Conference materials
UDC 53.089.52
DOI: https://doi.org/10.18721/JPM.163.168

Influence of detector dead time on the key generation rate in measurement-device-independent quantum key distribution

A.A. Dvurechenskiy [1, 2, 3, 4] ✉, I.V. Petrov [1, 2, 3, 4], A.S. Tumachek [6], D.D. Menskoy [1, 2, 3], I.S. Gerasin [1, 2, 3, 4], N.V. Rudavin [1, 3, 5], P.A. Kupriyanov [1, 2, 3, 4], R.A. Shakhovoy [1, 2, 3, 4, 6]

[1] QRate, Moscow, Russia;

[2] Moscow Institute of Physics and Technology, Dolgoprudny, Russia;

[3] NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow, Russia;

[4] Russian Quantum Center, Skolkovo, Moscow, Russia;

[5] HSE University, Moscow, Russia;

[6] MTUCI, Moscow, Russia

✉ a.dvurechenskiy@goqrate.com

Abstract. Single photon detectors are required for registration of qubits in quantum key distribution. Real detectors have non-zero dead time, which leads to a reduction in the key generation rate. In our work, we evaluate the influence of detector dead time on the key generation rate in measurement-device-independent quantum key distribution scheme with 4 detectors. We compare the analytical estimate of the key generation rate in assumption of synchronous dead time and numerical simulations where asynchronous dead time is assumed.

Keywords: quantum cryptography, quantum key distribution, measurement-device-independent quantum key distribution, MDI QKD, single-photon detector, dead time

Funding: The study was commissioned by JSCo “RZD”.

Citation: Dvurechenskiy A.A., Petrov I.V., Tumachek A.S., Menskoy D.D., Gerasin I.S., Rudavin N.V., Kuprianov P.A., Shakhovoy R.A., Influence of detector dead time on the key generation rate in measurement-device-independent quantum key distribution, St. Petersburg State Polytechnical University Journal. Physics and Mathematics. 16 (3.1) (2023) 374–378. DOI: https://doi.org/10.18721/JPM.163.168

Материалы конференции
УДК 53.089.52
DOI: https://doi.org/10.18721/JPM.163.168

Влияние мертвого времени детекторов на скорость генерации ключа в квантовом распределении ключей с недоверенным центральным узлом

А.А. Двуреченский [1, 2, 3, 4] ✉, И.В. Петров [1, 2, 3, 4], А.С. Тумачек [6], Д.Д. Менской [1, 2, 3], И.С. Герасин [1, 2, 3, 4], Н.В. Рудавин [1, 3, 5], П.А. Куприянов [1, 2, 3, 4], Р.А. Шаховой [1, 2, 3, 4]

[1] QRate, Москва, Россия;

[2] Московский физико - технический институт, г. Долгопрудный, Россия;

[3] НТИ Центр квантовых коммуникаций, Национальный исследовательский технологический университет "МИСиС", Москва, Россия;

[4] Российский Квантовый центр, Сколково, Москва, Россия;

[5] Национальный исследовательский университет «Высшая школа экономики», Москва, Россия;

[6] Московский технический университет связи и информатики, Москва, Россия
✉ a.dvurechenskiy@goqrate.com

Аннотация. Детекторы одиночных фотонов необходимы для регистрации кубитов при распределении квантовых ключей. Реальные детекторы имеют ненулевое мертвое время, что приводит к снижению скорости генерации ключей. В нашей работе мы оцениваем влияние мертвого времени детектора на скорость генерации в схеме распределения квантовых ключей с недоверенным центральным узлом, содержащей 4 детектора. В работе проводится аналитическая оценка скорости генерации ключей с синхронным мертвым временем и численное моделирование в предположении асинхронного мертвого времени.

Ключевые слова: квантовая криптография, квантовое распределение ключей, детектор-независимое квантовое распределение ключей, КРК с НЦУ, детектор одиночных фотонов, мертвое время

Финансирование: Исследовательская работа выполнена по заказу ОАО «РЖД».

Ссылка при цитировании: Двуреченский А.А., Петров И.В., Тумачек А.С., Менской Д.Д., Герасин И.С., Рудавин Н.В., Куприянов П.А., Шаховой Р.А., Влияние мертвого времени на скорость генерации ключа в КРК с недоверенным центральным узлом // Научно-технические ведомости СПбГПУ. Физико-математические науки. 2023. Т. 16. № 3.1. С. 374–378. DOI: https://doi.org/10.18721/JPM.163.168

Introduction

Measurement device independent quantum key distribution (MDI QKD) [1] is a protocol with great potential for development due to its unique features. It is easily scalable to create a network of quantum encryption devices. However, in practical implementation, there are many limitations that arise from imperfections in internal components that affect the key generation rate. The recovery time of the detectors does not affect the generation rate if the generation frequency is less than 1/τ, where τ is the detector dead time. However, modern frequencies, at which generation occurs, have an order of 108 Hz, while the dead time of commonly used single-photon avalanche detectors (SPAD) is 0.1–10 μs [2], i.e., 1/τ is of the order of 10^6 Hz. This fact clearly shows that we cannot neglect the detectors' dead time in calculations. In reality, we need to use at least two detectors, or four, as proposed in [3], where the key rate was estimated in assumption of a synchronous dead time (i.e., when all detectors turn off if there is a click in at least one of them). In this work, we examine in detail the impact of asynchronous detectors on the key generation rate in the MDI QKD protocol with four detectors.

Materials and Methods

Analytical analysis of the detectors' dead time influence on the sifted key generation rate in a scheme with four detectors and time-bin encoding is quite difficult. One of the advantages of this scheme compared to the scheme with two detectors [4] is the ability to register successful events even when one detector was triggered, which increases the key generation rate. The difference between these regimes is shown in Fig. 1.

Analytical analysis can be significantly simplified in assumption of a synchronous dead time, when we may exclude successful events if at least one of the detectors is in the recovery mode. In this case, influence of the dead time can be estimated as follows [3]:

$$R_{\text{sift}}^{\tau\neq0} = \frac{R_{\text{sift}}^{\tau=0}}{1+\tau R_{\text{tot}}}, \tag{1}$$

where R_{sift}^{τ} is sifted key rate; R_{tot} is the number of events where at least one SPAD is triggered.

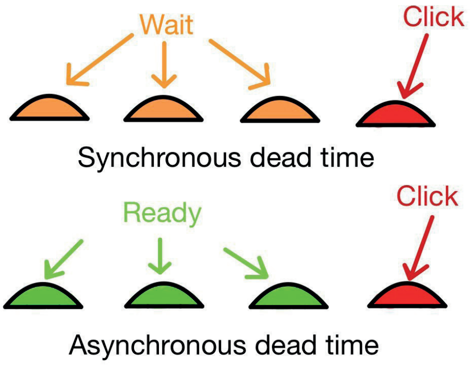

Fig. 1. Demonstration of the operation of detectors in various regimes. In the case of synchronous time, when at least one detector has been triggered ("Click"), the remaining detectors go into standby ("Wait") mode and do not register incoming states. In asynchronous dead time mode, the remaining detectors continue to register incoming events ("Ready")

The quantity can be estimated as

$$R_{\text{tot}} = f \sum_{\psi_{\text{ab}}} \Pr(n_{\text{click}} \geq 1 | \psi_{\text{ab}}) p(\psi_{\text{ab}}), \tag{2}$$

where $\Pr(n_{\text{click}} \geq 1|\psi_{\text{ab}})$ is the probability that at least one SPAD will be triggered given that the $|\psi_{\text{ab}}>|\psi_{\text{a}}>|\psi_{\text{b}}>$ state has arrived at the beam splitter; $p(\psi_{\text{ab}})$ is the probability that Alice sent state $|\psi_{\text{a}}>$, while Bob sent state $|\psi_{\text{b}}>$; f is the repetition rate of laser pulses. Results of this estimation are presented on Fig. 2. Sifted and secret key rates differ by compression ratio, which depends only on errors. It is same if we assume quantum bit error rate as a constant for whatever scheme is applied.

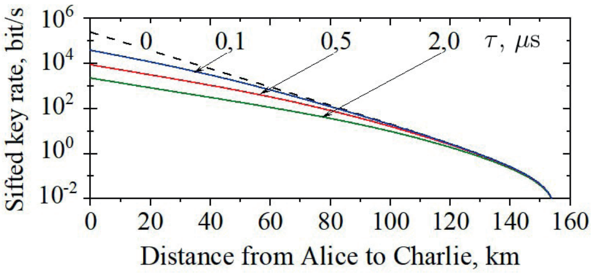

Fig. 2. Examples of estimation for 4 different detectors' dead time

We used Monte Carlo simulations to estimate the key generation rate in case of asynchronous detectors. Two slightly different methods have been developed: 1) a naïve approach, where we considered the detectors' dead time directly in the cycle of the main procedure, and 2) an approach with post-processing, where the dead time has been taken into account outside the main procedure.

The naïve implementation has a simple structure. First, we declare global variables: pulse repetition rate, dark count rate, detectors' efficiency and dead time, losses in quantum channels, intensity and probability of quantum states. Then, we declare necessary functions for processing, which return the probabilities for the detectors to click in response to the incoming pulses. We call this part "declaration". After declaration, a cycle begins in which we simulate the transfer of quantum states from transmitting blocks to an untrusted central node. The bases and values of bits are chosen randomly. For each "sent" pulse, we calculate the probability of clicks using the functions defined at the declaration stage. To account for the dead time, an additional counter is assigned to each detector. After clicking, the corresponding counter is assigned a value equal to the number of iterations required to completely restore the detector. With each iteration, the counter decreases by one, and when it reaches the value "0", the detector will again be ready to click.

With a typical desktop computer, the above method requires about 100 minutes to simulate just one second of the QKD session for the four-detector scheme with phase-time encoding at 312.5 MHz. To get enough statistics with such parameters, one needs to simulate at least 100 seconds of the QKD session, which requires almost a week for a single value of the key rate at a given distance. It is not feasible to calculate the dependence of the key rate on the distance by this method. The obvious solution to this problem is parallelization (in particular, using graphics cards – GPUs). In fact, 90% of the computation time in our case is the generation of randomness whereas graphics cards are known for their fast random number generation [5]. However, to consider the dead time, we had to introduce the dependence of the probability of detector clicks on previous events. Such a coupling severely limits the possibilities of parallelization; therefore, the naïve implementation cannot be efficiently accelerated on the GPU.

To solve the parallelization problem, we have developed another approach, where the probability of detector clicks is calculated in assumption of zero dead time, whereas the non-zero dead time is taken into account in a separate procedure, which can be implemented without GPU. The part of the procedure subject to parallelization is, in essence, equivalent to the naïve implementation without the piece of the code that is responsible for turning off the detectors. The output of such a "memoryless" procedure is a binary vector where '1' corresponds to a detector click and '0' corresponds to no click. This vector is calculated in parallel on all available GPU cores. Post-processing is a separate program that takes as input this vector as well as the values of the dead time of the detectors. The script goes through the entire vector, updating the dead time counters and the state of each detector. (The operation principle of the script is schematically shown in Fig. 3.) These counters are implemented in the same way as the corresponding counters in the naïve implementation. The resulting data are equivalent to the output of the naïve procedure.

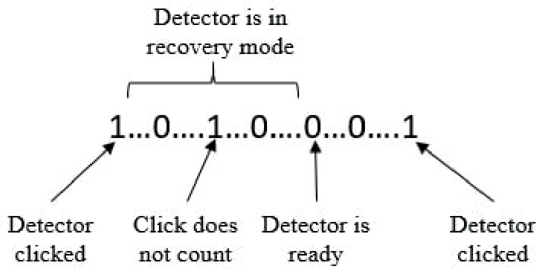

Fig. 3. Example of processing an incoming vector by a script

Results and Discussion

Using the approach with parallelization, we simulated the key generation rate for various distances and dead times of the detectors. The obtained results show that the generation rate is indeed higher in asynchronous mode. At distances close to 80 km between each transmitter and the central node (160 km between the transmitters) the increase of the generation rate is up to 30%. Results for the sifted key rate are shown in Table 1 and Table 2. As one may notice, the results of the analytical estimation made in [3] (column "Estimation") perfectly match the results of the simulation with synchronous dead time (column "Synchronous"). It is important that at large distances, the increase in the asynchronous dead time mode also steps up (column "Asynchronous").

Table 1

Results for $\tau = 4$ μs

L, km	Estimation	Synchronous	Asynchronous
1	989 bit/s	1009 bit/s	1054 bit/s
40	167 bit/s	168 bit/s	185 bit/s
80	18 bit/s	18 bit/s	25 bit/s

Table 2

Results for τ = 2 μs

L, km	Estimation	Synchronous	Asynchronous
1	1964 bit/s	2010 bit/s	2103 bit/s
40	320 bit/s	316 bit/s	348 bit/s
80	24 bit/s	23 bit/s	33 bit/s

Conclusion

In this work, we performed numerical simulations of the QKD session in the protocol with untrusted central node. We have developed an approach for parallelization on graphics processing units to speed up data processing. The obtained results confirm the assumptions made in [3].

REFERENCES

1. **Lo H.K., Curty M., Qi B.,** Measurement-device-independent quantum key distribution. Physical review letters, 108 (13) (2012) 130503.

2. **Hadfield R.H.,** Single-photon detectors for optical quantum information applications. Nature Photonics, 3 (12) (2009) 696–705.

3. **Petrov I.V., Menskoy D.D., Tayduganov A.S.,** Phase-time-encoding MDI QKD tolerant to detector imperfections. St. Petersburg State Polytechnical University Journal. Physics and Mathematics, 15 (3.3) (2022) 365–370.

4. **Ma X., Razavi M.,** Alternative schemes for measurement-device-independent quantum key distribution. Phys. Rev. A, 86 (2012).

5. **Sussman M., Crutchfield W., Papakipos M.,** Pseudorandom number generation on the GPU Graphics Hardware, (2006) 87–94.

THE AUTHORS

DVURECHENSKIY Alexander A.
dvurechenskii.aa@phystech.edu

PETROV Ivan V.
i.petrov@goqrate.com
ORCID:0000-0002-5422-2886

TUMACHEK Alexander S.
a.s.tumachek@mtuci.ru

MENSKOY Daniil D.
d.menskoy@goqrate.com

GERASIN Ilya S.
i.gerasin@goqrate.com

RUDAVIN Nikita V.
n.rudavin@goqrate.com
ORCID: 0000-0003-0264-5710

KUPRIYANOV Pavel A.
kupriianov.pa@phystech.edu

SHAKHOVOY Roman A.
r.shakhovoy@goqrate.com

Received 05.07.2023. Approved after reviewing 21.09.2023. Accepted 21.09.2023.