UNIVERSITÉ DE GENÈVE

Archive ouverte UNIGE
https://archive-ouverte.unige.ch

Article scientifique | Article | 2012

Published version | Open Access

This is the published version of the publication, made available in accordance with the publisher's policy.

Tight finite-key analysis for quantum cryptography

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

How to cite

TOMAMICHEL, Marco et al. Tight finite-key analysis for quantum cryptography. In: Nature communications, 2012, vol. 3, n° 634. doi: 10.1038/ncomms1631

This publication URL: https://archive-ouverte.unige.ch/unige:36558
Publication DOI: 10.1038/ncomms1631

© This document is protected by copyright. Please refer to copyright holder(s) for terms of use.

nature COMMUNICATIONS

OPEN

ARTICLE

Received 31 May 2011 | Accepted 2 Dec 2011 | Published 17 Jan 2012

DOI: 10.1038/ncomms1631

Tight finite-key analysis for quantum cryptography

Marco Tomamichel[1], Charles Ci Wen Lim[2], Nicolas Gisin[2] & Renato Renner[1]

Despite enormous theoretical and experimental progress in quantum cryptography, the security of most current implementations of quantum key distribution is still not rigorously established. One significant problem is that the security of the final key strongly depends on the number, *M*, of signals exchanged between the legitimate parties. Yet, existing security proofs are often only valid asymptotically, for unrealistically large values of *M*. Another challenge is that most security proofs are very sensitive to small differences between the physical devices used by the protocol and the theoretical model used to describe them. Here we show that these gaps between theory and experiment can be simultaneously overcome by using a recently developed proof technique based on the uncertainty relation for smooth entropies.

[1] Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland. [2] Group of Applied Physics, University of Geneva, 1211 Geneva, Switzerland. Correspondence and requests for materials should be addressed to M.T. (email: marcoto@phys.ethz.ch or marcotom.ch@gmail.com).

© 2012 Macmillan Publishers Limited. All rights reserved.

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 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 several 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 (refs 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 (ref. 12 for a discussion). In this work, we consider 'prepare-and-measure' quantum key distribution protocols, like the original Bennett–Brassard 1984 (BB84) protocol[1]. Here one party prepares quantum systems (for example, the polarization degrees of freedom of photons) and sends them through an insecure quantum channel to another party who then measures the systems. To analyse the security of such protocols, the physical devices used by both parties to prepare and measure quantum systems are replaced by theoretical device models. The goal, from a theory perspective, is to make these theoretical models as general as possible so that they can accommodate imperfect physical devices independently of their actual implementation. (This approach, in the context of 'entanglement-based' protocols, also led to the development of device-independent quantum cryptography; refs 13, 14 for recent results.)

Another weakness of many security proofs is the asymptotic resource assumption, that is, 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[15–21].

In this work, we apply a novel proof technique[22] that allows us to overcome the above difficulties. In particular, we 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[23] or, more precisely, its generalization to smooth entropies[22]. Compared with preexisting methods, our technique is rather direct. It therefore avoids various estimates, including the de Finetti theorem[24] and the Post-selection technique[25], 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. Moreover, we believe that the theoretical device model used for our security analysis is as general as possible for protocols of the prepare-and-measure type.

Results

Security definitions. We follow the discussion of composable security in ref. 26 and first take an abstract view on QKD protocols. A QKD protocol describes the interaction between two players, Alice and Bob. Both players can generate fresh randomness and have access to an insecure quantum channel as well as an authenticated (but otherwise insecure) classical channel. (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 ref. 27.)

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 $\mathbf{E}$ in general. These depend 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.

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

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

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

where ω_{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 ref. 28.

A QKD protocol is called secret, if, for any attack strategy, $\Delta = 0$ whenever the protocol outputs a key. It is called $\varepsilon_{\mathrm{sec}}$-secret, if it is $\varepsilon_{\mathrm{sec}}$-indistinguishable from a secret protocol. In particular, a protocol is $\varepsilon_{\mathrm{sec}}$-secret, if it outputs Δ-secure keys with $(1 - p_{\mathrm{abort}})\Delta \leq \varepsilon_{\mathrm{sec}}$, where p_{abort} is the probability that the protocol aborts. (To see that this suffices to ensure $\varepsilon_{\mathrm{sec}}$-indistinguishability, note that the secrecy condition is trivially fulfilled if the protocol aborts.)

In some applications, it is reasonable to consider correctness and secrecy of protocols separately, because there may be different requirements on the correctness of the key (that is, that Bob's key agrees 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, $\varepsilon_{\mathrm{cor}}$ may be chosen larger than $\varepsilon_{\mathrm{sec}}$.

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).

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 $\varepsilon_{\mathrm{cor}}$-correct and $\varepsilon_{\mathrm{sec}}$-secret with $\varepsilon_{\mathrm{cor}} + \varepsilon_{\mathrm{sec}} \leq \varepsilon$.

Finally, the robustness, $\varepsilon_{\mathrm{rob}}$, is the probability that the protocol aborts even though the eavesdropper is inactive. (More precisely, one assumes a certain channel model that 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 the Discussion section, thus enabling a comparison to the existing results.) 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 $\varepsilon_{\mathrm{rob}}$ in our estimate for the expected key rate (when the eavesdropper is inactive) and then optimize over the protocol parameters to maximize this rate.

© 2012 Macmillan Publishers Limited. All rights reserved.

Device model. 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 quantum states in two bases, $\mathbb{X}$ and $\mathbb{Z}$. In an optimal scenario, the prepared states are qubits and the two bases are diagonal, for example, $\mathbb{X}=\{|0\rangle,|1\rangle\}$ and $\mathbb{Z}=\{|+\rangle,|-\rangle\}$ with $|\pm\rangle := (|0\rangle \pm |1\rangle)/\sqrt{2}$. More generally, we characterize the quality of a source by its 'preparation quality', q. The preparation quality, as we will see in the following,is the only device parameter relevant for our security analysis. It achieves its maximum of $q=1$, if the prepared states are qubits and the bases are diagonal, as in the example above. In the following, we discuss two possible deviations from a perfect source and how they can be characterized in terms of q.

First, if the prepared states are guaranteed to be qubits, 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 have $q=-\log \max|\langle\psi_x|\psi_z\rangle|^2$, where the maximization is over all states ψ_x and ψ_z prepared in the $\mathbb{X}$ and $\mathbb{Z}$ basis, respectively. (In this work, log denotes the binary logarithm.) The maximum $q=1$ is achieved, if the basis states are prepared in diagonal bases, as is the case in the BB84 protocol.

In typical optical schemes, qubits are realized by polarization states of single photons. An ideal implementation therefore requires a single-photon source in Alice's laboratory. To take into account the sources that emit weak coherent light pulses instead, the analysis presented in this paper can be extended using photon tagging[29] and decoy states[30]. This approach, although beyond the scope of the present article, can be incorporated into our finite-key analysis. (See also refs 31–33 for recent results on the finite-key analysis of such protocols.)

Second, consider a source that prepares states in the following way: the source produces two entangled particles and then sends out one of them while the other is measured in one of two bases. The choice of basis for the measurement decides whether the states are prepared in the $\mathbb{X}$ or $\mathbb{Z}$ basis. Together with the measurement outcome, which is required to be uniformly random for use in our protocol, this determines which of the four states is prepared. For such a source, the preparation quality is given by $q=-\log\max\left\|\sqrt{M_x}\sqrt{N_z}\right\|_\infty^2$, where $\{M_x\}$ and $\{N_z\}$ are the elements of the positive operator-valued measurements that are used to prepare the state in the $\mathbb{X}$ and the $\mathbb{Z}$ basis, respectively. If the produced state is that of two fully entangled qubits and the measurements are projective measurements in diagonal bases, we recover BB84 and $q=1$ (ref. 34). Sources of this type have recently received increased attention as they can be used as heralded single photon sources[35,36] and have applications in (device-independent) quantum cryptography[37–39].

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. 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[40]. (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.)

Finally, we assume that it is theoretically possible to devise an apparatus for Bob which delays all the measurements in the $\mathbb{X}$-basis until after parameter estimation, but produces the exact same measurement statistics as the actual device he uses. This assumption is satisfied if Bob's actual measurement device is memoryless. (To see this, we could (in theory) equip such a device with perfect quantum memory that stores the received state until after the parameter estimation.) The assumption is already satisfied, if the measurement statistics are unaffected when the memory of the actual device is reset after each measurement. It is an open question whether this assumption can be further relaxed.

Protocol definition. We now define a family of protocols, $\Phi[n,k,\ell, Q_{\mathrm{tol}}, \varepsilon_{\mathrm{cor}}, \mathrm{leak}_{\mathrm{EC}}]$, 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, $\varepsilon_{\mathrm{cor}}$, and the error correction leakage, $\mathrm{leak}_{\mathrm{EC}}$. The protocol is 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[41].

These protocols are described in **Box 1**.

Box 1 | Protocol definition.

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 $p_x=(1+\sqrt{k/n})^{-1}$ and $\mathbb{Z}$ with probability $p_z=1-p_x$. (These probabilities are chosen to minimize the number M of exchanged particles before Alice and Bob agree on the basis $\mathbb{X}$ for n particles and on the basis $\mathbb{Z}$ for k particles.) Next, Alice chooses a uniformly random bit $y_i\in\{0,1\}$ and prepares the qubit in a state of basis a_i, given by y_i. Alternatively, if the source is entanglement-based, Alice will ask it to prepare a state in the basis a_i and record the output in 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 $y'_i\in\{0,1,\varnothing\}$, where '$\varnothing$' 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 $\mathcal{X}:=\{i: a_i=b_i=\mathbb{X}\wedge y'_i\neq\varnothing\}$ and $\mathcal{Z}:\{i: a_i=b_i=\mathbb{Z}\wedge y'_i\neq\varnothing\}$. 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 $\lambda:=\frac{1}{|\mathcal{Z}|}\Sigma y_i\oplus y'_i$, where the sum is over all $i\in\mathcal{Z}$. The protocol aborts if $\lambda>Q_{\mathrm{tol}}$.
Error correction: An information reconciliation scheme that broadcasts at most $\mathrm{leak}_{\mathrm{EC}}$ 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 $\lceil\log(1/\varepsilon_{\mathrm{cor}})\rceil$ by applying a random universal$_2$ hash function[46] 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[53,54]. (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[52] or constructions based on Trevisan's extractor[55]. These techniques allow for a reduction in the random seed length whereas the security claims remain almost unchanged.) The choice of function is communicated to Bob, who uses it to calculate $\hat{\mathbf{S}}$.

Security analysis. The following two statements constitute the main technical result of our paper, stating that the protocols described above are both $\varepsilon_{\mathrm{cor}}$-correct and $\varepsilon_{\mathrm{sec}}$-secure, if the secret key length is chosen appropriately. Correctness is guaranteed by the error-correction step of the protocol, where a hash of Alice's raw key is compared with the hash of its estimate on Bob's side. The following holds:

$$\text{The protocol } \Phi\left[n,k,\ell,Q_{\mathrm{tol}},\varepsilon_{\mathrm{cor}},\mathrm{leak}_{\mathrm{EC}}\right] \text{is } \varepsilon_{\mathrm{cor}}-\text{correct.}$$

The protocols are $\varepsilon_{\mathrm{sec}}$-secure if the length of the extracted secret key does not exceed a certain length. Asymptotically for large block sizes n, the reductions of the key length due to finite statistics and security parameters can be neglected, and a secret key of length

© 2012 Macmillan Publishers Limited. All rights reserved.

$\ell_{\max} = n(q - h(Q_{\text{tol}})) - \text{leak}_{\text{EC}}$ can be extracted securely. Here h denotes the binary entropy function. Because our statistical sample is finite, we have to add to the tolerated channel noise a term $\mu \approx \sqrt{1/k \cdot \ln(1/\varepsilon_{\text{sec}})}$ that accounts for statistical fluctuations. Furthermore, the security parameters lead to a small reduction of the key rate logarithmic in ε_{cor} and ε_{sec}. The following holds:

The protocol $\Phi[n, k, \ell, Q_{\text{tol}}, \varepsilon_{\text{cor}}, \text{leak}_{\text{EC}}]$ using a source with preparation quality q is ε_{sec}-secret if the secret key length ℓ satisfies

$$\ell \le n(q - h(Q_{\text{tol}} + \mu)) - \text{leak}_{\text{EC}} - \log \frac{2}{\varepsilon_{\text{sec}}^2 \varepsilon_{\text{cor}}} \quad \text{where} \quad \mu := \sqrt{\frac{n+k}{nk} \frac{k+1}{k} \ln \frac{2}{\varepsilon_{\text{sec}}}}. \tag{2}$$

A sketch of the proof of these two statements follows in the methods section and a rigorous proof of slightly more general versions of the theorems presented above can be found in Supplementary Material 1.

Discussion

In this section, we discuss the asymptotic behaviour of our security bounds and compare numerical bounds on the key rate for a finite number of exchanged signals with previous results. For this purpose, we assume that the quantum channel, in the absence of an eavesdropper, can be described as a depolarizing channel with quantum bit error rate Q. (This assumption is not needed for the security analysis of the previous section.) The numerical results are computed for a perfect single-photon source, that is, $q = 1$. Furthermore, finite detection efficiencies and channel losses are not factored into the key rates, that is, the expected secret key rate calculated here can be understood as the expected key length per detected signal.

The efficiency of a protocol Φ is characterized in terms of its expected secret key rate,

$$r(\Phi, Q) := (1 - \varepsilon_{\text{rob}}) \frac{\ell}{M(n,k)}, \tag{3}$$

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

Before presenting numerical results for the optimal expected key rates for finite n, let us quickly discuss its asymptotic behaviour 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 $\varepsilon > 0$. To see this, error correction can be achieved with a leakage rate of $h(Q)$ (for example, see ref. 42). Furthermore, if we choose, for instance, k proportional to $\sqrt{n}$, the statistical deviation in equation (2), 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, that is, $n/M(n,k) \to 1$. This asymptotic rate is optimal[43]. Finally, the deviations of the key length in equation (2) from its asymptotic limit can be explained as fluctuations that are due to the finiteness of the statistical samples we consider and the error bounds we chose. These terms are necessary for any finite-key analysis. In particular, one expects a statistical deviation μ that scales with the inverse of the square root of the sample size k as in equation (2) from any statistical estimation of the error rate. In this sense, our result is tight.

To obtain our results for finite block sizes n, we fix a security bound ε and define an optimized ε-secure protocol, $\Phi^*[n, \varepsilon]$, 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 $\text{leak}_{\text{EC}} = \xi n h(Q_{\text{tol}})$ with $\xi = 1.1$. Moreover, we bound the robustness ε_{rob} by the probability that the measured security parameter exceeds Q_{tol}, which (for depolarizing channels) decays exponentially in $Q_{\text{tol}} - Q$. (For general quantum channels, the error rate in the $\mathbb{X}$ and $\mathbb{Z}$ bases may be different. Hence, the error correction leakage is, in general, not a function of Q_{tol} but of the expected error rate in the $\mathbb{X}$ basis. Similarly, ε_{rob} generally is the sum of the robustness of parameter estimation as above and the robustness of the error correction scheme. In this discussion, the analysis is simplified as we consider a depolarizing channel, and, thus, the expected error rate is the same in both bases.)

In Fig. 1, we present the expected key rates $r = r(\Phi, Q)$ of the optimal protocols $\Phi^*[n, \varepsilon]$ as a function of the block size n. These rates are given for a fixed value of the security rate ε/ℓ, that is, 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

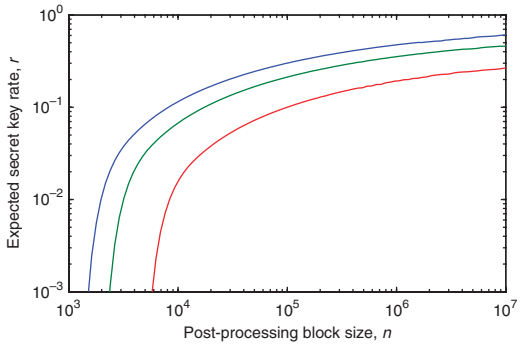

Figure 1 | Expected key rate as function of the block size. Plot of expected key rate r as a function of the block size n for channel bit error rates $Q \in \{1\%, 2.5\%, 5\%\}$ (from left to right). The security rate is fixed to $\varepsilon/\ell = 10^{-14}$.

Table 1 | Optimized parameters for security rate $\varepsilon/\ell = 10^{-14}$.

N	Q (%)	r (%)	r_{rel} (%)	p_z (%)	Q_{tol} (%)	ε_{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

The column labelled r_{rel} shows the deviation of the expected secret key rate from the corresponding asymptotic value, that is, $r_{\text{rel}} := r/(1 - 2h(Q))$.

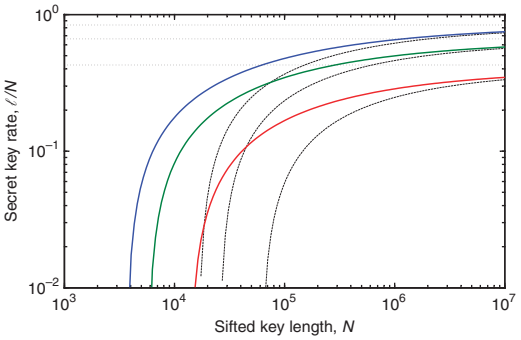

Figure 2 | Comparison of key rate with earlier results. The plots show the rate ℓ/N as a function of the sifted key length $N = n + k$ for various channel bit error rates Q (as in Fig. 1) and a security bound of $\varepsilon = 10^{-10}$. The (curved) dashed lines show the rates that can be proven secure using ref. 18. The horizontal dashed lines indicate the asymptotic rates for $Q \in \{1\%, 2.5\%, 5\%\}$ (from top to bottom).

© 2012 Macmillan Publishers Limited. All rights reserved.

key bit.) The plot shows that significant key rates can be obtained already for $n = 10^4$.

In Table 1, 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 Fig. 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[18]. For comparison with previous work, we plot the rate ℓ/n, that is, the ratio between key length and block size, instead of the expected secret key rate as defined by equation (3). 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 (Supplementary Note 2).

In conclusion, this article gives tight finite-key bounds for secure quantum key distribution with an asymmetric BB84 protocol. Our novel proof technique, based on the uncertainty principle, offers a conceptual improvement over earlier proofs that relied on a tomography of the state shared between Alice and Bob. Most previous security proofs against general adversaries[7,18,21,20], are arranged in two steps: An analysis of the security against adversaries restricted to collective attacks and a lifting of this argument to general attacks. The lifting is often possible without a significant loss in key rate using modern techniques[24,25]; hence, the main difference lies in the first part. In security proofs against collective attacks, Alice and Bob usually do tomography on their shared state, that is, they characterize the density matrix of their shared state. As the eavesdropper can be assumed to hold a purification of this state, it is then possible to bound the von Neumann entropy of the eavesdropper on Alice's measurement result. The min-entropy of the eavesdropper (which characterizes the probability of the eavesdropper guessing the secret key) is, in turn, bounded using the quantum asymptotic equipartition property[7,44], introducing a penalty scaling with $1/\sqrt{n}$ on the key rate. (A notable exception is[20] where the min-entropy is bounded directly from the results of tomography.)

In contrast, our approach bounds the min-entropy directly and does not require us to do tomography on the state shared between Alice and Bob. In fact, we are only interested in one correlation (between $\mathbf{Z}$ and $\mathbf{Z}'$) and, thus, our statistics can be produced more efficiently. (However, that this is also the reason why our approach does not reach the asymptotic key rate for the six-state protocol[45]. There, full tomography puts limits on Eve's information that go beyond the uncertainty relation in ref. 22.) Finally, as our considerations are rather general, we believe that they can be extended to other QKD protocols.

Methods

Correctness. The required correctness is ensured in the error-correction step of the protocol, when Alice and Bob compute a random hash function of their keys. If these hash values disagree, the protocol aborts and both players output empty keys (These keys are trivially correct.). Because arbitrary errors in the key will be detected with high probability when the hash values are compared[46], we can guarantee that Alice's and Bob's secret keys are also the same with high probability.

Secrecy. To establish the secrecy of the protocols, we consider a gedankenexperiment in which Alice and Bob, after choosing a basis according to probabilities p_x and p_z as usual, 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 secrecy then follows from the fact that, if Alice has a choice of encoding a string of n uniform bits in either the $\mathbb{X}$ or $\mathbb{Z}$ basis, the following holds: the better Bob is able to estimate Alice's string if she prepared in the Z basis, the worse Eve is able to guess Alice's string, if she prepared in the $\mathbb{X}$ basis. This can be formally expressed in terms of an uncertainty relation for smooth entropies[22],

$$H^{\epsilon}_{\min}(\mathbf{X}\,|\,E) + H^{\epsilon}_{\max}(\mathbf{Z}\,|\,\mathbf{Z}') \geq nq, \tag{4}$$

where $\epsilon \geq 0$ is called a smoothing parameter and q, as seen below, is the preparation quality defined previously. The smooth min-entropy, $H^{\epsilon}_{\max}(\mathbf{X}|E)$, introduced in ref. 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[47]. The smooth max-entropy, $H^{\epsilon}_{\max}(\mathbf{Z}|\mathbf{Z}')$, corresponds to the number of extra bits that are needed to reconstruct the value of $\mathbf{Z}$ using $\mathbf{Z}'$ up to a failure probability[48]. For precise mathematical definitions of the smooth min- and max-entropy, we refer to ref. 49.

The sources we consider in this article are either (a) qubit sources or (b) sources that create BB84 states by measuring part of an entangled state. In case b), a comparison with ref. 22 reveals that the bound on the uncertainty is given by $-\log c$, where c is the overlap of the two measurement employed in the source. For general positive operator-valued measurements, $\{M_x\}$ for preparing in the $\mathbb{X}$ basis and $\{N_z\}$ for preparing in the $\mathbb{Z}$ basis, this overlap is given by $c = \max \left\| \sqrt{M_x}\sqrt{N_z} \right\|^2_{\infty}$. This justifies the definition of the preparation quality $q = -\log c$ for such sources. In case a), the preparation process can be purified into an entanglement-based one of the type above. To see this, simply consider a singlet state between two qubits and projective measurements on the first qubit. It is easy to verify that the overlap of the prepared states in the two bases is equal to the overlap of the two projective measurements used to prepare them. Hence, the preparation quality of this source is given by $q = -\log c$, where c is the maximum overlap of the prepared states.

In the gedankenexperiment picture, the observed average error, λ, is calculated from 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, thus, $H^{\epsilon}_{\max}(\mathbf{Z}|\mathbf{Z}')$ is small. In fact, as the protocol aborts if λ exceeds Q_{tol}, the following bound on the smooth max-entropy (conditioned on the correlation test passing) holds:

$$H^{\epsilon}_{\max}(\mathbf{Z}\,|\,\mathbf{Z}') \leq nh(Q_{\mathrm{tol}} + \mu), \tag{5}$$

where μ takes into account statistical fluctuations and depends on the security parameter via Equation (5) is shown in Supplementary Note 2, using an upper bound by Serfling[50] on the probability that the average error on the sample, λ, deviates by more than μ from the average error on the total string[51].

In addition to the uncertainty relation, our analysis employs the Quantum Leftover Hash Lemma[7,52], 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

$$\Delta = \epsilon + \frac{1}{2}\sqrt{2^{\ell - H^{\epsilon}_{\min}(\mathbf{X}|E')}}. \tag{6}$$

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. For the protocol discussed here, a maximum of $\mathrm{leak}_{\mathrm{EC}} + \lceil \log(1/\epsilon_{\mathrm{cor}}) \rceil$ bits of information about $\mathbf{X}$ are revealed to the eavesdropper during the protocol. Hence, using a chain rule for smooth min-entropies, we can relate the smooth min-entropy before the classical post-processing, $H^{\epsilon}_{\max}(\mathbf{X}|E)$, with the min-entropy before privacy amplification, $H^{\epsilon}_{\max}(\mathbf{X}|E')$ as follows.

$$H^{\epsilon}_{\min}(\mathbf{X}\,|\,E') \geq H^{\epsilon}_{\min}(\mathbf{X}\,|\,E) - \mathrm{leak}_{\mathrm{EC}} - \log\frac{2}{\epsilon_{\mathrm{cor}}}. \tag{7}$$

Collecting the bounds on the smooth entropies we got from the uncertainty relation, (4), and the parameter estimation, (5), we further find that

$$H^{\epsilon}_{\min}(\mathbf{X}\,|\,E') \geq n(q - h(Q_{\mathrm{tol}} + \mu)) - \mathrm{leak}_{\mathrm{EC}} - \log\frac{2}{\epsilon_{\mathrm{cor}}}. \tag{8}$$

Combining this with the Quantum Leftover Hashing Lemma (6) and using the bound on the key length given in equation (2), we get

$$\Delta \leq \epsilon + \frac{1}{2}\sqrt{2^{\ell - H_{\min}(\mathbf{X}|E')}} \leq \epsilon + \frac{\epsilon_{\mathrm{sec}}}{2}. \tag{9}$$

Finally, the protocol is ϵ_{sec}-secret, if we choose ϵ proportional to ϵ_{sec} and sufficiently small.

References

1. Bennett, C. H. & Brassard, G. in *Proc. IEEE Int. Conf. on Comp. Sys. and Signal Processing* 175–179 (Bangalore, India, 1984).
2. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67,** 661–663 (1991).
3. Lo, H.- K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283,** 2050–2056 (1999).
4. Shor, P. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85,** 441–444 (2000).
5. Biham, E., Boyer, M., Boykin, P. O., Mor, T. & Roychowdhury, V. A proof of the security of quantum key distribution. *J. Cryptol.* **19,** 381–439 (2006).

© 2012 Macmillan Publishers Limited. All rights reserved.

6. Mayers, D. Unconditional security in quantum cryptography. *J. ACM* **48,** 351–406 (2001).
7. Renner, R. *Security of Quantum Key Distribution*. PhD thesis, ETH Zurich. Preprint arXiv:0512258 (2005).
8. Renner, R., Gisin, N. & Kraus, B. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A* **72,** 012332 (2005).
9. Takesue, H. *et al.* Quantum key distribution over 40 dB channel loss using superconducting single photon detectors. *Nat. Photon.* **1,** 343–357 (2007).
10. Dixon, A. R., Yuan, Z. L., Dynes, J. F., Sharpe, A. W. & Shields, A. J. Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. *Opt. Express* **16,** 18790–18979 (2008).
11. Stucki, D. *et al.* High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Phys.* **11,** 75003 (2009).
12. Scarani, V. & Kurtsiefer, C. The black paper of quantum cryptography: real implementation problems. Preprint arXiv:0906.4547 (2009).
13. Hänggi, E. *Device-Independent Quantum Key Distribution*. PhD thesis, ETH Zurich. Preprint arXiv:1012.3878 (2010).
14. Masanes, L., Pironio, S. & Acín, A. Secure device-independent quantum key distribution with causally independent measurement devices. *Nat. Commun.* **2,** 238 (2011).
15. Hayashi, M. Practical evaluation of security for quantum key distribution. *Phys. Rev. A* **74,** 022307 (2006).
16. Meyer, T., Kampermann, H., Kleinmann, M. & Bruß, D. Finite key analysis for symmetric attacks in quantum key distribution. *Phys. Rev. A* **74,** 042340 (2006).
17. Inamori, H., Lütkenhaus, N. & Mayers, D. Unconditional security of practical quantum key distribution. *Eur. Phys. J.* **41,** 599–627 (2007).
18. Scarani, V. & Renner, R. Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.* **100,** 200501 (2008).
19. Bouman, N. & Fehr, S. Sampling in a quantum population, and applications. Preprint arXiv:0907.4246 (2009).
20. Bratzik, S., Mertz, M., Kampermann, H. & Bruß, D. Min-entropy and quantum key distribution: nonzero key rates for, small numbers of signals. *Phys. Rev. A* **83,** 022330 (2011).
21. Sheridan, L., Le, T. P. & Scarani, V. Finite-key security against coherent attacks in quantum key distribution. *New J. Phys.* **12,** 123019 (2010).
22. Tomamichel, M. & Renner, R. Uncertainty relation for smooth entropies. *Phys. Rev. Lett.* **106,** 110506 (2011).
23. Berta, M., Christandl, M., Colbeck, R., Renes, J. M. & Renner, R. The uncertainty principle in the presence of quantum memory. *Nature Phys.* **6,** 659–662 (2010).
24. Renner, R. Symmetry of large physical systems implies independence of subsystems. *Nature Phys.* **3,** 645–649 (2007).
25. Christandl, M., König, R. & Renner, R. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.* **102,** 020504 (2009).
26. Canetti, R. in *Proc. 42nd IEEE Symp. on Foundations of Computer Science* 136–145 (2001).
27. Müller-Quade, J. & Renner, R. Composability in quantum cryptography. *New J. Phys.* **11,** 085006 (2009).
28. König, R., Renner, R., Bariska, A. & Maurer, U. Small accessible quantum information does not imply security. *Phys. Rev. Lett.* **98,** 140502 (2007).
29. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **61,** 052304 (2000).
30. Lo, H.- K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94,** 230504 (2005).
31. Hasegawa, J., Hayashi, M., Hiroshima, T. & Tomita, A. Security analysis of decoy state quantum key distribution incorporating finite statistics. Preprint arXiv:0707.3541 (2007).
32. Cai, R. Y. Q. & Scarani, V. Finite-key analysis for practical implementations of quantum key distribution. *New J. Phys.* **11,** 045024 (2009).
33. Song, T.- T., Zhang, J., Qin, S.- J., Gao, F. & Wen, Q.- Y. Finite-key analysis for quantum key distribution with decoy states. *Quant. Inf. Comput.* **11,** 0374–0389 (2011).
34. Bennett, C. H., Brassard, G. & Mermin, N. D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **68,** 557–559 (1992).
35. Pittman, T., Jacobs, B. & Franson, J. Heralding single photons from pulsed parametric down-conversion. *Opt. Commun.* **246,** 545–550 (2005).
36. Xiang, G. Y., Ralph, T. C., Lund, A. P., Walk, N. & Pryde, G. J. Heralded noiseless linear amplification and distillation of entanglement. *Nat. Photon.* **4,** 316–319 (2010).
37. Gisin, N., Pironio, S. & Sangouard, N. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. *Phys. Rev. Lett.* **105,** 070501 (2010).
38. Curty, M. & Moroder, T. Heralded-qubit amplifiers for practical device-independent quantum key distribution. *Phys. Rev. A* **84,** 010304 (2011).
39. Pitkänen, D., Ma, X. F., Wickert, R., van Loock, P. & Lütkenhaus, N. Efficient heralding of photonic qubits with apllications to device independent quantum key distribution. *Phys. Rev. A* **84,** 022325 (2011).
40. Lydersen, L. *et al.* Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.* **4,** 686–689 (2010).
41. Lo, H.- K., Chau, H. & Ardehali, M. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol.* **18,** 33–165 (2004).
42. Cover, T. M. & Thomas, J. A. *Elements of Information Theory* (Wiley, 1991).
43. Renner, R., Gisin, N. & Kraus, B. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A* **72,** 012332 (2005).
44. Tomamichel, M., Colbeck, R. & Renner, R. A fully quantum asymptotic equipartition property. *IEEE Trans. Inf. Theory* **55,** 5840–5847 (2009).
45. Bruß, D. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* **81,** 3018–3021 (1998).
46. Carter, J. L. & Wegman, M. N. Universal classes of hash functions. *J. Comp. Syst. Sci.* **18,** 143–154 (1979).
47. König, R., Renner, R. & Schaffner, C. The operational meaning of min- and max-entropy. *IEEE Trans. Inf. Theory* **55,** 4337–4347 (2009).
48. Renes, J. M. & Renner, R. One-shot classical data compression with quantum side information and the distillation of common randomness or secret keys. Preprint arXiv:1008.0452 (2010).
49. Tomamichel, M., Colbeck, R. & Renner, R. Duality between smooth min- and max-entropies. *IEEE Trans. Inf. Theory* **54,** 4674–4681 (2010).
50. Serfling, R. J. Probability inequalities for the sum in sampling without replacement. *Ann. Statist.* **2,** 39–48 (1974).
51. van Lint, J. H. *Introduction to Coding Theory (Graduate Texts in Mathematics)* (Springer, 1999).
52. Tomamichel, M., Schaffner, C., Smith, A. & Renner, R. Leftover hashing against quantum side information. *IEEE Trans. Inf. Theory* **57,** 5524–5535 (2011).
53. Bennett, C. H., Brassard, G., Crepeau, C. & Maurer, U. M. Generalized privacy amplification. *IEEE Trans. Inf. Theory* **41,** 1915–1923 (1995).
54. Renner, R. & König, R. in *Proc. TCC 3378 of LNCS* (ed. Kilian, J.) 407–425 (Springer, Berlin/Heidelberg, Cambridge, USA, 2005).
55. De, A., Portmann, C., Vidick, T. & Renner, R. Trevisan's Extractor in the Presence of Quantum Side Information. Preprint arXiv:0912.5514 (2009).

Acknowledgements

We thank Silvestre Abruzzo, Normand Beaudry, 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).

Author contributions

The main ideas were developed by all authors. M.T. and R.R. formulated and proved the technical claims and wrote the manuscript. C.L. provided numerical simulations and contributed to the technical derivations and write-up.

Additional information

Supplementary Information accompanies this paper at http://www.nature.com/naturecommunications

Competing financial interests: The authors declare no competing financial interests.

Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/

How to cite this article: Tomamichel, M. *et al.* Tight finite-key analysis for quantum cryptography. *Nat. Commun.* 3:634 doi: 10.1038/ncomms1631 (2012).

License: This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivative Works 3.0 Unported License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/3.0/

© 2012 Macmillan Publishers Limited. All rights reserved.