Tight Finite-Key Analysis for Quantum Cryptography

Tomamichel, Marco; Lim, Ci Wen; Gisin, Nicolas; Renner, Renato

Tight Finite-Key Analysis for Quantum Cryptography

Marco Tomamichel,[1, *] Charles Ci Wen Lim,[2, †] Nicolas Gisin,[2] and Renato Renner[1]

[1] *Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland*
[2] *Group of Applied Physics, University of Geneva, 1211 Geneva, Switzerland*

Despite enormous progress both in theoretical and experimental quantum cryptography, the security of most current implementations of quantum key distribution is still not established rigorously. One of the main problems is that the security of the final key is highly dependent on the number, M, of signals exchanged between the legitimate parties. While, in any practical implementation, M is limited by the available resources, existing security proofs are often only valid asymptotically for unrealistically large values of M. Here, we demonstrate that this gap between theory and practice can be overcome using a recently developed proof technique based on the uncertainty relation for smooth entropies. Specifically, we consider a family of Bennett-Brassard 1984 quantum key distribution protocols and show that security against general attacks can be guaranteed already for moderate values of M.

I. INTRODUCTION

Quantum Key Distribution (QKD), invented by Bennett and Brassard [1] and by Ekert [2], can be considered the first application of quantum information science, and commercial products[1] have already become available. Accordingly, QKD has been an object of intensive study over the past few years. On the theory side, the security of various variants of QKD protocols against general attacks has been proved [3–8]. At the same time, experimental techniques have reached a state of development that enables key distribution at MHz rates over distances of 100 km [9–11].

Despite these developments, there is still a large gap between theory and practice, in the sense that the security claims are based on assumptions that are not (or cannot be) met by experimental implementations. For example, the proofs often rely on theoretical models of the devices (such as photon sources and detectors) that do not take into account (experimentally unavoidable) imperfections (see [12] for a discussion).

In this work, we focus on the *asymptotic resource assumption*, i.e., the assumption that an arbitrarily large number M of signals can be exchanged between the legitimate parties and used for the computation of the final key. This assumption is quite common in the literature, and security proofs are usually only valid asymptotically as M tends to infinity. However, the asymptotic resource assumption cannot be met by practical realizations—in fact, the key is often computed from a relatively small number of signals ($M \ll 10^6$). This problem has recently received increased attention and explicit bounds on the number of signals required to guarantee security have been derived [13–19].

In this work, we apply a novel proof technique [20] to derive almost tight bounds on the minimum value M required to achieve a given level of security. The technique is based on an entropic formulation of the uncertainty relation [21] or, more precisely, its generalization to smooth entropies [20]. Compared to preexisting methods, our technique is rather direct. It therefore avoids various estimates that have previously led to too pessimistic bounds. Roughly speaking, our result is a lower bound on the achievable key rate which deviates from the asymptotic result (where M is infinitely large) only by terms that are caused by (probably unavoidable) statistical fluctuations in the parameter estimation step. An important additional feature of our technique is that the

[*] marcoto@phys.ethz.ch
[†] ciwen.lim@unige.ch
[1] Among the companies that are active in this field are ID Quantique and MagiQ Technologies Inc.

resulting security claims are robust against imperfections of the devices used to handle quantum states.

Our paper is organized as follows. In Section II, we state composable definitions for correctness and secrecy of QKD schemes. In Section III, we introduce the family of BB84-type protocols to which our analysis applies. Our main technical contribution, a finite-size security analysis against the most general attacks, is given in Section IV. The achievable secret key rates are then discussed and compared to previous results in Section V.

II. SECURITY OF QKD PROTOCOLS

We follow the discussion of composable security outlined in [22] and first take an abstract view on QKD protocols. A QKD protocol describes the interaction between two players, Alice and Bob. Both players have access to an insecure quantum channel as well as an authenticated (but otherwise insecure) classical channel.[2] Moreover, Alice and Bob can each generate fresh randomness.

The QKD protocol outputs a key, $\mathbf{S}$, on Alice's side and an estimate of that key, $\hat{\mathbf{S}}$, on Bob's side. This key is usually an ℓ-bit string, where ℓ, depends on the noise level of the channel, as well as the security and correctness requirements on the protocol. The protocol may also abort, in which case we set $\mathbf{S} = \hat{\mathbf{S}} = \perp$.

In the following, we define what it means for a QKD protocol to be *secure.* Roughly speaking, the protocol has to (approximately) satisfy two criteria, called *correctness* and *secrecy.* These criteria are conditions on the probability distribution of the protocol output, $\mathbf{S}$ and $\hat{\mathbf{S}}$, as well as the information leaked to an adversary, E. These depend, in general, on the attack strategy of the adversary, who is assumed to have full control over the quantum channel connecting Alice and Bob, and has access to all messages sent over the authenticated classical channel.

Definition 1. A QKD protocol is called *correct* if, for any strategy of the adversary, $\hat{\mathbf{S}} = \mathbf{S}$. It is called ϵ_{cor}-*correct* if it is ϵ_{cor}-indistinguishable from a correct protocol. In particular, a protocol is ϵ_{cor}-correct if $\Pr[\hat{\mathbf{S}} \neq \mathbf{S}] \leq \epsilon_{\text{cor}}$.

In order to define the secrecy of a key, we consider the quantum state $\rho_{\mathbf{S}\mathrm{E}}$ that describes the correlation between Alice's classical key $\mathbf{S}$ and the eavesdropper, E (for any given attack strategy). A key is called Δ-*secret* from E if it is Δ-close to a uniformly distributed key that is uncorrelated with the eavesdropper, i.e. if

$$\min_{\sigma_{\mathrm{E}}} \frac{1}{2} \| \rho_{\mathbf{S}\mathrm{E}} - \omega_{\mathbf{S}} \otimes \sigma_{\mathrm{E}} \|_1 \leq \Delta \,,$$

where $\omega_{\mathbf{S}}$ denotes the fully mixed state on $\mathbf{S}$. For a motivation and discussion of this particular secrecy criterion (in particular the choice of the norm) we refer to [23].

Definition 2. A QKD protocol is called *secret* if, for any attack strategy, $\Delta = 0$ whenever the protocol outputs a key. It is called ϵ_{sec}-*secret* if it is ϵ_{sec}-indistinguishable from a secret protocol. In particular, a protocol is ϵ_{sec}-secret if it outputs Δ-secure keys with $(1 - p_{\text{abort}})\Delta \leq \epsilon_{\text{sec}}$, where p_{abort} is the probability that the protocol aborts.[3]

In some applications it is reasonable to consider correctness and secrecy of protocols separately, since there may be different requirements on the correctness of the key (i.e., that Bob's key agrees

[2] Using an authentication protocol, any insecure channel can be turned into an authentic channel. The authentication protocol will however use some key material, as discussed in [22].

[3] To see that this suffices to ensure ϵ_{sec}-indistinguishability, note that the secrecy condition is trivially fulfilled if the protocol aborts.

with Alice's, implying that messages encrypted by Alice are correctly decrypted by Bob) and secrecy. In fact, in many realistic applications, an incorrect decoding of the transmitted data would be detected so that the data can be resent. For such applications, ϵ_{cor} may be chosen larger than ϵ_{sec}.

However, secrecy of the protocol alone as defined above does not ensure that Bob's key is secret from the eavesdropper as well. One is thus often only interested in the overall security of the protocol (which automatically implies secrecy of Bob's key).

Definition 3. A QKD protocol is called *secure* if it is correct and secret. It is called ϵ-*secure* if it is ϵ-indistinguishable from a secure protocol. In particular, a protocol is ϵ-secure if it is ϵ_{cor}-correct and ϵ_{sec}-secret with $\epsilon_{\mathrm{cor}} + \epsilon_{\mathrm{sec}} \leq \epsilon$.

Finally, the robustness, ϵ_{rob}, is the probability that the protocol aborts even though the eavesdropper is inactive.[4] Note that a trivial protocol that always aborts is secure according to the above definitions, and a robustness requirement is therefore necessary. In this work, we include the robustness ϵ_{rob} in our estimate for the expected key rate (when the eavesdropper is inactive) and then optimize over the protocol parameters to maximize this rate (see Section V).

III. THE PROTOCOLS

For the purpose of the following discussions, we consider the well known BB84 protocol [1]. However, the considerations are rather general and can be extended to similar *prepare-and-measure* protocols.

Recall that Alice and Bob are connected by an insecure quantum channel. On one side of this channel, Alice controls a device allowing her to prepare certain states of a two-level quantum system (a qubit).[5] Let $\mathbb{X}$ be an orthonormal basis of the two-dimensional Hilbert space describing Alice's system and let $\mathbb{Z}$ be the corresponding diagonal basis. We characterize the quality of Alice's device by the maximum fidelity it allows between states prepared in the $\mathbb{X}$ basis and states prepared in the $\mathbb{Z}$ basis. Namely, we define the *preparation quality*, $q = -\log \max |\langle \psi_x | \psi_z \rangle|^2$, where the maximization is over all states ψ_x and ψ_z prepared in the $\mathbb{X}$ and $\mathbb{Z}$ basis, respectively. In particular, if state preparation is fully reliable, Alice's device achieves $q = 1$.

On the other side of the channel, Bob controls a device allowing him to measure quantum systems in two bases corresponding to $\mathbb{X}$ and $\mathbb{Z}$. We will derive security bounds that are valid independently of the actual implementation of this device as long as the following condition is satisfied: we require that the probability that a signal is detected in Bob's device is independent of the basis choices ($\mathbb{X}$ or $\mathbb{Z}$) by Alice and Bob. Note that this assumption is necessary. In fact, if it is not satisfied (which is the case for some implementations) a loophole arises that can be used to eavesdrop on the key without being detected [25].[6]

We now define a family of protocols, $\mathbf{\Phi}[n, k, \ell, Q_{\mathrm{tol}}, \epsilon_{\mathrm{cor}}, \mathrm{leak}_{\mathrm{EC}}]$, which is parametrized by the *block size*, n, the number of bits used for parameter estimation, k, the *secret key length*, ℓ, the *channel error tolerance*, Q_{tol}, the required correctness, ϵ_{cor}, and the *error correction leakage*, $\mathrm{leak}_{\mathrm{EC}}$. The protocol may be asymmetric, so that the number of bits measured in the two bases (n bits in the $\mathbb{X}$ basis and k bits in the $\mathbb{Z}$ basis) are not necessarily equal [26]. A protocol in this family outputs a key of length ℓ and is ϵ_{cor}-correct as shown in Theorem 1. Its secrecy, $\epsilon_{\mathrm{sec}}(\mathbf{\Phi}, q)$, is established

[4] More precisely, one assumes a certain channel model which corresponds to the characteristics of the channel in the absence of an adversary. For protocols based on qubits, the standard channel model used in the literature is the depolarizing channel. We also chose this channel model for our analysis in Section V, thus enabling a comparison to the existing results.

[5] In typical optical schemes, the qubits are realized by single photons. An ideal implementation therefore requires a single-photon source on Alice's side. In order to take into account sources with a Poissonian distribution of the photon number, our analysis would need to be extended, e.g., along the lines of [24].

[6] Remarkably, this assumption can be enforced device-independently: Bob simply substitutes a random bit whenever his device fails to detect Alice's signal. If this is done, however, the expected error rate may increase significantly.

in Theorem 2 and depends on the protocol parameters as well as the preparation quality, q. The protocol is specified in the following.

State Preparation: The first four steps of the protocol are repeated for $i = 1, 2, \ldots, M$ until the condition in the Sifting step is met.

Alice chooses a basis $a_i \in \{\mathbb{X}, \mathbb{Z}\}$, where $\mathbb{X}$ is chosen with probability $p_x := \left(1 + \sqrt{k/n}\right)^{-1}$ and $\mathbb{Z}$ with probability $p_z := 1 - p_x$. Next, Alice chooses a uniformly random bit $y_i \in \{0, 1\}$ and prepares the qubit in the basis state of a_i given by y_i.

Distribution: Alice sends the qubit over the quantum channel to Bob. (Recall that Eve is allowed to arbitrarily interact with the system and we do not make any assumptions about what Bob receives.)

Measurement: Bob also chooses a basis, $b_i \in \{\mathbb{X}, \mathbb{Z}\}$, with probabilities p_x and p_z, respectively. He measures the system received from Alice in the chosen basis and stores the outcome in $y'_i \in \{0, 1, \emptyset\}$, where '$\emptyset$' is the symbol produced when no signal is detected.

Sifting: Alice and Bob broadcast their basis choices over the classical channel. We define the sets $\mathcal{X} := \{i : a_i = b_i = \mathbb{X} \wedge y'_i \neq \emptyset\}$ and $\mathcal{Z} := \{i : a_i = b_i = \mathbb{Z} \wedge y'_i \neq \emptyset\}$. The protocol repeats the first steps as long as either $|\mathcal{X}| < n$ or $|\mathcal{Z}| < k$.

Parameter Estimation: Alice and Bob choose a random subset of size n of $\mathcal{X}$ and store the respective bits, y_i and y'_i, into *raw key* strings $\mathbf{X}$ and $\mathbf{X}'$, respectively.

Next, they compute the average error $\lambda := \frac{1}{|\mathcal{Z}|} \sum y_i \oplus y'_i$, where the sum is over all $i \in \mathcal{Z}$. The protocol aborts if $\lambda > Q_{\text{tol}}$.

Error Correction: An information reconciliation scheme that broadcasts at most leak_{EC} bits of classical error correction data is applied. This allows Bob to compute an estimate, $\hat{\mathbf{X}}$, of $\mathbf{X}$.

Then, Alice computes a bit string (a hash) of length $\lceil \log(1/\epsilon_{\text{cor}}) \rceil$ by applying a random universal$_2$ hash function [27] to $\mathbf{X}$. She sends the choice of function and the hash to Bob. If the hash of $\hat{\mathbf{X}}$ disagrees with the hash of $\mathbf{X}$, the protocol aborts.

Privacy Amplification: Alice extracts ℓ bits of secret key $\mathbf{S}$ from $\mathbf{X}$ using a random universal$_2$ hash function [28, 29].[7] The choice of function is communicated to Bob, who uses it to calculate $\hat{\mathbf{S}}$.

IV. FINITE KEY SECURITY ANALYSIS

In this section, we analyze the security (i.e. the correctness and secrecy) of the protocols described above. The correctness is checked in the error correction step of the protocol.

Theorem 1. *The protocol* $\mathbf{\Phi}[n, k, \ell, Q_{\text{tol}}, \epsilon_{\text{cor}}, \text{leak}_{\text{EC}}]$ *is* ϵ_{cor}*-correct.*

Proof. The defining property of universal$_2$ hash functions [27] is that the probability that $F(\mathbf{X})$ and $F(\hat{\mathbf{X}})$ coincide — if $\mathbf{X}$ and $\hat{\mathbf{X}}$ are different and the hash function, F, is chosen at random — is at most $2^{-\lceil \log(1/\epsilon_{\text{cor}}) \rceil} \leq \epsilon_{\text{cor}}$. Since the protocol aborts if the hash values calculated from $\mathbf{X}$ and $\hat{\mathbf{X}}$ after error correction do not agree, it is thus ensured that $\Pr[\mathbf{S} \neq \hat{\mathbf{S}}] \leq \Pr[\mathbf{X} \neq \hat{\mathbf{X}}] \leq \epsilon_{\text{cor}}$. □

[7] Instead of choosing a universal$_2$ hash function, which requires at least n bits of random seed, one could instead employ almost two-universal$_2$ hash functions [20] or constructions based on Trevisan's extractor [30]. These techniques allow for a reduction in the random seed length while the security claims remain almost unchanged.

The secrecy of BB84 protocols follows from the observation that, if Alice has a choice of encoding a string of n uniform bits in either the $\mathbb{X}$ or $\mathbb{Z}$ basis, then only one of the following two things can be true: either Bob is able to estimate Alice's string accurately if she prepared in the $\mathbb{Z}$ basis or Eve is able to guess Alice's string accurately if she prepared in the $\mathbb{X}$ basis. This can be formally expressed in terms of an uncertainty relation for smooth entropies [20],[8]

$$H_{\min}^{\varepsilon'}(\mathbf{X}|\mathrm{E}) + H_{\max}^{\varepsilon'}(\mathbf{Z}|\mathrm{B}) \geq nq\,, \tag{1}$$

where $\varepsilon' \geq 0$ is a smoothing parameter and q is the preparation quality defined previously. The smooth min-entropy, $H_{\min}^{\varepsilon}(\mathrm{X}|\mathrm{E})$, introduced in [7], characterizes the average probability that Eve guesses $\mathbf{X}$ correctly using her optimal strategy with access to the correlations stored in her quantum memory [31]. The smooth max-entropy, $H_{\max}^{\varepsilon}(\mathrm{Z}|\mathrm{B})$, is a measure of the correlations between Z and Bob's data. For precise mathematical definitions of the smooth min- and max-entropy, we refer to [32].

Apart from the uncertainty relation (1), our analysis employs the Quantum Leftover Hash Lemma [33], which gives a direct operational meaning to the smooth min-entropy. It asserts that, using a random universal$_2$ hash function, it is possible to extract a Δ-secret key of length ℓ from $\mathbf{X}$, where

$$\Delta = \min_{\varepsilon'} \frac{1}{2}\sqrt{2^{\ell - H_{\min}^{\varepsilon'}(\mathbf{X}|\mathrm{E}')}} + \varepsilon'\,. \tag{2}$$

Here E' summarizes all information Eve learned about $\mathbf{X}$ during the protocol — including the classical communication sent by Alice and Bob over the authenticated channel. Furthermore, the extracted secret key is independent of the randomness that is used to choose the hash function.

The following theorem gives a sufficient condition for which a protocol $\mathbf{\Phi}$ using a source with preparation quality q is ϵ_{sec}-secret. The minimum value ϵ_{sec} for which it is ϵ_{sec}-secret is called the *secrecy of the protocol* and is denoted by $\epsilon_{\mathrm{sec}}(\mathbf{\Phi}, q)$.

Theorem 2. *The protocol $\mathbf{\Phi}[n, k, \ell, Q_{\mathrm{tol}}, \epsilon_{\mathrm{cor}}, \mathrm{leak}_{\mathrm{EC}}]$ using a source with preparation quality q is ϵ_{sec}-secret for some $\epsilon_{\mathrm{sec}} > 0$ if ℓ satisfies*[9]

$$\ell \leq \max_{\varepsilon, \bar{\varepsilon}} \left\lfloor n\Big(q - h\big(Q_{\mathrm{tol}} + \mu(\varepsilon)\big)\Big) - 2\log\frac{1}{2\,\bar{\varepsilon}} - \mathrm{leak}_{\mathrm{EC}} - \log\frac{2}{\epsilon_{\mathrm{cor}}}\right\rfloor, \tag{3}$$

where we optimize over $\varepsilon > 0$ and $\bar{\varepsilon} > 0$ s.t. $\varepsilon + \bar{\varepsilon} \leq \epsilon_{\mathrm{sec}}$ and

$$\mu(\varepsilon) := \sqrt{\frac{n+k}{nk}\,\frac{k+1}{k}\,\ln\frac{1}{\varepsilon}}\,.$$

Proof. In order to apply the uncertainty relation (1), we consider a *gedankenexperiment* in which Alice and Bob, after choosing a basis according to probabilities p_x and p_z as before, prepare and measure everything in the $\mathbb{Z}$ basis. We denote the bit strings of length n that replace the raw keys $\mathbf{X}$ and $\mathbf{X}'$ in this hypothetical protocol as $\mathbf{Z}$ and $\mathbf{Z}'$, respectively.

The observed average error, $\Lambda = \lambda$, is understood to be a random variable. Note that, in this picture, Λ is calculated from at least k measurements sampled at random from $n+k$ measurements in the $\mathbb{Z}$ basis. Hence, if Λ is small, we deduce that, with high probability, $\mathbf{Z}$ and $\mathbf{Z}'$ are highly correlated and $H_{\max}(\mathbf{Z}|\mathbf{Z}')$ is small. This is elaborated in Appendix A, Lemma 3, where it is shown

[8] To compare this with the formalism employed in [20], note that encoding a uniform bit in a basis state of $\mathbb{X}$ or $\mathbb{Z}$ can be simulated by measuring one part of a two-qubit singlet state in either the $\mathbb{X}$ or $\mathbb{Z}$ basis.

[9] Here, h is a truncated binary entropy function, i.e. $h : x \mapsto -x\log x - (1-x)\log(1-x)$ if $x \leq 1/2$ and 1 otherwise.

that, conditioned on the event that the correlation test passed ($\Lambda \leq Q_{\text{tol}}$), the following bound on the smooth max-entropy holds,

$$H_{\max}^{\varepsilon'}(\mathbf{Z}|\mathbf{Z}') \leq nh\big(Q_{\text{tol}} + \mu(\varepsilon)\big)\,,$$

where $\varepsilon' = \varepsilon/\sqrt{p_{\text{pass}}}$ and $p_{\text{pass}} \geq 1 - p_{\text{abort}}$ is the probability that the correlation test passes.

We now use the uncertainty relation, $H_{\min}^{\varepsilon'}(\mathbf{X}|\mathrm{E}) \geq nq - H_{\max}^{\varepsilon'}(\mathbf{Z}|\mathbf{Z}')$, to find a lower bound on the min-entropy that Eve has about Alice's bits prepared in the $\mathbb{X}$ basis. Since a maximum of $\text{leak}_{\text{EC}} + \lceil \log(1/\epsilon_{\text{cor}}) \rceil \leq \text{leak}_{\text{EC}} + \log(2/\epsilon_{\text{cor}})$ bits of information about $\mathbf{X}$ are revealed during error correction, we find[10]

$$\begin{aligned} H_{\min}^{\varepsilon'}(\mathbf{X}|\mathrm{E}') &\geq H_{\min}^{\varepsilon'}(\mathbf{X}|\mathrm{E}) - \text{leak}_{\text{EC}} - \log\frac{2}{\epsilon_{\text{cor}}} \\ &\geq nq - H_{\max}^{\varepsilon'}(\mathbf{Z}|\mathbf{Z}') - \text{leak}_{\text{EC}} - \log\frac{2}{\epsilon_{\text{cor}}} \\ &\geq n\Big(q - h\big(Q_{\text{tol}} + \mu(\varepsilon)\big)\Big) - \text{leak}_{\text{EC}} - \log\frac{2}{\epsilon_{\text{cor}}}\,. \end{aligned}$$

Thus, combining this with (2) and using the proposed key length (3), we find, for all ε and $\bar{\varepsilon}$,

$$\Delta \leq \varepsilon' + \frac{1}{2}\sqrt{2^{\ell - H_{\min}^{\varepsilon'}(\mathbf{X}|\mathrm{E}')}} \leq \varepsilon' + \bar{\varepsilon}\,. \tag{4}$$

The security of the protocol now follows since $(1 - p_{\text{abort}})\Delta \leq \varepsilon + \bar{\varepsilon} \leq \epsilon_{\text{sec}}$. □

V. ANALYSIS AND NUMERICAL RESULTS

For the following discussions, we assume that the quantum channel in the absence of an eavesdropper can be described as a binary symmetric channel with *quantum bit error rate* Q. The numerical results are computed for a perfect source, i.e. $q = 1$. Furthermore, finite detection efficiencies and channel losses are not factored into the key rates, i.e. the expected secret key rate calculated here can be understood as the expected key length per detected signal.

The efficiency of a protocol $\mathbf{\Phi}$ can be characterized in terms of its *expected secret key rate*,

$$r(\mathbf{\Phi}, Q) := \big(1 - \epsilon_{\text{rob}}(Q, Q_{\text{tol}})\big)\frac{\ell}{M(n,k)}\,, \tag{5}$$

where M is the expected number of qubits that need to be exchanged until n raw key bits and k bits for parameter estimation are gathered so that ℓ key bits can be generated (see protocol description).

Before presenting numerical results for the optimal expected key rates for finite n, let us quickly discuss its asymptotic behavior for arbitrarily large n. It is easy to verify that the key rate asymptotically reaches $r_{\max}(Q) = 1 - 2h(Q)$ for arbitrary security bounds $\epsilon > 0$. To see this, note that error correction can be achieved with a leakage rate of $h(Q)$ (see, e.g. [34]). Furthermore, if we choose k proportional to $\sqrt{n}$, the statistical deviation in (3), μ, vanishes and the ratio between the raw key length, n, and the expected number of exchanged qubits, $M(n,k)$, approaches one as n tends to infinity, i.e., $n/M(n,k) \to 1$. This asymptotic rate is optimal [35]. Finally, the deviations of the key length in (3) from its asymptotic limit can be explained as fluctuations that are due to

[10] Formally, this requires use of the chain rule $H_{\min}^{\varepsilon}(\mathbf{X}|\mathrm{EC}) \geq H_{\min}^{\varepsilon}(\mathbf{X}|\mathrm{E}) - \log|\mathrm{C}|$, where C is any classical information about $\mathbf{X}$.

n	Q (%)	r (%)	r_{rel} (%)	p_z (%)	Q_{tol} (%)	$\varepsilon_{\mathrm{rob}}$ (%)
10^4	1.0	11.7	14.0	38.2	2.48	2.3
	2.5	6.8	10.4	43.0	3.78	3.0
10^5	1.0	30.4	36.4	22.0	2.14	0.8
	2.5	21.5	32.6	23.3	3.58	1.0
10^6	1.0	47.8	57.1	12.5	1.73	0.6
	2.5	35.7	53.9	13.7	3.21	0.7

TABLE I. Optimized parameters for a given security rate $\epsilon/\ell = 10^{-14}$. The column labeled r_{rel} shows the deviation of the expected secret key rate from the corresponding asymptotic value, i.e., $r_{\mathrm{rel}} := r/(1-2h(Q))$.

the finiteness of the statistical samples we consider. As such, these terms are necessary and the result is essentially tight.

To obtain our results for finite block sizes n, we fix a security bound ϵ and define an optimized ϵ-secure protocol, $\mathbf{\Phi}^*[n,\epsilon]$, that results from a maximization of the expected secret key rate over all ϵ-secure protocols with block size n. For the purpose of this optimization, we assume an error correction leakage of $\mathrm{leak}_{\mathrm{EC}} = \xi\, n\, h(Q_{\mathrm{tol}})$ with $\xi = 1.1$. Moreover, we bound the robustness ϵ_{rob} by the probability that the measured security parameter exceeds Q_{tol}, which (for binary symmetric channels) decays exponentially in $Q_{\mathrm{tol}} - Q$ (see Eq. (A5) in Appendix A).

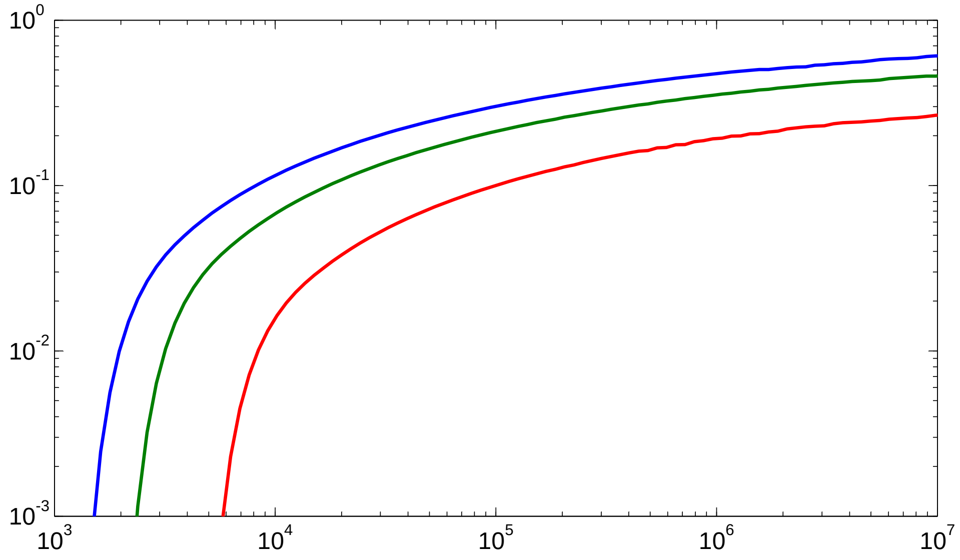

FIG. 1. Plot of expected key rate r as a function of the block size n for channel bit error rates $Q \in \{1\%, 2.5\%, 5\%\}$ (from left to right). The security rate is fixed to $\epsilon/\ell = 10^{-14}$.

In Figure 1, we present the expected key rates $r = r(\mathbf{\Phi}, Q)$ of the optimal protocols $\mathbf{\Phi}^*[n,\epsilon]$ as a function of the block size n. These rates are given for a fixed value of the *security rate* ε/ℓ, i.e., the amount by which the security bound ε increases per generated key bit. (In other words, ε/ℓ can be seen as the probability of key leakage per key bit.) The plot shows that significant key rates can be obtained already for $n = 10^4$.

In Table I, we provide selected numerical results for the optimal protocol parameters that correspond to block sizes $n = \{10^4, 10^5, 10^6\}$ and quantum bit error rates $Q \in \{1\%, 2.5\%\}$. These block sizes exemplify current hardware limitations in practical QKD systems.

In Figure 2, we compare our optimal key rates with the maximal key rates that can be shown secure using the finite key analysis of Scarani and Renner [16].[11] We show a major improvement in the minimum block size required to produce a provably secret key. The improvements are mainly due to a more direct evaluation of the smooth min-entropy via the entropic uncertainty relation and the use of statistics optimized specifically to the problem at hand (c.f. Appendix A).

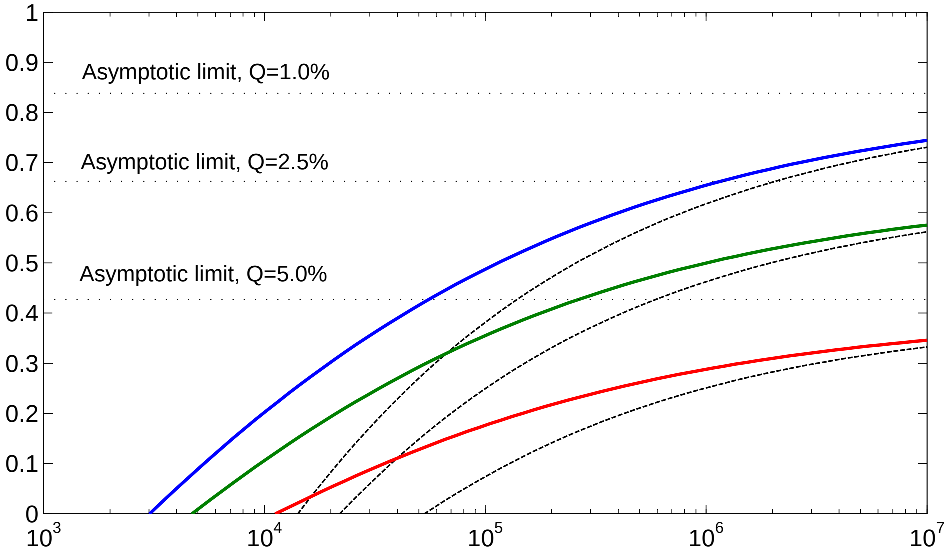

FIG. 2. The plots show the rate ℓ/n as a function of the sifted key size $N = n + k$ for various channel bit error rates Q (as in Fig. 1) and a security bound of $\epsilon = 10^{-10}$. The dashed lines show the rates that can be proven secure using [16].

ACKNOWLEDGMENTS

We would like to thank Silvestre Abruzzo, Dagmar Bruss, Hermann Kampermann, Markus Mertz, Norbert Lütkenhaus, Christoph Pacher, Momtchil Peev, and Hugo Zbinden for valuable comments and stimulating discussions. We acknowledge support from the National Centre of Competence in Research QSIT, the Swiss NanoTera project QCRYPT, the Swiss National Science Foundation (grant no. 200021-119868), and the European Research Council (grant No. 258932 and No. 227656).

Appendix A: Hamming Weight Statistics

This appendix specifically covers the statistical analysis of the classical data collected during the run of the BB84-type protocols described in this work. A more general framework for such an analysis can be found in [17].

We use the notation of the previous sections and define $N := n + k$. The fraction of bits that are used for parameter estimation is denoted as ν, i.e. $k = \nu N$ and $n = (1 - \nu)N$.

The statistical analysis is based on a *gedankenexperiment*, where Alice and Bob measure all N states with $i \in \mathcal{X} \cup \mathcal{Z}$ in the control basis, $\mathbb{Z}$, resulting in strings $\mathbf{Z}_{\text{tot}}$ and $\mathbf{Z}'_{\text{tot}}$ for Alice and

[11] For comparison with previous work, we plot the rate ℓ/n, i.e. the ratio between key length and block size, instead of the expected secret key rate as defined by Eq. (5).

Bob, respectively. The following random variables are of interest to us. The relative Hamming distance between Alice's and Bob's bit-string is defined as $\Lambda_{\text{tot}} = \frac{1}{N}\,|\mathbf{Z}_{\text{tot}} \oplus \mathbf{Z}'_{\text{tot}}|$, where $|\cdot|$ denotes the Hamming weight. Similarly, $\Lambda = \Lambda_{\text{pe}}$ denotes the relative Hamming distances between the random subsets $\mathbf{Z}_{\text{pe}}$ of $\mathbf{Z}_{\text{tot}}$ and $\mathbf{Z}'_{\text{pe}}$ of $\mathbf{Z}'_{\text{tot}}$ used for parameter estimation. Finally, Λ_{key} is the relative Hamming distance between the remainders of the strings, denoted $\mathbf{Z} = \mathbf{Z}_{\text{key}}$ and $\mathbf{Z}' = \mathbf{Z}'_{\text{key}}$. Clearly,

$$\Lambda_{\text{tot}} = \nu\Lambda + (1-\nu)\Lambda_{\text{key}}\,.$$

The k bits used for parameter estimation are chosen at random from N bits. Hence, if we fix $\Lambda_{\text{tot}} = \lambda_{\text{tot}}$ for the moment, the random variables Λ and Λ_{key} can be seen as emanating from sampling without replacement. We apply the bound [36]

$$\Pr\left[\Lambda_{\text{key}} \geq \lambda_{\text{tot}} + \delta \,|\, \Lambda_{\text{tot}} = \lambda_{\text{tot}}\right] \leq e^{-2\frac{nN}{k+1}\delta^2}\,. \tag{A1}$$

We now derive a bound on the probability that Λ_{key} exceeds Λ by more than a constant μ conditioned on the event that we passed the correlation test. (Note that, while Λ is accessible during the protocol, Λ_{key} is the quantity we are actually interested in.) We find, using Bayes' theorem,

$$\Pr\left[\Lambda_{\text{key}} \geq \Lambda + \mu \,|\, \text{“pass”}\right] \leq \frac{1}{p_{\text{pass}}} \Pr\left[\Lambda_{\text{key}} \geq \Lambda + \mu\right],$$

where we keep $p_{\text{pass}} = \Pr[\text{“pass”}] = \Pr[\Lambda \leq Q_{\text{tol}}]$ as a parameter and further bound

$$\begin{aligned}\Pr\left[\Lambda_{\text{key}} \geq \Lambda + \mu\right] &= \Pr\left[\Lambda_{\text{key}} \geq \Lambda_{\text{tot}} + \nu\mu\right] \\ &= \sum_{\lambda_{\text{tot}}} \Pr\left[\Lambda_{\text{tot}} = \lambda_{\text{tot}}\right] \Pr\left[\Lambda_{\text{key}} \geq \lambda_{\text{tot}} + \nu\mu \,|\, \Lambda_{\text{tot}} = \lambda_{\text{tot}}\right] \leq e^{-2\frac{kn}{N}\frac{k}{k+1}\mu^2}\,.\end{aligned}$$

We used (A1) to bound each summand individually. Finally, defining $\varepsilon := e^{-\frac{kn}{N}\frac{k}{k+1}\mu^2}$, we write

$$\Pr\left[\Lambda_{\text{key}} \geq \Lambda + \mu \,|\, \text{“pass”}\right] \leq \frac{\varepsilon^2}{p_{\text{pass}}}\,. \tag{A2}$$

The above result can be used to bound the uncertainty Bob has about Alice's measurement outcomes in the $\mathbb{Z}$-basis, as expressed using the smooth max-entropy of $\mathbf{Z}$ given $\mathbf{Z}'$ and Λ. The entropy is evaluated for the probability distribution conditioned on the event that the correlation test passed, which we denote $\mathbb{P}_{\mathbf{ZZ}'\Lambda}(\mathbf{z},\mathbf{z}',\lambda) = \Pr\left[\mathbf{Z} = \mathbf{z} \wedge \mathbf{Z}' = \mathbf{z}' \wedge \Lambda = \lambda \,|\, \text{“pass”}\right]$.

Lemma 3. *Let $\varepsilon > 0$. Then*

$$H_{\max}^{\varepsilon'}(\mathbf{Z}|\mathbf{Z}')_{\mathbb{P}} \leq nh\big(Q_{\text{tol}} + \mu\big)\,, \quad \textit{where} \quad \varepsilon' := \frac{\varepsilon}{\sqrt{p_{\text{pass}}}} \quad \textit{and} \quad \mu := \sqrt{\frac{N}{nk}\,\frac{k+1}{k}\,\ln\frac{1}{\varepsilon}}\,.$$

Proof. According to (A2), the probability that Λ_{key} exceeds Λ by more than μ is bounded. In fact, we can find a probability distribution,

$$\mathbb{Q}_{\mathbf{ZZ}'\Lambda}(\mathbf{z},\mathbf{z}',\lambda) := \begin{cases} \frac{\mathbb{P}_{\mathbf{ZZ}'\Lambda}(\mathbf{z},\mathbf{z}',\lambda)}{\Pr[\Lambda_{\text{key}}<\Lambda+\mu\,|\,\text{“pass”}]} & \text{if} \quad \lambda_{\text{key}}(\mathbf{z},\mathbf{z}') < \lambda + \mu \\ 0 & \text{else} \end{cases}\,,$$

which is ε'-close to $\mathbb{P}_{\mathbf{ZZ}'\Lambda}$ in terms of the purified distance. To see this, note that the fidelity between the two distributions satisfies

$$F(\mathbb{P},\mathbb{Q}) := \sum_{\mathbf{z},\mathbf{z}',\lambda} \sqrt{\mathbb{P}_{\mathbf{ZZ}'\Lambda}(\mathbf{z},\mathbf{z}',\lambda)\,\mathbb{Q}_{\mathbf{ZZ}'\Lambda}(\mathbf{z},\mathbf{z}',\lambda)} = \sqrt{\Pr[\Lambda_{\text{key}} < \Lambda + \mu \,|\, \text{“pass”}]}\,,$$

which can be bounded using (A2). The purified distance between the distributions is then given by $P(\mathbb{P},\mathbb{Q}) := \sqrt{1-F^2(\mathbb{P},\mathbb{Q})} = \varepsilon'$. Hence, under the distribution Q, we have $\Lambda_{\text{key}} < \Lambda + \mu \leq Q_{\text{tol}} + \mu$ with certainty. In particular, the total number of errors on n bits, $W := n\Lambda_{\text{key}}$, satisfies

$$W \leq \lfloor n(Q_{\text{tol}} + \mu) \rfloor . \tag{A3}$$

The max-entropy, $H_{\max}(\mathbf{Z}|\mathbf{Z}')$, is upper bounded by the minimum number of bits of additional information about $\mathbf{Z}$ needed to perfectly reconstruct $\mathbf{Z}$ from $\mathbf{Z}'$ [37]. This value can in turn be upper bounded by the logarithm of the maximum support of $\mathbf{Z}$ conditioned on any value $\mathbf{Z}' = \mathbf{z}'$. Since the total number of errors under Q satisfies (A3), we may write

$$H^{\varepsilon}_{\max}(\mathbf{Z}|\mathbf{Z}')_{\mathbb{P}} \leq H_{\max}(\mathbf{Z}|\mathbf{Z}')_{\mathbb{Q}} \leq \log \sum_{w=0}^{\lfloor n(Q_{\text{tol}}+\mu)\rfloor} \binom{n}{w} \leq nh\big(Q_{\text{tol}} + \mu\big) . \tag{A4}$$

The last inequality is shown in [38], Section 1.4. This concludes the proof of Lemma 3. □

Finally, we calculate a bound which is used to quantify the robustness of the protocol. According to [39], the probability that Λ exceeds $Q + \eta$ cannot exceed[12]

$$\Pr\big[\Lambda \geq Q + \eta\big] \leq e^{-k\eta^2\varphi(Q)} , \tag{A5}$$

where $\varphi(Q) = \frac{1}{1-2Q}\ln(\frac{1-Q}{Q})$ for $Q < \frac{1}{2}$.

[1] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process.*, pages 175–179, Bangalore, 1984. IEEE.

[2] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6):661–663, Aug. 1991.

[3] H.-K. Lo and H. F. Chau. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. *Science*, 283(5410):2050–2056, Mar. 1999. DOI: 10.1126/science.283.5410.2050.

[4] P. Shor and J. Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.*, 85(2):441–444, July 2000.

[5] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury. A Proof of the Security of Quantum Key Distribution. *J. Cryptology*, 19(4):381–439, Apr. 2006. DOI: 10.1007/s00145-005-0011-3.

[6] D. Mayers. Unconditional security in quantum cryptography. *J. ACM*, 48(3):351–406, May 2001.

[7] R. Renner. Security of Quantum Key Distribution. *PhD thesis, ETH Zurich, Dec. 2005.* arXiv: quant-ph/0512258.

[8] R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72(1):012332, July 2005.

[9] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto. Quantum key distribution over 40 dB channel loss using superconducting single photon detectors. *Nat. Photonics*, 1(6):343–357, June 2007.

[10] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields. Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. *Opt. Express*, 16(23):18790–18979, Nov. 2008.

[11] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Phys.*, 11(7):75003, 2009.

[12] V. Scarani and C. Kurtsiefer. The black paper of quantum cryptography: real implementation problems. June 2009. arXiv: 0906.4547.

[12] Note that $\varphi(Q) \geq 2$ for all Q, from which the usual form of the Hoeffding bound, $\exp(-2k\eta^2)$, follows. However, for small Q the bound (A5) is significantly tighter. For example, $\varphi(0.05) > 3.27$ and $\varphi(0.01) > 4.68$.

[13] M. Hayashi. Practical evaluation of security for quantum key distribution. *Phys. Rev. A*, 74(2):022307, Aug. 2006. DOI: 10.1103/PhysRevA.74.022307.

[14] T. Meyer, H. Kampermann, M. Kleinmann, and D. Bruß. Finite key analysis for symmetric attacks in quantum key distribution. *Phys. Rev. A*, 74(4), Oct. 2006. DOI: 10.1103/PhysRevA.74.042340.

[15] H. Inamori, N. Lütkenhaus, and D. Mayers. Unconditional security of practical quantum key distribution. *Eur. Phys. J. D*, 41(3):599–627, Jan. 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.*, 100(20):200501, May 2008.

[17] N. Bouman and S. Fehr. Sampling in a Quantum Population, and Applications. July 2009. arXiv: 0907.4246.

[18] S. Bratzik, M. Mertz, H. Kampermann, and D. Bruß. Min-entropy and quantum key distribution: non-zero key rates for "small" numbers of signals. 2010. arXiv: 1011.1190.

[19] L. Sheridan, T. P. Le, and V. Scarani. Finite-key security against coherent attacks in quantum key distribution. *New J. Phys.*, 12:123019, Aug. 2010.

[20] M. Tomamichel and R. Renner. Uncertainty Relation for Smooth Entropies. *Phys. Rev. Lett.*, 106(11), Mar. 2011. DOI: 10.1103/PhysRevLett.106.110506.

[21] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner. The uncertainty principle in the presence of quantum memory. *Nat. Phys.*, 6(9):659–662, July 2010. DOI: 10.1038/nphys1734.

[22] J. Müller-Quade and R. Renner. Composability in quantum cryptography. *New J. Phys.*, 11(8):085006, Aug. 2009. DOI: 10.1088/1367-2630/11/8/085006.

[23] R. König, R. Renner, A. Bariska, and U. Maurer. Small Accessible Quantum Information Does Not Imply Security. *Phys. Rev. Lett.*, 98(14), Apr. 2007. DOI: 10.1103/PhysRevLett.98.140502.

[24] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comput.*, 4(5):325–360, Sept. 2004. arXiv: quant-ph/0212066.

[25] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics*, 4(10):686–689, Aug. 2010. Available online: http://dx.doi.org/10.1038/nphoton.2010.214.

[26] H.-K. Lo, H. Chau, and M. Ardehali. Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security. *J. Cryptology*, 18(2):133–165, Mar. 2004. DOI: 10.1007/s00145-004-0142-y.

[27] J. L. Carter and M. N. Wegman. Universal Classes of Hash Functions. *J. Comp. Syst. Sci.*, 18(2):143–154, 1979.

[28] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer. Generalized Privacy Amplification. *IEEE Trans. on Inf. Theory*, 41(6):1915–1923, 1995.

[29] R. Renner and R. König. Universally Composable Privacy Amplification Against Quantum Adversaries. In *Proc. TCC*, volume 3378 of *LNCS*, pages 407–425, Cambridge, USA, 2005. Springer.

[30] A. De, C. Portmann, T. Vidick, and R. Renner. Trevisan's Extractor in the Presence of Quantum Side Information. Dec. 2009. arXiv: 0912.5514.

[31] R. König, R. Renner, and C. Schaffner. The Operational Meaning of min- and max-Entropy. *IEEE Trans. on Inf. Theory*, 55(9):4337–4347, 2009.

[32] M. Tomamichel, R. Colbeck, and R. Renner. Duality Between Smooth Min- and Max-Entropies. *IEEE Trans. on Inf. Theory*, 56(9):4674–4681, Sept. 2010. DOI: 10.1109/TIT.2010.2054130.

[33] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. Leftover Hashing Against Quantum Side Information. Feb. 2010. arXiv: 1002.2436.

[34] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley, 1991.

[35] R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72(1), July 2005. DOI: 10.1103/PhysRevA.72.012332.

[36] R. J. Serfling. Probability Inequalities for the Sum in Sampling without Replacement. *Ann. Stat.*, 2(1):39–48, Jan. 1974.

[37] J. M. Renes and R. Renner. One-Shot Classical Data Compression with Quantum Side Information and the Distillation of Common Randomness or Secret Keys. Aug. 2010.

[38] J. H. van Lint. *Introduction to Coding Theory*. Graduate Texts in Mathematics. Springer, third edition, Oct. 1999.

[39] W. Hoeffding. Probability Inequalities for Sums of Bounded Random Variables. *J. Amer. Statistical Assoc.*, 58:13–30, Mar. 1963.