Conference materials
UDC 535
DOI: https://doi.org/10.18721/JPM.153.210

Synchronization protocol for MDI-QKD systems

N. V. Rudavin [1,2] ✉, I. S. Gerasin [1,3,4], E. E. Mekhtiev [3,4,5],
A. V. Duplinsky [1,4,5], Y. V. Kurochkin [1,3,4,5]

[1] NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow, Russia;
[2] HSE University, Moscow, Russia;
[3] Moscow Institute of Physics and Technology, Dolgoprudny, Moscow Region, Russia;
[4] Russian Quantum Center, Skolkovo, Moscow, Russia;
[5] QRate, Moscow, Russia
✉ n.rudavin@goqrate.com

Abstract. Commercial fiber quantum key distribution systems require the implementation of a protocol for synchronizing the frequency synthesizers of the transmitter and receiver nodes. Frequency mismatch may be due to temperature fluctuations, mechanical effects and imperfections in the technological processes. In this work, an algorithm for automatically adjusting Alice's and Bob's frequency to Charlie's frequency is proposed. After optimizing the algorithm parameters, it was tested on optical lines of different lengths.

Keywords: measurement-device-independent quantum key distribution, MDI-QKD, synchronization protocol, PD controller

Funding: The study was commissioned by JSCo «RZD».

Citation: Rudavin N. V., Gerasin I. S., Mekhtiev E. E., Duplinsky A. V., Kurochkin Y. V., Synchronization protocol for MDI-QKD systems, St. Petersburg State Polytechnical University Journal. Physics and Mathematics. 15 (3.2) (2022) 56–60. DOI: https://doi.org/10.18721/JPM.153.210

Материалы конференции
УДК 535
DOI: https://doi.org/10.18721/JPM.153.210

Протокол синхронизации для систем MDI-QKD

Н.В. Рудавин [1,2] ✉, И.С. Герасин [1,3,4], Е.Е. Мехтиев [3,4,5],
А.В. Дуплинский [1,4,5], Ю.В. Курочкин [1,3,4,5]

[1] Центр НТИ «Квантовые коммуникации», Национальный исследовательский технологический университет МИСиС, г. Москва, Россия;
[2] Национальный исследовательский университет «Высшая школа экономики», г. Москва, Россия;
[3] Московский физико-технический институт, г. Долгопрудный, Московская область, Россия;
[4] Российский квантовый центр, Инновационный центр Сколково, г. Москва, Россия;
[5] КуРэйт, г. Москва, Россия
✉ n.rudavin@goqrate.com

Аннотация. Промышленная система квантового распределения ключей требует реализации протокола синхронизации генераторов опорных частот узлов передатчика и приемника. Расхождение частот может быть связано с температурными флуктуациями, механическим воздействием и неидеальностью технологических процессов. В данной работе предложен алгоритм автоматической подстройки частоты Алисы и Боба под частоту Чарли. После оптимизации параметров алгоритма было проведено его тестирование на оптических линиях различной длины.

Ключевые слова: детектор-независимое квантовое распределение ключей, КРК, протокол синхронизации, PD – регулятор

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

Ссылка при цитировании: Рудавин Н. В., Герасин И. С., Мехтиев Э. Э., Дуплинский А. В., Курочкин Ю. В. Протокол синхронизации для систем MDI-QKD // Научно-технические ведомости СПбГПУ. Физико-математические науки. 2022. Т. 15. № 3.2. С. 56–60. DOI: https://doi.org/10.18721/ JPM.153.210

Introduction

Nowadays, the commercial implementation of fiber quantum key distribution (QKD) systems use crystal oscillators and several frequency multipliers as frequency synthesizers to generate the operating frequency. At the same time, the existing technological production process does not allow obtaining frequency synthesizers with identical output parameters. Moreover, modern crystal oscillators do not have high stability over long periods of time due to temperature fluctuations or mechanical stress. The discrepancy between the frequencies of the synthesizers is crucial for key generation. So, it is necessary to organize frequency synchronization system for experimental measurement-device-independent QKD protocol (MDI-QKD) fiber setup.

There are three main approaches to organize the synchronization protocol in QKD systems. The most common method for time synchronization of nodes in MDI-QKD fiber setups is to use a frequency synthesizer as a reference for all nodes. In this scheme, the generator is typically installed on Charlie's device and connected to Alice's and Bob's control boards via electrical cables [1, 2]. This synchronization method is traditionally used in proof of principle experiments. However, a significant disadvantage of this approach is that it is impossible to distribute Alice's and Bob's devices at a large distance from Charlie. Accordingly, this is critical for the commercial implementation of the QKD system but is excellent for laboratory testing.

The second method is based on computing the cross-correlation of transmitted and received qubit sequences [3]. The disadvantage of this approach is the necessity to use single photon detectors (SPD), which are the most technologically complex node of modern QKD systems. The last approach is to use high energy optical pulses sent by Alice through a quantum channel [4] or an additional fiber [5] to transmit the frequency of Alice's synthesizer. The use of a second fiber imposes additional requirements on the integration of the QKD system into existing telecommunication networks and increases the cost of the system.

Materials and Methods

In the MDI-QKD protocol the secret key is distributed between the two transmitters (Alice and Bob) using the untrusted central node (Charlie). Since SPDs are located at Charlie's node, we cannot use qubit-based synchronization method. Therefore, for experimental MDI-QKD fiber setup we suggest to use quantum channel to transmit the synchronization signal. Since Alice and Bob are not connected by an optical fiber, we use a laser and a 50/50 beamsplitter to generate a synchronization signal on Charlie. The wavelengths of the synchronization laser and the signal laser are in different DWDM channels. In this configuration the sync pulses propagate in the opposite direction through the quantum channel. To eliminate their influence on the quantum signal and the SPDs, we use time-division multiplexing and WDM optical filters.

From the point of view of the theory of control of technical systems, the task of adjusting the frequency of one synthesizer to the frequency of another synthesizer can be considered as the task of designing and implementing an industrial control system (ICS). A phase-locked loop (PLL) system was chosen as the ICS. We use photodetectors to register the optical synchronization signal and to convert it into an electrical signal.

To obtain a phase error value between the synthesizers, the synchronization signal is sent to one of the inputs of the phase detector (PD). The signal from Alice's (Bob's) synthesizer is sent to the second PD input. Then we tune the frequency by changing the voltage supplied to Alice's (Bob's) synthesizer. The value of the control signal is calculated using a proportional – derivative controller (PD controller). In general, the integral term is also used to calculate the correction, but during the experiments it was decided not to use it to simplify the optimization process of the gain coefficients. By using third and fifth order derivative terms we can achieve a high frequency tuning rate even if the initial frequencies of the synthesizers are very different:

$$u(n) = P + D + D^3 + D^5 + u(n-1) \tag{1}$$

where P is the proportional term, where D is the derivative term, where $u(n-1)$ is the voltage on the frequency synthesizer, calculated in the previous iteration of the protocol. Terms for $u(n)$ calculates as follows:

$$P = K_p \cdot \left(e(n) - \Delta e_{const}\right), \tag{2}$$

$$D = K_d \cdot \left(e(n) - e(n-1)\right), \tag{3}$$

$$D^3 = K_{d3} \cdot \left(e(n) - e(n-1)\right)^3, \tag{4}$$

$$D^5 = K_{d5} \cdot \left(e(n) - e(n-1)\right)^5, \tag{5}$$

where K_p is the proportional term coefficient, where K_d is the derivative term coefficient, where K_{d3} is the third order derivative term coefficient, where K_{d5} is the fifth order derivative term coefficient, where $e(n)$ is the phase error value on current iteration, where $e(n-1)$ is the phase error value on the previous iteration, where Δe_{const} is the target phase error value.

Results

For proof of principle experiment we built experimental setup, consisting of Alice and Charlie. The proposed synchronization protocol has four hyperparameters – the gain coefficients of the terms of the controller. Using the method of experimental tuning with different sets of coefficients, their optimal values were found (Table 1).

Table 1

PD controller coefficients

Coefficient	Value
K_p	2×10^{-3}
K_d	8×10^{-3}
K_{d3}	3.2×10^{-10}
K_{d5}	1.6×١٠^{-8}

To estimate the accuracy of the synchronization, we measured the frequency ratio of Alice's and Charlie's synthesizers with 75 km of fiber. During the experiment, the Keysight 53220A 350 MHz universal frequency counter was used, and the sampling rate was 1/60 Hz (Fig. 1). During the tests with optimal coefficients, we were able to achieve stable synchronization with accuracy up to the twelve decimal place. The experiment confirmed that the proposed protocol can be used in MDI-QKD experimental setups.

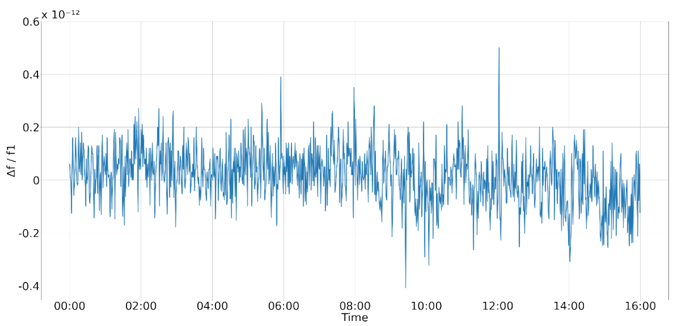

Fig. 1. The frequency ratio of Alice's and Charlie's synthesizers with 75 km of fiber for 16 hours

For the next experiment, the MDI-QKD fiber experiment setup was built and the proposed protocol was implemented on it. Both Alice and Bob were connected to Charlie by 75 kilometers of standard single-mode telecommunication optical fiber SMF-28e. As frequency counter was used Keysight 53220A with sampling rate of 1/60 Hz. We run the synchronization process using the coefficients from Table 1 and measured the frequency ratio during 16 hours (see Fig. 2). We can see the accuracy of the synchronization is up to the twelve decimal place, which is consistent with the results of the previous experiment.

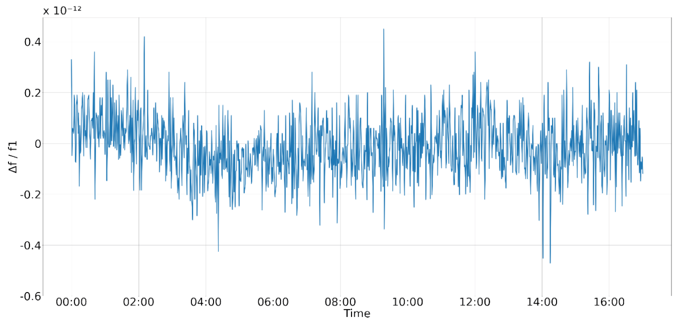

Fig. 2. The frequency ratio of Alice's and Bob's synthesizers with 150 km of fiber for 16 hours

Conclusion

We have demonstrated frequency synchronization protocol for MDI-QKD setups, utilizing a laser and a 50/50 beamsplitter to transmit the synchronization signal and a PLL system to calculate the value of the control signal. Importantly, this method allows the use of a single optical fiber to transmit quantum and synchronization signals. The obtained results show that our approach allows us to maintain frequency synchronization at a high level. It is worth pointing out that this work has been carried out in a laboratory with fiber coils. It is necessary to perform a similar demonstration in the scenario of real telecommunication networks to confirm the robustness of the proposed protocol.

REFERENCES

1. **Tang Z., Liao Z., Xu F., Qi B., Qian L., Lo H. K.,** Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution, Physical review letters. 112 (19) (2014) 190503.

2. **Tang Z., Wei K., Bedroya O., Qian L., Lo H. K.,** Experimental measurement-device-independent quantum key distribution with imperfect sources, Physical Review A. 93 (4) (2016) 042308.

3. **Cochran R., Gauthier D.,** Qubit-based clock synchronization for QKD systems using a Bayesian approach, Entropy. 23 (8) (2021) 988.

4. **Tang Y. L., Yin H. L., Chen S. J., Liu Y., Zhang W. J., Jiang X., Pan J. W.,** Measurement-device-independent quantum key distribution over 200 km, Physical review letters. 113 (19) (2014) 190501.

5. **Korzh B., Lim C. C. W., Houlmann R., Gisin N., Li M. J., Nolan, D., Zbinden H.,** Provably secure and practical quantum key distribution over 307 km of optical fibre, Nature Photonics. 9 (3) (2015) 163–168.

THE AUTHORS

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

GERASIN Ilia S.
i.gerasin@goqrate.com
ORCID: 0000-0001-5084-7056

MEKHTIEV El E.
mekhtiev@phystech.edu
ORCID: 0000-0002-9756-7016

DUPLINSKY Alexander V.
a.duplinsky@goqrate.com
ORCID: 0000-0003-2222-0752

KUROCHKIN Yury V.
yk@goqrate.com
ORCID: 0000-0001-5376-6358

Received 12.08.2022. Approved after reviewing 31.08.2022. Accepted 31.08.2022.