Quantum Information and Computation, Vol. 12, No. 3&4 (2012) 0203–0214

IMPROVED DATA POST-PROCESSING IN QUANTUM KEY DISTRIBUTION AND APPLICATION TO LOSS THRESHOLDS IN DEVICE INDEPENDENT QKD

XIONGFENG MA NORBERT LÜTKENHAUS
Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo
200 University Ave W., Waterloo, ON, Canada N2L 3G1

xfma@iqc.ca *nlutkenhaus@uwaterloo.ca*

Received September 28, 2011
Revised December 6, 2011

Security proofs of quantum key distribution (QKD) often require post-processing schemes to simplify the data structure, and hence the security proof. We show a generic method to improve resulting secure key rates by partially reversing the simplifying post-processing for error correction purposes. We apply our method to the security analysis of device-independent QKD schemes and of detection-device-independent QKD schemes, where in both cases one is typically required to assign binary values even to lost signals. In the device-independent case, the loss tolerance threshold is cut down by our method from 92.4% to 90.9%. The lowest tolerable transmittance of the detection-device-independent scheme can be improved from 78.0% to 65.9%.

Keywords:
Communicated by: B Kane & G Milburn

1 Introduction

Quantum key distribution (QKD) [1, 2] provides a means of distributing secure keys between two distant parties, Alice and Bob. It uses a quantum channel and an authenticated classical channel. The security of specific abstract QKD protocols has been proven in literature under varying definitions of security [3, 4, 5]. A clear framework for security proofs including finite-size effects has been put forward by Renner [6]. For a review of the subject, one can refer to [7, 8, 9] and references therein.

When it comes to real optical implementations, security proofs have to be able to take non-ideal devices into consideration. A lot of effort has been made to achieve the security of QKD with realistic devices [10, 11, 12, 13, 14]. One approach is based on exact models of the devices. As security proofs have to apply to the infinite-dimensional Hilbert space of optical modes, one seeks methods to simplify the analysis. One method is to apply coarse-graining of data, by which we mean a postprocessing of data. Let us give two examples for this coarse-graining.

The first example is the random assignment of double-click events in the BB84 protocol with threshold detectors. This assignment allows the construction of a squashing model [14]

so that the security of the optical implementation can be tied directly to a corresponding abstract qubit protocol.

The other example is the treatment of loss in QKD. The possibility of transmission and detection losses can be easily incorporated in the security proofs as long as it holds that the loss probability is independent of the chosen measurement basis. However, as demonstrated in [15, 16, 17, 18] this assumption is violated in typical implementations by adversarial action. As a result, QKD schemes can be completely broken if they do not address this point [19]. One way to patch this loophole is to assign measurement outcomes even to lost signals. The typical choice is a random assignment. In this way, signal loss is converted into an effective error rate on the data. Using this patch, it is now possible to circumvent the need for precise characterization of devices in the paradigm of device-independent (originally known as self-testing) QKD schemes. Since the early work by Mayers and Yao in 1998 [20], a few more realistic [21, 22] and generalized [23] schemes have been proposed. Recently, the security analysis of device-independent schemes has made progress [22, 24, 25, 26]. The main drawback of these schemes are their severe constraints on physical devices in practice. For example, the security analysis of Pironio et al. [24] gives a tolerable error rate is 7.1% which translates to a required minimum transmittance of 92.4%. Less restrictive schemes are detection-device-independent schemes which assume some generic structure on the source side, but makes no assumption on the detection devices. Examples of this approach include [3, 27, 28].

The post-processing schemes mentioned above (random assignment of data to double-clicks, random assignment of lost signals) are done for convenience. So for the purpose of the security proofs, we erase the history of the assignment, meaning that we ignore the knowledge which of the data have been affected by the postprocessing. It is clear that security proofs can be also obtained without this erasure, however, these proofs will be more complicated to obtain. In this paper we address the question whether we can improve the key rate by making use of our knowledge of the positions within the data string that, for example, have been assigned random values. We will demonstrate a generic way of making use of the knowledge, without the need to revisit the full security proof. Of course, this approach will work only if the QKD protocol and the security proof follows some generic structure. In Section 2 we outline these generic structures. Then, in Section 3 we provide the generic method to use our extra knowledge to improve the key rate. We then illustrate the effect of our method for two examples, for the detection-device-independent scheme in Sec. 3.3, and for the full device-independent scheme in Sec. 3.4.

2 Protocols and Security proofs

QKD protocols typically involve two phases: the quantum phase, in which quantum signals are distributed and measured, resulting in correlated classical data shared between Alice and Bob, and a classical phase, where these classical data are processed by classical communication protocols. The classical phase has the goal to establish a secure key. By definition, a secure key should be *identical* between Alice and Bob, and *private* (unknown to an eavesdropper, Eve). For an example of data processing procedures, one can refer to [6, 29, 30]. A typical classical data processing can be divided into three steps:

1. **data pre-processing**, which includes

(a) **Sifting processes:** any post-selection of signals, for example based on basis settings or non-detection events. Sifting always uses two-way classical communication;

(b) **Coarse graining:** data processing aiming at simplifying the data structure, such as random bit assignments for double clicks, or random bit assignments for non-detected signals; coarse graining is always a local process and does not involve any communication. All following steps are based on the coarse-grained data only;

(c) **advanced pre-processing:** further pre-processing, locally or by two-way communication, based on the coarse-grained data, for example advantage distillation [31], especially the so-called *B steps* [32, 33]), and adding noise [34];

(d) **parameter estimation:** parameter estimation of the correlations shared between Alice and Bob, thus drawing limits on the correlations between Alice and Eve by quantum mechanics. This includes the estimation of the error rate, but also includes the decoy state analysis [35, 36, 37].

2. **error correction**, which ensures the key shared by Alice and Bob to be *identical*;

3. **privacy amplification**, which ensures the key to be *private*.

In this work, we assume that the step of error correction is performed in a uni-directional way from one party to the other, without loss of generality from Alice to Bob. As a result, the final key can be determined by Alice already after the data pre-processing step, as she sends out error correction information to Bob which enables Bob to correct his data to Alice's, and the privacy amplification step can be done with a hashing function chosen by Alice. Our results may be extended to scenarios without this assumption, as long as Alice's data determine the final key.

There are many security proofs for QKD protocols that follow the outlined procedure, see references in [7, 8, 9]. These proofs are using different techniques and give a rate R at which secure key can be generated. We illustrate our finding in the infinite key limit, denoted as rate R_∞, although our method will be directly applicable also for any analysis that includes finite size statistics. For our generic protocol, this key rate takes the form

$$R_\infty \geq H(A) - fH(A|B) - I_{pa}, \tag{1}$$

where $H(A)$ entropy of Alice's data after the data pre-processing step. Further, $H(A|B)$ is the entropy on Alice's data given Bob's data, so that this term amounts to the minimum number of bits (Shannon limit) that Alice has to send to Bob per retained signal in order for Bob to be able to correct his data to match it to Alice's data. The factor $f \geq 1$ is an efficiency factor that characterizes the actual error correction protocol that has been followed. The Shanon limit corresponds to $f = 1$, while in practice we find typical values of $f \in (1.05, 1.25)$. The last term, I_{pa}, is some measure of Eve's information on the key, leading to a key reduction in privacy amplification. The form of I_{pa} depends on the exact form of the security definition of the key, the exact QKD protocol, and potentially also on the security proof technique. It is the latter reason that we refer to these key rates as lower bounds, as any valid security proof guarantees that at least this amount of secret key can be extracted during the QKD protocol, while improved security proofs may give higher secret key rates without changing the protocol.

There are three widely used approaches for security analysis:

1. **Entanglement distillation based:** Shor-Preskill [5], based on [38, 4], with $I_{pa} = h[e_p]$, where e_p is the phase error rate of qubit signals and $h[x] = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function; This approach is designed for fully characterized devices and typically requires specifically constructed error correction methods (e.g. linear codes).

2. **Entropy based: characterized devices** Based on ideas by Ben-Or, this approach has been advanced by Devetak and Winter [39], and made rigerous by Renner [6]. In the infinite key limit, we obtain with $I_{pa} = \chi_E$ and χ_E is the Holevo bound [40] on Eve's information about Alice's key. This approach can also be used to perform a security analysis of device independent QKD in the infinite key limit assuming collective attacks [24] and infinite key limit with general attacks [25, 26].

3. **Entropy based: Complementarity** This approach has been first proposed by Koashi [10, 27] and recently put into a rigorous framework by Tomamichel et al. [41]. We obtain for qubits again $I_{pa} = h[e_p]$. This approach has been suggested to remain valid even if uncharacterized detection devices are used.

In all these proofs, the key rate can be viewed as the rate at which signals emerge from the initial data pre-processing, shortened by the amount of information of error correction sent from Alice to Bob and also shortened by a privacy amplification term I_{pa}. As stated before, for our analysis the exact details of the security analysis leading to the term I_{pa} will not be important, as we will deal with the error correction part of the protocol. For this, however, it is important to understand how the effective key rate R_∞ comes about. Let us outline some of the approaches that deal with the influence of error correction on the key rate.

The first method uses encryption of the data sent from Alice and Bob by a one-time pad during error correction. This idea has been proposed in [42] and later refined by [43]. This approach allows to decouple error correction from privacy amplification. Then privacy amplification needs only to address the initially available correlations between Alice and Eve. As we use one-way error correction, Alice's data are not affected by this error correction at all. So we generate a secret key at rate $H(A) - I_{pa}$, but we use up secret key at a rate of $fH(A|B)$ to encrypt the error correction information, resulting in the net rate shown in Eq. (1).

The second method is to keep track of the amount of information that becomes available to Eve during error correction. In this approach, privacy amplification has to shorten the key in order to cut out not only Eve's initial correlations with Alice's data, but also those correlations between Alice and Eve that result from Eve listening to the extra information becoming available during error correction. The result is again the net rate Eq. (1), though the argumentation behind this form differs between the different security approaches. In the entanglement based approach, the argumentation follows directly from the structure of quantum error correction codes that are used to effectively distill entanglement. In the two entropy based approaches, instead, one uses results that show that the entropy of Eve's system conditioned on Alice's data can be reduced at most by one bit per bit of data announced by Alice during error correction. As the amount of required key shortening during privacy amplification depends exactly on Eve's entropy about the key before privacy amplification, we obtain again the key rate shown in Eq. (1).

3 Advanced Efficient Error Correction

As we have seen in the above discussion, the key rates that result from the various security proofs depend only on the actual amount of error correction information that is being sent from Alice to Bob. Our key observation is that this amount of information can be reduced if Bob accesses his refined knowledge about his detection events. Moreover, accessing the refined information by Bob for the purpose of error correction in this setting does not affect the correlations between Alice and Eve, and hence does not affect the term I_{pa}. We will now make these statements more precise. For our arguments, we continue to refer for illustrative purposes to the asymptotic key rate in QKD, but we emphasize again that all arguments also hold in the case of finite key sizes.

We start with the cost of error correction, denoted by $B^{(c)}$, the refined data known to Bob after sifting, coarse graining and advance pre-processing. Then $B^{(r)}$ are the same data, extended by the refined data on which the coarse-graining was based. Then it follows from the data-processing inequality [44] that

$$H(A|B^{(c)}) \geq H(A|B^{(r)})$$

so that we have the opportunity to enable Bob to reconcile his data with Alice's data string with less error correction data by making use of the refined knowledge of Bob.

3.1 Background

Next, we need to investigate the effect the use of the refined data have on the full security proof, and thus on the term I_{pa}. If we use the method of encrypting the error correction information using the one-time pad encryption of the error correction information, then it is clear that if the larger amount $H(A|B^{(c)})$ of information is sent encrypted and the resulting key is secure, then the security is not affected if the smaller amount of information according to $H(A|B^{(r)})$ is sent, as from Eve's point of view nothing changes. However, as a result, the net key rate increases. Note that also the amount of encrypted error correction information does not change Eve's view: Eve can predict the statistics of the refined information on Bob's side from her eavesdropping action, and also Alice can only make use of this statistics to design the error correction information.

If we use an entanglement based approach, including a structured quantum error correction method, then the correction of bit-errors decouples from the correction of phase-errors. The refined data then serve as a side-information to Bob to help him to be more efficient in correcting the bit-errors. The correction of phase-errors (and hence the privacy amplification) is not affected by this.

Finally, using entropy-based security proof approaches, note that again the refined knowledge can be considered as local side-information at Bob's side. As it is not known to Eve or even Alice, it does not affect the initial correlations between Alice's and Eve's data. The entropy-based security proofs only count the actual number of error correction bits that Alice sends out to Bob to allow Bob to perform error correction. If this number goes down, the effective secret key rate goes up by the same amount.

Note that all these arguments also hold in the case of finite key sizes as in all security proof approaches the final key size depends on the actual number of bits exchanged during error correction. Moreover, the decoupling arguments for error correction information and I_{pa}

holds also in both cases. Therefore our method is compatible with finite size security proofs including [45, 46, 29, 30, 6, 41].

3.2 BB84 protocol

To illustrate the effect of our method, let us start by considering the BB84 protocol [1]. The secure key rate for the qubit based protocol is given by

$$R_{BB84}^{qubit} = 1 - h[e] - h[e] \tag{2}$$

where e is the observed quantum bit error rate. This rate can be proven to be secure by many different methods [3, 5, 27, 6], where the results of Mayers and Renner can also be shown to hold for lossy channels. In the latter case, the base of the secret key rate are the detected signals. We separated the individual terms corresponding to error correction at the Shannon limit as $H(A|B) = h[e]$ from the privacy amplification term $I_{pa} = h[e]$.

In optical systems, even using ideal single photon sources as qubit sources, we need to deal with the fact that the detectors operate on optical modes. By assigning double clicks [47] to randomly assigned binary values, one can use the existence of a squashing model [14, 13] for the photo-detector set-up to uplift the secure key rate for the qubit protocol over lossy qubit channels to the the same protocol over lossy optical channels with threshold detectors.

Doing the coarse-graining of assigning double-clicks to single click events, we find an effective quantum bit error rate for the coarse grained data as

$$e^{(c)} = e_s P_s + \frac{1}{2}(1 - P_s), \tag{3}$$

where P_s is the rate of single clicks within the detected signals, which exhibit some error rate e_s so that $1 - P_s$ is the rate double clicks, which lead through random-bit assignment to an error rate of $1/2$. This results in a key rate

$$R_{BB84}^{(c)} = 1 - 2h[e^{(c)}] \, . \tag{4}$$

We now give Bob access to refined data, so that he knows at which positions he assigned random single click outcomes instead of the double click outcomes. The entropy $H(A|B^{(r)})$ corresponds to that of an erasure channel with error rate e_s, so we find

$$H(A|B^{(r)}) = P_s h[e_s] + (1 - P_s) \, . \tag{5}$$

With that, the key rate improves over Eq. (2) to

$$R_{BB84}^{(r)} = P_s \left(1 - h[e_s]\right) - h[e^{(c)}] \, . \tag{6}$$

As discussed before, the data processing inequality guarantees that this method improves the secret key rate. The number of double-clicks in typical experiments is not very high, so the difference between the two secure key rates is not very big. Our next example will show a scenario where the difference is more important, as there we will be forced to deal with loss of signal. Signal loss is by far the dominating effect in QKD secure key rates compared to the effect of errors within the detected signals.

3.3 Detection-device-independent scheme

In many QKD security proofs, one starts with a full characterization of sources and detection devices. This scenario can be relaxed by having only characterized sources, while the detection devices remain uncharacterized. A security proofs following these lines is the one by Mayers [3], but also the proofs of Koashi [27] and Tomamichel [41] have been suggested to have this property. However, in order to deal with transmission and detection losses, one has either to assume that the detection efficiency of the receiver is basis independent, and then can discard all lost signals, or one does not adopt any additional assumption, and then has to coarse-grain the non-detection event into the (binary) outcome events in order for these proofs to apply directly.

We are interested in the case where we do not make additional assumption on the receiver, and instead randomly assign binary values to no-click and double click events. Koashi has indicated that, given a source which emits signals such that the density matrix averaged over the signals of each basis are independent of this basis, the secret key rate for the standard coarse-grained data processing is given by once again by Eq. (4) with the corresponding error rate given by Eq. (3). In that error rate, the single click probability P_s and error rate e_s is now the complement not only of the double clicks, but also of the no-click events, all of which are now coarse-grained by mapping them into random events.

To illustrate the improvement we perform a simulation of the observed parameters to predict the key rates. For this purpose we will neglect detector dark counts, as our simulations will give secret keys only for total transmissivities over 50% and therefore the rate of detected events will, typically, be many orders of magnitude higher than the dark count rate. The key rates are shown in the infinite-key limit with error correction being performed in the ideal case reaching the Shannon limit. For sources we assume perfect single-photon sources, so that $P_s = \eta$ where η is the single-photon transmissivity of the overall system, including transmission and detection loss. The result also hold for parametric down-conversion sources as long as the heralding set-up assures that for the heralded signals the average density matrix for the two basis is still basis independent. In this picture, the single-click event error rate e_s is due to factors such as misalignment and decoherence mechanisms in the channel.

The simulation result is shown in Figure 1 for the ideal case where we have no errors at all that ordinate from single clicks ($e_s = 0$). Of particular interest is the threshold for the transmittance above which secret keys can be generated. For the standard coarse-graining data processing one finds for this threshold the value of 78.0% (corresponding to about 11% error rate), which is consistent with the result of Shor-Preskill's proof [5]. The transmittance threshold for the advanced data processing scheme based on the refined data is case is 65.9%. From the time-shift attack, we know that the lower bound of tolerable transmittance for this untrusted detection device case is 50% [48].

To show the effect of a non-zero error rate within the single-click events, we plot the thresholds for the two methods as a function of the single-click event error rate e_s in Figure 2. There is no positive key for $e_s > 11.0\%$, which is consistent with the result in [5].

3.4 Fully device-independent scheme

In fully device-independent QKD, none of the devices of sender and receiver are characterized. These schemes are entanglement based QKD schemes, so that Alice and Bob have two

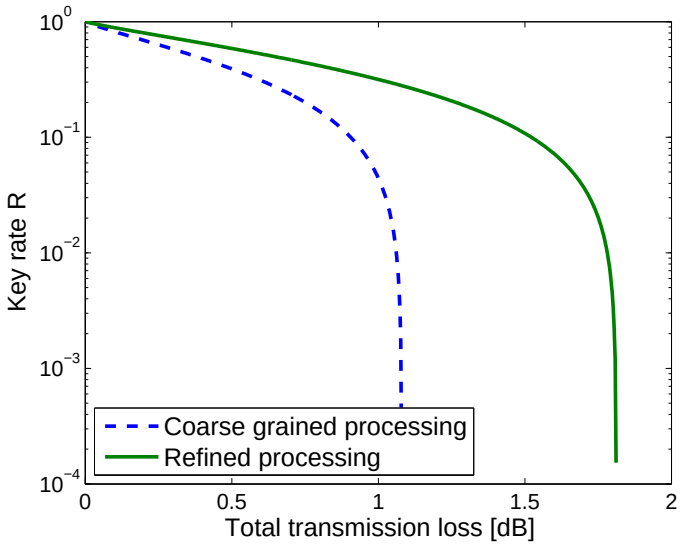

Fig. 1. Plot of key rate of the two data processing schemes for the detection-device-independent scheme. The lowest tolerable transmittance of the coarse-grain processing scheme is 78.0%, while that of refined-grain processing scheme is 65.9%. Here we assume there is no error for single-clicks ($e_s = 0$) and the error correction reaches the Shannon limit.

detection devices each, while the adversary Eve is in control of the source. Alice and Bob each choose actively between their uncharacterized devices. Security proofs for these schemes, assuming collective eavesdropping attacks, have been given in [22, 24]. This proof assumes that the data are coarse-grained into binary outcomes. In contrast to earlier coarse-graining, we will in this case follow reference [24] and assign a pre-agreed *fixed* binary value to lost signals, rather than random binary values, as this gives a slight advantage. Note that this choice also influences the Shannon entropy $H(A)$ in Eq. (1), which is now less than one. The privacy amplification term is given by

$$I_{pa} = h\left[\frac{1+\sqrt{(S/2)^2-1}}{2}\right] \tag{7}$$

where S is the CHSH [49] Bell parameter. To simulate this parameter for experiments, we neglect the double click events, assuming a perfect photon-pair source. Within single clicks events on both sides, there is an observed error rate e_s when measuring in the same basis. We assume this error rate to be the parameter of a depolarizing channel in order to predict the correlations when Alice and Bob do measure in different bases in order to determine S. The depolarizing channel maintains the signal perfectly with probability $1 - 2e_s$, while it randomizes the signal with probability $2e_s$. A perfect signal leads to a Bell parameter $S = 2\sqrt{2}$, while a randomized signals gives $S = 0$. The transmittance between source and Alice and Bob is given by η_A and η_B respectively.

There are three contributions to the value of S: The first describes that case when both sides detect single clicks, which happens with probability $P_s = \eta_A\ \eta_B$. The S parameter in this case is given by $2\sqrt{2}(1-2e_s)$. The second contribution comes happens if both signals are lost,

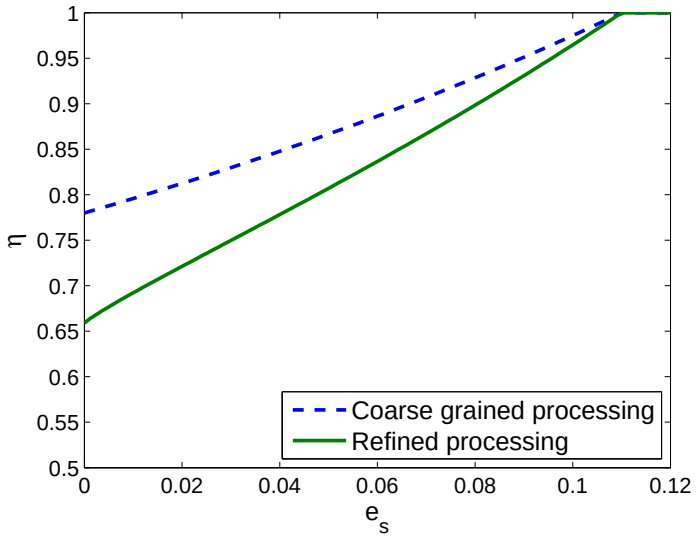

Fig. 2. Plot of the tolerable e_s and η for the two data processing schemes.

which happens with probability $(1-\eta_A)(1-\eta_B)$. Since the binary outcomes are predetermined in this case and perfectly correlated, we find $S = 2$. Finally, the third contribution has one detected photon and one lost photon. The fixed assignment leads to uncorrelated data between Alice and Bob, and thus to $S = 0$. Overall, we find then for the Bell parameter

$$S = 2\sqrt{2}(1-2e_s)\eta_A\eta_B + 2(1-\eta_A)(1-\eta_B)\,. \tag{8}$$

The key is generated by measurements where Alice and Bob perform measurements in identical bases. Therefore the error rate of the coarse-grained data is given by

$$e^{(c)} = P_s e_s + ((1-\eta_B)\eta_A + (1-\eta_A)\eta_B)\,\frac{1}{2}\,. \tag{9}$$

Note that positions where neither Alice nor Bob do detect a photon do no contribute to an error rate, as Alice and Bob would assigned the same bit value to these events. However, the entropy of Alice's data is now given by $H(A) = h\left[\frac{1}{2}\eta_A + (1-\eta_A)\right]$.

Overall, this particular coarse grained data processing leads to the key rate

$$R_{DI}^{(c)} = h\left[\frac{1}{2}\eta_A + (1-\eta_A)\right] - h[e^{(c)}] - h\left[\frac{1+\sqrt{(S/2)^2-1}}{2}\right]\,. \tag{10}$$

For the refined data processing, Alice keeps her coarse graining method as these data define the key. However, Bob now accesses the refined data. The key rate is shown in Figure 3, using the same modeling as in the previous section, including the choice of $e_s = 0$. In contrast to the detection device independent case, we now assume the source to be symmetric located with respect to Alice and Bob, leading to the choice $\eta_A = \eta_B \equiv \eta$. The tolerable transmittance η for a single link for the standard processing is 92.4% (corresponding to a

total transmittance of η^2, or 82.6%), which is consistent with the result shown in [22]. With the advanced data processing scheme, the tolerable single link transmittance can be improved to 90.9%.

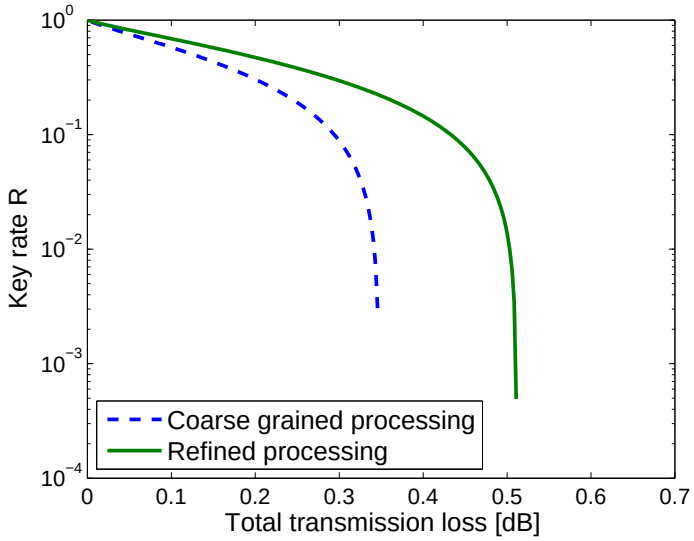

Fig. 3. Plot of key rate for the device-independent QKD scheme with a double link setup and $\eta_A = \eta_B = \eta$. The lowest tolerable transmittance of a single link for the coarse-grain processing scheme is 92.4%, while that of refined-grain processing scheme is 90.9%. Here we assume there is no error for single-clicks ($e_s = 0$) and the error correction reaches the Shannon limit.

4 Conclusion

We presented a generic method to improve the secret key rate for QKD systems. This method applies in situations, where information of the receiving party has been coarse-grained in order to apply some security proof method. We showed that the refined information can be accessed for error correction purposes, thus increasing the effective key rate.

While we demonstrated our method in the scenario of one-direction error correction, we would like to point out that the framework of Renner [6] has as its essential feature only that the final key is derived from the data on one side. This can also be achieved by two-way error correction mechanism and the key rate depends only on the actual amount of information leaked to the adversary during error correction. Therefore, our method can be extended to this situation even without encryption of the error correction information. For the same reason, the extension to entanglement based protocols is contained in our analysis.

Acknowledgements

We thank Hoi-Kwong Lo for enlightening discussions. This work is supported by NSERC via the Innovation Platform Quantum Works, the Discovery grant programme, and the Strategic Project Grant FREQUENCY, and by the Ontario Research Fund (ORF).

References

1. C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, Bangalore, India, 1984), pp. 175–179.
2. A. K. Ekert, Phys. Rev. Lett. **67**, p.661 (1991).
3. D. Mayers, Journal of the ACM (JACM) **48**, p.351 (2001).
4. H.-K. Lo and H. F. Chau, Science **283**, p.2050 (1999).
5. P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, p.441 (2000).
6. R. Renner, Ph.D. thesis, Swiss Federal Institute of Technology (2005), also available in Int. J. Quant. Inf. **6**, p.1 (2008).
7. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, p.145 (2002).
8. H.-K. Lo and N. Lütkenhaus, Phys. Canada **63**, p.191 (2007).
9. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, p.1301 (2009).
10. M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, p.057902 (2003).
11. H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, p.599 (2007).
12. D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comput. **4**, p.325 (year2004).
13. T. Tsurumaru and K. Tamaki, Phys. Rev. A **78**, p.032302 (2008).
14. N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, p.093601 (2008).
15. V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, p.022313 (2006).
16. B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quant. Inf. Comput. **7**, p.073 (2007).
17. Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, p.042333 (2008).
18. V. Makarov, New Journal of Physics **11**, p.065003 (18pp) (2009), also in http://stacks.iop.org/1367-2630/11/065003.
19. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature photonics **4**, p.686 (2010).
20. D. Mayers and A. Yao, in *FOCS, 39th Annual Symposium on Foundations of Computer Science* (IEEE, Computer Society Press, Los Alamitos, 1998), p.503.
21. A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, p.120405 (2006).
22. A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Physical Review Letters **98**, 230501 (2007).
23. M. McKague and M. Mosca, in *Proceedings of the TQC'10 5th conference on Theory of quantum computation, communication, and cryptography*, pp113-130 (Springer-Verlag, Berlin, Heidelberg, 2011).
24. S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New Journal of Physics **11**, p.045021 (2009).
25. L. Masanes, S. Pironio, and A. Acín, Nature Communications **2**, 238 (2011).
26. E. Hänggi and R. Renner, arXiv:1009.1833 (2010).
27. M. Koashi, New Journal of Physics **11**, p.045018 (2009), http://stacks.iop.org/1367-2630/11/045018.
28. M. Berta, M. Christandl, R. Colbeck, J. Renes, and R. Renner, Nature Physics **6**, p.659 (2010).
29. X. Ma, C.-H. F. Fung, J.-C. Boileau, and H. F. Chau, *Computers & Security* **30** p.172 (2011).
30. C.-H. F. Fung, X. Ma, and H. F. Chau, Phys. Rev. A **81**, p.012318 (2010).
31. U. Maurer, IEEE Transactions on Information Theory, **39**, p.733 (1993).
32. D. Gottesman and H.-K. Lo, IEEE Transactions on Information Theory **49**, p.457 (2003).
33. X. Ma, C.-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.-K. Lo, Phys. Rev. A **74**, p.032330 (2006).
34. B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, p.080501 (2005).
35. W.-Y. Hwang, Phys. Rev. Lett. **91**, p.057901 (2003).
36. H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, p.230504 (2005).
37. X.-B. Wang, Phys. Rev. Lett. **94**, p.230503 (2005).
38. C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, p.3824 (1996).

39. I. Devetak and A. Winter, Proc. R. Soc. London Ser. A. **461**, p.207 (2005).
40. A. S. Holevo, Probl. Peredachi Inf. **9**, p.3 (1973), engl. Transl. Probl. Inf. Trans. vol. 9, no. 3, pp. 177-183, (1973).
41. M. Tomamichel, C. Lim, N. Gisin, and R. Renner, arXiv:1103.4130 (2011).
42. N. Lütkenhaus, Phys. Rev. A **59**, p.3301 (1999).
43. H.-K. Lo, New J. Phys. **5**, p.36 (2003).
44. T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley-Interscience, New York, 2006), 2nd ed.
45. M. Hayashi, Phys. Rev. A **74**, 022307 (2006).
46. V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).
47. N. Lütkenhaus, Appl. Phys. B **69**, p.395 (1999b).
48. X. Ma, T. Moroder, and N. Lütkenhaus, arXiv:0812.4301 (2008).
49. J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, p.880 (1969).