QKD key generation control protocol

N V Rudavin1,5, I S Gerasin1,2,4, E E Mekhtiev1,2,4, A V Duplinsky1,3,4 and Y V Kurochkin1,2,3,4

1 QRate, Novaya av. 100, Moscow, Russia
2 Moscow Institute of Physics and Technology, 9 Institutskiy per., Dolgoprudny, Moscow Region, 141701, Russian Federation
3 NTI Center for Quantum Communications, National University of Science and Technology MISiS, Leninsky prospekt 4, Moscow 119049, Russia
4 Russian Quantum Center, Bolshoy Boulevard 30, bld. 1, Skolkovo, Moscow 121205, Russia
5 Federal State Budget Educational Institution of Higher Education, MIREA—Russian Technological University, 78, Vernadskogo avenue, 119454 Moscow, Russia

n.rudavin@goqrate.com

Abstract. Polarization-encoding fiber QKD requires compensation of polarization distortion caused by birefringence in optical fiber. Solving this task inevitably requires losing some effectiveness in terms of the final key rate. In this work, a time-division multiplexing protocol for polarisation calibration is suggested. This protocol was implemented in a QRate commercial QKD fiber system, utilizing BB84-protocol. Parameters of the protocol were optimized to maximize the secret key rate.

1. Approaches to QKD key generation control

Quantum technologies evolve rapidly and now the quantum key distribution (QKD) fiber systems become more and more available. The fiber QKD systems have the advantage that they can be directly deployed on existing telecom optical fiber infrastructure. However, for polarization-encoding protocols polarization control is required since in single-mode optical fiber any given input polarization of light passing through optical fiber suffers time-dependent disturbance. To provide a high secure key-rate efficient polarization calibration protocol should be used.

There are two main approaches to organize polarisation calibration protocols: (i) interrupting scheme (time-division multiplexing, TDM) and (ii) real-time scheme. The first approach requires stopping the key generation process in order to send a sequence of calibration pulses (either quantum or classical) [1]. The second method implies utilizing wave-division multiplexing (WDM) for calibration signals [2] or using some part of the secret key to estimate QBER [3]. WDM systems require some additional equipment to multiplex signals which leads to the cost increase. Interrupting schemes allow to send high-intensity calibration pulses that can gather statistics for error estimation faster than from the weak pulses used for secret key generation. Another advantage of the TDM approach, that the calibration pulses pass the same optical path, which is used by signal pulses. In this work, we propose interrupting calibration protocol with flexible switch criteria.
2. Protocol description

2.1. Problem statement
During the calibration mode, key generation is impossible so one needs to decide when to switch into key generation regime and back. Consider the work of some iteration algorithm that minimizes QBER (e.g. gradient descent). Usually, iteration algorithms do not have well-defined stop criteria. On the one hand, if protocol switches to the key-generation mode too early during the convergence, the final QBER value is not optimal and the maximum secure key rate is not achieved. On the other hand, if protocol switches to the generation too late, the key rate is maximized but key generation time is decreased. Thus, for interrupting protocol, a crucial thing is to choose switching criteria efficiently in terms of secret key length. We aim to develop adaptive switching criteria, which can be tuned by some parameters. Varying the parameters manually or automatically, the optimal ones can be found. Moreover, we trying to avoid the adding of some additional equipment.

2.2. Flexible criteria
On each iteration of the convergence algorithm, we measure M values of QBER (each point is measured during the same time interval $\tau$, see Figure 1). Parameter M is introduced to change the accuracy of the gathered QBER values. The longer the measured time (larger M), the more accurate measurement. Then mean $\overline{QBER}$ and the standard deviation $\sigma_{CM}$ is calculated for each iteration that lasts $M\tau$. $\overline{QBER}$ is passed to convergence algorithm. Switching criteria is based on QBER linear interpolation as a function of time via MSE ($N$ last mean $\overline{QBER}$ points are used) and a comparison of the slope with some threshold, which is dynamically calculated on each iteration of the convergence algorithm. The threshold is calculated as $k_0 = -\sigma_{CM}/NM\tau$. The $k_0$ is an estimation of the minimal slope of the MSE line. Increasing M with fixed N allows manipulating threshold value. Thus, by changing M and N we can operate the time needed for calibration and the minimal QBER value achieved during calibration.

2.3. Proposed protocol
The whole process of QKD is divided into two parts: key-generation mode (GM) and calibration mode (CM). During GM $\overline{QBER}$ is calculated from decoy-state clicks and $\sigma_{GM}$ is estimated as the standard deviation of the ratio of two random values $N_{\text{wrong clicks}} / N_{\text{total clicks}}$ with the Poissonian distribution. Generally, $\sigma_{GM}$ can be chosen in other ways depending on QBER estimation technique.

![Figure 1. Criteria principle.](image-url)
during key generation. Moving back to the CM is regulated with a certain threshold based on QBER statistics analysis. The proposed protocol works as follows:

1) enable polarization calibration mode
2) wait until the convergence algorithm makes N steps
3) using the last N points \((QBER_i, t_i)\) approximate \(QBER(t)\) as a linear function through MSE method:
   \[ QBER = kt + b \]
4) calculate the threshold slope \(k_0 = \frac{\sigma_{CM}}{NMF} \)
5) if \( k < k_0 \) then
   - make another iteration of the convergence algorithm
   - go to step 3
6) else if \( k \geq k_0 \) then
   - set \( QBER_{thrs} = \overline{QBER}_N + 3\sigma_{GM} \)
7) enable key-generation mode
8) monitor \( QBER \) until \( QBER > QBER_{thrs} \)
9) go to step 1

3. Experimental results
The proposed protocol was implemented and tested on QRate commercial QKD fiber system [4]. This system, utilizing BB84 protocol, uses one-way polarization encoding optical scheme [5]. In the experimental setup, transmitter (Alice) and receiver (Bob) was connected by 50 kilometers of standard single-mode telecommunication optical fiber SMF-28e. As polarization controller was used PolaRITE III, developed by General Photonics. M and N are hyperparameters to be optimized. We run the key distribution process with the fixed parameters \((M, N) \in \{4, 6, 8\} \otimes \{5, 7, 9\}\) and measure the average secret key rate during 3 hours for each pair. The obtained results are represented in Table 1. We can notice that choice of hyperparameters does not influence much. Thus, we choose \((M, N) = (6, 7)\) as optimal pair of parameters for our system.

| N \ M | 4   | 6   | 8   |
|------|-----|-----|-----|
| 5    | 14.76 | 14.84 | 14.86 |
| 7    | 14.87 | 14.97 | 14.85 |
| 9    | 15.02 | 14.70 | 14.40 |

Acknowledgments
We thank many colleagues at the Russian Quantum Center, QRate, for motivating discussions, management, and coordination. This work was supported by The Russian Science Foundation (Grant No. 17-71-20146)

References
[1] Chen J, Wu G, Li Y, Wu E, and Zeng H 2007 Active polarization stabilization in optical fibers suitable for quantum key distribution Optics express 15 pp 17928-17936
[2] Xavier G B, Vilela de Faria G, Temporão G P, and von der Weid J P 2008 Full polarization control for fiber optical quantum communication systems using polarization encoding Optics express 16 1867-1873
[3] Ding Y-Y, Chen W, Chen H, Wang C, Li Y-P, Yin Z-Q, Wang S, Guo G-C, Han Z-F 2017 Polarization basis tracking scheme for quantum key distribution with revealed sifted key bits Optics Letters 42 1023-1026
[4] Duplinskiy A, Ustimchik V, Kanapin A, Kurochkin V, and Kurochkin Y 2017 Low loss QKD optical scheme for fast polarization encoding Optics express 25 28886-28897

[5] Bennett C H, Brassard G, and Mermin N D 1992 Quantum cryptography without Bell’s theorem Physical Review Letters 68 577