Article

Chinese Science Bulletin

Quantum Information

August 2011 Vol.56 No.22: 2305–2311
doi: 10.1007/s11434-011-4570-4

Real-time compensation of phase drift for phase-encoded quantum key distribution systems

ZHANG LiJun[1], WANG YongGang[1*], YIN ZhenQiang[2*], CHEN Wei[2], YANG Yang[1], ZHANG Tao[1], HUANG DaJun[1], WANG Shuang[2], LI FangYi[2] & HAN ZhengFu[2]

[1] *Department of Modern Physics, University of Science and Technology of China, Hefei 230026, China;*
[2] *Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China*

Received March 18, 2011; accepted April 19, 2011

Phase drift is an inherent problem in phase-encoded quantum key distribution (QKD) systems. The current active phase tracking and compensation solutions cannot satisfy the requirements of a system with nonlinearity in phase modulation. This paper presents a four-phase scanning method, which is based on the quantitative analysis of the quantum bit error rate (QBER) from phase drift and the performance requirements of phase compensation. By obtaining the four interference fringes and adjusting the coding matrix of the system, this method automatically calculates the accurate driving voltages for the phase modulator. The implementation and experimental tests show that the proposed method can compensate phase drift caused by environmental changes and the system's nonlinearity, and is applicable to large-scale QKD networks.

quantum key distribution, phase-coding, phase drift, active phase compensation, four-phase scanning method, FPGA

Citation: Zhang L J, Wang Y G, Yin Z Q, et al. Real-time compensation of phase drift for phase-encoded quantum key distribution systems. Chinese Sci Bull, 2011, 56: 2305–2311, doi: 10.1007/s11434-011-4570-4

Quantum key distribution (QKD) offers a secure way of separating parties to establish a shared cryptographic key over a non-protected communication channel. The first quantum cryptography protocol, BB84 [1], defined by Bennett and Brassard in 1984, makes it possible to implement the one-time-pad encryption in practice. This has attracted the attention of many researchers in the field of information security. Following the developments over the past two decades, QKD systems have progressed from laboratory studies to applicable commercial products.

Optical fiber based QKD systems using optical fiber to provide the quantum transmission channel, encode the bit information using the quantum states of single photons. Most early optical fiber based QKD systems used the polarization coding scheme [2]. This scheme can easily be realized in a laboratory, but it is not the best choice for fiber based QKD systems because of the inherent birefringence effect on the single-mode fiber. The birefringence effect can destroy the polarization states of photons, causing a higher quantum bit error rate (QBER) as the transmission distance increases [3,4].

The phase coding scheme is the scheme of choice for current implementations of fiber based QKD systems [5,6]. With an interferometer pair on the two communication sides, the sender (Alice) encodes the bit information as a phase delay in the interferometer and the receiver (Bob) decodes the phase delay to obtain the transmitted information. Figure 1 shows the structure of an asymmetric Faraday-Michelson interferometer (F-MI) QKD system [7]. There are two F-M interferometers located on either side of Alice and Bob which are connected by an optical fiber. Photons emitted by the sender can follow one of two paths when passing through the interferometers at both sender and receiver — one path is the short arm in the interferometer and the other is the long arm. Therefore, the counting histogram of the single photon detector (SPD) in Bob will have three peaks. The first peak corresponds to the 'short-short' path, the last peak corresponds to the 'long-long' path, and

*Corresponding authors (email: wangyg@ustc.edu.cn, yinzheqi@mail.ustc.edu.cn)

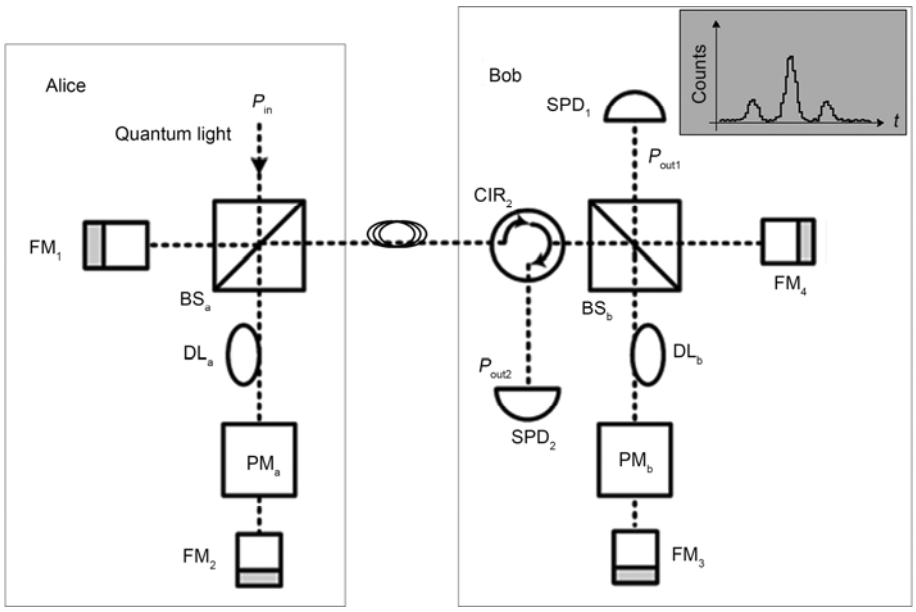

Figure 1 The principle of a phase-encoded QKD system based on F-M interferometers. BS, 50/50 beam splitter; FM, Faraday mirror; SPD, single photon detector; CIR, circulator; DL, fiber delay line.

the second peak corresponds to either the 'short-long' path or the 'long-short' path. The two cases in the second peak are indistinguishable. By detecting the second peak using a timing window technique, Alice and Bob can safely exchange a cryptographic key.

Phase drift is an inherent problem for phase-encoded QKD systems because the phase of Alice and Bob's interferometers response differently to the ambient temperature. This phase drift will directly increase the QBER, and even result in the QKD system becoming out of control. Generally, there are two solutions to minimize phase drift [7]. One is to stabilize the ambient temperature of the interferometers, for example by placing the experimental setups on an isolated and temperature controlled optical platform. However, because this method is very expensive and complicated it is only suitable for laboratory studies. Instead, active phase tracking and compensation, which are currently being investigated by corresponding research groups, are effective solutions for both laboratory and practical applications. Normally an online accurate phase scanning is needed if these methods are applied.

Current investigations on phase drift and compensation [8,9] assume that the control voltage of the phase modulator has a linear relationship with the actual phase change in the interferometer (these are known as single-phase scanning solutions). For those systems that do not have a linear relationship between the control voltage and phase change, the effectiveness of the single-phase scanning is very limited. During the actual testing of a multi-node QKD network in our laboratory [10,11], we also found that the v-φ relation for some modulators is not linear [9,12–14], which means that a new phase tracking and compensation method has to be researched. In addition, besides the optical phase modulator, the control electronics system also contributes to the nonlinearity of the system, which includes the nonlinearity of the digital-to-analog converter, voltage signal amplification, and so on. All these aspects decrease the accuracy of the phase scanning, especially for high-speed QKD systems.

In this paper, we investigate and implement an accurate phase scanning and compensation method, which is called the "four-phase scanning method", to track and compensate phase drift. By measuring and scanning the output at Bob's side, the accumulated phase drift of the system, including that of Alice's side and the connecting channel, is measured and compensated at Bob's side. We provide an accurate algorithm to analyze the scanning result and adjust the phase voltage to Bob's phase modulator. To carry out the scanning and compensation algorithm on the fly, we implemented the algorithm using an FPGA so that the extra time for the scanning and compensation is negligible. The test results show that our new method can effectively enhance the performance of our QKD system. It has also been used successfully in our commercial products.

1 Phase drift in the phase-encoded QKD system

In the implementation of a phase-encoded QKD system, Alice selects one of the four phase shifts (0, $\pi/2$, π, $3\pi/2$) through the phase modulator located in the long arm of the interferometer. She randomly chooses a base, (0, π) or ($\pi/2$, $3\pi/2$) and assigns the bit value according to a pre-defined coding scheme. For instance, bit value 0 is represented as phase 0 or phase $\pi/2$, while bit value 1 is represented as phase π or phase $3\pi/2$. Bob also randomly chooses his measuring base through his phase modulator. Only if Alice

and Bob choose the same bases, can Bob obtain the deterministic result which is used to infer the bit value that the opposite side has registered. The intensity in the output SPD1 port is expressed by [8]

$$I_{\text{out1}} = I_{\text{in}} \cos^2\left(\frac{\phi_{\text{A}} - \phi_{\text{B}}}{2}\right), \tag{1}$$

where ϕ_{A} is the phase shift in Alice's phase modulator, and ϕ_{B} is the phase shift in Bob's phase modulator. The count of SPD1 I_{out1} reaches its maximum value when $\phi_{\text{A}}-\phi_{\text{B}} = 0$, and its minimum value when $\phi_{\text{A}}-\phi_{\text{B}} = \pi$. Defining ϕ_{e} as the phase drift in the whole system, the QBER caused by ϕ_{e} is

$$\begin{aligned} e &= \frac{I_{\text{in}} \cos^2\left(\frac{(\phi_{\text{A}} - \phi_{\text{B}})_{\pi} + \Delta\phi_{\text{e}}}{2}\right)}{I_{\text{in}} \cos^2\left(\frac{(\phi_{\text{A}} - \phi_{\text{B}})_{0} + \Delta\phi_{\text{e}}}{2}\right) + I_{\text{in}} \cos^2\left(\frac{(\phi_{\text{A}} - \phi_{\text{B}})_{\pi} + \Delta\phi_{\text{e}}}{2}\right)} \\ &= \frac{I_{\text{in}} \sin^2\left(\frac{\Delta\phi_{\text{e}}}{2}\right)}{I_{\text{in}} \cos^2\left(\frac{\Delta\phi_{\text{e}}}{2}\right) + I_{\text{in}} \sin^2\left(\frac{\Delta\phi_{\text{e}}}{2}\right)} \\ &= \sin^2\left(\frac{\Delta\phi_{\text{e}}}{2}\right). \end{aligned} \tag{2}$$

The relationship between the QBER and the phase drift shown in eq. (2) is depicted in Figure 2. In an applicable QKD system, the QBER is required to be below 11% [15], so the phase drift has to be smaller than 38°. To a decoy-state protocol QKD system or a low coherence light source system [16], the QBER is required to be below 5%, so the phase drift has to be smaller than 25.5°.

Phase drift is an inherent problem in a phase-encoded QKD system [9]. To quantitatively measure the phase drift in our present QKD system, we carried out the following experiment. Alice fixes her phase modulation voltage. Bob scans his phase modulation voltage from 0 to the full scale range of the DAC in a large number of steps. In each step, he counts the number of photons detected by the SPD. Counting through all the steps, Bob can ascertain the minimum counts versus the phase voltage. This voltage represents exactly the phase where the destructive interference takes place. Repeating the measurement of the voltage every 2.5 s, the curve of destructive interference voltage versus time is plotted in Figure 3. This curve reflects the phase drift of the whole system, from Alice to Bob, over time. The results of the experiment show that the average speed of the phase drift is 0.15 rad/min and the fastest speed is about 0.4 rad/min, which could cause the QBER in one minute to change by 0.57% on average, while the largest variation could be more than 4% in the worst case. Therefore, for a QKD system to keep running stably for a long time, it is very necessary to measure the phase drift quickly and compensate it online. The quicker the compensation is carried out, the lower will be the QBER caused by phase drift. In the light of this need, our system uses a four-phase scanning method to identify the correct phase modulating voltages in a timely fashion to actively compensate this kind of phase drift.

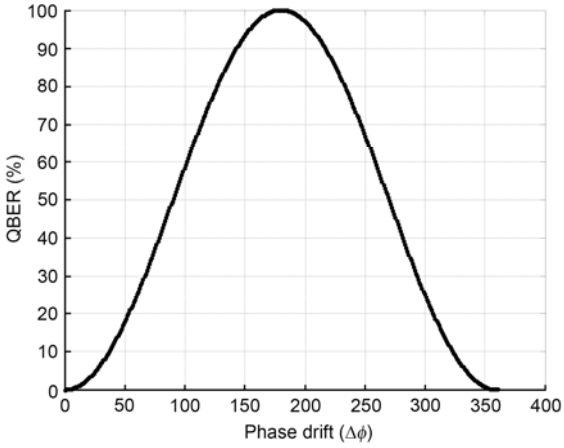

Figure 2 QBER versus phase drift curve.

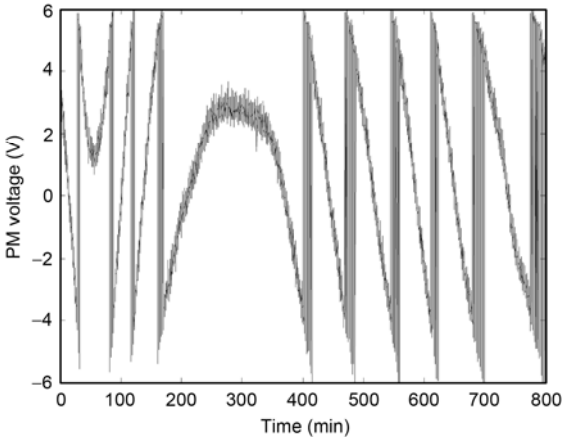

Figure 3 Phase drift versus time curve.

2 Four-phase scanning method

The four-phase scanning method is based on two concepts: the interference fringe and the coding matrix. The interference fringe is the curve of the relationship between the SPD counts and the phase difference between Alice's and Bob's phase modulators. Either site, for example, Alice, fixes its phase modulation voltage as V_{ref}, which denotes the corresponding phase shift as ϕ_{ref}. The opposite site, i.e. Bob, scans its phase modulation voltage from 0 to the full scale range of the DAC (its output voltage controls the phase shift) in a number of steps. In our setup, the phase modulation voltage ranging from −6 V to 6 V corresponds the phase shift ranging from 0 rad to more than 2π rad. Therefore, scanning the control voltage will traverse 0 to 2π phase differences. At each scanning step, Alice transmits a certain number of photons, and at the same time Bob counts the number of photons detected by the SPD, giving the curve of

counting intensity versus phase difference (Figure 4). The process of fixing the A-side at $V_{a,ref}$ and traversing the B-side is called scanning B (relative to $V_{a,ref}$). Through the interference fringe from scanning B, we obtain two important parameters for the B-side modulator. One is the half-wave voltage (denoted by $V_{b,half}$), which is the voltage difference of the half cycle of the interference fringe. The second parameter is the destructive interference voltage, which is the voltage at the valley of the interference fringe, and is denoted as $V_{b,ref\pm\pi}$. The phase difference between voltages $V_{a,ref}$ and $V_{b,ref\pm\pi}$ is π rad. Through the process of-scanning A, we obtain the following two parameters for the A-side modulator: $V_{a,half}$ and $V_{a,ref\pm\pi}$.

Table 1 shows the theoretical coding matrix for phase-encoded systems. The first column represents Alice's four phase shifts, while the first row represents Bob's four phase shifts. Each element in the 4 by 4 matrix represents the SPD counts for the combination of the phase shifts selected by Alice and Bob. As the number of elements can differ between the ideal coding matrix and the measured coding matrix, the measured coding matrix could provide the means for evaluating the performance of the phase modulation. The more accurately the phase shifts on both sides are modulated, the closer the matrix approaches the ideal coding matrix.

The main steps in the four-phase scanning method are as follows (Figure 5).

(1) Similar to the process of the single-phase scanning method, Alice first gets her half-wave voltage ($V_{a,half}$) by scanning her interference fringe. Assuming its zero phase modulation voltage is $V_{a,0}$, Alice can estimate her voltages for the four phase shifts ($V_{a,0}$, $V_{a,\pi/2}$, $V_{a,\pi}$, $V_{a,3\pi/2}$) as ($V_{a,0}$, $V_{a,0}+1/2V_{a,half}$, $V_{a,0}+V_{a,half}$, $V_{a,0}+3/2V_{a,half}$), respectively.

(2) Setting Alice's phase modulation voltage $V_{Alice,ref}$ as 0, $\pi/2$, π, $3\pi/2$ in turn, Bob scans his interference fringes. From these four interference fringes, Bob obtains his destructive interference voltages as ($V_{b,0\pm\pi}$, $V_{b,\pi/2\pm\pi}$, $V_{b,\pi\pm\pi}$, $V_{b,3\pi/2\pm\pi}$). These are exactly equal to Bob's four phase modulating voltages ($V_{b,\pi}$, $V_{b,3\pi/2}$, $V_{b,0}$, $V_{b,\pi/2}$).

(3) By observing the difference between the ideal coding matrix and the calculated coding matrix, tune Alice's four phase modulation voltages ($V_{a,0}$, $V_{a,\pi/2}$, $V_{a,\pi}$, $V_{a,3\pi/2}$) and repeat steps (2) and (3) until the difference is sufficiently small.

(4) The current voltages ($V_{a,0}$, $V_{a,\pi/2}$, $V_{a,\pi}$, $V_{a,3\pi/2}$) and their scanning results ($V_{b,\pi}$, $V_{b,3\pi/2}$, $V_{b,0}$, $V_{b,\pi/2}$) will be used in the normal transmission process.

The four-phase scanning process can be implemented in two forms: off-line scanning and adjustment, which involves steps (1) to (4), and real-time scanning and compensation, which only involves steps (2) and (4). The real-time scanning process and the quantum key transmission process are carried out in an interleaved mode, i.e. before one frame of the quantum key is transmitted, the real-time four-phase scanning process is executed once (A to B in Figure 5).

To minimize the time needed for scanning in one frame of the quantum key transmission cycle, we divide the process into two steps: a coarse scanning step and a fine scan-

Table 1 Ideal coding matrix

A/B	0	$\pi/2$	π	$3\pi/2$
0	1	0.5	0	0.5
$\pi/2$	0.5	1	0.5	0
π	0	0.5	1	0.5
$3\pi/2$	0.5	0	0.5	1

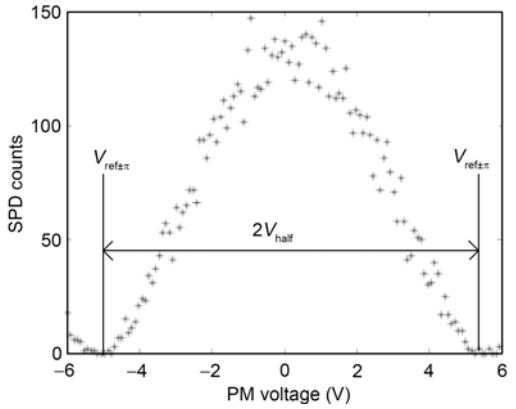

Figure 4 Interference fringe.

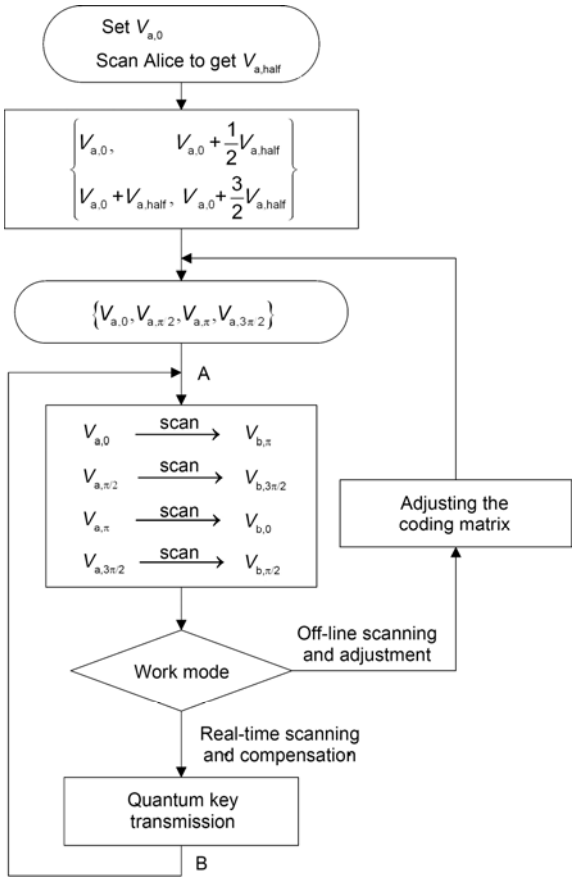

Figure 5 Flow diagram of the four-phase scanning method.

ning step. In the coarse scanning step, the system performs the scanning using a bigger step voltage to find an approximate range of the voltage for the phase shift. This is then followed by the fine scanning step, which uses a lower step voltage. To improve accuracy further, we use a 5-point moving average to smooth the SPD counting curve before the voltages in the valley are determined.

3 FPGA based real-time scanning implementation

Figure 6 gives an overview of the structure of our QKD system. Both sender Alice and receiver Bob consist of optical devices and control electronics systems. They are connected to each other via a single-photon transmission fiber, a synchronizing pulse transmission fiber, and a classical transmission channel. The control electronics system is constructed by an embedded mother-board and a QKD sub-board [17]. The QKD sub-board takes charge of generating the driving signals for the optical devices or processing detected signals on Bob's side. All the necessary logic operations and the real-time scanning function are carried out by an FPGA Cyclone II EP2C20F484 in the QKD sub-board under the control of the mother-board. The mother-board, based on an embedded processor MPC8260 running the GNU/LINUX operating system, is responsible for system control and the high level processing of the BB84 protocol.

The four-phase scanning algorithm proposed in this paper can be implemented by high level software without adding any hardware devices, but the performance of the algorithm is limited as the phase drift is rather fast in phase-encoded systems. In our setup, we implemented the scanning algorithm using the FPGA on the QKD sub-board. Figure 7 depicts an outline of the implementation. Under the control of the MPC8260 via its local bus, the counter and comparator I control the number of photon pulses transmitted by Alice during one step of scanning, while the adder and comparator II control the stepping. Registers in the FPGA store the parameters related to the scanning. When the scanning is finished, an interrupt signal is generated to notify the mother-board to read the scanning results from the DDR on the sub-board. A typical scanning result is similar to that shown in Figure 4.

Because the parameters of the QKD system can be configured flexibly by writing registers in the FPGA, we configured different operating parameters during the different periods of one QKD cycle, such as different ATT values, different SPD dead times, different pulse repetition rates, and so on, to realize different working modes. Using this flexibility, the time period for scanning, which occupies the cycle of one frame of transmission, could be minimized.

4 Experimental results and performance analysis

For the experiment, Alice used a low coherence light source with a pulse repetition rate of 20 MHz and the single photon was detected at Bob's side by an InGaAs SPD, which was developed by Princeton Lightwave. The system software (coded in C) running on the mother-board controlled the sub-board to complete the whole QKD process. Using the four-phase scanning method with the coarse and fine scanning steps and the moving average curve smoothing, the QKD system ran the "scanning-transmission" mode continuously for 14 h without any manual adjustment or special temperature control. Each QKD cycle was about 2.5 s, which included 1.12 s for transmitting quantum states, 0.95 s for generating random numbers, 0.4 s for reconciling bases [18–20], estimating QBER, and system scheduling. Therefore, the proportion of scanning time to the total time was less than 6%. In future experiments, we expect to implement the random number generation in real-time. In this case, the time spent on random number generation can be avoided, and the proportion of scanning time to the total time will be less than 10%. Figure 8 shows how the QBER varies over time, while Figure 9 shows the QBER distribution. The system QBER, which may be caused by phase drift, SPD dark counts, and optical imperfection, remains around 1.6% for a long time. This demonstrates that the

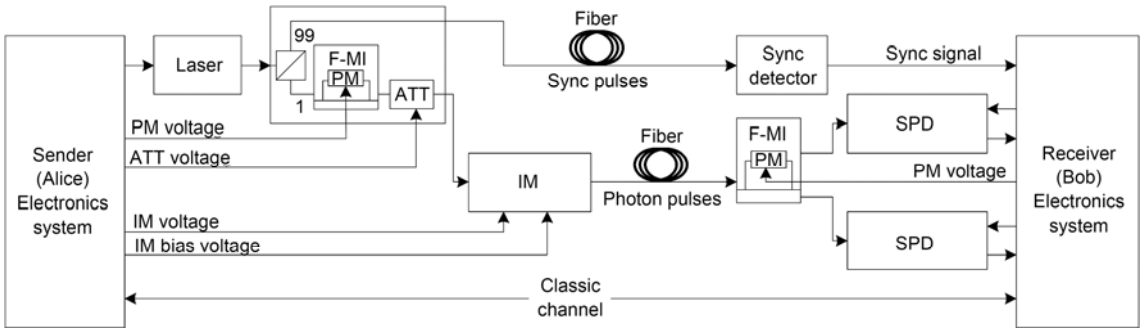

Figure 6 Structure of the phase-encoded QKD experimental system. PM, phase modulator; IM, intensity modulator; ATT, attenuation; F-MI, Faraday-Michelson interferometer.

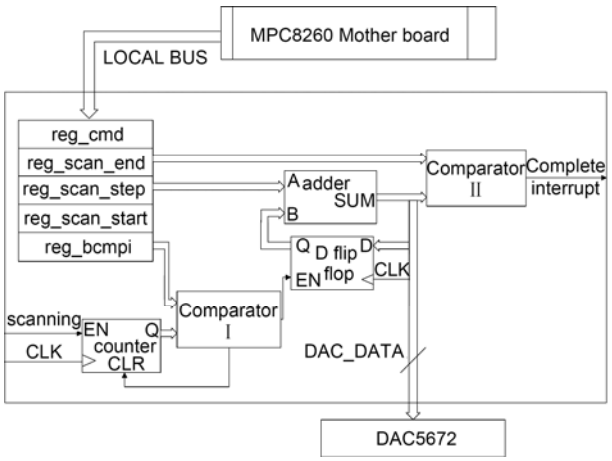

Figure 7 FPGA implementation of the scanning algorithm.

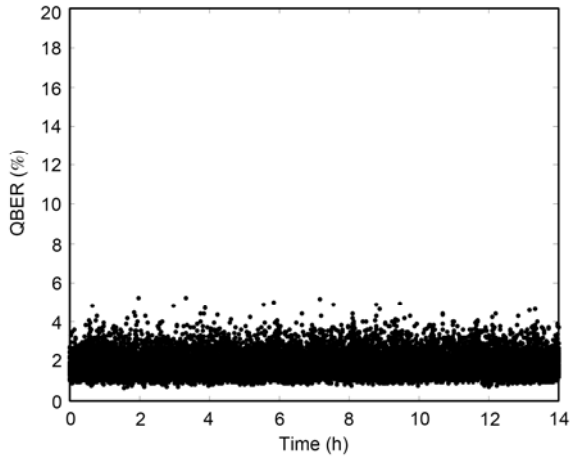

Figure 8 QBER versus time curve.

four-phase scanning and compensation method introduced in this paper can effectively suppress the effect of phase drift.

With the experimental devices mentioned above, we also implemented a five-node practical QKD network [10] using the four-phase scanning method. Table 2 shows how the QBER varies with different transmitted light wavelengths and different channel attenuation. This proves once again that the four-phase scanning method is a general and effective solution for solving the phase drift problem in phase-encoded QKD systems.

5 Conclusion

We have quantitatively described the QBER resulting from phase drift in phase-encoded QKD systems and the requirements for phase compensation. We proposed an algorithm of the four-phase scanning and compensation method to obtain the four interference fringes and adjust the coding matrix. Using this method, the QKD system automatically

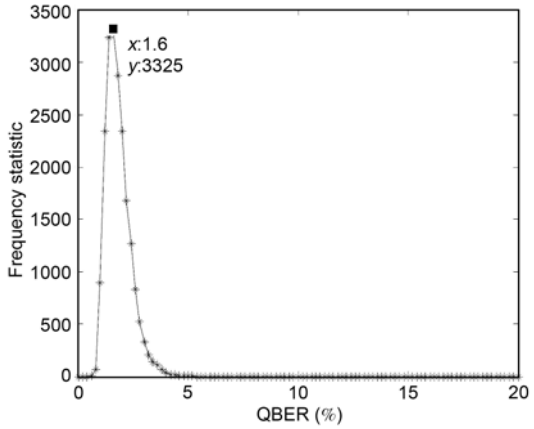

Figure 9 QBER distribution curve.

Table 2 Test results of the five-node QKD network

Wavelength (nm)	Attenuation (dB)	QBER (%)
1530	7.24	2.92
1550	8.78	2.84
1550	10.79	2.78
1530	14.77	3.76

obtains the four voltages for the phase modulator on Bob's side to compensate the phase drift of the system. We implemented the algorithm using an FPGA so that it could perform the scanning and compensation in real-time. The new method has been successfully utilized in our commercial oriented prototype. During a 14 h test run without any manual adjustment and special temperature control, our QKD performed stably and maintained the QBER within 1.6%. The realization of a five-node QKD network also proves that the four-phase scanning method and its implementation is an efficient, accurate, stable solution for solving the phase drift problem caused by environmental differences and the system's nonlinearity.

This work was supported by the National Basic Research Program of China (2006CB921900) and the National Natural Science Foundation of China (60921091).

1 Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of International Conference on Computers, Systems and Signal Processing, 1984. 175–179
2 Smolin J A. The early days of experimental quantum cryptography. IBM J Res Develop Phys Inform, 2004, 48: 47–52
3 Muller A, Zbinden H, Gisin N. Underwater quantum coding. Nature, 1995, 378: 446–449
4 Wang W Y, Wang C, Zhang G Y, et al. Arbitrarily long distance quantum communication using inspection and power insertion. Chinese Sci Bull, 2009, 54: 158–162
5 Marand C, Townsend P D. Quantum key distribution over distances as long as 30 km. Opt Lett, 1995, 20: 1695–1697
6 Townsend P D. Quantum cryptography on optical fiber networks. Opt Fiber Tech, 1998, 4: 345–370
7 Mo X F, Zhu B, Han Z F, et al. Faraday-Michelson system for quan-

tum cryptography. Opt Lett, 2005, 30: 2632–2634
8 Makarov V, Brylevski A, Hjelme D R. Real-time phase tracking in single-photon interferometer. Appl Opt, 2004, 43: 4385–4392
9 Chen W, Han Z F, Mo X F, et al. Active phase compensation of quantum key distribution system. Chinese Sci Bull, 2008, 53: 1310–1314
10 Wang S, Chen W, Yin Z Q, et al. Field test of the wavelength-saving quantum key distribution network. Opt Lett, 2010, 35: 2454–2456
11 Xu F X, Chen W, Wang S, et al. Field experiment on a robust hierarchical metropolitan quantum cryptography network. Chinese Sci Bull, 2009, 54: 2991–2997
12 Liang C, Fu D J, Liang B, et al. Quantum key distribution over 1.1 km in an 850 nm experimental all-fiber system. Acta Phys Sin, 2001, 50: 1429–1433
13 Noe A O, Jonathan M H. Convenient method for calibrating nonlinear phase modulators for use in phase-shifting interferometry. Opt Eng, 1998, 37: 2501–2505
14 Katherine C. Phase measurement interferometry: Beware these errors. Proc SPIE, 1991, 1553: 213–219
15 Norbert L. Estimates for practical quantum cryptography. Phys Rev A, 1999, 59: 3301–3319
16 Zhang S L, Zou X B, Li C F, et al. A universal coherent source for quantum key distribution. Chinese Sci Bull, 2009, 54: 1863–1871
17 Zhang T. High speed electronics of quantum key distribution system. Ph.D. Thesis. Hefei: University of Science and Technology of China, 2010
18 Gilles B, Salvail L. Secret-key reconciliation by public discussion. Lecture Notes Comput Sci, 1994, 765: 410–423
19 Buttler W T, Lamoreaux S K, Torgerson J R, et al. Fast, efficient error reconciliation for quantum cryptography. Phys Rev A, 2003, 67: 052302
20 Lu Z X, Yu L, Li K, et al. Reverse reconciliation for continuous variable quantum key distribution. Sci China: Phys Mech Astron, 2010, 53: 100–105