CHIN. PHYS. LETT. Vol. 27, No. 9 (2010) 090301

A New Quantum Key Distribution Scheme Based on Frequency and Time Coding *

ZHU Chang-Hua(朱畅华)**, PEI Chang-Xing(裴昌幸), QUAN Dong-Xiao(权东晓), GAO Jing-Liang(高晶亮), CHEN Nan(陈南), YI Yun-Hui(易运晖)

State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071

(Received 15 March 2010)

A new scheme of quantum key distribution (QKD) using frequency and time coding is proposed, in which the security is based on the frequency-time uncertainty relation. In this scheme, the binary information sequence is encoded randomly on either the central frequency or the time delay of the optical pulse at the sender. The central frequency of the single photon pulse is set as ω_1 for bit 0 and set as ω_2 for bit 1 when frequency coding is selected. However, the single photon pulse is not delayed for bit 0 and is delayed in τ for 1 when time coding is selected. At the receiver, either the frequency or the time delay of the pulse is measured randomly, and the final key is obtained after basis comparison, data reconciliation and privacy amplification. With the proposed method, the effect of the noise in the fiber channel and environment on the QKD system can be reduced effectively.

PACS: 03.67.Dd, 42.50.Dv DOI: 10.1088/0256-307X/27/9/090301

In 1984, a quantum key distribution (QKD) protocol based on Heisenberg uncertainty principle and the no-cloning theorem was proposed by Bennett and Brassard.[1] This protocol, known as BB84, can provide unconditional security. Since then, the theory and experiments of QKD have obtained rapid development.[2] Various QKD schemes based on polarization coding,[1,3–5] phase coding,[6–10] frequency coding,[11–13] time coding,[14–16] and entanglement[2,17,18] were proposed. In these schemes, the one based on polarization coding is influenced by polarization mode dispersion and polarization dependent loss, and the polarization state should be recovered at the receiver for the QKD system in an optical fiber. In the one based on phase coding the quantum bit error rate (QBER) is related to the interference visibility which is influenced by the noise in the fiber and environment, and the methods to keep the stability of the interferometer should be adopted. Thus, the bidirectional auto-compensation structure[8] and differential phase coding schemes[19–21] were introduced. The one based on frequency coding needs a modulator, e.g. a phase modulator or an acousto-optic modulator, accordingly it is limited by the performance of these devices. In the one based on time coding the coherence of light pulse needs to be tested in order to determine the security of QKD.

In this Letter, a QKD scheme using frequency coding and time coding is proposed to reduce the influence of the channel noise. A similar QKD method based on the energy-time uncertainty relation was also presented.[22] Compared to the present scheme, the precious one can be applied to a continuous variable system, needs a single photon detector with time resolution for time measurement, and also needs many detectors for frequency measurement. Thus it is high in cost.

The principle of the proposed protocol is shown in Fig. 1. At the sender (Alice), there are three lasers, attenuators (Att), coupler, time delay module (TDM), control and driver module (CDM), and a personal computer (PC). Lasers 1 and 2 produce wide pulses (in time domain) with central frequencies ω_1 and ω_2, respectively. Laser 3 produces narrow pulses (in time domain) with central frequency ω_3. Let the frequency spectrum envelope of the lasers 1, 2 and 3 be Gaussian, with the bandwidth as $\sigma_{\omega 1}$, $\sigma_{\omega 2}$ and $\sigma_{\omega 3}$, respectively. Here the frequency spectrum of the narrow pulse produced by laser 3 covers the frequency spectrum of the pulses produced by laser 1 and laser 2. The wide pulse produced by lasers 1 and 2 covers the time duration of the light pulse produced by laser 3 and the delayed one (with time τ). Thus, the light pulses in the two coding basis are overlayed in time domain and frequency domain. Of course, the pulse width of the lasers is less than the coherence length. The time delay of a pulse is induced by TDM. At the receiver (Bob), there are optical switch (OS), circulator (Cir), fiber Bragg grating (FBG) filter, single photon detector (SPD), data collection module (DCM), and personal computer (PC). The frequency components with central frequency ω_2 and bandwidth $\sigma_{\omega 2}$ can be reflected by the FBG, while other frequency components of light pulses can propagate through the FBG. We name the proposed protocol as the FT protocol in brief.

*Supported by the National Natural Science Foundation of China under Grant Nos 60572147 and 60672119, the 111 Project (B08038), and the State Key Lab of Integrated Services Networks (ISN 02080002, ISN 090307).

**Email: chhzhu@xidian.edu.cn

© 2010 Chinese Physical Society and IOP Publishing Ltd

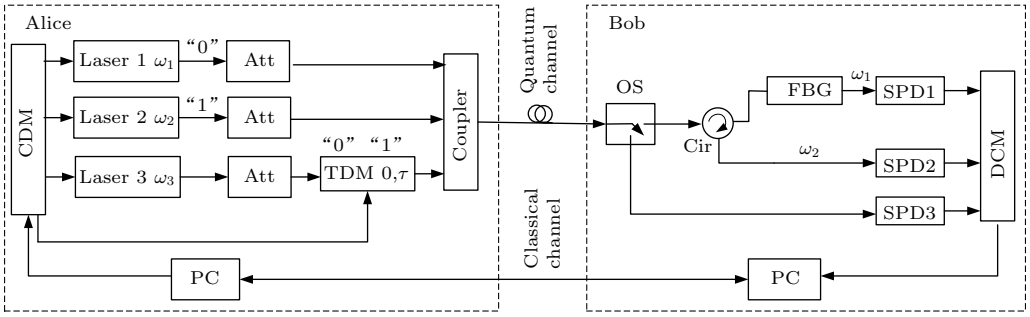


Fig. 1. The principle of QKD based on frequency and time coding.

The working process of the FT protocol is as follows:

(1) Alice generates two random binary bit sequences: information bit sequence $\{a_n, n = 1, 2, 3, \cdots\}$ and coding bit sequence $\{b_n, n = 1, 2, 3, \cdots\}$. (i) If $b_n = 0$, then frequency coding is selected. Laser 1 is fired when $a_n = 0$, the other two lasers are disabled; laser 2 is fired when $a_n = 1$, the other two lasers are disabled. The mean photon number per light pulse is 0.1 after being attenuated. (ii) If $b_n = 1$, then time coding is selected. Laser 3 is fired, the others are disabled. The delay value is 0 when $a_n = 0$; the delay value is τ when $a_n = 1$.

(2) The coded light pulse propagates to Bob through optical fiber channel. Bob performs frequency or delay measurement randomly by controlling the optical switch, as shown in Fig. 1. (i) If frequency measurement is selected, then the photon with central frequency ω_2 and bandwidth $\sigma_{\omega 2}$ is reflected by FBG and is detected by SPD2 with the help of the circular, and the photon with central frequency ω_1 is detected by SPD1. If SPD1 clicks, then the received bit $g_n = 0$; if SPD2 clicks, then the received bit $g_n = 1$. (ii) If time measurement is selected, the photon is detected by SPD3. The received bit $g_n = 0$ when delay is 0, the received bit $g_n = 1$ when delay is τ. (iii) Let $g_n = -1$ whether all the three detectors do not click or photon count occurs under the two basis at the same time, that is, SPD1 or SPD2 clicks and SPD3 also clicks.

(3) Bob tells Alice the measurement types (frequency or time delay) by public classical channel.

(4) Alice tells Bob the measurement types which are consistent with the coding types and keeps the element of $\{a_n, n = 1, 2, 3, \cdots\}$ with the same types as the sifted key sequence $\{s_m, m = 1, 2, 3, \cdots\}$.

(5) Bob keeps the element of the received sequence $\{g_n, n = 1, 2, 3, \cdots\}$ with the same types of measurement and coding as the sifted key $\{r_m, m = 1, 2, 3, \cdots\}$.

(6) Alice compares part bits of $\{s_m, m = 1, 2, 3, \cdots\}$ and part bits of $\{r_m, m = 1, 2, 3, \cdots\}$ with Bob by classical channel. Then she calculates QBER. If QBER $>$ $\mathrm{QBER_{th}}$, then eavesdropper (Eve) exists, QKD becomes false and Alice returns to (1). Otherwise, Alice performs (7).

(7) Alice and Bob obtain the final key after data reconcilliation and privacy amplification by classical channel.

The security of the FT protocol can be analyzed elementarily as follows: (1) since the weak coherent light pusles coded in frequency and time delay overlay each other in frequency domain and time domain, the states in the two bases are non-orthogonal and can not be discriminated correctly. In fact, Eve can not measure the frequency and time delay of the light pulse accurately and simutaneuosly because of frequency-time uncertainty relation, $\sigma_\omega \sigma_t \geq 1$, where σ_ω and σ_t is the width of frequency spectrum and time.[23] (2) For intercept-resend attack, Eve can obtain the information bit correctly with a probability of 50% when the measurement type of Eve is different from the coding type, e.g. when Alice performs frequency coding, Eve measures the time delay and he can obtain 0 or 1 with the same probability for the light pulse with central frequencies ω_1 or ω_2 and time interval covering $0 \sim \tau$; when Alice performs time coding, Eve measures the frequency and he can obtain the correct result with a probability of 50% for the light pulse with frequency bandwidth covering ω_1 and ω_2. Thus, Bob can detect Eve's attack easily by QBER estimation. (3) Trojan attack can not be implemented for the light pulse of QKD propagates along the fiber in one-way.

The feasibility of the FT protocol is mainly determined by the devices that meet with the parameters requirement of the system. Let the pulse width of the lasers 1, 2 and 3 in time domain is σ_{t1}, σ_{t2} and σ_{t3}, respectively. We set ω_1 and ω_2 as the telecommunication band (1550nm), $\omega_3 = (\omega_1 + \omega_2)/2$. The parameters have the following relations: $\sigma_{\omega 3} \geq \sigma_{\omega 1} + \sigma_{\omega 2}$, $\sigma_{t1} \geq 2\sigma_{t3}$, $\sigma_{t1} = \sigma_{t2}$, $\sigma_{\omega 1} = \sigma_{\omega 2}$. The delay τ should be $\sigma_{t1} - \sigma_{t3} \geq \tau \geq \sigma_{t3}$ for correct discrimination of the pulse and the delayed one. In this system, τ should be larger than trigging interval of single photon detector. Recently, single photon detector based on superconductor has the trigging frequency over GHz and is low in dark count.[24] The lasers that meet with these requirements can be obtained in the market.

Now, we analyze the quantum bit error rate

(QBER) and final key rate of the FT protocol. Let μ denote the mean photon number of each weak coherent pulse. The photon number n in each pulse is poisson distributed, $p_n = \frac{\mu^n}{n!}e^{-\mu}$. Let α (dB/km) denote the fiber loss, l (km) denote the fiber length. Then the transmission rate of the fiber $t_f = 10^{-\alpha l/10}$. If the transmission rate of the quantum channel at the receiver is t_B, the efficiency of the detector is η_D, then the whole transmission rate of the system $t = t_f t_B \eta_D$. Assume that the transmission of the photons in each pulse is independent. Thus, the count rate at the receiver for the pulse with n photons is $t_{n,nd} = 1-(1-t)^n$ when dark count is not taken into account, and the count rate is $t_n = t_{n,nd} + mp_d(1-t_{n,nd})$ when dark count is taken into account, where p_d is the dark count probability, m is the number of the detectors in each basis. From the statistical point of view, when dark count is not taken into account the mean count rate R_{nd} of weak coherent pulse at the receiver is $R_{nd} = \sum_{n=0}^{\infty} p_n t_{n,nd} = 1 - e^{-\mu t}$. When dark count is taken into account the mean count rate R of weak coherent pulse is $R = \sum_{n=0}^{\infty} p_n t_n = 1 - e^{-\mu t} + mp_d e^{-\mu t}$. Thus, the sifted key rate $R_{\rm sift}$ can be given as

$$R_{\rm sift} = R \cdot p_s = (1 - e^{-\mu t} + mp_d e^{-\mu t}) p_s, \qquad (1)$$

where p_s denotes the percentage of qubit used to the sift key.

Here QBER means the error ratio of the information bit obtained by the receiver after basis comparison, denoted as Q. Qubit error comes from two ways, one is the incorrect clicks of the detectors because of channel noise, the other is the dark count of detectors. Based on these QBER can be given as

$$Q = \frac{\left[R_{nd} p_{\rm opt} + \frac{m}{2}(1 - R_{nd}) p_d\right] p_s}{R_{\rm sift}}, \qquad (2)$$

where $p_{\rm opt}$ denotes the probability with which photons arrive at incorrect detectors, $\frac{1}{2}$ is the error probability from dark count, $p_{s_{\rm FT}} = \frac{1}{2}$, $m = 2$. Thus the sifted key rate $R_{\rm sift_FT}$ is $R_{\rm sift_FT} = [1 - e^{-\mu t} + 2p_d e^{-\mu t}] p_{s_{\rm FT}}$. For the FT protocol, let $\sigma_{t1}(\sigma_{t2})$ be 1–1.2 ns, σ_{t3} be 500–600 ps, the associated bandwidth $\sigma_{\omega 1}(\sigma_{\omega 2}) = 1.047$–$1.257 \times 10^{10}$ rad/s, $\sigma_{\omega 3} = 2.094$–$2.513 \times 10^{10}$ rad/s, and the detection gate duration be twice the width of the pulse sent. Thus, the effect of time spread and frequency spread from dispersion on detection results can be omitted, that is, $p_{\rm opt} \approx 0$ when the basis is the same, QBER $Q_{\rm FT}$ of the QKD system can be given as

$$Q_{\rm FT} = \frac{(1 - R_{nd}) p_d p_{s_FT}}{R_{\rm sift_FT}}. \qquad (3)$$

For the BB84 QKD system, in which polarization coding or phase coding based on M-Z interferometer is applied, $p_{s_{\rm BB84}} = \frac{1}{2}$. The sifted key rate of the BB84 QKD system $R_{\rm sift_BB84} = [1 - e^{-\mu t} + 2p_d e^{-\mu t}] p_{s_{\rm BB84}}$, the QBER can be given as[14]

$$Q_{\rm BB84} = \left[R_{nd}\frac{1-V}{2} + (1 - R_{nd}) p_d\right] \frac{p_{s_{\rm BB84}}}{R_{\rm sift_BB84}}. \qquad (4)$$

In Eq. (4), V denotes the visibility, $0 \le V \le 1$. For phase coding, V denotes the visibility of the interferometer. For polarization coding, V denotes the degree to which polarization rotation because of polarization mode dispersion affects the measurement results.

In the proposed protocol, the weak coherent light pusles coded in frequency and time delay are in two non-orthogonal states, the error and information obtained by Eve is removed after data reconciliation and privacy amplification, being the same as the BB84 protocol, and the final secure key rate can be given as[2]

$$R_{\rm net} = R_{\rm sift}\left(I_{\rm AB} - I_{\rm AE}\right), \qquad (5)$$

where $I_{\rm AB}$ denotes the mutual information between Alice and Bob, and $I_{\rm AB} = 1 - H_2(Q)$. $H_2(Q)$ is the binary entropy, $H_2(Q) = -Q\log_2(Q) - (1-Q)\log_2(1-Q)$. $I_{\rm AE}$ denotes the mutual information between Alice and Eve. We assume that Eve perform photon number splitting (PNS) attacks first and no error occurs, that is, the photons are split to Eve with a proportion $1 - t_f$ and the residual photons are transmitted to Bob with a proportion t_f through a channel without loss. Hence, the mean photon number of the light pulse obtained by Eve is $\mu(1 - t_f)$ and Eve can obtain the information with the probability $\mu(1 - t_f)$ from each pulse sent by Alice. Then, Eve performs intercept-resend attack against the pulses in which the detectors of Eve do not click in PNS attack.

Since the visibility is the ratio of the subtraction of the number of photon count by the incorrect detector from the number of photon count by correct detector over the total number of photon count, the incurred bit error rate to Bob can be given as $\frac{1-V}{2}$ under the assumption of the photon counting of the incorrect detector derives from intercept-resend attack. For BB84 and FT protocol, if the probability with which Eve performs intercept-resend attack is $p_{\rm IR}$, the error rate is $0.25p_{\rm IR}$ and the information Eve obtains is $0.5p_{\rm IR}$,[25] so the information Eve obtains can be given as $1 - V$. The mutual information between Alice and Eve $I_{\rm AE_FT} = \mu(1 - t_f) + (1 - V)$, the final key rate can be given as follows:

$$R_{\rm net_FT} = R_{\rm sift_FT}\left[1 - H_2(Q_{\rm FT}) - I_{\rm AE_FT}\right]. \qquad (6)$$

Accordingly, for the BB84 protocol with polarization coding or phase coding, the mutual information between Alice and Eve is $I_{\rm AE_BB84} = \mu(1 - t_f) + (1 -$

V).[14] Then the final key rate is

$$R_{\text{net_BB84}} = R_{\text{sift_BB84}} \left[1 - H_2(Q_{\text{BB84}}) - I_{\text{AE_BB84}}\right]. \quad (7)$$

Let $t_B = 1$, $\eta_D = 0.1$, $\alpha = 0.25$, $p_d = 10^{-5}$, $V = 1$, 0.9, 0.8, 0.7 respectively. The relations of the final key rates to the distance are shown in Fig. 2. As shown in Fig. 2, when $V = 0.7$, the communication distance of FT protocol is increased by 65 km. When $V = 0.8$, the distance is increased by 12 km. When $V < 0.7$, the scheme with polarization coding and phase coding can not work, while the scheme with the FT protocol can work correctly. Thus the scheme with frequency and time coding can work in worse visibility compared with the BB84 protocol using polarization coding or phase coding.

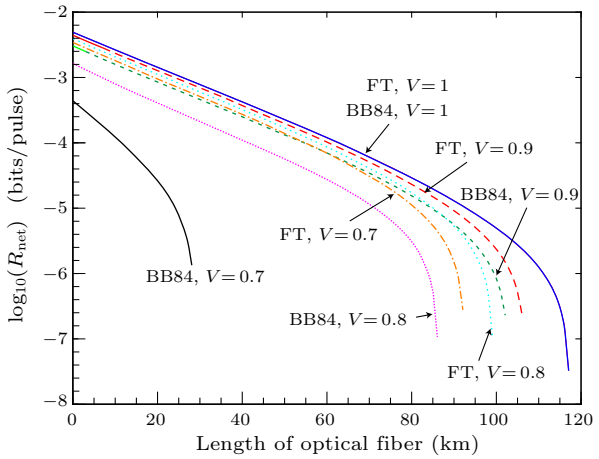


Fig. 2. The relation of final key rate and length of fiber.

In conclusion, based on time-frequency uncertainty principle a new QKD scheme using frequency and time coding has been proposed. Compared with polarization coding and phase coding, the effect of birefringence and interference instability on the performance of the QKD system is reduced. The analysis results of final key rates show that the FT protocol can work at worse visibility. A rigorous proof of the security of the FT protocol remains a work in progress. Furthermore, the theory of decoy states can be applied to increase the distance further and overcome the shortcomings by weak coherent pulse.[26,27]

References

[1] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (Bangalore, India) p 175

[2] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phy.* **74** 145

[3] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 *J. Cryptol.* **5** 3

[4] Chen J, Li Y, Wu G and Zeng H P 2007 *Acta Phys. Sin.* **56** 5243 (in Chinese)

[5] Liu W T, Wu W, Liang L M, Li C Z and Yuan J M 2006 *Chin. Phys. Lett.* **23** 287

[6] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[7] Zbinden H, Gautier J D, Gisin N, Huttner B, Muller A and Tittel W 1997 *Electron. Lett.* **33** 586

[8] Muller A, Herzog T, Huttner B, Tittel W, Zbinden H and Gisin N 1997 *Appl. Phys. Lett.* **70** 793

[9] Liang C, Fu D H, Liang B, Liao J, Wu L A, Yao D C and Lv S W 2001 *Acta Phys. Sin.* **50** 1429 (in Chinese)

[10] Miao E L, Mo X F, Gui Y Z, Han Z F and Guo G C 2004 *Acta Phys. Sin.* **53** 2123 (in Chinese)

[11] Mèrolla, J M, Mazurenko Y, Goedgebuer J P and Rhodes W T 1999 *Phys. Rev. Lett.* **82** 1656

[12] Bloch M, McLaughlin S W, Merolla J M and Patois F 2007 *Opt. Lett.* **32** 301

[13] Zhang T, Yin Z Q, Han Z F and Guo G C 2008 *Opt. Commun.* **281** 4800

[14] Stucki D, Brunner N, Gisin N, Scarani V and Zbinden H 2005 *Appl. Phys. Lett.* **87** 194108

[15] Debuisschert T and Boucher W 2004 *Phys. Rev.* A **70** 042306

[16] Stucki D, Barreiro C, Fasel S, Gautier J D, Gay O, Gisin N, Thew R, Thoma Y, Trinkler P, Vannel F and Zbinden H 2009 *Opt. Expr.* **17** 13326

[17] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[18] Huang X, Li S M and Wang A M 2007 *Chin. Phys. Lett.* **24** 2479

[19] Inoue K, Waks E and Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 037902

[20] Li M M, Wang F Q, Lu Y Q, Zhao F, Chen X, Liang R S and Liu S H 2006 *Acta Phys. Sin.* **55** 4642 (in Chinese)

[21] Wang W Y, Wang C, Wen K and Long G L 2007 *Chin. Phys. Lett.* **24** 1463

[22] Qi B 2006 *Opt. Lett.* **31** 2795

[23] Donnelly T D and Grossman C H 1998 *Am. J. Phys.* **66** 677

[24] Goltsman G, Korneev A and Divochiy A 2009 *J. Mod. Opt.* **56** 1670

[25] Ma R L 2006 *Quantum Cryptography Communications* (Beijing: Science Press) (in Chinese)

[26] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901

[27] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503