained under the limiting assumption that Eve performs collective attacks [1], [2]. In this case, the measured QKD quantities were represented by independent and identically distributed (i.i.d.) random variables that were bounded using the Clopper-Pearson (CP) confidence interval [32]-[34] for the Binomial distribution. By combining such bounds with the proof method described in [4], [7] and refined in [17]-[19], the security of the protocol was finally obtained.

Recently, a class of QKD protocols have been proven secure using the uncertainty relation for smooth entropies [35], [36]:

\[ H_{\min}^e(Z|E) + H_{\max}^e(X|X') \geq \gamma n. \]  

Eq. (1) holds if the transmitter is endowed with a perfect single photon source. The parameter \( \gamma \in [0,1] \) is a quality factor related to the bias between the bases used by the transmitter [36]. If the emitted states are in two mutually unbiased bases, e.g. Z and X, like in the ideal BB84 protocol, then \( \gamma = 1 \). The conditional smooth min entropy \( H_{\min}^e(Z|E) \) quantifies how many random bits are contained in Z that are independent of Eve and \( \epsilon \)-close to a uniform distribution, with \( \epsilon \geq 0 \) the smoothing parameter [37], \( H_{\max}^e(X|X') \), the conditional smooth max entropy, gives the number of additional bits necessary to reconstruct X from X’ with failure probability \( \epsilon \). The key rate resulting from Eq. (1) is secure under general attacks so it can be used to drop the assumption of collective attacks from the efficient decoy-state BB84 protocol, as in [38].

However, additional work is required to guarantee security against the most general attack related to how the QKD quantities are sampled in a situation where the size of the sample is finite. The sampled quantities are random variables obeying a given distribution, in most cases Binomial, due to the two-valued nature of QKD observables. The Binomial distribution well represents experimental results under the i.i.d. assumption, or when measurements can be described as an operation of sampling with replacement. In some cases, however, this kind of sampling is not possible even in principle, for example, when sampling in the basis X prevents sampling in the complementary basis Z, or vice versa [35], [39]. Under these circumstances, sampling without replacement has to be considered instead, and the Binomial distribution has to be replaced by the Hypergeometric distribution [35].

Below, we review the protocol of Ref. [24] and show its security under Eq. (1), along the lines described in [35] and [38]. We generalize the estimation procedure so as to cover both
the Binomial and the Hypergeometric distributions. This is done using a map by Ahrens described in [40]. It allows to reduce the general case to one that deals with Binomial distributions only. In turn, this allows to continue using the CP confidence interval for the Binomial distribution to provide worst-case bounds to the parameters of the protocol, as it was done in [24].

In Section II, we give some preliminary description of the Ahrens map and the CP confidence interval for the Binomial distribution. In Section III, we provide a detailed description of our protocol. In Section IV, we discuss the protocol security. Section V is left for the concluding remarks.

II. PRELIMINARIES

In the following, we give the basic notions about the Ahrens map and the CP confidence interval for the Binomial distribution. We will use them later for the protocol description and the security analysis.

A. The Ahrens map

Consider a total population of $N$ balls in an urn containing $K$ white balls and $N-K$ black balls. A sample of $n$ elements ($n < N$) is drawn at random from the urn. A success is when a white ball is selected. If the sampled elements are not replaced in the urn, then the probability to draw $k$ white balls is given by the Hypergeometric distribution (HG):

$$HG(n, n, K, k) = \binom{K}{k} \binom{N-K}{n-k} / \binom{N}{n},$$

which is positive for $\max(0, n - N + K) \leq k \leq \min(n, K)$. If the sampled elements are replaced in the urn, the probability of a successful event is constant, equal to $p = K/N$, and the probability to draw $k$ white balls from the urn is given by the Binomial distribution (Bi):

$$BI(n, p, k) = \binom{n}{k} p^k (1-p)^{n-k},$$

which is positive for $0 \leq k \leq n$.

The Ahrens map [40] is a permutation of the parameters $n, K, N-n, N-K$ so to obtain a new BI with the following property:

$$HG(n, n, K, k) \leq \sqrt{2} BI(\tilde{n}, \tilde{K}/N, \tilde{k}),$$

where the tilde indicates the permuted parameters, as defined by the following selection rules:

$$\tilde{n} = \min(n, K, N-n, N-K)$$

if $\tilde{n} = n \lor (N-n)$ then $\tilde{K} = \min(K, N-K)$

if $\tilde{n} = K \lor (N-K)$ then $\tilde{K} = \min(n, N-n)$.

The permutation of the parameters is always possible, so there is no need to specify a range of application for it. In the top diagram of Fig. 1 we illustrate the Ahrens map, using a particular choice of the parameters. The curve (i) is the distribution of $k$ according to $BI(n, K/N, k)$; the curve (ii) is $HG(n, n, K, k)$; the curve (iii) is the upper bound $\sqrt{2} BI(\tilde{n}, \tilde{K}/N, \tilde{k})$ provided by the permuted BI distribution. The standard BI distribution has a larger variance than the corresponding HG, but it does not upper bound it on the whole range. On the contrary, the permuted BI distribution multiplied by $\sqrt{2}$ is always above the HG, so it can be used to upper bound it.

In some cases, the standard BI still provides bounds that are looser than those of the permuted BI. Our system automatically selects the loosest bounds, for each QKD session, so to guarantee the highest security level. This also simplifies the analysis because we only have to deal with BI distributions, either permuted or not.

B. CP confidence interval

Consider a sequence of Bernoulli experiments in which the probability to obtain a success is constant, $p$. A sample of $n$ elements would then provide $k$ successes with the probability specified in Eq. (3).

Rather than obtaining the probability for $k$ successes, we are interested in confidence bounds for $k$, assessing that for any $\epsilon > 0$, the true value of $k$ belongs to the interval $(k_\epsilon, \tilde{k}_\epsilon)$ with confidence $\geq 1 - \epsilon$, where $k_\epsilon, \tilde{k}_\epsilon$ are lower and upper bounds to the number of successes, respectively. This is obtained by solving in $p$ the following equations for the cumulative BI distribution [32], [41]:

$$P(k \leq k) = \sum_{k=0}^{k} \binom{n}{k} p^k (1-p)^{n-k} = \epsilon, \quad (6)$$

$$P(k \geq k) = \sum_{k=\infty}^{n} \binom{n}{k} p^k (1-p)^{n-k} = \epsilon. \quad (7)$$

The solutions of Eqs. (6) and (7) are respectively $p$ and $\tilde{p}$, and can be efficiently computed [41]. When the above equations are simultaneously solved, the resulting CP confidence interval contains $k$ with probability $1 - 2\epsilon$. When the permuted BI is used to bound a HG distribution, Eqs. (6), (7) have to be solved with $\epsilon/\sqrt{2}$ replacing $\epsilon$, in order to obtain results with the same confidence. The system resets from $\epsilon$ to $\epsilon/\sqrt{2}$ automatically, if necessary.

In the bottom diagram of Fig. 1, we pictorially illustrate the lower bounds obtained though the CP approach, for the same probability distributions considered in the top diagram of Fig. 1. Lower bounds with confidence $1 - \epsilon$ are given by the intersections of the cumulative functions with the line $\epsilon$. In the example of the figure, the loosest bound is provided by the non-permuted BI distribution, labelled with (i). So, in this case, our system would automatically select this bound to assess the security of the protocol. However, it is not always guaranteed that the non-permuted BI distribution upper bounds the HG distribution, labelled with (ii). For that, we can use the upper bound provided by the Ahrens map, Eq. (4), labelled with (iii).

III. PROTOCOL DESCRIPTION

In this Section, we modify the protocol described in Ref. [24] in order to generalize its security. In the following, we adopt a basis index $b = \{b_1, b_2\} = \{Z, X\}$ to indicate the bases chosen by the users, and a class index $\mu = \{\mu_1, \mu_2, \mu_3\} = \{u, v, w\}$ to indicate the intensity, or photon flux, used by the transmitter in
With probability $p_{dt}$, the transmitter (Alice) prepares a phase-randomised coherent state with intensity $\mu$. She then selects a basis $b$ with probability $p_b$ and a bit value 0 or 1 with probability 50%. She uses these values to encode a state that is sent to the receiver over the quantum channel.

### B. Receiver

The receiver (Bob) chooses a basis $b$ with the same probability $p_b$ as Alice and then measures the incoming state using two threshold detectors $D_0$ and $D_1$. If no detector clicks, a vacuum count is recorded; if only detector $D_0$ ($D_1$) clicks, a bit value 0 (1) is recorded; if both detectors click, a random bit value, 0 or 1, is assigned and recorded [44], [45].

### C. Reconciliation and determination of samples size

After a predetermined number of $N$ states have been sent by Alice and measured by Bob, users analyse the statistics associated to the states over an authenticated public channel. The very first time, the channel can be authenticated using a pre-shared secret string and universal hashing [46]. Then, the secret string can be regenerated from the quantum key at every new session. At first, Bob discloses bases and timestamps of his non-vacuum counts. Then Alice announces bases and classes for these counts, together with the bit values in the $X$ basis and in the decoy and vacuum pulses. With these information, users form raw keys from all the counts in the class $\mu = u$ and matched bases $b_i = b_j = Z$, where $b_i$ and $b_j$ refer to Alice and Bob, respectively, and $i,j \in \{1,2\}$. The length of the raw keys is denoted as $C_{\text{raw}}$. Similarly, the size of the set of non-vacuum counts with generic class and bases is denoted as $C_{\text{nba}}$. The users can measure these quantities exactly.

From public communication, users can also compute the exact quantities $N_{\text{nba}}$, i.e., the total number of pulses in the class $\mu$ and in the same basis $b_i = b_j = b$. In some cases, these quantities are very large and it is more practical to estimate upper and lower bounds for $N_{\text{nba}}$ rather than determining the exact value on the classical channel. Due to the large size of the samples, the resulting bounds are tight and the confidence level very close to unity. To simplify the description, we omit the details of this issue in what follows and we just refer to the exact values $N_{\text{nba}}$. The drawing of $C_{\text{nba}}$ counts from $N_{\text{nba}}$ pulses, in turn selected from a total population $N$, can give rise to a HG distribution, as first noted in [35]. As explained in Section I.A, the protocol automatically considers this possibility and, if necessary, treats it via Eq. (4). Because all the bits for $X$ basis, decoy and vacuum have been revealed, a direct comparison between Alice’s and Bob’s strings can tell the exact number of errors $E_{\text{d}z}$, $E_{\text{w}z}$ and $E_{\text{xx}}$.

The users run a classical error correction (EC) algorithm to correct possible errors in the raw keys obtained from signals in the $Z$ basis. We call $E_{\text{d}z}$ the total number of errors in the raw keys and $E_{\text{ec}}$ the parity bits revealed in order to correct them. After EC, the users verify that error corrected keys are identical using universal2 hashing. If the keys are found to be different, the protocol aborts and data are discarded. We call $e_{\text{ver}}$ the probability that the keys are different but the protocol does not abort. In some cases, the verification step can be postponed until the authentication step, which is also performed using universal2 hash functions. As a result of EC and verification, the
users can estimate the number of errors $E_{uZZ}$ with confidence equal to or bigger than $1 - \varepsilon_{ver}$.

D. Bounds to fluctuations and parameter estimation

At this point, the quantities $N_{\mu b}$, $C_{\mu b}$ and $E_{\mu b}$ are known to the users. They run the following steps to bound the finite-size fluctuations and estimate the unknown parameters of the protocol:

1. Bound yields and error rate in the minority basis using the CP confidence interval. Mean values and bounds are respectively $Y_b^{(\mu)} = C_{\mu b} / N_{\mu b}$, $\bar{Y}_b^{(\mu)}$, $\bar{Y}_b^{(\mu)}$ for the yields and $B_X^{(\mu)} = E_{uxx} / N_{uxx}$, $\bar{B}_X^{(\mu)}$, for the $X$ error rate. To obtain the bounds, the following distributions are considered. For the yields: $BI(N_{\mu b}, Y_b^{(\mu)}, C_{\mu b})$ and $HG(N, N_{\mu b}, N_{\mu b}, Y_b^{(\mu)}, C_{\mu b})$; for the $X$ error rate: $BI(N_{uxx}, E_{uxx}^{(\mu)} / N_{uxx}), HG(N, N_{uxx}, N_{uxx}, E_{uxx}^{(\mu)} / N_{uxx})$. The HG distribution is bounded by the corresponding BI through the Ahrens map. Worst-case bounds are eventually selected, as described in Section II.

2. Numerical constrained optimization and decoy-state technique are combined with the bounds above to estimate $Y_b^{(\mu)}$ and $Y_b^{(\mu)}$, i.e. lower and upper bounds of the yields of the pulses containing $k$ photons ($k = \{0, 1\}$) in the basis $b = \{Z, X\}$. Bounds to the number of $k$-photon pulses in the $b$ basis are then obtained as: $\bar{N}_b^{(\mu)} = \left[ N_{\mu b} \frac{Y_b^{(\mu)} (1 + e^{-u^k})}{k!} \right]$, $\bar{N}_b^{(\mu)} = \left[ N_{\mu b} \frac{Y_b^{(\mu)} (1 + e^{-u^k})}{k!} \right]$. The condition $\bar{N}_b^{(\mu)} \gg \bar{N}_b^{(\mu)}$ is verified by the users, otherwise the protocol aborts. This condition is always met for $P_Z \gg P_X$.

3. In a similar way, the upper bound to the bit error rate of the 1-photon pulses in the $X$ basis, $\bar{q}_{\text{bit}, X}$, is obtained. This is used as upper bound to the phase error rate in the $Z$ basis (see Section IV). If $\bar{q}_{\text{bit}, X}$ is larger than a predetermined threshold $q_{\text{tol}, Z}$, protocol aborts. We call $p_{\text{ab}}$ the overall probability that the protocol aborts.

In Table I, we summarize all the quantities of the protocol, with their associated failure probability.

Table I. Predetermined, measured and estimated quantities in the protocol, with their associated failure probability.

| Symbol | Quantity | Failure probability |
|--------|----------|---------------------|
| $N$ | number predetermined triggers | exactly known, $\emptyset$ |
| $N_{\mu b}$ | sizes of samples in class $\mu$ and basis $b$ | exactly known to Alice, $\emptyset$ |
| $N_{\mu b}$ | sizes of samples in class $\mu$ and matching bases $b$ | exactly known in principle |
| $C_{\mu b}$ | size of measured count samples | estimated, $2\epsilon$ |
| $E_{\mu b}$ | errors in class $\mu$ and basis $Z$ | estimated, $\epsilon_{ver}$ |
| $E_{\mu b}$ | errors in $\mu b \neq uZZ$ | exactly known, $\emptyset$ |
| $B_X^{(\mu)}$ | upper bound to $X, u$ BER | estimated, $\epsilon$ |
| $q_{\text{tol}, Z}$ | upper bound to $X$ QBER of 1-photon pulses | estimated, $1\epsilon$ |

where $\varepsilon_{sec} = 10^{-10}$ defines the overall secrecy of the protocol\(^1\). The protocol is $\varepsilon_{ver} + \varepsilon_{sec}$ secure, meaning that it is $\varepsilon_{ver}$-correct and $\varepsilon_{sec}$-secret [35]. This definition of security is composable and allows to use the quantum key in cryptographic applications [37].

IV. SECURITY

The security of the above protocol stems from two aspects. On one side, there is the estimation of Eve’s information, quantified via the min-entropy [37], [38] and then upper bounded using the uncertainty principle [36], Eq. (1), and the max-entropy bound [47], [35]. On the other side, there is parameter estimation (PE). This is a refinement of the one adopted in [24]. However, we need to justify its application in this new context.

Let us start from a recap of what has been already achieved in terms of security for the efficient decoy-state BB84 protocol and compare it with our approach.

A. State of the Art and Comparison

In [19], the security of the efficient decoy-state BB84 (eds-BB84) protocol was initially demonstrated using the proof method in [17], [18], which holds under the assumption of collective attacks by Eve\(^2\). Due to non-optimized decoy-state

---

\(^1\) It was conjectured that the mentioned proof method holds for general attacks too, not only for collective ones. Recently, an attempt to prove this conjecture was made in [48] and it was found that a few extra bits have to be sacrificed during privacy amplification to go from collective to general attacks.
bounds, the resulting performance in terms of key rate and working distance was quite poor. In [24, 49], the compatibility of the mentioned proof method with the CP approach and numerical PE was first demonstrated for the \textit{eds-BB84} protocol. This allowed to improve the decoy-state bounds and achieve experimental key rates beyond 1 Mbps over a 50 km optical fiber link, still under the condition of collective attacks [24]. In [50], the same numerical PE based on BI distribution as in [24] and [49] was used to prove for the first time the security of the \textit{eds-BB84} protocol against general attacks, assuming a perfect vacuum state prepared by Alice and the quantities analogous to \( N_{\text{ubb}} \) (see Table I) exactly known. The resulting HG distribution was upper bounded by the sum of two BI distributions [50]. Later on, a simpler proof of \textit{eds-BB84} security against general attacks, based on the entropic uncertainty relations [35], [36], was provided in [38]. In this case, the PE exploits Hoeffding’s inequality [49], which is used to bound observable quantities analogous to \( C_{\text{ubb}} \) and \( E_{\text{ubb}} \) in Table I. Also, analytical expressions were used to estimate the parameters entering the key rate equation.

Here, we use the entropic uncertainty relations to quantify Eve’s information and the CP confidence interval and numerical optimization to perform the PE. Differently from Eve’s information and the CP confidence interval and key rate equation, expressions were used to estimate the parameters entering the quantities 

\[
E_{\text{ui}} \leq \frac{1}{2} \ln \left( \frac{1}{1 - \epsilon} \right),
\]

which holds with probability \( 1 - 2\epsilon \).

Here, we do a similar operation using the CP method instead, applied to a (permutated or non-permutated) BI distribution, and numerical optimization, as explained in Section II.B. Specifically, given \( C \) counts from \( N \) pulses, the average detection probability is \( Y = C/N \) and the bounds are \( Y_{\min} - Y \), obtained with confidence \( 1 - 2\epsilon \) using the CP method. Hence, because \( N \) is constant, we also have \( |C^* - C| = N[Y^* - Y] \leq N(Y_{\min} - Y) \). The bounds \( Y_{\min}^{(\mu)}, \bar{Y}_{\min}^{(\mu)} \) and \( \bar{B}_X^{(\mu)} \) in Table I are obtained in this way. The last one, \( \bar{B}_X^{(\mu)} \), upper bounds the ratio \( E_{\text{ui}XX}/N_{\text{ui}XX} \), i.e., the bit error rate (BER) in the \( X \) basis. These bounds are used, in turn, to estimate parameters that are not directly measurable, like \( y_p^{(k)} \) and \( q_{ph,k}^{(1)} \). This is done through constrained optimization [53], as described in points E.2 and E.3 of the protocol. An example of optimization problem solved in our system is as follows [49]:

\[
\min_{\mu} y_{2}^{(\mu)},
\]

where \( \Gamma \) is a set of constraints determined by: the measured quantities; the usual positivity and completeness conditions for probabilities; the following decoy-state QKD relations:

\[
Y_{\min}^{(\mu)} \leq e^{-\mu} \sum_{k} \frac{\mu^k}{k!} \gamma_{z}^{(k)} \leq \bar{Y}_{\min}^{(\mu)} \quad (\mu = \{u, v, w\}).
\]

The optimization problem is linear and so efficiently solved. In the estimation of \( y_{2}^{(\mu)} \), three two-side nontrivial constraints are involved. Hence the overall \( \epsilon \)-value for the simultaneous fulfillment of all constraints is conservatively bounded as \( 6\epsilon \). With optimization problems similar to the one in Eqs. (10), (11), \( k \)-photon yields \( (k = \{0, 1\}) \) in any basis can be obtained.

C. Upper bound to the phase error rate

Numerical optimization is also used to upper bound the 1-photon quantum bit error rate (QBER) in the minority basis \( X \) by solving the following problem:

\[
\max_{\Gamma^*} q_{\text{bit}X}^{(1)},
\]

where \( \Gamma^* \) contains the same constraints as for \( y_{2}^{(1)} \), plus the following one:

\[
e^{-\mu} \sum_{k} \frac{\mu^k}{k!} \gamma_{X}^{(k)} \leq \bar{B}_X^{(\mu)}.
\]

The above problem can be reduced to the following bound [49]:

\[
q_{\text{bit}X}^{(1)} \leq \bar{q}_{\text{bit}X}^{(1)} = \left( e^{u \bar{B}_X^{(\mu)} - 1} \frac{1}{2} \gamma_{X}^{(0)} \right)^{1/2} \left( u \gamma_{X}^{(1)} \right).
\]

Two-sided and one-side nontrivial constraints are

\[
4 \quad \text{Notice that this is different from the more common ratio} \quad E_{\text{ui}XX}/N_{\text{ui}XX} \text{ known as “quantum bit error rate” (QBER) [33, 34].}
\]

For this reason we conservatively state that the proof method only guarantees security against collective attacks.  

\[3 \text{ See, e.g., Eq. (F.2) in [50], which is used to sample the Binomial distribution as in the Clopper-Pearson estimation method.}\]
involved in achieving this bound starting from the optimization problem in Eqs. (12) and (13). By weighting each of them with the same \(\varepsilon\) value, we obtain that Eq. (14) holds with confidence \(1 - 19\varepsilon\). To make the connection with security, we need to estimate the 1-photon phase error rate in the Z basis, \(q_{\text{ph},Z}^{(1)}\). For single photons, QKD theory guarantees that the asymptotic values of the QBER in the basis \(X\) and the phase error rate in the basis \(Z\) are the same:

\[
q_{\text{bit},X}^{(1)} = q_{\text{ph},Z}^{(1)}. \tag{15}
\]

On the other side, the asymptotic value of a certain quantity coincides with its true value, and we know from the CP method that the QBER true value is bounded by \(\hat{q}_{\text{bit},X}^{(1)}\) with confidence \(1 - 19\varepsilon\). Therefore, the phase error rate is bounded by the same quantity with the same confidence:

\[
q_{\text{ph},Z}^{(1)} \leq \hat{q}_{\text{bit},X}^{(1)}. \tag{16}
\]

Let us recall that this bound holds for both BI and HG distributions, because of the presence of the Ahrens map. In order to relate it to the security proof of [35] and [38], we need to add some details.

First, in Ref. [35] it is not the true value of the phase error rate to be used, but rather the bound to the phase error rate that a hypothetical observer would see if he tested a finite sample of size \(n_{Z}^{(1)}\) in a population of \(n_{Z}^{(1)} + n_{X}^{(1)}\) elements. Let us call \(q_{\text{ph},Z}^{(1)}\) such a bound. We show here that \(\hat{q}_{\text{bit},X}^{(1)}\) is a more conservative bound than \(q_{\text{ph},Z}^{(1)}\), i.e., \(\hat{q}_{\text{bit},X}^{(1)} \leq q_{\text{ph},Z}^{(1)}\). This implies that Eq. (16) still holds. Because \(n_{Z}^{(1)} \geq n_{Z}^{(3)}\) (point III.D.2 of the protocol) we have that \(q_{\text{ph},Z}^{(1)} \leq \hat{q}_{\text{bit},X}^{(3)}\), where \(\hat{q}_{\text{bit},X}^{(3)}\) is estimated from \(n_{Z}^{(1)}\) single photons. We also have that \(\hat{q}_{\text{bit},X}^{(3)} \leq \hat{q}_{\text{bit},X}^{(1)}\) because, by negating this statement, we would obtain the absurd result that a bound estimated from a certain amount of coherent states via the decoy-state technique is tighter than one estimated directly from the same amount of single-photon states. This proves our statement.

Second, differently from [38], we keep the quality factor \(\gamma\) of Eq. (1) in the estimation of the smooth min entropy via the uncertainty principle (compare with Appendix B in [38]). This leads to the factor \(\gamma n_{Z}^{(1)}\) in Eq. (8).

Third, we recalculate the bound to the smooth max-entropy according to the argument given in [35]. For that, we notice that all the steps in the supplementary materials of [35] can be repeated with the Serfling inequality [52] replaced by the CP confidence interval. In particular, the total number \(W_{\text{ph},Z}\) of Z phase errors can be bounded as:

\[
W_{\text{ph},Z} \leq \left(\frac{\hat{n}_{Z}^{(1)}}{\hat{\pi}_{Z}^{(1)}}\right) q_{\text{tol},X}, \tag{17}
\]

with \(q_{\text{tol},X}\) a predetermined threshold larger than \(\hat{q}_{\text{bit},X}^{(1)} + O(1/\hat{n}_{Z}^{(1)})\). In turn, this implies that the smooth max-entropy is upper bounded by:

\[
\hat{\pi}_{Z}^{(1)} h(q_{\text{tol},X}), \tag{18}
\]

where \(\hat{\pi}_{Z}\) is the truncated binary entropy function. It could be worth remarking that Eq. (18) contains the upper bound to \(n_{Z}^{(1)}\), which is clearly more conservative than the lower bound \(n_{Z}^{(1)}\) present in [38].

V. CONCLUSION

In this work, we extended the security proof of the efficient decoy-state BB84 protocol for QKD presented in [24] to cover the most general attack allowed by the laws of physics. We also added extra features to the protocol, like the possibility to drop the assumption of a perfect state preparation at Alice’s side. This imperfection is included in the quality factor \(\gamma\), which should be characterized by the users beforehand in a safe location.

Given the wider security range of the protocol, it is natural to ask whether its key rate is degraded respect to previous realizations. In Table II, we report values for the new protocol key rate versus optical fibre distance, and compare it with the protocol in [24], secure against collective attacks. At 50 km, the new protocol still provides beyond 1Mbps rate with 22.5% detection efficiency, well within the reach of current detectors [54]-[56]. Furthermore, the maximum achievable distance is more than 110 km. The new protocol compares well against the one in [24], whose key rate is recalculated and given in Table II, featuring on average only a 10% reduction.

The proof method in [35], adopted in our analysis, entails a reduced sensitivity to finite-size effects. The term \(A\) in Eq. (9) does not include the detrimental contribution proportional to the square root of the length of the raw key, \(\sqrt{C_{\text{zzz}}\leq Z}\), which was present in [24]. In Fig. 2, we numerically simulate the secure
key rate of the protocol (vertical axis) versus the size of the data block (top horizontal axis), which is varied by acting on the acquisition time (bottom horizontal axis). It can be seen that up to a block size of $10^5$, the key rate remains at more than 20% its asymptotic value. The minimum size of the sample providing a positive key rate is $1.6 \times 10^4$ bits.

Overall, the performance of the here-presented decoy-state efficient BB84 protocol is comparable with what reported in the past [24], despite the wider class of attack covered in the new protocol and the single basis used to distill secure key bits. This is mainly due to the substantially unchanged numerical optimization in the parameter estimation stage. It still runs based on sampling from a Binomial distribution, which can be accomplished efficiently in several existing software packages.

The gap between the Binomial and the Hypergeometric distributions, relevant for going from collective to general attacks, is bridged by the Ahrens map [40], that can be run automatically as a sub-routine of the numerical optimization program. We expect this to become a useful tool in other quantum communications protocols.

**REFERENCES**

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” Rev. Mod. Phys., vol. 74, pp. 145-195 (2002).

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” Rev. Mod. Phys., vol. 81, pp. 1301-1350 (2009).

[3] D. Mayers, in Advances in Cryptology: Proceedings of CRYPTO (Lecture Notes in Computer Science), D. Coppersmith, Ed. New York, NY, USA: Springer-Verlag, 1995, pp. 124-135.

[4] H. K. Lo and H. F. Chau, “Unconditional security of quantum key distribution over arbitrarily long distances”, Science, vol. 283, pp. 2050-2056 (1999).

[5] P. W. Shor, J. Preskill, “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol”, Phys. Rev. Lett., vol. 85, pp. 441-444 (2000).

[6] R. Renner, N. Gisin, and B. Kraus, “Information-theoretic security proof for quantum-key-distribution protocols,” Phys. Rev. A, vol. 72, p. 012332 (2005).

[7] B. Kraus, N. Gisin, and R. Renner, “Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication,” Phys. Rev. Lett., vol. 95, pp. 080501 (2005).

[8] M. Peev, C. Pacher, R. Alleaume, C. Barreiro, J. Bouda, W. Bosleytner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Légrè, R. Lieger, J. Lodewyck, T. Lorinser, N. Lütkenhaus, A. Marhold, T. Matysou, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Riboiry, S. Rohr, L. Salvail, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tuaille-Broui, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, “The SECOQC quantum key distribution network in Vienna,” New J. Phys., vol. 11, p. 075001 (2009).

[9] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, Y. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, T. Tokura, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, Y. Tokura, J. F. Dynes, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, “Coexistence of high-bit-rate quantum key distribution and data on optical fiber,” Phys. Rev. X, vol. 2, p. 041010 (2012).

[10] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, “A quantum access network,” Nature, vol. 501, pp. 69-72, 2013.

[11] K. A. Patel, J. F. Dynes, M. Lucamarini, I. Choi, A. W. Sharpe, Z. L. Yuan, R. V. Penty, and A. J. Shields, “A quantum access network,” Nature, vol. 501, pp. 69-72, 2013.

[12] M. Hayashi, “Practical evaluation of security for quantum key distribution,” Phys. Rev. A, vol. 74, p. 022307 (2006).

[13] S. Watagane, R. Matsumoto, and T. Uematsu, “Noise tolerance of the BB84 protocol with random privacy amplification,” Int. J. Quantum Inf., vol. 4, p. 935 (2006).

[14] H. Inamori, N. Lütkenhaus, and D. Mayers, “Unconditional security of practical quantum key distribution,” Eur. Phys. J. D, vol 41, p. 599 (2007).

[15] M. Hayashi, “Upper bounds of eavesdropper’s performances in finite-length code with the decoy method,” Phys. Rev. A, vol. 76, p. 012329 (2007).

[16] V. Scarani and R. Renner, “Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing,” Phys. Rev. Lett., vol. 100, p. 200501 (2008).

[17] V. Scarani and R. Renner, “Security bounds for quantum cryptography with finite resources,” in Theory of Quantum Computation, Communication, and Cryptography, vol. 5106 of Lecture Notes in Computer Science, (Berlin Springer, 2008), pp. 83-95.

[18] R. Y. Q. Cai and V. Scarani, “Finite-key analysis for practical implementations of quantum key distribution,” New J. Phys., vol. 11, p. 045024 (2009).
IEEE JOURNAL OF SELECTED TOPICS IN QUANTUM ELECTRONICS, VOL. 21, NO. 3, MAY/JUNE 2015

[20] J. Hasegawa, M. Hayashi, T. Hiroshima, A. Tanaka, and A. Tomita, “Experimental decoy state quantum key distribution with unconditional security incorporating finite statistics,” arXiv:0705.3081 (2007).

[21] D. Rosenberg, C. G. Peterson, J. W. Harrington, P. R. Rice, N. Dallmann, K. T. Tyagi, K. P. McCahel, S. Nam, B. Baek, R. H. Hadfield, R. J. Hughes and J. E. Nordholt, “Practical long-distance quantum key distribution system using decoy levels,” New J. Phys., vol. 11, p. 045009 (2009).

[22] P. Jouquet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, “Experimental demonstration of long-distance continuous-variable quantum key distribution,” Nat. Phot., vol. 7, pp. 378-381 (2013).

[23] D. Bacco, M. Canale, N. Laurenti, G. Vallone, and P. Villoresi, “Experimental quantum key distribution with finite-key security analysis for noisy channels,” Nat. Comm., vol. 4, pp. 2363 (2013).

[24] M. Lucamarini, K. Patel, J. Dynes, B. Fröhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, “Efficient decoy-state quantum key distribution with quantified security,” Opt. Express, vol. 21, pp. 24550-24565 (2013).

[25] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing, Bangalore, India, December 10-12, 1984, pp. 175-179.

[26] H.-K. Lo, H. F. Chau, and M. Ardehali, “Efficient quantum key distribution scheme and proof of its unconditional security,” J. of Crypt. vol 18, p. 133 (2005).

[27] C. Erven, X. Ma, R. Laflamme, and G. Weihs, “Entangled quantum key distribution with a biased basis choice,” New J. Phys., vol. 11, p. 045025 (2009).

[28] W. Y. Hwang, “Quantum key distribution with high loss: toward global secure communication,” Phys. Rev. Lett., vol. 91, p. 057901 (2003).

[29] X.-B. Wang, “Beating the photon-number-splitting attack in practical quantum cryptography,” Phys. Rev. Lett., vol. 94, p. 230503 (2005).

[30] H.-K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” Phys. Rev. Lett., vol. 94, pp. 230504 (2005).

[31] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key distribution,” Phys. Rev. A, vol. 72, p. 012326 (2005).

[32] C. C. Y. Law, K. S. Lam, and V. Hon, “One-shot classical data compression with quantum side information and the distillation of common randomness or secret keys”, arXiv:1008.0452 (2010).

[33] M. Mertz, H. K. Berlin, H. Bratzik, and D. Bruß, “Secret key rates for coherent attacks”, Phys. Rev. A, vol. 87, p. 012315 (2013).

[34] M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, “Practical treatment of quantum bugs,” Proc. SPIE 8542, Electro-Optical Remote Sensing, Photonic Technologies, and Applications VI (2012).

[35] M. Hayashi and R. Nakayama, “Security analysis of the decoy method with the Bennett-Brassard 1984 protocol for finite key lengths,” New J. Phys. vol. 16, p. 063009 (2014).

[36] W. Hoeffding, “Probability inequalities for sums of bounded random variables,” J. Amer. Stat. Assoc., vol. 58, pp. 13-30 (1963).

[37] R. J. Serfling, “Probability Inequalities for the Sum in Sampling without Replacement”, Ann. Stat., vol. 2, pp. 39-48 (1974).

[38] S. Boyd and L. Vandenberghe, Convex Optimization, Cambridge University Press New York (2004).

[39] Y. Nambu, S. Takahashi, K. Yoshino, A. Tanaka, M. Fujiiwara, M. Sasaki, A. Tajima, S. Yorozu, and A. Tomita, “Efficient and low-noise single-photon avalanche photodiode for 1.244-GHz clocked quantum key distribution,” Opt. Express, vol. 19, pp. 20531-20541 (2011).

[40] L. C. Comandar, B. Fröhlich, M. Lucamarini, K. A. Patel, A. W. Sharpe, J. F. Dynes, Z. L. Yuan, R. V. Penty, and A. J. Shields, “Room temperature single-photon detectors for high bit rate quantum key distribution”, Appl. Phys. Lett., vol. 104, p. 021101 (2014).

[41] M. L. Comandar, B. Fröhlich, J. F. Dynes, A. W. Sharpe, M. Lucamarini, Z. L. Yuan, R. V. Penty, and A. J. Shields, “Gigahertz-gated InGaAsInP single-photon detector with detection efficiency exceeding 55% at 1550 nm”, J. Appl. Phys., vol. 117, p. 083109 (2015).