NUCL SCI TECH (2016) 27:15
DOI 10.1007/s41365-016-0012-y

TDC-GPX-based synchronization scheme for QKD system

Lian-Jun Jiang[1,2] · **Shi-Biao Tang**[1,2] · **Ze-Jie Yin**[1,2]

Received: 8 December 2014 / Revised: 2 February 2015 / Accepted: 13 February 2015 / Published online: 27 February 2016

Abstract To meet the needs of signal alignment between the transmitter and receiver in a quantum key distribution (QKD) system, we put forward a TDC-GPX-based synchronization scheme, which is based on high-precision time measurement. We send a low-frequency repeat optical pulse synchronized with associated quantum signals on the receiver's side by using a time-to-digital converter (TDC) module, the time intervals between quantum signals, and synchronization signals measured and converted to corresponding temporal orders to complete the synchronization. We state the principle of the synchronization scheme in detail and then verify it in an actual QKD test bed. The test results show that our TDC-GPX-based synchronization can obtain a time resolution better than 100 ps, and the proposed scheme shows full feasibility for an actual QKD system.

Keywords Quantum key distribution · Synchronization · Time-to-digital converter · TDC-GPX · Time measurement

✉ Shi-Biao Tang
tangsb@ustc.edu.cn

[1] State Key Laboratory of Particle Detection and Electronics, University of Science and Technology of China, Hefei 230026, China

[2] Department of Modern Physics, University of Science and Technology of China, Hefei 230026, China

1 Introduction

Quantum communication [1] has been attracting more and more attention in the field of secure communication, due to its unconditionally secure property. The pace of practical application is also accelerating [2, 3]. The BB84 protocol-based [4] key distillation, which is extensively used in quantum key distribution (QKD) systems, requires synchronization between the transmitter and the receiver to complete the key generation. The synchronization system is critical, for it can affect the running of the basis sifting directly and influence the efficiency of key distillation.

Generally, we use optical synchronization in practical implementation. There are two types of signals in the QKD system, quantum signal and synchronization signal. Quantum signal adopts single photons as carriers of quantum information to generate a secure key [5], while the synchronization signal is some kind of classical periodic signal, which is mainly used for synchronization of the two sides [6].

Common system synchronization uses one quantum signal following one synchronization signal. This scheme is simple and reliable in low-speed QKD systems, but it has an obvious disadvantage in supporting high-speed QKD systems. On the one hand, during the transmission, since the synchronization signal has a strong intensity light, while the quantum signal has a very weak intensity light, the strong light will have influence over the weak light in simultaneous transmission. This may result in failure of the high-speed QKD system. On the other hand, a more complex synchronization scheme is required, along with the increase in system frequency [7–9].

To solve the problems mentioned above, we put forward a novel synchronization scheme based on TDC [10–13],

which allows multiple quantum signals following one synchronization signal, and verify the feasibility of this scheme in an actual QKD system. The scheme not only reduces the influence of the synchronization signal on the quantum signal during transmission, but also simplifies the synchronization system.

2 Principle of scheme

According to BB84 protocol, the two parties (the transmitter is called "Alice" and the receiver is called "Bob") of QKD need to have the same temporal order of quantum signal before executing basis sifting. The synchronization is to map the temporal order information of the quantum signal detected by the receiver with that sent by the transmitter.

The temporal order of the quantum signal in the transmitter can be predetermined; therefore, we only need to obtain the temporal order of the quantum signal in the receiver. To achieve this goal, we use high-precision time measurement technology, which can convert the time information of the quantum signal into the corresponding digital temporal information, and match it with the transmitter.

The synchronization scheme focuses on two aspects: the frequency of the synchronization signal of the transmitter and the time interval between the two adjacent quantum signals.

The module of the receiver used to detect the time information [14, 15] is called the "high-precision time measurement module." As the core unit of the whole synchronization system, its structure and performance directly determine the process of synchronization and the precision of system. The module mentioned above adopts a "start-and-stop" measuring method, that is, a single "start" signal and multiple "stop" signals. Each "stop" signal refers to its previous "start" signal, and the module obtains the time interval information between the "start" and "stop" signals.

The illustrative diagram of the time measurement-based synchronization scheme is shown in Fig. 1.

Firstly, Alice sends the sequence of synchronization signal pulses S0, S1, ..., Sn (time interval for adjacent synchronization signal is $t1$) and the sequence of quantum signal pulses AP0, AP1, ..., APn (time interval for adjacent quantum signal is $t2$).

Secondly, Bob detects the synchronization signals and quantum signals. The sequence of synchronization signals can all be detected, while only a few of the quantum signals can be detected, for most are lost due to path attenuation. The supposed quantum signals, BPi and BPk, are detected

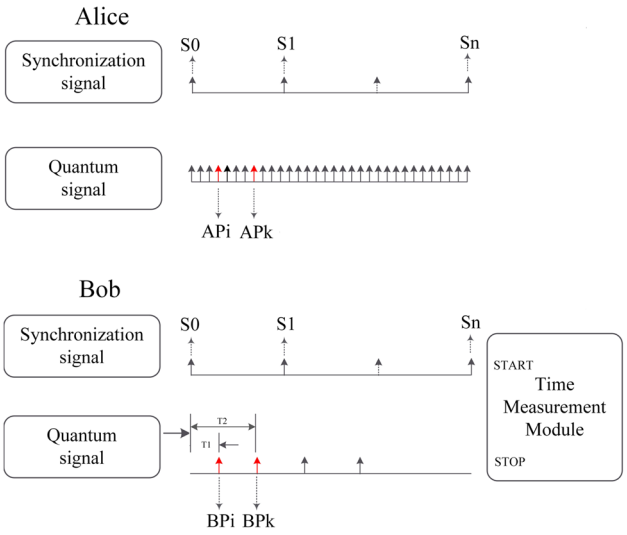

Fig. 1 (Color online) Schematic diagram of the time measurement-based synchronization scheme

by Bob, and the two detected quantum signals correspond to APi and APk from Alice, respectively.

Then, Bob calculates the time information of each quantum signal. The calculation process is as follows (take Bpi as an example):

1. Record the number of synchronization signals ahead of the BPi quantum signal as m, then multiply by the cycle time $t1$. The product is regarded as coarse timing. The coarse timing is $m \times t1$.
2. Record the time interval between the BPi quantum signal and its previous synchronization signal as $T1$. This serves as fine timing.
3. Obtain the sum of the coarse timing and fine timing as total time $T, T = m \times t1 + T1$.

Finally, Bob converts the total time to the corresponding temporal order of each quantum signal; temporal order is T / $t2$. The temporal order of each quantum signal that is figured out by Bob, corresponds to one of the values in the quantum signal sequence, AP0, AP1, ..., APn, of Alice.

3 Experimental

In order to verify the feasibility of this synchronization scheme in QKD system, we designed a time measurement module and complete the relevant experimental work on an actual platform of the QKD system.

3.1 Time measurement module test

The main chip of the time measurement module is TDC-GPX, which is produced by the ACAM Company of

Germany. It has eight independent channels, and its maximum sampling rate is 40 MHz [16]. Figure 2 is a test block diagram of the time measurement module. We used a signal generator as a source which can output two LVTTL signals with the same frequency. One serves as the "start" signal and the other serves as the "stop" signal. Moreover, the "start" signal is ahead of the "stop" signal, and the delay time between the "stop" and the "start" is adjustable. The TDC-GPX chip is in I mode and the time BIN is set as 100 ps. FPGA is used to read the data from TDC-GPX and upload it to a PC.

We set the "start-stop" signal time interval value from 1 to 9 μs on the signal generator. The module obtains the measured data of each time event and uploads it to a PC for analysis. The linearity between the time interval value and the measured data is shown in Fig. 3. The horizontal axis is the set time interval value between the "start" signal and "stop" signal on the signal generator. The axis unit is μs. The vertical axis is the measured data from the time measurement module. The axis unit is time BIN. We can see that the measured data increase with the length of the time interval value. The data show good linearity.

Then, we set a typical fixed time interval 5 μs between the "start" and "stop" on the signal generator. The distribution of output data is shown in Fig. 4. The unit of the horizontal axis is 100 ps, and that of vertical axis is the number of counts. Meanwhile, the total sample number is 50 000. From Fig. 4, we can see that the output data of TDC-GPX basically meet the law of normal distribution: The central value is 5.0940 μs; the bottom width (the total data of 99 %) is five times the time unit, that is, $5 \times 100\,\text{ps} = 500\,\text{ps}$; the full width half maximum (FWHM) is $1.35 \times 100\,\text{ps} = 135\,\text{ps}$; and the sigma is $0.57 \times 100\ \text{ps} = 57\ \text{ps}$.

According to the test results, if the frequency of the quantum signal is 200 MHz, the minimum time interval between the two adjacent signals that arrived at Bob is 5 ns. The bottom width of the TDC-GPX's output is far less than the time interval between two adjacent quantum signals, so TDC-GPX can distinguish the arrival time of the two quantum signals accurately.

3.2 Validation of the QKD system

On an actual QKD hardware platform, the frequency of the quantum signal is 200 MHz and the frequency of the synchronization signal is 200 kHz. The hardware block diagram of the platform of the QKD system is shown in Fig. 5.

Fig. 2 Test block diagram of the time measurement module

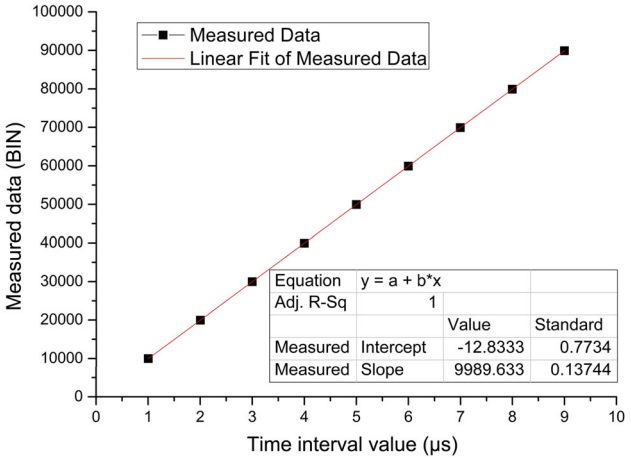

Fig. 3 (Color online) The linearity between time interval value and measured data

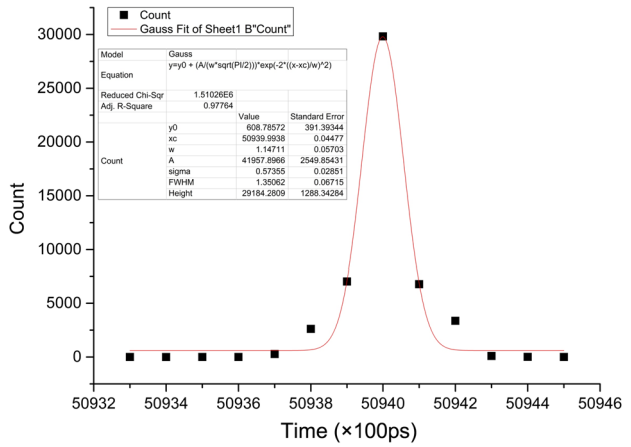

Fig. 4 (Color online) Distribution of the test data

This is a typical QKD system [17, 18]. The FPGA of Alice receives random data from the PC and generates driving signals for the "synchronization laser" and the "quantum laser." The "synchronization laser" generates synchronization optical signals, and the "quantum laser" generates quantum optical signals. Both of the two types of optical signal should get through an attenuator (ATT), respectively, before going to the optical fiber for transmission. The optical fiber length is 50 km, and the path attenuation between the transmitter and the receiver is adjustable. When the synchronization signal and quantum signal arrived at the receiver, they, respectively, go to the detector for the synchronization signal and the detector for the quantum signal. The synchronization detector converts the optical signal into an electrical signal which goes into a fan-out chip to become double signals. One goes to the

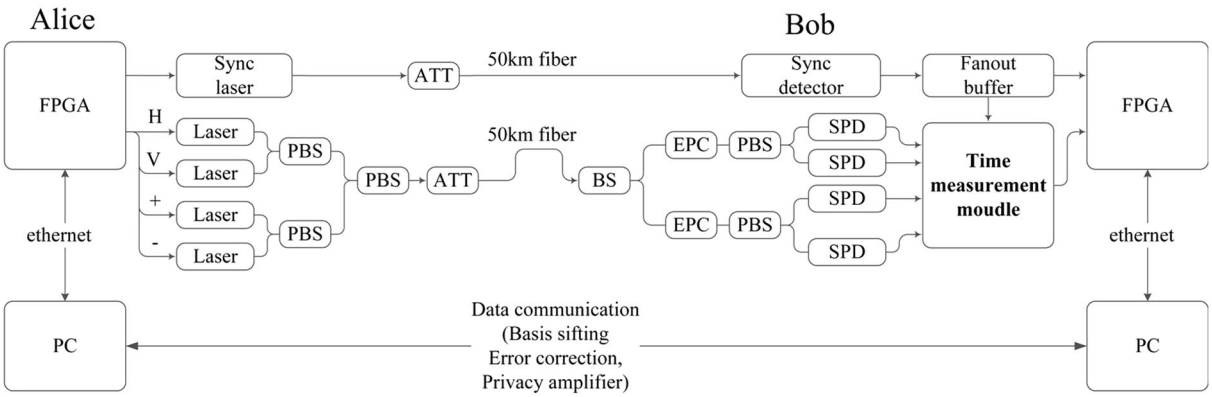

Fig. 5 Hardware block diagram of the platform of QKD system

time measurement module and serves as the "start" signal, while the other enters into FPGA for calculating coarse timing. The detector for the quantum signal is a kind of single-photon detector (SPD), which can convert the quantum signal into an electrical signal. The converted signal goes into the time measurement module and serves as the "stop" signal. After that, the FPGA of Bob reads the data from the module and uploads it to the PC. Finally, the key distillation process is done on the PC from both sides.

In the actual system, since the synchronization signal and the quantum signal have different transmission paths, the receiver needs to do a time-base offset compensation between the two signals. Figure 6 shows the principle of the time-base offset compensation.

1. Alice sends a low-frequency pulse sequence of the synchronization signal S0, S1, ..., Sn and the same frequency pulse sequence of the quantum signals AP0, AP1, ..., APn. Each synchronization signal follows a quantum signal, and the time interval between the two signals is fixed, which is recorded as *Ta*;

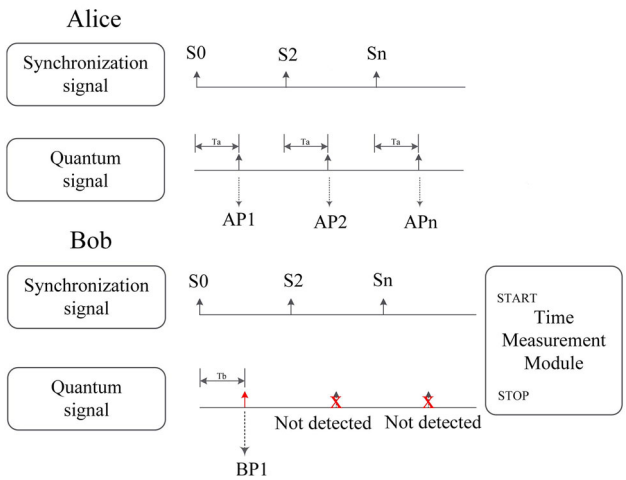

Fig. 6 Principle of the time-base offset compensation

2. Bob records the time intervals between each arrived quantum signal and its previous synchronization signal, and then figures out the average value as *Tb*.
3. Bob calculates the *D*-value between *Tb* and *Ta* as Δt, so, $Ta = Tb + \Delta t$. Δt is the value of the time-base offset compensation.

The data from the time measurement module should add a Δt bias as the "correct time." Key distillation will begin after the FPGA of Bob converts the "correct time" to a corresponding temporal order. The QKD system can output sifted keys continuously without increasing the quantum bit error rate. The test result shows that this synchronization scheme can accurately map the temporal order information of the receiver with that of the transmitter.

4 Conclusion

The time measurement based synchronization scheme proposed in this paper adopts multiple quantum signals following one synchronization signal. From the above experimental data, the following conclusions can be obtained: The measured data of the time measurement module show good linearity. Moreover, the test data show that the module has a good time resolution. These good performances allow the module to be applied in an actual QKD system. In the actual QKD platform, the frequency of the quantum signal is set to 200 MHz, and with the frequency of the synchronization signal set to 200 kHz, the time information can be accurately converted to the corresponding temporal order.

The synchronization scheme is novel and practical, and it can support a wide frequency range of the QKD system. It is not only applicable in low-speed QKD systems, but also proved to be feasible in high-speed QKD systems. Furthermore, this scheme is not sensitive to the distance of the two sides and as result is a good choice in a long-distance QKD system.

Acknowledgments This work was supported by National Natural Science Foundation of China (Nos. 11375195, 11375263 and 11105143) and National Magnetic Confinement Fusion Energy Development Research (No. 2013GB104003).

References

1. N. Gisin, G. Ribordy, W. Tittel et al., Quantum cryptography. Rev. Mod. Phys. **74**, 145–195 (2002). doi:10.1103/RevModPhys.74.145
2. M. Peev, C. Pacher, R. Allaume et al., The SECOQC quantum key distribution network in Vienna. Proc. Soc. Photo Opt. Instrum. (2009). doi:10.1088/1367-2630/11/7/075001
3. W. Weigel, G. Lenhart, Standardization of quantum key distribution in ETSI. Wirel. Pers. Commun. **58**, 145–157 (2011). doi:10.1007/s11277-011-0293-8
4. C.H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing. Theor. Comput. Sci. **560**, 7–11 (2014). doi:10.1016/j.tcs.2014.05.025
5. A. Mink, S. Frankel, R. Perlner, Quantum key distribution (QKD) and commodity security protocols: introduction and integration. Int. J. Netw. Secur. Its A (IJNSA) **1**, 101–110 (2009). http://arxiv.org/ftp/arxiv/papers/1004/1004.0605
6. G.B. Xavier, N. Walenta, G. Vilela de Faria et al., Experimental polarization encoded quantum key distribution over optical fibers with real-time continuous birefringence compensation. New. J. Phys. **11**, 045015 (2009). doi:10.1088/1367-2630/11/4/045015
7. X. Tang, L. Ma, A. Mink et al., Experimental study of high speed polarization-coding quantum key distribution with sifted-key rates over Mbit/s. Opt. Express **14**, 2062–2070 (2006). doi:10.1364/OE.14.002062
8. D.B. Horoshko, D.I. Pustakhod, S.Y. Kilin, Time-shift quantum key distribution: sensitivity to losses. Opt. Spectrosc. **111**, 685–688 (2011). doi:10.1134/S0030400X11110129
9. H. Xu, L. Ma, A. Mink et al., 1310-nm quantum key distribution system with up-conversion pump wavelength at 1550 nm. Opt. Express **15**, 7247–7260 (2007). doi:10.1364/OE.15.007247
10. L.F. Wei, R. Zhou, C.W. Yang, Design and realization of the ICF neutron time-of-flight measurement circuit. Nucl. Tech. **38**, 070403 (2015). doi:10.11889/j.0253-3219.2015.hjs.38.070403. **(in Chinese)**
11. L. Dong, J.F. Yang, K.Z. Song, Carry-chain propagation delay impacts on resolution of FPGA-based TDC. Nucl. Sci. Tech. **25**, 030401 (2014). doi:10.13538/j.1001-8042/nst.25.030401
12. X. Qin, S.B. Liu, Q. An, An USB-based time measurement system. Nucl. Sci. Tech. **21**, 366–369 (2010). doi:10.13538/j.1001-8042/nst.21.366-369
13. F. Dou, H. Liang, L. Zhou et al., A precise time measurement evaluation board for a radiography system of high-Z materials. Nucl. Sci. Tech. **23**, 284–288 (2012). doi:10.13538/j.1001-8042/nst.23.284-288
14. Q. Shen, S. Liao, S.B. Liu et al., An FPGA-based TDC for free space quantum key distribution. IEEE Trans. Nucl. Sci. **60**, 3570–3577 (2013). doi:10.1109/TNS.2013.2280169
15. S.K. Gupta, J. Christiansen, Y. Hayashi et al., Measurement of arrival time of particles in extensive air showers using TDC32. Exp. Astron. **35**, 507–526 (2013). doi:10.1007/s10686-012-9320-3
16. TDC-GPX Ultra-High Performance 8 Channel Time-To-Digital Converter Datasheet. Jan. 18, 2007. http://www.acam.de/fileadmin/Download/pdf/English/DB_GPX_e
17. Y. Liu, T.Y. Chen, J. Wang et al., Decoy-state quantum key distribution with photon polarization over 200 km. Opt. Express **18**, 8587–8594 (2010). doi:10.1364/OE.18.008587
18. R.S. Soorat, A.S. Vudayagiri, Polarization shift keying for free space QKD: effect of noise on reliability of the QKD protocols, in *International Conference on Fiber Optics Photonics, OSA Technical Digest* (2012). doi:10.1364/PHOTONICS.2012.WPo.19