Improved Error Correction in Quantum Key Distribution Protocols

Stefan Rass[1], Christian Kollmitzer[2]
1: Institute of Applied Informatics, System Security Group, Klagenfurt University, Universitätsstrasse 65-67, 9020 Klagenfurt, stefan.rass@uni-klu.ac.at
2: Austrian Research Centers GmbH – ARC smart systems Division, TechGate Vienna Donau-City-Strasse 1, 1220 Wien, Austria, christian.kollmitzer@arcs.ac.at)

Abstract

We present an extension to the error correction facility that is at the core of classical quantum cryptographic key exchange in the spirit of the BB84 protocol. The Cascade error correction scheme proposed along with the experimental implementation of BB84 can significantly be improved by endowing it with an adaptive initial block size selection strategy that takes into account information from past protocol executions. Additionally, our model comes with learning capabilities enabling the protocol to adapt itself not only according to its past, but also to different environmental conditions which the link is subject to. At the same time, the procedure can widely be automated and can be implemented using known algorithms. We demonstrate the feasibility and efficiency of our proposal using experiments, comparing the classical approach to the dynamic extension, showing a significant efficiency benefit that we gain from an adaptive initial block size choice.

Introduction

Errors in physical transmission media often exhibit burst structures, that is, a sequence of consecutive errors is more likely to occur than a random scattering. Consequently, a common trick is to randomize bits prior to any error correction in order to chop down long bursts into small pieces, ideally leaving an almost uniform pattern of erroneous bits in the result. This is the first step in a protocol which has become known under the name Cascade [2]. After having agreed on a publicly known permutation of bits, Alice and Bob take their randomized strings and partition it into blocks of size k, such that a single block is believed to contain no more than one error with high probability. In [1], as well as in [2], a theoretical treatment of the optimal choice of block size is missing, and this is precisely the gap we intend to close in this work.

The full version of this paper has been submitted to the third International conference on Quantum, Nano and Micro Technologies [4].

Adaptive Initial Block Size Selection

Our goal is replacing the static error frequency estimate at the beginning of the Cascade protocol by a dynamic one, which takes into account information from previous protocol executions. A variety of different solutions can be imagined, and we shall summarize a selection here, restricting ourselves to two high-level approaches:

1. Choose the block size at the beginning and leave it constant over the whole execution time of Cascade's first stage, resulting in an equidistant partitioning. The initial choice is made using past knowledge about error distributions. We refer to this approach as with fixed initial block size. This variant is suitable if the error rate remains constant over short periods, but varies in the long run (due to slow, seasonal variations). The resulting scheme will hence be the choice either for quick establishment of short keys, or in situations where conditions can artificially be kept almost constant over a long time.

2. If the error rates are frequently varying within the duration of the protocol execution, then we may adapt it in real-time during the first stage. The resulting model can either be a deterministic one, if the error rates exhibit repeating patterns (i.e. some kind of periodicity), or completely stochastic, if no such underlying pattern can be identified. In case we are dealing with fully non-deterministic scattering of errors, we propose using Bayesian statistics for adapting the error rate model to the particular conditions of a link. In that sense, we can endow Cascade with learning capabilities in order to self-adapt to changing conditions. We refer to this variant as with dynamic initial block size. This approach will receive closer attention below.

Stochastic Process based Error Models

If changes in the error frequency can exhibit regular (perhaps periodic) behaviour, then we may approximate these using deterministic models that we learn from the available information. Consequently, we may set up a stochastic process which models errors that are randomly occurring according to a deterministic scattering model.

Due to the structure of the Cascade error correction method, we have blocks within errors have been located, and the number of these is available after the protocol terminates. Enumerating the blocks and recording the center of each block along with the number of errors that have been spotted within the block, we are left with a classical curve-fitting problem upon a given data set, which can be solved by

standard techniques such as least-squares fitting. This technique is particularly appealing due to its computational simplicity and the possibility to update a given estimate upon information from subsequent protocol executions.

Using a stochastic process in combination with a given error scattering we can find the optimal block size such that the probability of one counted error within the interval (t, t + h) is close to one. If we wish to choose the blocks such that with high probability there is only 1 error within each block, we find the block size as ≈ f / e(t), where f is the frequency of bits. This induces an initial partitioning that becomes coarser if errors are less frequently occurring, and refines itself upon increasing error frequency.

Experiments

For performance evaluation of the dynamic initial block size selection strategy of Cascade, let the dashed line in Figure 1 be the exact error rate over the interval [0, T], covering the duration of one single QKD execution. Simulation of a stochastic process according and calculating the average number of errors in equidistantly distributed bins across the period [0, T] gives a set of points for which an approximating function f(t) is sought. Figure 1 shows an example where this has been done and a polynomial model (solid line) has been fitted. Figure 2 displays the empirical probability of encountering blocks with 1, 2, 3… errors, showing that the variations in the local error rates can indeed be smoothed by our proposal. In the example, we estimated the function e(t) from the simulated error scattering and derived the constant block size using the classical approach (see [1, 2]). Comparing the results demonstrates that a deterministic time-varying model is more suitable if rapid changes of errors are to be expected, whereas an equidistant partitioning resulting from an assumed constant error rate will perform worse under strong perturbations.

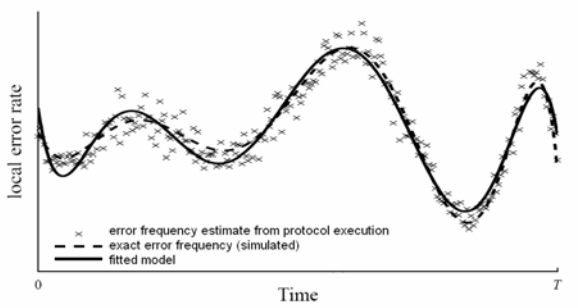

Figure 1: Example of estimating local error rates and fitting amodel to the empirical data

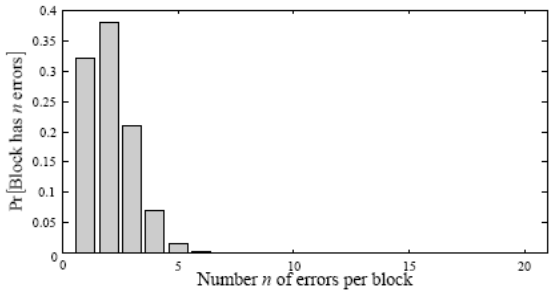

Figure 2: Example empirical probabilities for blocks with 1,2,3,... errors for Cascade with dynamic initial block size.

Conclusion

Our results show that adapting the block size to variations of the local error rate is indeed worthwhile, since it significantly increases the efficiency of the error correction by reducing the number of bits that become revealed to the adversary during the Cascade protocol. This results in a considerable improvement of the QKD in terms of efficiency.

References

1. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. J. Cryptology, 5:3–28, 1992.
2. G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. In Eurocrypt, pages 410–423, 1993.
3. J. Illian, A. Penttinen, H. Stoyan, and D. Stoyan. Statistical Analysis and Modeling of Spatial Point Patterns. Wiley, 2008.
4. S. Rass, C. Kollmitzer. Adaptive Error Correction with Dynamic Initial Block Size in Quantum Cryptographic Key Distribution Protocols, submitted to the third international conference on Quantum, Nano and Micro Technologies.