QKD: a million signal task

Valerio SCARANI [a,1]

[a] *Centre for Quantum Technologies and Department of Physics, National University of Singapore, Singapore.*

Abstract. I review the ideas and main results in the derivation of security bounds in quantum key distribution for keys of finite length. In particular, all the detailed studies on specific protocols and implementations indicate that no secret key can be extracted if the number of processed signals per run is smaller than $10^5 - 10^6$. I show how these numbers can be recovered from very basic estimates.

Keywords. Quantum key distribution, finite-keys

1. Introduction

In the very first proof of unconditional security of quantum key distribution (QKD), Mayers already stressed the need to obtain *finite-key bounds* and paved the path for this task [1]. The complex development of QKD, which has been reviewed elsewhere [2], explains why this task was finally achieved only recently.

This text is a concise presentation of finite-key security proofs, written for readers that are already familiar with the main notions of QKD. I use the approach developed by Renato Renner in his thesis [3] and applied later to the specific study of finite-key effects [4,5,6]. Independently, and actually some months earlier than Renner and myself, Hayashi has also developed finite-key analysis [7,8,9]. A recent work by Fung, Ma and Chau tackles the problem from yet another approach [10]. It must be stressed that all these approaches are recognized to be ultimately based on the same definition of security and lead to the same order of magnitude for the finite-key corrections, although there may be differences in details.

2. Finite-key corrections

In a QKD protocol, Alice and Bob have to infer the information that could have leaked to the eavesdropper Eve on the basis of some measured parameters: error rates, detection rates, and others. These parameters and the way of measuring them define the protocol. Let us refer to them as $\mathbf{V}$ measured value of the parameters.

Let N be total number of signals exchanged by Alice and Bob in a run of key exchange, n the number of signals kept for the key (i.e. the length of the raw key) and m

[1] Corresponding Author: Centre for Quantum Technologies, 3 Science Drive 2, Singapore 117543. E-mail: physv@nus.edu.sg.

the number of signals used for parameter estimation. The length of the secret key to be extracted is denoted by ℓ. The usually quoted number is the *secret key fraction* $r = \frac{\ell}{N}$.

It is important to note from the start that a *run of key exchange* is defined as the number of signals that shall be processed together: obviously, the duration of the key exchange cannot increase its security. In all this text, I focus on one-way post-processing without pre-processing, so specifically a run is defined by the size of the blocks on which privacy amplification is performed.

In the asymptotic limit, the expression of r is by now well-known:

$$r_\infty = \lim_{N\to\infty} \frac{\ell}{N} \; = \min_{E|\mathbf{V}} H(A|E) - H(A|B) \tag{1}$$

It has an intuitive meaning: the fraction that can be extracted is the uncertainty of Eve minus the uncertainty of Bob (or equivalently, the information of Bob minus the information of Eve) on Alice's key.

The finite-key bound, to be proved below, reads

$$r_N = \frac{\ell}{N} \; = \; \frac{n}{N}\left[\min_{E|\mathbf{V}\pm\mathbf{\Delta V}} H(A|E) - \Delta(n) - \mathrm{leak}_{EC}/n\right] . \tag{2}$$

Four differences between (1) and (2) are worth stressing:

1. $\frac{n}{N}$: in the asymptotic case, the protocol can be adapted so that almost all the signals are used for the raw key and only a negligible fraction is used for parameter estimation [11]. This is of course no longer the case in the finite-key regime: one needs to devote enough many signals to parameter estimation in order to have good statistics.
2. $V \pm \Delta V$: the statistical estimates of the parameters come with fluctuations for finite sampling.
3. leak$_{EC}$: this is the information that leaks out to Eve during error correction; in the asymptotic case, it is given by the Shannon bound $H(A|B)$, but for practical codes on finite samples the Shannon bound may not be reached.
4. $\Delta(n)$: while the three previous items are pretty obvious and and had in fact been anticipated in many works, both theoretical and experimental, this term is the challenging one. It comes as an overhead to privacy amplification: the task itself cannot be carried out perfectly on finite samples.

In summary, the theoretical challenge of finite-key analysis mainly consists of obtaining an expression for $\Delta(n)$. As we shall show, once this expression is obtained, one can study which of the corrections has the largest effect; it will turn out that the most dramatic correction comes from the "obvious" need to take into account ΔV, the statistical fluctuations in the estimate of the parameters.

3. Derivation of the finite-key bound

3.1. Scenario

The following equation summarizes the steps of a QKD exchange:

$$\begin{aligned}\Phi_{AB}^{\otimes N} \xrightarrow{\text{Eve}} \Psi_{A^N B^N E} &\xrightarrow{\text{Meas.}} \sum_{\underline{a},\underline{b}\in\{0,1\}^n} p(\underline{a},\underline{b})|\underline{a}\rangle\langle\underline{a}|\otimes|\underline{b}\rangle\langle\underline{b}|\otimes\rho_E^{\underline{a},\underline{b}} \;\text{ and parameters } \mathbf{V}\\ &\xrightarrow{\text{EC}} \sum_{\underline{a}\in\{0,1\}^n} p(\underline{a})|\underline{a}\rangle\langle\underline{a}|\otimes|\underline{a}\rangle\langle\underline{a}|\otimes\rho_{\mathcal{E}}^{\underline{a}}\\ &\xrightarrow{\text{PA}(\mathbf{V})} \Big(\sum_{\underline{k}\in\{0,1\}^\ell}\frac{1}{2^\ell}|\underline{k}\rangle\langle\underline{k}|\otimes|\underline{k}\rangle\langle\underline{k}|\Big)\otimes\rho_{\mathcal{E}} \;\equiv\rho_U\otimes\rho_{\mathcal{E}}\;.\end{aligned}$$

In words: on the quantum channel, Eve interacts with the N signals flying between Alice and Bob; by giving Eve a purification of the whole state, we give her the maximal possible information. When Alice and Bob measure, the total state becomes a classical-classical-quantum (ccq) state. After error correction (EC), Alice's and Bob's classical lists are equal, but Eve has gained some additional classical information: $\rho_{\mathcal{E}}^{\underline{a}} = \sum_{\underline{b}} p(\underline{b}|\underline{a})\rho_E^{\underline{a},\underline{b}}\otimes|C(\underline{b}\to\underline{a})\rangle\langle C(\underline{b}\to\underline{a})|$. After privacy amplification (PA), the lists of Alice and Bob are shorter, but still equal and now drawn from a completely random distribution, on which Eve has no information.

This is for the ideal case. In order to estimate ℓ, the first step consists in defining a security parameter. The most convenient choice, actually the only one with the suitable properties known to date (see [4] for a discussion), is the *probability that the processed state differs from the ideal one*:

$$\epsilon = \frac{1}{2}\,\mathrm{Tr}\,|\rho_{KE}-\rho_U\otimes\rho_E|\;. \tag{3}$$

So, now we choose a value for ϵ (say 10^{-9}, i.e. I want at most one run in one billion to go wrong), our data processing defines N: how to get the corresponding ℓ? This is the subject of the next paragraph.

3.2. Renner's version of Murphy's law

The recipe is: quantify everything that can go wrong, going backwards, i.e. starting from PA and going up to parameter estimation. Here is what it gives in detail:

1. First step: **Privacy amplification**. The probability that PA fails even if everything has been perfectly carried out is

$$\epsilon_{PA} = 2^{-\frac{1}{2}\left(H_{min}^{\bar\epsilon}(A^n|\mathcal{E})-\ell\right)}\,. \tag{4}$$

As usual, for the proof and the exact definitions I refer to the original papers quoted above. Let us however get an intuition of this result. The symbol $\mathcal{E}$ represent all that Eve has learned, both from attacking the quantum channel and from listening to error correction. Alice's information is denoted by A^n to remind that it is a sequence of n bits. The main object introduced here is $H_{min}^{\bar\epsilon}(\cdot|\cdot)$ is the quantum conditional *smooth min-entropy*, with $\bar\epsilon$ the smoothing parameter. It is not astonishing that a min-entropy appears here: as we said above, the final key should be randomly distributed given Eve's knowledge. In classical information theory, the min-entropy precisely quantifies the fraction of completely random bits one can extract from a given list of partially random bits. The challenge consisted in defining the quantity that plays the same role, in the case where an ad-

versary has quantum information. This was done in Renner's thesis [3]. So, in a sense, (4) can be seen as a definition of smooth min-entropy, or better, as one of the desiderata: the smooth min-entropy must be such that (4) holds.
Now, for the right-hand side of (4) to be bounded, one must have

$$\ell \,\leq\, H_{min}(A^n|\mathcal{E}) - 2\log\frac{1}{\epsilon_{PA}}\;. \tag{5}$$

It is crucial to understand that this is *already* the desired bound for ℓ. Unfortunately, there is no easy way of computing $H_{min}(A^n|\mathcal{E})$: the next steps will be merely bound on this last quantity, reaching to an ultimately computable expression.

2. Second step: **error correction**. First, we have to add an ϵ_{EC} to the failure probability ϵ. This measures the probability that the EC procedure was apparently successful but some uncorrected errors remain[2]. Moreover, as we said, during EC, additional data C has been provided to Eve, giving an amount of information leak_{EC}; by using a chain rule, one can split this information from the one acquired in attacking the quantum channel, denoted by E. So we obtain the expression

   $$H_{min}(A^n|\mathcal{E}) = H_{min}(A^n|E) - \text{leak}_{EC}\;. \tag{6}$$

   Theory predicts $\text{leak}_{EC} \approx fH_0(A^n|B^n) + \log\frac{2}{\epsilon_{EC}}$, but ultimately this is number of bits *really* exchanged during EC: it does not need theoretical modeling (unless one is working on designing a better EC code), just pick it from the real run of the EC code.
3. Third step: **Eve's attack on the quantum channel**. Now we are back at the level of quantum interaction and we have to compute $H_{min}(A^n|E)$: how much information Eve might have acquired, given the observed disturbances $\mathbf{V}$. Under the assumption of collective attacks, one finds

   $$H_{min}(A^n|E=E^n) \leq n\left[H(A|E) - 7\sqrt{\frac{\log(2/\bar{\epsilon})}{n}}\right]\;. \tag{7}$$

   The assumption of collective attacks is not restrictive for the Bennett-Brassard 1984 (BB84) protocol and many others, under the validity of the squashing condition[3]. In order to remove this assumption, one could resort to the suitable De Finetti theorem, but the bound scales very badly. A much more promising approach is based on Ref. [14], but to my knowledge it has not been applied yet in the context of finite-keys.
4. Fourth step: **Optimize over Eve's attacks**. Since we don't know which attack Eve has actually performed, $H(A|E)$ must be computed for the best possible attack compatible with the measured parameters $\mathbf{V}$. But these parameters have

[2] This may sound cumbersome at first reading, but it is actually clear. Any EC procedure has a possible red-flag outcome: "Sorry, the procedure was not successful". In this case, one just discards the raw key, without compromising the security. Problems arise only when there are still uncorrected errors left but the red flag is not raised.

[3] This condition means that one can prove the security of a protocol on the level of qubits, even if physically light fields are infinitely dimensional systems. In other words, one can "squash" the meaningful degrees of freedom down to qubits. This statement has been rigorously proved for the BB84 protocol [12,13].

been measured on a finite sample: they are subject to fluctuations $\mathbf{\Delta V}$. Specifically, if a value V_m has been obtained after averaging on m samples, one has[4]

$$\Delta V = \sqrt{\frac{\ln(1/\epsilon_{PE}) + d\ln(m+1)}{2m}}\,. \tag{8}$$

with ϵ_{PE} the probability that the fluctuation is actually larger than ΔV and d the minimal number of outcomes of the POVM that is used to estimate V (typically, $d = 2$ for errors on bits: one has to estimate the probabilities of the event "bits equal" and of the event "bits different").

Putting everything together, one obtains (2) with

$$\Delta(n) = \frac{2}{n}\log\frac{1}{\epsilon_{PA}} + 7\sqrt{\frac{\log(2/\bar{\epsilon})}{n}}\,. \tag{9}$$

Since failure probabilities add, the total error is

$$\epsilon = \epsilon_{PA} + \bar{\epsilon} + n_{PE}\epsilon_{PE} + \epsilon_{EC} \tag{10}$$

with n_{PE} the number of parameters to be estimated.

This concludes our overview of the meaning and derivation of the finite-key bound (2). As we mentioned, there are alternative approaches [7,8,9,10]: as they stand, these approaches are specifically tailored for the BB84 protocol; but there is no reason to doubt that they can be adapted to other protocols as well.

4. Rapid estimates of finite key effects

To date, the bound (2) has been applied to the BB84 protocol, both in the ideal single photon case [4] and in more realistic scenarios [6], as well as to ideal implementations of the six-state protocol [4] and of a modified Ekert protocol [5]. In spite of the differences and for a wide range of reasonable values of parameters, a common feature is observed: r_N becomes larger than 0 only for $N \approx 10^5 - 10^6$. Here, we show with a simple estimate that this is indeed the case.

We suppose that all epsilons are of the order $10^{-3} \approx 2^{-10}$. This is quite a poor requirement: it means that the key exchange may fail once every thousand runs only; but anyway, one would only get a small overhead by choosing 10^{-9} instead, because the dependence in the epsilons is logarithmic.

Another useful approximation is $m \approx n \approx N/2$. Close to the critical point where r_N passes from being 0 to be positive, this is always observed in exact numerical estimates of (2), and it is quite reasonable: in the critical regime, one tries to devote enough many signals to the parameter estimation, without compromising the key.

Under these two assumption, we have the following approximate values for (9) and (8) respectively:

$$\Delta(n) \approx \frac{40}{N} + 7\sqrt{\frac{12}{N}}\ ,\ \Delta V \approx \sqrt{\frac{9+2\ln(N)}{N}}\,. \tag{11}$$

[4] Note added: the following equation is imprecise for $d > 2$: see a better discussion in L. Sheridan and V. Scarani, Phys. Rev. A **82**, 030301(R) (2010).

Let's consider two case studies:

1. **Case study: effect of** $\Delta(n)$. Suppose we are in a regime of parameters such that $r_\infty = 0.1$. Neglecting the parameter fluctuations ΔV, from (2) one has $r_N \approx r_\infty - \Delta(n)$. This quantity is positive for $N \approx 10^5$. Of course, the estimate becomes worse, the smaller r_∞ is (for instance, as a function of the distance in a practical implementation). In summary, the finite-sample corrections to privacy amplification force a lower bound of $N \approx 10^5$ signals per run.
2. **Case study: effect of** ΔV. Consider V as the most typical parameter in QKD, namely an error rate. Because of the quality of optical setups, errors normally range around $1 - 2\%$. At which point r_N is zero depends on many variables and of course on the protocol, so we cannot be very specific here. But if one requests that error rates are known to a precision $\Delta V \approx 0.5\%$, one needs $N \approx 10^6$ signals per run.

From these case studies, we see how the estimate $N > 10^5 - 10^6$ arise from quite trivial estimates of the finite-key effects, independently of the details of the protocols.

5. Conclusion

Claims of security of QKD could not be complete without integrating the effects of finite sampling, or finite-key in short. Thanks to the work of several authors, this task has now been accomplished. One of the most striking features is the fact that, to have any final key whatsoever, approximately one million signals must be processed in each run — and the more, the better. In this text, after reviewing the main ingredients of the finite-key bounds, I have stressed that the lower bounds on the number of signals can be obtained from very simple estimates and are therefore rather robust. While the performances of QKD may still be improved in many aspects, it seems unavoidable that QKD will always be a *million-signal task*; or, to put it more positively, I would consider it as a milestone if someone could find a way of improving significantly on these bounds.

Acknowledgements

I thank all the participants to the workshop "Quantum cryptography with finite resources" (Singapore, 4-6 December 2008) for very valuable comments and queries. This work was supported by the National Research Foundation and the Ministry of Education, Singapore.

References

[1] D. Mayers, in: Advances in Cryptology — Proceedings of Crypto '96 (1996) (Springer Verlag, Berlin), p. 343

[2] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, Rev. Mod. Phys. **81** (2009), 1301

[3] R. Renner, *Security of Quantum Key Distribution*, PhD thesis, Diss. ETH No 16242; published in: Int. J. Quant. Inf. **6** (2008), 1

[4] V. Scarani, R. Renner, Phys. Rev. Lett. **100** (2008), 200501

[5] V. Scarani, R. Renner, in: *Proceedings of TQC2008*, Lecture Notes in Computer Science **5106** (2008) (Springer Verlag, Berlin), pp. 83-95; and arXiv:0806.0120

[6] R.Y.Q. Cai, V. Scarani, New J. Phys. **11** (2009), 045024

[7] M. Hayashi, Phys. Rev. A **76** (2007), 012329

[8] J. Hasegawa, M. Hayashi, T. Hiroshima, A. Tomita, arXiv:0707.3541.

[9] M. Hayashi, Phys. Rev. A **79** (2009), 032303(R)

[10] C.-H.F. Fung, X. Ma, H.F. Chau, arXiv:0910.0312

[11] H.-K. Lo, H. F. Chau, M. Ardehali, J. Cryptology **18** (2005), 133; and quant-ph/9803007.

[12] N.J. Beaudry, T. Moroder, N. Lütkenhaus, Phys. Rev. Lett. **101** (2008), 093601

[13] T. Tsurumaru, K. Tamaki, Phys. Rev. A **78** (2008), 032302

[14] M. Christandl, R. Koenig, R. Renner, Phys. Rev. Lett. **102** (2009), 020504