Finite-key analysis for practical implementations of quantum key distribution

To cite this article: Raymond Y Q Cai and Valerio Scarani 2009 *New J. Phys.* **11** 045024

New Journal of Physics
The open-access journal for physics

Finite-key analysis for practical implementations of quantum key distribution

Raymond Y Q Cai and Valerio Scarani[1]
Centre for Quantum Technologies and Department of Physics,
National University of Singapore, Singapore
E-mail: physv@nus.edu.sg

New Journal of Physics **11** (2009) 045024 (20pp)
Received 24 November 2008
Published 30 April 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/4/045024

Abstract. The lists of bits processed in quantum key distribution are necessarily of finite length. The need for finite-key unconditional security bounds was recognized long ago, but the theoretical tools have become available only very recently. We provide finite-key unconditional security bounds for two practical implementations of the Bennett–Brassard 1984 coding: prepare-and-measure implementations without decoy states and entanglement-based implementations. A finite-key bound for prepare-and-measure implementations with decoy states is also derived under a simplified treatment of the statistical fluctuations. The presentation is tailored to allow direct application of the bounds in experiments. Finally, the bounds are also evaluated on *a priori* reasonable expected values of the observed parameters.

[1] Author to whom any correspondence should be addressed.

Contents

1. Introduction

In 1984, Bennett and Brassard remarked that quantum physics provides a solution to the cryptographic task of distributing a secret key and provided the first explicit protocol, known as BB84 [1]. This fact was rediscovered in 1991 by Ekert [2]. Since then, quantum key distribution (QKD) has grown into a mature field, spanning a wide range of competences; several reviews have been devoted to it [3]–[6].

The fast development of QKD can be tracked down to the interplay of two factors. Firstly, QKD allows *unconditional security* [7]–[14], which means that security can be guaranteed in an information-theoretical sense, without any assumption on the computational power of the eavesdropper. Therefore, the task in itself is interesting, because it reaches beyond anything that can be done with classical communication alone. Secondly QKD can be implemented without entanglement [1] or with one entangled pair [2] and has therefore been well within reach of existing experimental technologies for several decades.

The matching of a theoretical security proof to a real device is, however, a delicate matter. On the one hand, while unconditional security does not put any constraint on the eavesdropper, the proofs *do* contain assumptions about the behavior of the devices of the authorized partners: the quantum states that are prepared, the model of the detectors, the procedures used for the classical post-processing of the data. On the other hand, imperfections of the real devices may leak information inside channels or allow for Trojan horse attacks or other purely classical hacking attacks [15]–[17]: it is clearly impossible to devise a security proof that would take all these failures into account (for the so-called *device-independent* approach to security and its assumptions, we refer to [18, 19]). The development of checking procedures based on testable assumptions is one of the most urgent tasks at the present stage of development of QKD.

Among the assumptions made in most unconditional security proofs, one is manifestly at odds with the behavior of a real device: namely, the fact that bounds are usually provided only in the asymptotic limit of infinitely long keys. On this issue, no convergence is possible

unless theorists make the effort of developing *finite-key analysis*. Remarkably, all the elements for a rigorous finite-key analysis were already present in the very first unconditional security proof by Mayers [7]. However, his work was too innovative and also too complex to be duly appreciated. His subsequent work with Inamori *et al* [20] also went rather unnoticed; moreover, it was shown later that their approach does not yield composable security [21, 22] and must therefore be abandoned. Other partial estimates showed that the finite-key correction is quite important in the usual range of operation of QKD systems [23]–[26].

The first study in which finite-key analysis is integrated in a proof of composable unconditional security, is Hayashi's analysis of the BB84 protocol with decoy states [27]. This is, to our knowledge, the only finite-key bound to have been applied to experimental data as of today [28]. Independently, Renner and one of us also developed security proofs in the non-asymptotic limit [29, 30] based on the formalism developed in [13]. In the present paper, we use this approach to derive explicit finite-key security bounds for practical implementations of the BB84 coding. In section 2, we provide the general elements of finite-key formalism following [29, 30]. In section 3, we apply these tools to one-way prepare-and-measure implementations of BB84 with weak coherent pulses, both without and with decoy states: we derive an unconditional security bound for the first and a partial bound for the second. Part of the results overlap with those of Hayashi and co-workers [31]. In section 4, we repeat the same study for entanglement-based implementations of the BB84 coding, i.e. for the Bennett–Brassard–Mermin 1992 (BBM92) protocol [32].

2. Finite-key formalism

2.1. Asymmetric BB84 protocol

We consider the BB84 coding with asymmetric role of the bases [23]: the key is obtained from the events in which both Alice and Bob have used the Z basis, while the correlations in the X basis are used to estimate Eve's knowledge. We write p_Z the probability that the Z basis is chosen and $p_X = 1 - p_Z$ the probability that the X basis is chosen (to keep things simple in this general survey, we assume that these probabilities are the same for Alice and Bob). Therefore, denoting N as the length of Alice's and Bob's lists before sifting (basically, the number of signals detected by Bob), the raw key will be of length $n = Np_Z^2$, Eve's information is estimated on a sample consisting of $m = Np_X^2$, and $2Np_Zp_X$ signals are discarded in sifting. We denote by $\mathbf{e_Z}$ and $\mathbf{e_X}$ the measured error rates in the two bases (in the whole paper, we use boldface fonts for the quantities that are directly measured in the protocol).

2.2. Finite-key bound for the secret fraction

Although the finite-key formalism has been generalized to accommodate more general forms of classical post-processing [30], in this paper we consider the extraction of a secret key through one-way post-processing without pre-processing. Out of the n pairs of bits that form the raw key, Alice and Bob want to extract a secret key of length $\ell \leqslant n$. We refer to the ratio $r = \ell/N$ as to the *secret fraction*. The asymptotic value of r is given by the well-known Devetak–Winter bound [33]

$$\lim_{N\to\infty} r = S(X|E) - H(X|Y), \tag{1}$$

where $S(X|E) := S(XE) - S(E)$ and $H(X|Y) := H(XY) - H(Y)$ are the conditional von Neumann and Shannon entropies, respectively, evaluated for the joint state of Alice and Bob's raw key and the system controlled by Eve (after the sifting step). The main result of [29, 30] says that the finite-key version of this bound can also be cast in a rather simple form, namely

$$r = p_Z^2 \left[S_\xi(X|E) - \Delta(n) - \mathrm{leak}_{\mathrm{EC}} \right], \tag{2}$$

whose terms we comment upon below.

- The first correction to the asymptotic bound is the factor $n/N = p_Z^2$. Its meaning is pretty obvious: only n signals out of N form the raw key. In the limit $N \to \infty$, one can choose $p_Z \to 1$ because a small fraction of signals will give an accurate enough estimation of the parameters—typically, $m \propto \sqrt{N}$, i.e. $p_X \propto N^{1/4}$ [29, 34]; see also our study below.
- The second correction is the one represented by the notation $S_\xi(X|E)$, the modification of Eve's uncertainty on single copies $S(X|E)$. Its meaning is also obvious. Eve's information is estimated using measured parameters, e.g. error rates. In a finite-key scenario, these parameters are estimated on samples of finite length: therefore, one has to allow for statistical fluctuations.

  Specifically, let λ be one of the parameters that enter Eve's information (to fix ideas, think of e_X); and let d be the number of outcomes of a positive operator-valued measure (POVM) needed to estimate it (for error rates of bits, $d = 2$ since the outcomes are 'Alice = Bob' and 'Alice $\neq$ Bob'). Suppose then that m' signals have been used to estimate λ: then the deviation of the estimate $\lambda_{m'}$ from the ideal estimate λ_∞ can be quantified by

$$|\lambda_{m'} - \lambda_\infty| \leqslant \xi(m', d) = \frac{1}{2}\sqrt{\frac{2\ \ln(1/\varepsilon_{\mathrm{PE}}) + d\ \ln(m'+1)}{m'}}, \tag{3}$$

  where $\varepsilon_{\mathrm{PE}}$ is the failure probability of the parameter estimation[2]. We shall write the upper and the lower bounds compatible with the fluctuations as

$$\lambda^{\mathrm{U}} = \min(\lambda + \xi, 1),\ \lambda^{\mathrm{L}} = \max(\lambda - \xi, 0) \tag{4}$$

  because all the λs estimated below are probabilities (error rates, fraction of multi-photon pulses, etc). In all that follows, for simplicity of notation we shall omit the max and min.

  We stress that the notation $\lambda^{\mathrm{U,L}}$ was first introduced in [24]. Here the expressions are different, since they considered relative errors drawn from a normal distribution, while our estimate (3) quantifies absolute errors and does not assume any specific form for the underlying distribution. This is a requirement of the finite-key formalism we are using. This difference will lead to some minor discrepancies with previously published works, see section 3.3.2. The possibility of rephrasing the formalism in terms of relative errors is listed among the open issues at the end of this paper.

[2] The law of large numbers we are using reads $\sum_{k=1}^{d} |\lambda_m(k) - \lambda_\infty(k)| \equiv \sum_{k=1}^{d} |\Delta_m(k)| \leqslant \sqrt{[2\ \ln(1/\varepsilon_{\mathrm{PE}}) + d\ \ln(m+1)]/m}$ (we refer to theorem 12.2.1 and lemma 12.6.1 in [37]). The constraint $\sum_{k=1}^{d} \lambda_m(k) = \sum_{k=1}^{d} \lambda_\infty(k) = 1$, i.e. $\sum_{k=1}^{d} \Delta_m(k) = 0$, implies that the deviation for the parameter $\lambda = \lambda(1)$ that we want to estimate is given by equation (3)—more precisely, equation (3) is exact for $d = 2$, while for $d > 2$ it represents the largest possible deviation. The factor $1/2$ was missing in previous works [29, 30], therefore the lower bounds presented there may be made slightly more optimistic. After inspection, the net result is that the curves obtained for N can actually be obtained already for $N' \sim N/2$.

- The third correction to be commented on is

$$\Delta(n) = 7\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{n}} + \frac{2}{n}\log_2(1/\varepsilon_{\mathrm{PA}})\,. \tag{5}$$

This numerical term is all that is left of the technicalities of unconditional security proofs. We give here only a very rapid sketch of its origin and refer to [29, 30] for all details. Eve's uncertainty is quantified by a generalized conditional entropy called smooth min-entropy and denoted $H_{\min}^{\bar{\varepsilon}}(X^{(n)}|E^{(N)})$. The parameter $\bar{\varepsilon}$ quantifies the 'smoothing': it is a parameter of the theory, whose value can be optimized numerically (see below).

The smooth min-entropy cannot be computed because it is virtually impossible to parameterize the most general state $\rho_{X^nY^nE^{(N)}}$ compatible with the few observed parameters. In a first step therefore, one estimates the deviation that is obtained assuming that the state consists of n independent realizations of a given single-copy state, i.e. $\rho_{X^nY^nE^{(N)}} = (\sigma_{XYE})^{\otimes n}$. In general, this estimate requires a de Finetti-type theorem [13], which leads however a very pessimistic overhead in finite-key analysis (though a recent new approach should provide a much tighter estimate [36]). For BB84 however, it turns out that no deviation is expected at all: because of the symmetry of the protocol, the state can be written as a convex combination of products of Bell states without loss of generality [12, 35]. The product form of the state being thus justified, it can further be proved that the smooth min-entropy is lower bounded by $n[S_\xi(X|E) - \delta]$, where δ is the first term of the sum in (5). The second term in the sum comes from the fact that, in the non-asymptotic case, the task of privacy amplification itself may fail with probability $\varepsilon_{\mathrm{PA}}$.

- Finally, $\mathrm{leak}_{\mathrm{EC}}$ replaces $H(X|Y)$ as the fraction to be removed in error correction. It is also well-known that practical error-correction codes do not reach the Shannon limit. Typically,

$$\mathrm{leak}_{\mathrm{EC}} \approx f_{\mathrm{EC}} H(X|Y) + \frac{1}{n}\log_2(2/\varepsilon_{\mathrm{EC}}), \tag{6}$$

where $f_{\mathrm{EC}} > 1$ depends on the code and $\varepsilon_{\mathrm{EC}}$ is the failure probability of the error-correction procedure. In a practical implementation, this quantity is a direct outcome of running the error-correcting code (although one must be careful in the case where a two-way error-correction code is actually used [38]).

Even if everything has been carried out 'perfectly', there is no such thing as perfect security. In our formalism, the security parameter ε has an operational meaning: it represents the maximum probability failure that is tolerated on the key extraction protocol (for instance, $\varepsilon = 10^{-10}$ can be loosely read as: 'one can distribute 10^{10} keys before something may go wrong'). With this interpretation, it is clear that the total security parameter is simply the sum of the probabilities of failures of each procedure described above, so that

$$\varepsilon = \varepsilon_{\mathrm{EC}} + \bar{\varepsilon} + n_{\mathrm{PE}}\,\varepsilon_{\mathrm{PE}} + \varepsilon_{\mathrm{PA}}, \tag{7}$$

where n_{PE} is the number of parameters that must be estimated (for simplicity, we set all the corresponding $\varepsilon_{\mathrm{PE}}$ as equal).

2.3. Putting finite-key bounds into practice

In the previous paragraph, we have sketched the elements that enter the calculation of the secret fraction r for BB84 coding in a finite-key scenario. A few remarks are needed to complete the

picture. First of all, the performance of an implementation is not quantified by r alone, but by the *secret-key rate*

$$K = \mathbf{R}\, r, \tag{8}$$

where $\mathbf{R}$ is the detection rate. In this paper, we use rates per sent qubit; the usual rates per second are obtained by multiplying our results with the frequency at which the source is operated.

An actual experiment is described by the following parameters:

- The user must set his/her desired bound ε on the total failure probability of the key distribution task: how often is one willing to tolerate the final outcome of the post-processing *not* being a perfect secret key.
- The post-processing code determines the size of the blocks on which privacy amplification is applied. This is the exact meaning of the parameter n: the length of the raw key as it is processed. Indeed, the raw key itself can be made longer by running the experiment for a longer time, but this mere fact cannot increase the security if the data are sliced and processed in blocks.
- The choice of an error-correcting code determines leak_{EC}, i.e. f_{EC} and ε_{EC}.

All the other parameters can be chosen to optimize K. The three auxiliary security parameters $\bar{\varepsilon}$, ε_{PE} and ε_{PA} are necessary in the derivation of the bound but need not be specified by the user. Their value can be optimized at the moment of computing r, under the constraints of being positive and satisfying (7). The parameters that enter in the design of the experiment, however, must obviously be chosen before the experiment is run. Explicitly, the flow of operations goes as follows:

1. Find n, f_{EC} and ε_{EC} as given by the chosen post-processing code; choose ε.
2. Provide *a priori* expected values of the parameters that are going to be measured: detection rate R, error rate in either basis e_X and e_Z, and others. Insert these expressions in the finite-key bound and optimize the design of the experiment: i.e. find the values of the light intensity I, of p_X and possibly of other quantities, that maximize K.
3. Run the experiment.
4. Insert the *measured* values $\{\mathbf{R}, \mathbf{e_X}, \mathbf{e_Z}, \ldots\}$ in the finite-key bound and run again the optimization of r over the ε's but using the value of I, p_X, etc used in the experiment—which may not be optimal for the measured values, especially if these differ significantly from the expected ones. This gives how much privacy amplification must be performed.
5. Run classical post-processing and obtain the secret key.

The procedure we have just sketched has been implicitly assumed in many previous papers, but to our knowledge has not been explicitly spelled out before. It is therefore worth while elaborating more on it, at the risk of some redundancy. Consider for instance the intensity I of the light source: it must obviously be chosen before the experiment is run. This choice involves an optimization between two effects: on the one hand, the detection rate (so the raw key length) will increase linearly with I; on the other hand, high I leads to some nuisances (e.g. Eve's information increases in prepare-and-measure schemes, or the error rate increases in entanglement-based schemes; see later). In order to find the optimal value of I, one has to provide some *a priori* expected expressions of the detection rate, Eve's information, error rate,

etc as functions of I. For instance, if, at the calibration stage, the transmission of the quantum channel and the efficiency of the detectors have been measured to be, respectively, t and η; then *a priori* one expects $R \approx I\, t\eta$.

Now, once the experiment is run, there is no guarantee that the measured **R** will be equal, or even close, to R: Eve's attack may introduce many more losses than expected. Actually, anything can happen: for instance, in an entanglement-based scheme, one may observe that the error rate does not vary with the intensity, if Eve decides to block all the multiple-pair pulses. We do not know *why* Eve would do that, just as we do not question why she has introduced a given amount of error and not more or less: the only thing we must ensure is that, given the *measured* parameters, Eve's information is always upper bounded. Of course, the value of I that we have chosen, and that would have been optimal in the expected conditions, may turn out to be seriously sub-optimal given the measured values. But again, this is perfectly fine: it just means that Eve's attack is too strong for any secrecy to be extractable.

In this paper, we take care of distinguishing clearly the security bounds, always formulated in terms of measured quantities and therefore applicable to any experiment, from the derived numerical bounds obtained using some *a priori* expected values.

In what follows, we provide the finite-key bounds (both the general expression and its numerical evaluations for *a priori* expected values) for different practical implementations of the BB84 coding.

3. Prepare-and-measure implementations with weak coherent pulses

3.1. Asymptotic bounds

3.1.1. Generalities. We consider a source producing a train of weak coherent pulses of average intensity μ; the following analysis is valid provided there is no phase coherence between successive pulses [39]. In this case, the signal sent by Alice can equivalently be described as a Poissonian distribution of Fock states, such that the probability of sending a k-photon pulse is

$$p_{\mathrm{A}}(k|\mu) = \mathrm{e}^{-\mu}\,\frac{\mu^k}{k!}\,. \tag{9}$$

Asymptotic bounds for unconditional security of such implementations have been derived using several approaches [40]–[42]; we refer to these papers and to section IV of [5] for all details. Without loss of generality, one can assume that (i) Eve learns the number of photons in each pulse and adapts her strategy to it, and (ii) Eve forwards single-photon signals to Bob. An important step in such proofs is the reduction, or 'squashing', of the state of the physical signal into a qubit. Specifically, one assumes that the measurement performed by the photon counters can be described by first squashing the signal on a finite-dimensional Hilbert space, then performing a measurement in this space [40]. When those proofs were proposed, the squashing property of detectors was conjectured; recently, this property has been proved to hold in the case of BB84 [43, 44].

The probability that Bob detects something, given that the pulse contained k photons, is given by $p_{\mathrm{B}}(k|\mu) = p_{\mathrm{A}}(k|\mu)\, f_k$, where f_k is the probability that Eve forwards a photon to Bob. Note that all the losses, both those due to the transmission line and those due to the detector efficiency, are included in f_k and are therefore given to Eve: this is the so-called uncalibrated-device scenario, the only one in which unconditional security can be proved as of

today [5, 43] and also justified by some clever realistic attacks [45]. The $p_{\mathrm{B}}(k|\mu)$ are submitted to the constraint that their sum must match the total observed detection rate:

$$\mathbf{R} = \sum_k p_{\mathrm{A}}(k|\mu)\, f_k\,. \tag{10}$$

It is customary to write

$$Y_k(\mu) = \frac{p_{\mathrm{A}}(k|\mu)\, f_k}{\mathbf{R}}. \tag{11}$$

Also, on k-photon pulses, Eve introduces the error rate $e_{X,Z}(k)$ in either basis. The measured error rates constrain these parameters to satisfy

$$\mathbf{e_{X,Z}} = \sum_k Y_k(\mu)\, e_{X,Z}(k)\,. \tag{12}$$

The set of f_k and $e_{X,Z}(k)$ fully parameterize Eve's attack.

Finally, under the additional assumption that Alice's and Bob's raw keys have maximal entropy (i.e. that the bit values 0 and 1 both occur with probability 1/2), the asymptotic expression for $S(A|E)$ for a given choice of μ is

$$S(A|E) = \min_{\mathrm{Eve}} \left\{ Y_0(\mu) + Y_1(\mu) \left[1 - h(e_X(1))\right] \right\}, \tag{13}$$

where h is binary entropy and the minimum must be taken over all possible choices of the f_k and the $e_{X,Z}(k)$ compatible with the measured parameters. Note that $\mathbf{e_Z}$ does not appear in Eve's information: this is a consequence of the fact that Eve's information on the Z basis is a function of the error introduced in the complementary basis[3]. Therefore, in discussing $S(A|E)$ and its finite-key correspondent $S_\xi(A|E)$, we do not mention $\mathbf{e_Z}$ any more.

3.1.2. Implementations without decoy states. In the case of implementations *without decoy states*, the optimal choice of parameters is given by $f_0 = 0$, $f_k = 1$ and $e_X(k) = 0$ for $k \geqslant 2$; the estimates $\tilde{Y}_1(\mu)$ and $\tilde{e}_X(1)$ are therefore fully determined by (10) and (12), leading to

$$S(A|E) \;=\; \tilde{Y}_1(\mu)\left[1 - h(\tilde{e}_X(1))\right], \;\text{ with }\; \tilde{Y}_1(\mu) = 1 - \frac{p_{\mathrm{A}}(k \geqslant 2|\mu)}{\mathbf{R}} \;\text{ and }\; \tilde{e}_X(1) = \frac{\mathbf{e_X}}{\tilde{Y}_1(\mu)}, \tag{14}$$

where obviously $p_{\mathrm{A}}(k \geqslant 2|\mu) = 1 - \mathrm{e}^{-\mu}(1+\mu)$.

3.1.3. Implementations with decoy states. Implementations *with decoy states* aim at estimating the f_k and $e_X(k)$ more directly [46]–[48]. For each pulse, Alice picks at random an intensity $\mu \in \{\mu_\gamma\}_{\gamma\in\Gamma}$ from a set of possible values (the protocol should specify *which* these values are and with what probability q_γ each one is chosen, but of course not which one will be used for each pulse). For the items in which Bob announces a detection, Alice reveals which μ_γ was used; she and Bob can therefore estimate parameters conditioned on this information. However, the parameters f_k and the $e_{X,Z}(k)$ that define Eve's attack must be the same for all μ_γ. Therefore,

[3] As well known, one must be careful in using this intuitive argument: in the case of the six-state protocol, for instance, $\mathbf{e_Z}$ does enter in the expression of Eve's information even for an asymmetric implementation, see e.g. appendix A of [5].

the constraints (10) and (12) become a set of $2|\Gamma|$ constraints

$$\mathbf{R}^{\gamma} = \sum_{k} p_{\mathrm{A}}(k|\mu_{\gamma})\, f_k, \tag{15}$$

$$\mathbf{e}_{\mathbf{X}}^{\gamma} = \sum_{k} Y_k(\gamma)\, e_X(k), \tag{16}$$

where $Y_k(\gamma) = p_{\mathrm{A}}(k|\mu_{\gamma})\, f_k/\mathbf{R}^{\gamma}$. Through this method, Eve's attack can in principle be exactly parameterized [48], but this requires $|\Gamma| = \infty$. However, only f_0, f_1 and $e_X(1)$ enter the expression (13) of $S(A|E)$, and it is evident that a pretty good estimate is already obtained with a few values of μ_{γ} [47]. Asymptotically,

$$S(A|E) \equiv S(A|E, \bar{\gamma}) = \tilde{Y}_0(\bar{\gamma}) + \tilde{Y}(\bar{\gamma}) \left[1 - h(\tilde{e}_X(1))\right], \tag{17}$$

where $\tilde{Y}_k(\gamma) = p_{\mathrm{A}}(k|\mu_{\gamma})\, \tilde{f}_k/\mathbf{R}^{\gamma}$ and where $\bar{\gamma}$ is defined as the value of γ that maximizes $K_{\gamma} = \mathbf{R}^{\gamma}[S(A|E, \gamma) - h(\mathbf{e}_{\mathbf{Z}}^{\gamma})]$. This is the case because, in the asymptotic regime, one can set $q_{\bar{\gamma}} \to 1$ and use the other intensities in a negligible fraction of cases. In the finite-key regime, this can no longer be the case: below, for simplicity, we shall consider the case where the key is extracted only out of one of the intensities.

3.1.4. An example of decoy states. For the explicit finite-key study below, we consider a specific choice of decoy state implementation, first studied in the pioneering paper by Wang [47]. The protocol uses *three intensities*, one of which is actually $\mu_{\emptyset} = 0$, while the other two are denoted μ_{I} and μ_{II} (we note here that, in theory, the condition $\mu = 0$ seems trivial to realize: just shut down the power or put an obstacle in the light path; but if the pulsing rate is required to be high, i.e. if the switch has to operate with high speed, it may actually be very difficult to shut down the power completely). The relations $\mu_{\mathrm{I}} \leqslant \mu_{\mathrm{II}}$ and $\mu_{\mathrm{I}} \mathrm{e}^{-\mu_{\mathrm{I}}} \leqslant \mu_{\mathrm{II}} \mathrm{e}^{-\mu_{\mathrm{II}}}$, i.e. $p_{\mathrm{A}}(0|\mathrm{I}) \geqslant p_{\mathrm{A}}(0|\mathrm{II})$ and $p_{\mathrm{A}}(1|\mathrm{I}) \leqslant p_{\mathrm{A}}(1|\mathrm{II})$, are assumed to be valid.

When $\mu = \mu_{\emptyset}$, all the pulses are empty so $p_{\mathrm{A}}(k|\emptyset) = \delta_{k,0}$ and one immediately obtains the estimates

$$\tilde{f}_0 = \mathbf{R}^{\emptyset}, \tilde{e}_X(0) = \mathbf{e}_{\mathbf{X}}^{\emptyset}. \tag{18}$$

The estimate for f_1 can be extracted using either $\mathbf{R}^{\gamma} = p_{\mathrm{A}}(0|\mu_{\gamma})\, \tilde{f}_0 + p_{\mathrm{A}}(1|\mu_{\gamma})\, \tilde{f}_1 + \mathbf{R}^{\gamma} \Delta^{\gamma}$ where Δ^{I} and Δ^{II} are given respectively by equations (13) and (15) of [47]; explicitly

$$\tilde{f}_1 = \frac{1}{\mu_{\mathrm{II}} - \mu_{\mathrm{I}}} \left[\mathbf{R}^{\mathrm{I}} \frac{\mu_{\mathrm{II}}}{p_{\mathrm{A}}(1|\mathrm{I})} - \mathbf{R}^{\mathrm{II}} \frac{\mu_{\mathrm{I}}}{p_{\mathrm{A}}(1|\mathrm{II})} \right] - \tilde{f}_0 \frac{\mu_{\mathrm{II}} + \mu_{\mathrm{I}}}{\mu_{\mathrm{II}} \mu_{\mathrm{I}}}. \tag{19}$$

To obtain an estimate for $e_X(1)$, we note that (16) becomes $\mathbf{e}_{\mathbf{X}}^{\gamma} = \tilde{Y}_0(\gamma)\, \tilde{e}_X(0) + \tilde{Y}_1(\gamma)\, \tilde{e}_X(1) + Y_{\Delta}(\gamma)\, \tilde{e}_X(\Delta, \gamma)$ where $Y_{\Delta}(\gamma) = \Delta^{\gamma}/\mathbf{R}^{\gamma}$. Now, the two $\tilde{e}_X(\Delta, \gamma)$ depend on γ and are unknown, but must be non-negative; this implies that the largest value of $\tilde{e}_X(1)$ is

$$\tilde{e}_X(1) = \min_{\gamma \in \{\mathrm{I}, \mathrm{II}\}} \left(\frac{\mathbf{e}_{\mathbf{X}}^{\gamma} - \tilde{Y}_0(\gamma)\, \tilde{e}_X(0)}{\tilde{Y}_1(\gamma)} \right). \tag{20}$$

3.2. Finite-key security bounds

In the previous paragraph, we have collected the necessary notations and the known asymptotic bounds. Note that the only quantity that varies according to the implementation is $S_{\xi}(X|E)$ and

the recipe to obtain it from the known asymptotic bounds $S(X|E)$ is straightforward: replace the estimate of each parameter by its worst-case value compatible with the deviation $\xi(m', d)$ given in (3). Here we derive $S_\xi(A|E)$ from $S(A|E)$, both for implementations without and with decoy states.

3.2.1. Implementations without decoy states: unconditional security bound. We have to identify which parameters are subject to statistical fluctuations among those that enter in equation (14):

- First we note that $\mathbf{R}$ is just the number of signals detected by Bob, N, divided by the number of signals sent by Alice, in the given run of the experiment. No statistical estimate is involved, therefore there is no fluctuation here. This statement may seem surprising. To understand it fully, one must come back to the difference between measured values and *a priori* expected values (end of section 2.3). Indeed, the *expected value* $R \approx \mu t \eta$ will surely be subject to fluctuations; but this just means that the observed value of $\mathbf{R}$ may differ from $\mu t \eta$. When assessing security, however, one must plug in the *measured* value, and there is no reason to burden this value with a fluctuation.
- The fraction $\tilde{Y}_1(\mu)$ is an estimate of the fraction of signals that reach Bob arising from a single-photon pulse; it depends explicitly on the probability that Alice's pulse contains more than two photons, and this quantity is obviously subject to fluctuations (by 'bad luck', Alice might have sent out only two-photon pulses!). All the N signals are involved in this estimate, which could in principle be done with a two-outcomes POVM ('$k < 2$' versus '$k \geqslant 2$'). Therefore, with probability $1 - \varepsilon_{\mathrm{PE}}$, the real $p_{\mathrm{A}}(k \geqslant 2)$ differs from the expected one $p_{\mathrm{A}}(k \geqslant 2|\mu)$ at most by $\xi(N, 2)$.
- The real error rate in X basis may deviate from the observed fraction of wrong events $\mathbf{e_X}$; because m signals are used for the measurement, the deviation is bounded by $\xi(m, 2)$.

In summary, there are two parameters subject to fluctuations ($n_{\mathrm{PE}} = 2$) and

$$S_\xi(A|E) = Y_1^{\mathrm{L}}(\mu)\left[1 - h(e_X^{\mathrm{U}}(1))\right] \tag{21}$$

with

$$Y_1^{\mathrm{L}}(\mu) = 1 - \frac{[1 - \mathrm{e}^{-\mu}(1+\mu)] + \xi(N, 2)}{\mathbf{R}} \quad \text{and} \quad e_X^{\mathrm{U}}(1) = \frac{\mathbf{e_X} + \xi(m, 2)}{Y_1^L(\mu)}. \tag{22}$$

Note that $Y_1^{\mathrm{L}}(\mu) = \tilde{Y}_1(\mu) - \frac{\xi(N,2)}{\mathbf{R}}$ and $e_X^{\mathrm{U}}(1) \approx \frac{\mathbf{e_X}+\xi(m,2)}{\tilde{Y}_1(\mu)} + \frac{\xi(N,2)}{\mathbf{R}} = \tilde{e}_X(1) + \frac{\xi(m,2)}{\tilde{Y}_1(\mu)} + \frac{\xi(N,2)}{\mathbf{R}}$. In particular, *two* finite-statistics effects provide corrections to the estimate of $e_X(1)$: the fact that the total error rate $\mathbf{e_X}$ was estimated on m samples and the fact that the fraction of single-photon pulses was inferred from N samples.

3.2.2. Implementations with decoy states: approximate bound. For decoy states protocols, three parameters have to be estimated, namely f_0, f_1 and $e_X(1)$; so $n_{\mathrm{PE}} = 3$. The recipe to obtain $S_\xi(A|E)$ from $S(A|E)$ is:

- In the first constraint (15), one introduces fluctuations to the $p_{\mathrm{A}}(k|\mu_\gamma)$, then solves the system of equations for the measured values $\mathbf{R}^\gamma$ and obtains the finite-key estimates for the f_k.
- One inserts these estimates into the second constraint (16), adds the fluctuations to the estimated error rates $\mathbf{e}_\mathbf{X}^\gamma$ and solves for the $e_X^{\mathrm{U}}(k)$.

While this second step is easy to implement, the first one is much harder and its full treatment goes beyond the scope of this paper[4]. Here we follow a simpler recipe: we solve first (15) without fluctuations, obtain the expressions for f_0 and f_1, then add a fluctuation to the $Y_k(\gamma) = p_A(k|\gamma) f_k$. Of course, having opted for this simplified treatment, we cannot claim unconditional security for the derived bound.

We particularize directly to the three-intensity protocol sketched above (section 3.1.4). Since the zero-pulse fractions $Y_0(\gamma)$ are estimated using only $\mu_\emptyset = 0$, and the POVM can be rendered by the two outcomes 'detection' versus 'no-detection', we have

$$Y_0^{\mathrm{L}}(\gamma) = \left[p_A(0|\gamma)\mathbf{R}^{\emptyset} - \xi(N_\emptyset, 2)\right] / \mathbf{R}^{\gamma} . \tag{23}$$

Similarly, once the parameter f_1 is estimated as (19), we obtain

$$Y_1^{\mathrm{L}}(\gamma) = \left[p_A(1|\gamma)\, \tilde{f}_1 - \xi(N_\gamma, 2)\right] / \mathbf{R}^{\gamma} \tag{24}$$

because all the N_γ signals are involved in the virtual two-outcome POVM 'less than two photons' versus 'two and more photons'. Finally, the recipe to obtain $e_X^{\mathrm{U}}(1)$ is the usual one: insert the finite estimates $Y_k^{\mathrm{L}}(\gamma)$ and increase the measured error rates by the corresponding fluctuations. For this last term, however, two points are worth noting. Firstly, the worst case fluctuation is the one that reduces $\mathbf{e}_{\mathbf{X}}^{\emptyset}$, because this amounts to increasing $e_X^{\mathrm{U}}(1)$. Secondly, all the $N_\emptyset$ events can be used to estimate this error rate: obviously, if Alice's pulse is empty, there is no difference between encoding in X or in Z; so Bob can assume that he has always used the 'right' basis to measure these signals. All in all,

$$e_X^{\mathrm{U}}(1) = \min_{\gamma \in \{\mathrm{I},\mathrm{II}\}} \left(\frac{e_X^{\gamma,\mathrm{U}} - Y_0^{\mathrm{L}}(\gamma)\, e_X^{\emptyset,\mathrm{L}}}{Y_1^{\mathrm{L}}(\gamma)} \right), \tag{25}$$

with $e_X^{\gamma,\mathrm{U}} = \mathbf{e}_{\mathbf{X}}^{\gamma} + \xi(m_\gamma, 2)$ and $e_X^{\emptyset,\mathrm{L}} = \mathbf{e}_{\mathbf{X}}^{\emptyset} - \xi(N_\emptyset, 2)$.

3.3. A priori expected values for experiment design

For simplicity in this paper we plot curves for a fixed value of N, the length of the unsifted key[5]. The expected values that we choose for our *a priori* expected values depend on the parameters t, the transmittivity of the channel Alice–Bob, η and p_{d}, the quantum efficiency and the dark count rate of Bob's detectors, respectively.

[4] Let us mention one of the reasons for such a complexity: while one has to consider f_0^L and f_1^L because of (17), it is not evident which fluctuation should be retained for the $f_{k\geqslant 2}$. In other words, given that the eavesdropper is allowed to take advantage of deviations from the Poissonian behavior, it is hard to quantify how Eve is going to redistribute the fluctuations removed from f_0 and f_1 among the other f_k's.

[5] We mentioned in section 2.3 that the parameter that really defines an experiment is n (the size of the blocks on which post-processing is applied) and not N. Of course, one could in principle run optimizations for fixed n; but this requires the introduction of additional assumptions. For instance, if only n is fixed and one sets $N = n/p_Z^2$, then the obvious optimal is $p_Z = 0$, i.e. $N = \infty$ signals are used, most of them to estimate the parameters. To avoid such situations, one may set $p_X \leqslant p_Z$. However, leaving aside that this choice is *a priori* arbitrary, the situation becomes even more complicated in decoy states: for instance, one must make sure that none of the intensities is used infinitely many times. To avoid such complications, we find it more clear in this paper to keep the number of detected quantum signals fixed. *A posteriori*, one always finds $n = Np_Z^2 \approx N - O(\sqrt{N})$.

The expected value of the detection rate we use is[6]

$$R(\mu) = 1 - (1 - 2p_{\mathrm{d}})\,\mathrm{e}^{-\mu t\eta} \tag{26}$$

Accordingly, error rates will be assumed to take the form

$$e_Z(\mu) \;=\; e_X(\mu) = \frac{\left(1 - \mathrm{e}^{-\mu t\eta}\right) Q \;+\; \mathrm{e}^{-\mu t\eta} p_{\mathrm{d}}}{R(\mu)}, \tag{27}$$

where Q, often called optical quantum bit error rate, is the error induced by the channel; in a depolarizing channel with visibility V, the BB84 coding leads to $Q = (1 - V)/2$.

3.3.1. Implementations without decoy states. We consider first implementations without decoy states. We have to optimize

$$K = R(\mu)\, p_Z^2 \left[S_\xi(A|E) - \Delta(n) - \mathrm{leak}_{\mathrm{EC}}(e_Z)\right] \tag{28}$$

for $S_\xi(A|E)$ given in (21), over μ and over the finite-key parameters. The result is shown in figure 1 for a choice of parameters corresponding to today's state-of-the-art. We see that at least $N \approx 10^7$ signals are required to extract a secret key. As for the optimal parameters: μ is found to be very close to the well-known value $t\eta$ [5, 38] irrespective of N; far from the critical distance, p_X is constant with the transmittivity and varies as $N^{-1/4}$, when $m \sim \sqrt{N}$.

3.3.2. Implementations with decoy states: case study. We turn now to implementations with decoy states. As we said, we consider the case where the key is extracted only out of the signals of intensity $\mu_{\mathrm{I}} < \mu_{\mathrm{II}}$. In this case, Alice can set $p_X(\mathrm{II}) = 1$: whenever she sends out a pulse of intensity μ_{II}, she can prepare it in the X basis because these pulses will anyway be used only for parameter estimation. Bob's value of p_X of course cannot depend on the intensities, and is supposed to be the same as the $p_X(\mathrm{I})$. The bound to be optimized therefore reads

$$K = q_{\mathrm{I}}\, R(\mu_I)\, p_Z(\mathrm{I})^2 \left[S_\xi(A|E, \mathrm{I}) - \Delta(n) - \mathrm{leak}_{\mathrm{EC}}(e_Z(\mathrm{I}))\right], \tag{29}$$

where $S_\xi(A|E, \mathrm{I}) = Y_0^{\mathrm{L}}(\mathrm{I}) + Y_1^{\mathrm{L}}(\mathrm{I})[1 - h(e_X^{\mathrm{U}}(1))]$ with the expressions (23)–(25). There is a new set of parameters that needs to be optimized, namely the probabilities q_γ of using each intensity. The results are plotted in figure 2. We observe that, as expected, the rates are much better than the ones obtained without decoy states. The optimal rates can actually be achieved by several pairs of $(\mu_{\mathrm{I}}, \mu_{\mathrm{II}})$; we fixed $\mu_{\mathrm{II}} = 0.65$ and further optimized μ_{I}: we found that $\mu_{\mathrm{I}} \approx 0.5$, independent of t and slightly depending on N. Again, far from the critical distance p_X varies as $N^{-1/4}$. More interesting is the behavior of the q_γ: q_{II} decreases with N, as expected; $q_\emptyset$, however, is nonzero only for $N = 10^{15}$. This behavior can be easily understood because the only role of the zero-intensity pulses is to provide an estimate of the dark counts. Now, on the one hand the dark count rate is small, so one needs many signals to estimate it conveniently; on the other hand, the benefit of subtracting the dark count contribution is rather small.

[6] In the expression of $R(\mu)$, we have neglected the contribution of double-clicks. This does not mean that double-clicks can just be neglected in an implementation (more in section 4). Actually, since our bounds are based on squashing, they must be replaced by a random bit and therefore contribute in a similar way to the dark counts. We neglect them in the *a priori* expected values because their contribution is numerically small.

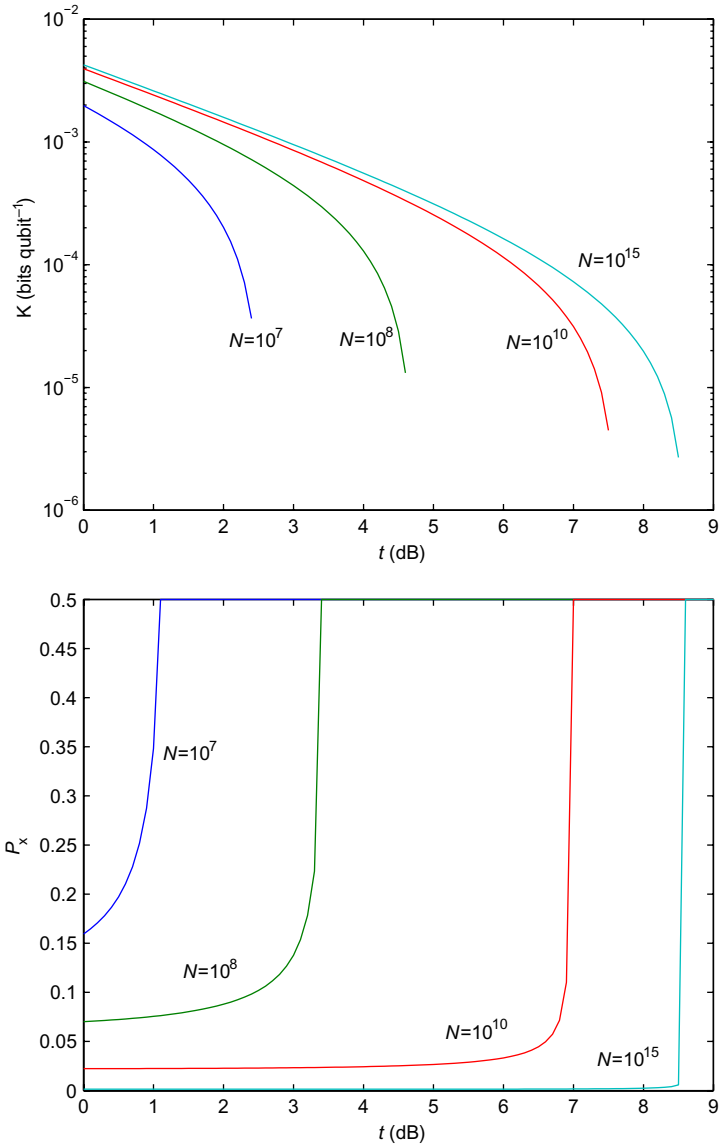

Figure 1. Finite-key study of implementations of BB84 with weak coherent pulses, without decoy states. As a function of the transmittivity of the channel t: upper graph, secret-key rate K from equation (28); lower graph: corresponding optimal value of p_X. Parameters: $\varepsilon = 10^{-5}$, $\varepsilon_{\mathrm{EC}} = 10^{-10}$, $\mathrm{leak}_{\mathrm{EC}}(e) = 1.05\, h(e)$, $Q = 0.5\%$, $\eta = 0.1$ and $p_{\mathrm{d}} = 10^{-5}$.

Finally, we compare our results with previous estimates available in the literature. The very first papers on decoy states realized the importance of taking statistical fluctuations of the parameters into account [24, 25, 47]. These works differ from ours, in that they assume a normal distribution for the fluctuations (see section 2.2); moreover, they do not have the finite-key correction $\Delta(n)$ and are therefore, strictly speaking, not providing lower bounds (neither were they claiming it, of course). However, their final estimates ultimately agree very well with ours. For instance, they had estimated that $N \approx 10^{9}$–10^{10} is a 'reasonable number of signals' and we arrive close to the asymptotic bound for similar values. More specifically, our plots for

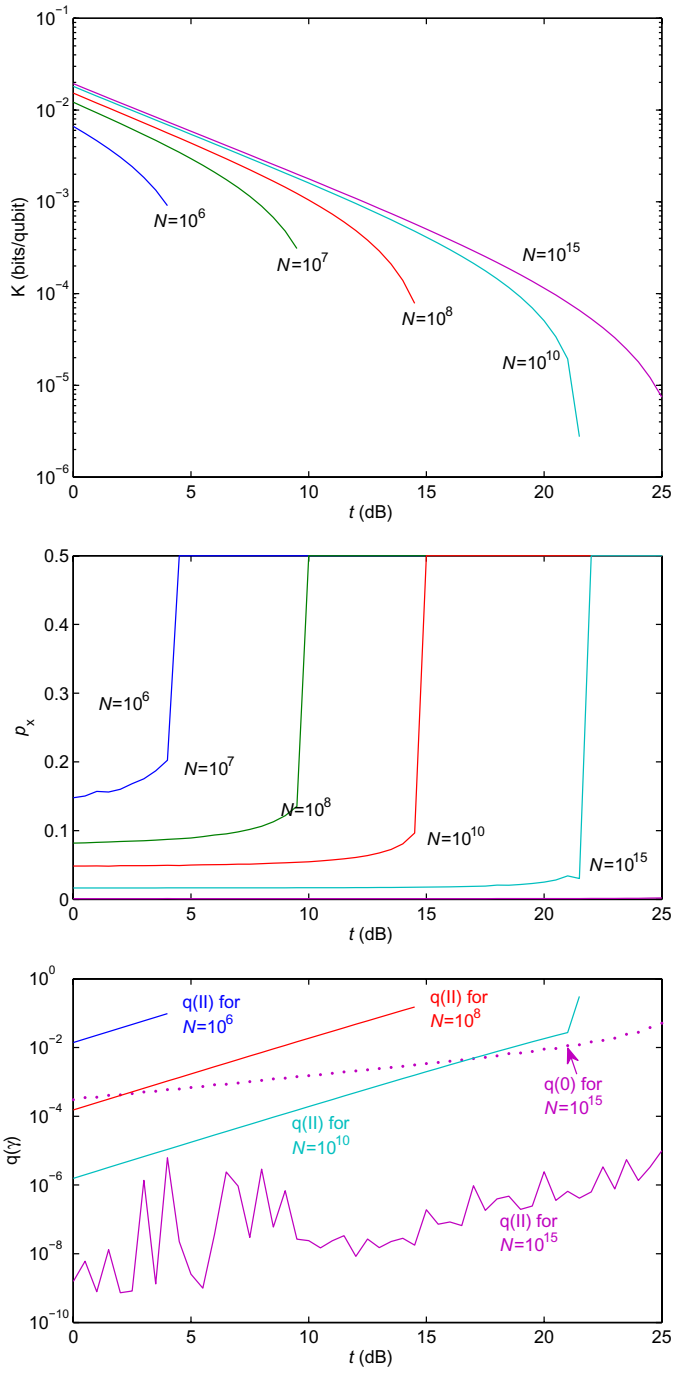

Figure 2. Finite-key study of implementations of BB84 with weak coherent pulses for the three-intensity decoy state protocol described in the text and assuming that only the intensity μ_1 is used for the key. As a function of the transmittivity of the channel t: upper graph, secret-key rate K from equation (29); middle graph: corresponding optimal values of p_X; lower graph: corresponding values of $q_\emptyset$ and q_{II} (regarding the large fluctuations in q_{II} for $N = 10^{15}$: we have not tried to optimize with further precision, given that the value is anyway $q_{\mathrm{II}} \sim 10^{-7}$). Parameters as in figure 1: $\varepsilon = 10^{-5}$, $\varepsilon_{\mathrm{EC}} = 10^{-10}$, $\mathrm{leak}_{\mathrm{EC}}(e) = 1.05\, h(e)$, $Q = 0.5\%$, $\eta = 0.1$ and $p_{\mathrm{d}} = 10^{-5}$.

the achievable secret key rate are in remarkable agreement with those obtained in [24], once some differences in the choice of the numerical values of parameters are taken into account. Of course, due to the different way fluctuations are introduced, some details differ. For instance, Ma *et al* [24] found the optimal value of $q_\emptyset$ to be approximately 4×10^{-2} already at $N = 10^{10}$, while, as stressed just above, this value is zero in our approach for the same N. However, the discrepancy seems to be restricted to the choice of *optimal* values for quantities that are anyway small; whence a suboptimal choice does not have a significant influence on the total result.

More recently, Hayashi and co-workers [31] have provided another approach to compute a lower bound for decoy state protocols. When compared to ours, a striking fact is that they obtain a non-negligible finite-key rate for N as small as 10^4 [31], while we do not obtain any key for $N < 10^6$ signals. The comparison is not straightforward, since they are considering another decoy state protocol and the values of the parameters are different; nevertheless, their results suggest that our bounds might be improved.

4. Entanglement-based implementations

4.1. Asymptotic bounds

At the time of writing, two asymptotic bounds are available for unconditional security of an entanglement-based implementation of the BB84 coding (BBM92 protocol). Under the squashing model for Bob's detectors, whose validity has been proved for BB84 coding [43, 44], Ma *et al* [49] proved

$$S(A|E) = 1 - h(\mathbf{e}_\mathbf{X}) \,. \tag{30}$$

This means that, even if the source is not a single-pair source, all its imperfections are taken into account in the measured error rate, a feature anticipated by Koashi and Preskill [50]. This result is remarkable, since it is formally identical to the one obtained for single-photon sources. As such, for the finite key-bound within our formalism we can refer to [29].

More recently, Koashi and co-workers have proved a different bound [51], which differs in the treatment of double-click events. In squashing, a physical double-click event is taken into account by adding a random bit to the raw key; the fraction of such events does not need to be measured. In the present approach, the double-click events are deleted from the raw key but their fraction δ_{2c} is estimated. Let $\mathbf{R}$ be the detection rate including double clicks, which is also the detection rate in the squashing model; and let $\mathbf{R}'$ be the rate obtained once double-click events are removed (i.e. $\mathbf{R} - \mathbf{R}'$ is the measured number of double clicks). Asymptotically one has the exact estimate

$$\delta_{2c} = \frac{\mathbf{R} - \mathbf{R}'}{\mathbf{R}} \,. \tag{31}$$

The error rates observed in the raw key for the present approach are written $\mathbf{e}'_\mathbf{X}$ and $\mathbf{e}'_\mathbf{Z}$; they are related to the error rates that would be obtained by processing the same data with the squashing model through

$$\mathbf{e}_{\mathbf{X},\mathbf{Z}} = (1 - \delta_{2c})\, \mathbf{e}'_{\mathbf{X},\mathbf{Z}} + \delta_{2c}/2. \tag{32}$$

In particular, in the case where the $\mathbf{e}'_{\mathbf{X},\mathbf{Z}}$ are very small (e.g. for very high optical visibility), the present approach shows basically no errors. Specifically, let $F(\delta_{2c}) \equiv (1 - 4\delta_{2c})/(1 - \delta_{2c})$: for

$\mathbf{e}'_{\mathbf{X}} \lesssim 0.08\, F(\delta_{2c})$ one has[7]

$$S(A|E) = F(\delta_{2c}) \left[1 - h\left(\frac{\mathbf{e}'_{\mathbf{X}}}{F(\delta_{2c})}\right)\right]. \tag{33}$$

Indeed, in the regime of small errors, the asymptotic secret-key rate K computed with (33) is larger than the one computed from (30). However, the former implies the estimation of an additional parameter, namely δ_{2c}. It is therefore interesting to compare the two approaches in the finite-key scenario.

4.2. Finite-key security bounds and a priori expected values

The finite-key secret-key rate associated with the first approach (30) is

$$K = \mathbf{R}\, p_Z^2 \left[1 - h(e_X^{\mathrm{U}}) - \Delta(n) - \mathrm{leak}_{\mathrm{EC}}(\mathbf{e_Z})\right] \tag{34}$$

with $e_X^{\mathrm{U}} = \mathbf{e_X} + \xi(m, 2)$. As in the case of single-photon sources, the only parameter that needs to be estimated is the error rate (so $n_{\mathrm{PE}} = 1$). Similarly, for the second approach (33) one obtains

$$K = \mathbf{R}'\, p_Z^2 \left\{F(\delta_{2c}^{\mathrm{U}}) \left[1 - h\left(\frac{e'^{\mathrm{U}}_X}{F(\delta_{2c}^{\mathrm{U}})}\right)\right] - \Delta(n) - \mathrm{leak}_{\mathrm{EC}}(\mathbf{e}'_{\mathbf{Z}})\right\} \tag{35}$$

with $e'^{\mathrm{U}}_X = \mathbf{e}'_{\mathbf{X}} + \xi(m, 2)$ and $\delta_{2c}^{\mathrm{U}} = (\mathbf{R} - \mathbf{R}')/(\mathbf{R}) + \xi(N, 2)$. Obviously here $n_{\mathrm{PE}} = 2$.

In order to compare the two approaches *a priori*, we need to insert an expected value of the measured parameters and run the optimization over the free parameters left. We consider an implementation with continuous-wave pumping, following paragraph VII.A.1 of [5], where all details can be found; for a more detailed description, see [49], especially equations (9) and (10). The pump intensity is such that μ' pairs are produced within the coincidence window $\Delta\tau$; we work in the limit $y \equiv \mu'\Delta\tau \ll 1$ and neglect dark counts on Alice's side. Therefore, whenever Alice detects a photon, which happens with probability $\approx y$, the signal traveling to Bob is distributed according to $p_{\mathrm{A}}(1) \approx 1$, $p_{\mathrm{A}}(2) \approx y$ and $p_{\mathrm{A}}(n > 2) \approx 0$. The expected values for the single-click rate R_{1c} and the corresponding error rate Q are given by

$$R_{1c}/y = R_{\mathrm{p}}/y + R_{\mathrm{d}}/y \approx t\eta\,[p_{\mathrm{A}}(1) + p_{\mathrm{A}}(2)(2 - t\eta)] + 2p_{\mathrm{d}}\left[p_{\mathrm{A}}(1)(1 - t\eta) + p_{\mathrm{A}}(2)(1 - t\eta)^2\right], \tag{36}$$

$$Q = [(1 - V + y)R_{\mathrm{p}} + R_{\mathrm{d}}]/2R_{1c} \tag{37}$$

(note the presence of the two-pair fraction y as a linear decrease in the observed two-photon visibility V). The detection rate of double clicks is

$$R_{2c}/y = p_{\mathrm{A}}(2)\frac{1}{2}(t\eta)^2 + [p_{\mathrm{A}}(1) + p_{\mathrm{A}}(2)(1 - t\eta)][t\eta p_{\mathrm{d}} + (1 - t\eta)p_{\mathrm{d}}^2]. \tag{38}$$

So we have the *a priori* expected values $R = R_{1c} + R_{2c}$, $R' = R_{1c}$ and $\delta_{2c} = R_{2c}/(R_{1c} + R_{2c})$. As for the error rates, we identify $e'_X = e'_Z = Q$, when (32) implies $e_X = e_Z = (1 - \delta_{2c})\, Q + \delta_{2c}/2$.

[7] At this stage, it is useful to explain some differences in notation between us and [51]. Our $\mathbf{e}'_{\mathbf{X}}$ and $\mathbf{e}'_{\mathbf{Z}}$ are the error rates in the raw key, i.e. with the double-click events already removed; Koashi and co-workers assume $\mathbf{e}'_{\mathbf{X}} = \mathbf{e}'_{\mathbf{Z}} = \epsilon/(1 - \delta)$. Our expression (33) is obtained by inserting equation (20) into $1 - \tau(\delta, \epsilon)/(1 - \delta)$ from equation (3). Indeed, in our case $S(A|E)$ is Eve's uncertainty per bit of the raw key; the global factor $(1 - \delta)$ will be accounted for in the detection rate $\mathbf{R}'$ defined below.

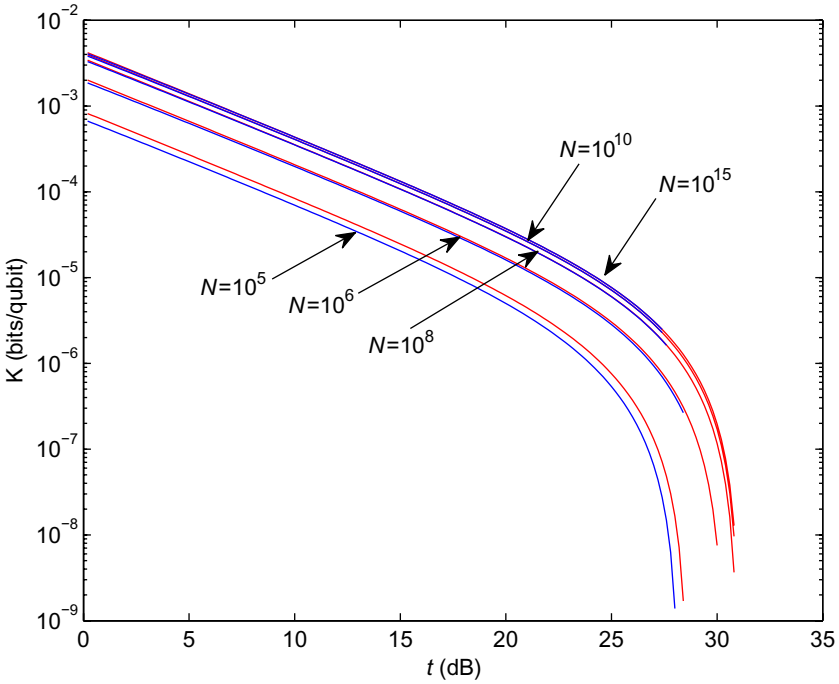

Figure 3. Key rate K as a function of the attenuation t for entanglement-based implementations of the BB84 coding. Red curves: bound with squashing (34), adapted from the asymptotic bound of [49]. Blue curves: bound with estimate of double-clicks (35), adapted from the asymptotic bound of [51]. Parameters as in figures 1 and 2: $\varepsilon = 10^{-5}$, $\varepsilon_{\mathrm{EC}} = 10^{-10}$, $\mathrm{leak}_{\mathrm{EC}}(e) = 1.05\, h(e)$, $V = 0.99$ (corresponding to $Q = 0.5\%$ if one neglects the effect of double pairs), $\eta = 0.1$ and $p_{\mathrm{d}} = 10^{-5}$.

The result of the numerical optimization over y and the finite-key parameters is shown in figure 3. As expected, for small numbers of signals the squashing bound outperforms the double-click one, because the latter needs to estimate a second parameter. For larger numbers of signals, the two bounds give identical rates (the very small difference can be attributed to our approximations, like neglecting the cases when $n > 2$ pairs are created). The values of y and p_X are also basically identical for both bounds. As observed in the prepare-and-measure schemes, y varies little with N ($y \approx 0.05$ for $N = 10^5$, $y \approx 0.1$ for large N), while p_X scales as $\sim N^{-1/4}$.

5. Conclusion

In summary, we have provided security bounds for keys of finite length for several practical implementations of the BB84 coding. The bounds for prepare-and-measure implementations without decoy states and for entanglement-based implementations guarantee unconditional security; the bound for prepare-and-measure implementations with decoy states has been derived using a simplified treatment of the statistical fluctuations.

We have computed these bounds for *a priori* expected values of the parameters that will be observed, thus providing some guidelines for the design of experiments. In all cases, for $N \gtrsim 10^{15}$, we recover the asymptotic bounds (compare e.g. with the plots in [5]). However,

prepare-and-measure implementations based on weak coherent pulses seem to require at least $N \sim 10^7$ signals to produce a key; while implementations using entangled states, similarly to the ideal single-photon case, provide a key already for $N \sim 10^5$.

Let us conclude with a critical review of the possible extensions and open issues. The bounds presented in this paper have been derived under some assumptions. Some of them are assumptions on Alice and Bob, mostly inherited from the asymptotic studies from which $S(A|E)$ was obtained. Specifically:

- First, we recall that, in the case of decoy states, we have used a partial treatment of the statistical fluctuations; also, we have provided an actual bound only for a specific choice (one intensity for the key signals, two for the decoys, one of which being zero).
- In all weak coherent pulses implementations we have supposed that there is no phase coherence between successive pulses; in the case of entanglement-based schemes, we have assumed continuous pumping.
- All the bounds we used assume that the bit values '0' and '1' appear the same number of times in both Alice's and Bob's raw keys. A systematic deviation from this assumption is expected if the detectors have different efficiencies, which is often the case in practice. The tools to study this case are available in the asymptotic scenario [52], their finite-key generalization should be the object of further work. Of course, in the case where one bit value is more frequent than the other, a conservative security bound is obtained by adding the number of excess bits to the information of Eve to be removed during privacy amplification; therefore one can use our formulae with this modification.
- The prepare-and-measure bounds given above are not valid for plug-and-play configurations, even if the difference is ultimately expected to be small. The reason is that the 'source' on Alice's side cannot be assumed to produce exact weak coherent pulses, because these pulses are obtained by attenuating an in principle unknown strong incoming signal. An asymptotic bound for unconditional security of plug-and-play configurations has been given in [53]. Its generalization to finite keys may be done by following the same procedure as in this paper.
- When we provide *a priori* expected values, we have always performed an optimization over p_X. Some systems may be such that this optimization cannot be easily performed (e.g. in a passive detection setup, one would have to change the beam-splitter that chooses between the bases).

A second group of assumptions is related to the fact that our bounds may be the object of improvements:

- First of all, the fact of having used the formalism developed in [29, 30] guarantees unconditional security, but it is not known whether the bounds are tight. Indeed, all the different approaches to security are known to coincide in the asymptotic regime, but this is not yet clear for the finite-key regime—and we hinted in section 3.3.2 at an actual discrepancy between ours and other estimates in the case of decoy states implementations. Most of the information-theoretical estimates are generally regarded to be tight [13]; however, we have bounded statistical fluctuations using absolute errors (3); improvements may be obtained by using relative errors.
- We have computed the security bounds for the case when the extraction of the secret key is done through one-way post-processing without pre-processing. In principle, the tools

are available to compute finite-key bounds for two-way post-processing and including pre-processing [30]. For typical error rates, the improvements are supposed to be significant only close to the critical distance.

- For simplicity, we have considered asymmetric implementations of the BB84 coding, in which the Z basis is used for the key and the X basis for parameter estimation. If both bases are used for the key (while each basis serves to estimate Eve's attack on the other), one obtains similar more complicated expressions, but basically (assuming $p_X \leqslant p_Z$) the effect is to increase K by a factor $1 + (p_X/p_Z)^2$. A similar argument can be made in the case of decoy states protocols, where we have assumed for simplicity that only one intensity is used for the key.

Acknowledgments

We thank all the participants of the workshop 'Quantum cryptography with finite resources' (Singapore, 4–6 December 2008) for very valuable comments. We are grateful to Hongwei Li (USTC, Hefei, China) for bringing to our attention the possibility of improving the estimate given in equation (3). This work was supported by the National Research Foundation and the Ministry of Education, Singapore.

References

[1] Bennett C and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* (*Bangalore, India, December 1984*) pp 175–9
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[4] Dušek M, Lütkenhaus N and Hendrych M 2006 *Progress in Optics* vol 49, ed E Wolf (Amsterdam: Elsevier) p 381
[5] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2008 arXiv:0802.4155
[6] Lo H-K and Zhao Y 2008 arXiv:0803.2507
[7] Mayers D 1996 *Advances in Cryptology—Proceedings of Crypto '96* (Berlin: Springer) p 343
[8] Lo H-K and Chau H F 1999 *Science* **283** 2050
[9] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[10] Mayers D 2001 *J. ACM* **48** 351 (arXiv:quant-ph/9802025)
[11] Ben-Or M 2002 *Security of BB84 QKD Protocol* Slides available at http://www.msri.org/publications/ln/msri/2002/quantumintro/ben-or/2/
[12] Kraus B, Gisin N and Renner R 2005 *Phys. Rev. Lett.* **95** 080501
Renner R, Gisin N and Kraus B 2005 *Phys. Rev.* A **72** 012332
[13] Renner R 2008 Security of quantum key distribution *PhD Thesis* Diss. ETH No. 16242
Renner R 2008 *Int. J. Quantum Inf.* **6** 1
[14] Koashi M 2006 *J. Phys. Conf. Ser.* **36** 98
[15] Kurtsiefer C, Zarda P, Mayer S and Weinfurter H 2001 *J. Mod. Opt.* **48** 2039
[16] Makarov V and Hjelme D R 2005 *J. Mod. Opt.* **52** 691
Makarov V, Anisimov A and Skaar J 2006 *Phys. Rev.* A **74** 022313
[17] Zhao Y, Fung C-H F, Qi B, Chen C and Lo H-K 2008 *Phys. Rev.* A **78** 042333
[18] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
[19] Pironio S, Acín A, Brunner N, Gisin N, Massar S and Scarani V 2009 *New J. Phys.* **11** 045021
[20] Inamori H, Lütkenhaus N and Mayers D 2007 *Eur. J. Phys.* D **41** 599 (arXiv:quant-ph/0107017)

[21] Ben-Or M, Horodecki M, Leung D W, Mayers D and Oppenheim J 2005 *Second Theory of Cryptogr. Conf. TCC (Lecture Notes in Computer Science* vol 3378) (Berlin: Springer) pp 386–406 (arXiv:quant-ph/0409078)
[22] König R, Renner R, Bariska A and Maurer U 2007 *Phys. Rev. Lett.* **98** 140502
[23] Lo H-K, Chau H F and Ardehali M 2005 *J. Cryptol.* **18** 133 (arXiv:quant-ph/9803007)
[24] Ma X, Qi B, Zhao Y and Lo H-K 2005 *Phys. Rev.* A **72** 012326
[25] Wang X-B 2005 *Phys. Rev. Lett.* **94** 230503
[26] Meyer T, Kampermann H, Kleinmann M and Bruß D 2006 *Phys. Rev.* A **74** 042340
[27] Hayashi M 2007 *Phys. Rev.* A **76** 012329
[28] Hasegawa J, Hayashi M, Hiroshima T, Tanaka A and Tomita A 2007 arXiv:0705.3081
[29] Scarani V and Renner R 2008 *Phys. Rev. Lett.* **100** 200501
[30] Scarani V and Renner R 2008 *Proc. TQC2008 (Lecture Notes in Computer Science* vol 5106*)* (Berlin: Springer) pp 83–95 (arXiv:0806.0120)
[31] Hasegawa J, Hayashi M, Hiroshima T and Tomita A 2007 arXiv:0707.3541
[32] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[33] Devetak I and Winter A 2005 *Proc. R. Soc.* A **461** 207
[34] Hayashi M 2009 *Phys. Rev.* A **79** 020303
[35] Gottesman D and Lo H-K 2003 *IEEE Trans. Inf. Theory* **49** 457
[36] Christandl M, König R and Renner R 2009 *Phys. Rev. Lett.* **102** 020504
[37] Cover T M and Thomas J A 1991 *Elements of Information Theory Wiley Series in Telecommunications* (New York: Wiley)
[38] Lütkenhaus N 1999 *Phys. Rev.* A **59** 3301
[39] Lo H-K and Preskill J 2007 *Quantum Inf. Comput.* **8** 431
[40] Gottesman D, Lo H-K, Lütkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[41] Fung C-H F, Tamaki K and Lo H-K 2006 *Phys. Rev.* A **73** 012337
[42] Kraus B, Branciard C and Renner R 2007 *Phys. Rev.* A **75** 012316
[43] Beaudry N J, Moroder T and Lütkenhaus N 2008 *Phys. Rev. Lett.* **101** 093601
[44] Tsurumaru T and Tamaki K 2008 *Phys. Rev.* A **78** 032302
[45] Makarov V, Anisimov A and Sauge S 2008 arXiv:0808.3408
[46] Hwang W-Y 2003 *Phys. Rev. Lett.* **91** 057901
[47] Wang X-B 2005 *Phys. Rev. Lett.* **94** 230503
[48] Lo H-K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[49] Ma X, Fung C-H F and Lo H-K 2007 *Phys. Rev.* A **76** 012307
[50] Koashi M and Preskill J 2003 *Phys. Rev. Lett.* **90** 057902
[51] Koashi M, Adachi Y, Yamamoto T and Imoto N 2008 arXiv:0804.0891
[52] Fung C-H F, Tamaki K, Qi B, Lo H-K and Ma X 2009 *Quantum Inf. Comput.* **9** 131
[53] Zhao Y, Qi B and Lo H-K 2008 *Phys. Rev.* A **77** 052327