Dual-Threshold Balanced Homodyne Detection at 1550 nm Optical Fiber Quantum Key Distribution System

Q. Xu, M. Sabban, M. B. Costa e Silva, P. Gallion, *Senior Member, IEEE*, and F. J. Mendieta, *Member, IEEE*

***Abstract*—We present a flexible quantum key distribution (QKD) system implementation using quadrature phase-shift keying (QPSK) encoding. Two detection techniques are implemented and compared: a photon counting detection scheme using single photon avalanche diodes (SPAD) and a dual-threshold balanced homodyne detection (BHD) using standard PIN diodes in which the weak signal is time-multiplexed with a strong reference. The interferometer instability and the system phase fluctuations are compensated by an optoelectronic feedback loop that allows an automatic continuous operation. We compare the QKD system performance for both schemes in terms of BER and key generation efficiency. Finally, we analyze the BHD QKD system security under the potential individual intercept-resend attack and the intermediate-base attack.**

***Index Terms*—BB84 protocol, homodyne detection, quadrature phase-shift keying (QPSK), quantum cryptography.**

I. Introduction

QUANTUM CRYPTOGRAPHY (QC), a protocol proposed by Brassard and Bennett in 1984 (BB84) [1], guarantees the unconditional security of the communications based on quantum mechanical laws [2]. QC is now moving from the promise of physics to the hard reality of the electrical engineering world and is obviously handling with the full quantum nature of light. Limited by the low quantum efficiency of single photon avalanche diodes (SPAD) at 1550 nm, the present efforts in quantum key distribution (QKD) systems in optical fibers at telecommunications wavelengths are directed towards the increase in the key generation rates and the transmission distances, as well as their compatibility with the current optical infrastructure and with the end user opportunities in terms of speed, reliability and cost.

Homodyne detection has already been investigated to provide accurate quadrature measurements in QKD using continuous variables [3]. As polarization is strongly affected by fiber propagation, homodyne detection allows a diversity of modulation formats on the sender Alice's optical field, including more favorable multiple phase-shift keying (MPSK). In the BB84 protocol, Alice encodes her Q-bits in two orthogonal bases with two antipodal symbols in each base, leading to a QPSK modulation format.

Interferometric arrangements are usually used for the implementation of phase detection, in which the key issue is to obtain a phase reference at the receiver end. However using a separate fiber for reference transmission leads to difficult stabilization on an interferometer over the complete span of the transmission link. Gisin's group [4] first proposed a "plug & play" phase encoding approach based on two Mach--Zehnder interferometers containing similar short-long arms. They have also performed the first experiment of the "plug & play" system [5] by combining the ideas of time multiplexing with Faraday mirrors that passively compensate all optical and mechanical fluctuations. However such a round-trip system has to face a doubled transmission distance, requiring precise backscattered light control, and is especially menaced by the Trojan horse attacks [6]. Therefore, a one-way and single path configuration is mandatory to avoid round trip penalty. For that reason, Merolla has proposed [7] a phase referencing QKD system in the frequency domain that utilizes phase modulation of sidebands. A differential phase-shift keying (DPSK) is also an effective way to provide phase reference by relaxing the phase stabilization over time duration of the same order of the bit period. DPSK demodulation by delay line has been extensively discussed during the early age of optical communications [8]–[10] and more recently [11], [12].

In the optical telecom band, photon counters (PC) using avalanche diodes that work in Geiger mode under low and precise temperature control, exhibit inherent low quantum efficiency, high dark count rate, and inevitable residual after-pulse phenomenon due to the macroscopic avalanche process. On the other hand, in the race for speed and distance, balanced homodyne detection (BHD) scheme using PIN photodiodes, facilitated by a strong local oscillator (LO), may constitute an interesting alternative as compared to photon counting. In BHD only one quadrature is measured and there is no additional noise to the zero-point fluctuation of the signal field. As reported by Yuen [13] the input signal quantum noise is, in this case, the only noise limitation and the LO noise has a negligible influence, therefore the output noise is only dominated by vacuum fluctuation entering in the signal port. Consequently, using a LO of suitable power provides high mixing gain to

Manuscript received March 14, 2008; revised November 07, 2008. First published April 17, 2009; current version published July 20, 2009. This work was supported in part by a grant of ANR RNRT HQNET project from French government.

Q. Xu, M. Sabban, M. B. Costa e Silva, and P. Gallion are with Ecole Nationale Supérieure des Télécommunications, TELECOM ParisTech, CNRS, LTCI UMR 5141, Paris 75013, France (e-mail: qxu@enst.fr; sabban@enst.fr; mcosta@enst.fr; gallion@enst.fr).

F. J. Mendieta is with Ecole Nationale Supérieure des Télécommunications, TELECOM ParisTech, CNRS, LTCI UMR 5141, Paris 75013, France, on leave from CICESE, Tijuana, Ensenada, Baja California 22800, México (e-mail: mendieta@enst.fr).

Digital Object Identifier 10.1109/JLT.2008.2009949

overcome the thermal noise [14]. In addition, the conventional PIN photodiodes operating at room temperature present much higher quantum efficiency and faster response speed as compared to the PC [15], also their cost is much lower and the supply requirements are much simpler.

Since homodyne detection provides a measurement of the single signal non corresponding to the LO [16], the receiver must perform the extraction of optical carrier in order to generate the LO reference field [17]–[19]. Furthermore, when the phase demodulation is performed with interferometric optical delay lines, the receiver must be designed to compensate for the phase drift in the interferometers and the other link elements [21], [22].

Postdetection, filtering, threshold and symbol synchronization stages must also be properly designed as in BHD the decision process is carried out *a posteriori* [23], [24], in opposite to photon counting that inherently performs built-in decision [25], [26], making a difficult compromise between detection efficiency and false symbol detection. As well BHD leads to a classical bit error rate (BER) whereas a quantum bit error rate (QBER) is considered in photon counting.

In Section II, we first recall the basics of the homodyne detection system, then we introduce the two receiver structures that we have used for the QKD application. Next in Section III, we present the experimental setup of a one-way BB84 QKD system using weak coherent pulses (WCP) QPSK format encoding at the sender Alice's end and BPSK base switching at the receiver Bob's end. Photon counting and dual-threshold BHD are both performed with optical phase synchronization. The configuration of our one-way system is close to Gisin's two-way phase encoding and time-multiplexing approach using PC measurements, but we use a polarization splitting scheme so that the signal and LO pulses arrive precisely at the same time window of observation without coupler loss, and we compensate the polarization fluctuations passively and the phase fluctuations actively with an optoelectronic feedback loop. Additionally, in BHD we time-multiplex the strong LO pulses and the weak signal pulses to combat the thermal noise at the receiver's end, allowing the use of fast and high sensitivity PIN photodiode instead of PC.

Then in Section IV, we compare the performance of the two receivers in terms of detection efficiency and BER (or QBER). Provided that the guarantee of security lies either on the mutual information gain or the perception of eavesdroppers' intervention, finally in Section V we analyze the security issues of the BHD QKD system under the "intercept-resend" attack and the "intermediate base" attack, as well as the power modifying mixed attacks.

II. Homodyne Detection for Quantum Cryptography

Coherent optical transmission at the telecommunications wavelength has been studied for more than three decades [8], [11]–[13], [15], due to its unique features concerning the mixing gain and the possibility to use complex amplitude modulations that allow lower optical signal-to-noise rate (OSNR) for a given postdetection BER, as well as a better spectral efficiency. The standard quantum limited (SQL) reception is attainable when a strong LO field is used. Furthermore, the use of constant envelope formats, in opposition to the traditional intensity modulation with direct detection (IM/DD), is more tolerant to the fiber nonlinear impairments [27].

A. BPSK Encoding of Coherent States

Glauber's coherent state model is expressed as a sum of Fock's number states $|n\rangle$. As we will work with strongly attenuated laser pulse we use the form [17]

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{(n!)^{1/2}} |n\rangle \tag{1}$$

Two coherent quantum state vectors $|\alpha_1\rangle$ and $|\alpha_2\rangle$ are nonorthogonal, since the squared overlap is

$$|\langle\alpha_1|\alpha_2\rangle|^2 = e^{-|\alpha_1-\alpha_2|^2} \tag{2}$$

Because of the noncommutativity of the nonorthogonal state projective measurement, a simple Von Neumann projective measurement cannot conclusively distinguish the different states.

For the sake of concision, we will only consider here the case of binary phase-shift keying (BPSK) in which two equally probable modulated binary symbols (0, 1) are represented by two antipodal phase states $(0, \pi)$. This corresponds to a simple constant envelope modulation, in which the antipodal signals maximize the signal distance, and therefore minimize the square overlap. As well the average received power is the same when the symbol 1 or 0 is transmitted.

In BPSK encoding, the two signal coherent states are devoted as $|\alpha_1\rangle = |\alpha\rangle$ and $|\alpha_2\rangle = -|\alpha\rangle$; the average signal photon number is $N_S = |\alpha|^2$, and the signal overlap is $\langle\alpha_1|\alpha_2\rangle = e^{-2N_S}$. The SQL is attainable when an in-phase LO field with phase coherence is used, and the detection of the mixed field assuming unit quantum efficiency PIN detectors in the absence of the thermal noise gives the BER as [18], [28]

$$\mathrm{BER} = \frac{1}{2}\mathrm{erfc}(\sqrt{2N_S}). \tag{3}$$

In BB84 protocol, from two orthogonal bases chosen randomly by Alice, four quantum eigenstates can be generated separately (the symbols 0 and 1 on two different bases $\{|\alpha\rangle, -|\alpha\rangle\}$ and $|\{|i\alpha\rangle, -|i\alpha\rangle\}$), constituting a QPSK type constellation. After the random base switching at the receiver Bob's end, the states of base coincidence turn to a BPSK constellation whereas the states of base anticoincidence are discarded and do not contribute to the shared information and therefore not to the BER.

B. Coherent Homodyne Receiver

In telecom applications, the coherent detection process consists of mixing the signal field E_S and a strong LO field E_{OL} in a 2×2 coupler at the receiver end.

PC, exploiting the photon-triggered avalanche current of a reverse biased p-n junction to detect an incident radiation, is specifically designed to operate with a reverse bias voltage well

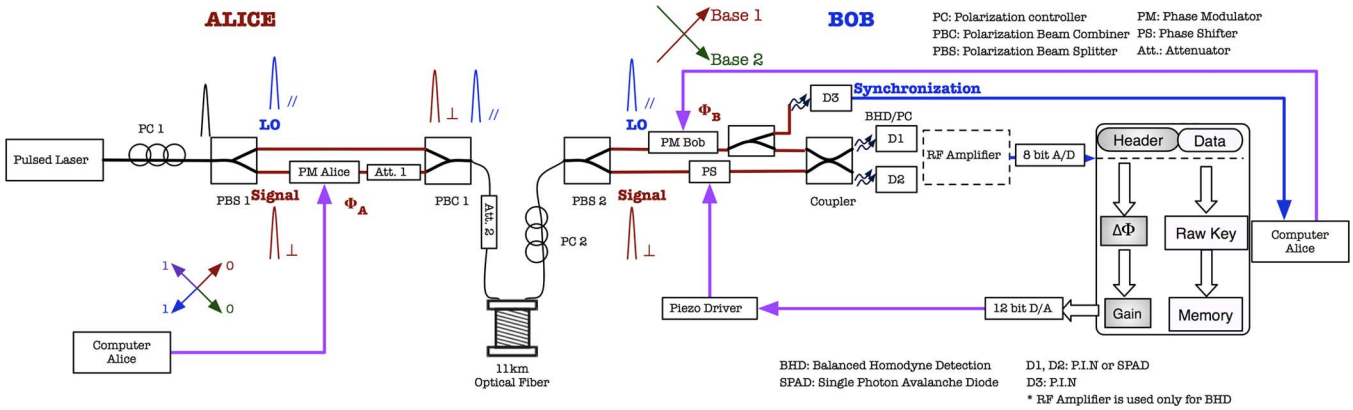

Fig. 1. Experimental setup of QKD system using photon counting/BHD.

above the breakdown voltage [25], [26]. This kind of operation is also called Geiger mode and an indispensable quenching process limits its operation frequency to 4–8 MHz, also its quantum efficiency is limited to approximately 0.1 at 1550 nm telecom band. PC cannot accommodate strong LO field in an interferometer arrangement. As shown in Fig. 1 when $|E_{\rm LO}| = |E_S|$, the photon arrives at the output D_1 when the phase difference $\theta = 0$ or arrives on the output D_2 when $\theta = \pi$.

The BER is limited by the interferometer contrast and the after-pulse effects induced by the precedent avalanche.

By mixing a weak signal field with a strong LO field before intensity detection, i.e., $|E_{\rm LO}| \gg |E_S|$, the BHD technique is potentially capable of overcoming nondesirable effects of PC. Nevertheless, the different coherent states generated by conventional light sources are not orthogonal, leading to an inherently finite error rate and making a decision process mandatory. Optimal and practical implementations have been widely discussed [18]–[20].

III. Experimental Arrangement

We have implemented an experimental one-way and one-path QKD system with QPSK modulation. Both photon counting scheme and BHD scheme are implemented. A flexible arrangement has been designed so that only slight changes have to be done to switch the detection scheme from photon counting to BHD.

As shown in Fig. 1, we use a 1550 nm ILM (integrated laser/modulator, AVANEX) electro-absorption modulated light source to generate laser pulses of 5 ns width with 25 dB intensity extinction ratio. In the photon counting detection scheme, the operational frequency is limited to 4 MHz. As for the BHD scheme, much higher repetition rates are attainable, however in this paper we chose to use 4 MHz as well for the comparison. Our balanced amplified photodetector has a flat response passband from DC to 150 MHz (Thorlabs InGaAs switchable gain PDB150C-EC).

A polarization splitting method is used in our arrangement to improve the isolation of the signal and the strong reference field, since the 25 dB intensity extinction ratio alone is not enough for the time-multiplexing of the weak signal and the strong LO field. Alice's laser pulses are separated by a polarization-beam-splitter (PBS) with a polarization extinction ratio of 30 dB, the horizontally polarized component passes through the upper arm and the vertically polarized component passes through the lower arm of a Mach--Zehnder interferometer constructed with polarization maintaining (PM) fibers. A polarization controller is used to adjust the signal-LO relative power levels.

Alice encodes her vertically polarized pulses ($\Phi_{\rm A} : \pi/4$ and $-3\pi/4$ in base $\rm A_1$; $-\pi/4$ and $3\pi/4$ in base $\rm A_2$) on a Lithium Niobate phase modulator (Photline MPX) [23], [24], constituting a QPSK modulation. The weak signal and the un-modulated LO pulses are time-multiplexed by a polarization-beam-combiner (PBC), and the delay between the two components is set to be 20 ns, i.e., 4 m optical fiber. Orthogonally polarized, the signal pulses and the LO pulses propagate with a high degree of isolation. Attenuator 1 is used to generate the weak coherent states (WCS) signal pulses and attenuator 2 is used only in the photon-counting scheme to change the signal and LO pulses level together while performing measurements over a wide range of signal level without readjusting the receiver's configuration.

Then the combined signal-LO pulses pass through a QKD link of 11 km length in a standard telecom single mode fiber (SMF). Bob uses another PBS to separate the horizontally polarized LO pulses and the vertically polarized signal pulses. A small portion of the LO component is picked up for the receiver synchronization, using a PIN diode D3.

Bob's receiver has a similar Mach--Zehnder interferometer structure. He performs the LO phase shift in the upper arm on a Lithium Niobate phase modulator to apply his base choice ($\Phi_{\rm B} : \pi/4$ in Base $\rm B_1$, $-\pi/4$ in Base $\rm B_2$), constituting a BPSK conversion in which $\Phi = \Phi_{\rm A} - \Phi_{\rm B}$. The delay between the signal and the LO pulses is carefully adjusted to 20 ns to optimize the time overlap on the PM coupler's input ports with the same state of polarization (SOP).

The differential delay interval between signal and reference pulses caused by the long and short arms of Alice's and Bob's interferometers should be kept stable so as to allow a continuous QKD operation. Nevertheless the interferometers should be operative in different location; moreover they are subject to different temperature, pressure and mechanical stress conditions. As in all coherent systems, the phase control is a key issue due to the drift in the optical paths in the Mach--Zenhder interferometers. To keep the system unconditionally secured, the QBER

threshold must remain under 11% with a reduced key generation rate, and the corresponding phase error is $\Delta\Phi \approx 27^\circ$ [21], [22].

In our experimental setup, the phase drift $\Delta\Phi$ is compensated by an optoelectronic feedback using a phase shifter (PS) in Bob's lower arm. A periodical interval of M bits is used as "training frame header" so as to compute the phase drift in the system in order to feedback on the PS. The training frames contain predetermined sequences of which Alice and Bob agree on the symbols and bases. The piezodriver fiber actuator allows a dynamic range $[-8\pi, 8\pi]$ and a response time of few milliseconds.

The mean value of M bits in the "training frame header" is close to the normal distribution $\mathrm{N}(\mu, \sigma/\sqrt{M})$, in which μ is the expected value and σ is the standard deviation of an individual sample. When an uncertainty in amplitude estimation less than error E is expected, the following condition must be met

$$\mathrm{erfc}(\sqrt{2M}/2\sigma) \approx 2\exp(-M/2\sigma^2) < E. \tag{4}$$

A. Photon Counting Experiment

In the photon counting detection scheme, we use two single photon detection modules (SPDM, id 200, id Quantique) as D1 and D2 in Fig. 1. The output of the SPDM is a pulse of 100 ns width when a detection event occurs. We have implemented an 8-bit analog/digital converter (ADC) for the pulse detection and to record the arrival time of the detection events.

For a short gate operation of 2.5 ns, we consider that the dark count probability for SPDM1 and SPDM2 are ε_1 and ε_2, respectively; the quantum efficiencies are ρ_1 and $\rho_2 (\rho_1, \rho_2 < 0.1)$; and the interferometer visibility is V. Then, during this gating operation, the probabilities that SPDM1 or SPDM2 record a detection event are

$$\begin{cases} P_{D1}(\Phi) = \varepsilon_1 + \rho_1 \frac{1+V\cos\Phi}{2} \\ P_{D2}(\Phi) = \varepsilon_2 + \rho_2 \frac{1-V\cos\Phi}{2} \end{cases}. \tag{5}$$

During the "training frame header" interval, we use eight registers to record the incoming events, i.e., $\{\mathrm{R_{D1,0}}, \mathrm{R_{D1,\pi/2}}, \mathrm{R_{D1,\pi}}, \mathrm{R_{D1,3\pi/2}}\}$ for SPDM1 and $\{\mathrm{R_{D2,0}}, \mathrm{R_{D2,\pi/2}}, \mathrm{R_{D2,\pi}}, \mathrm{R_{D2,3\pi/2}}\}$ for SPDM2 to store the number of detection events for $\Phi = 0, \pi/2, \pi, 3\pi/2$.

For SPDM1,

$$\begin{cases} P_{D1}\left(\frac{3\pi}{2}\right) - P_{D1}\left(\frac{\pi}{2}\right) = \rho_1 V \sin\Delta\Phi \\ P_{D1}(0) - P_{D1}(\pi) = \rho_1 V \cos\Delta\Phi \end{cases}. \tag{6}$$

For SPDM2,

$$\begin{cases} P_{D2}\left(\frac{3\pi}{2}\right) - P_{D2}\left(\frac{\pi}{2}\right) = -\rho_2 V \sin\Delta\Phi \\ P_{D2}(0) - P_{D2}(\pi) = -\rho_2 V \cos\Delta\Phi \end{cases}. \tag{7}$$

From (6) and (7), we can easily obtain an approximate value of the real-time phase error $\Delta\Phi$. A 12-bit digital/analog converter (DAC) outputs the voltage to be applied on the PS that compensates the phase error. Fig. 2 shows our experimental results for a long-term measured phase error and the residual QBER when the signal mean photon number per bit N_S is 0.5. We observe that the residual phase error is controlled under 15 degrees.

B. Balanced Homodyne Detection Experiment

In the BHD scheme, the LO level is unchanged, and only the signal level is strongly attenuated with attenuator 1. We use a balanced photo-detector (Thorlabs PDB150C-EC) for the photo-detection together with a passband voltage amplifier (Femto, Series DHPVA, 200 MHz) to obtain an optimized resolution for the high-speed 8-bit ADC PCI transient recorder that works at a sample rate up to 200 Mbits/s (Spectrum M2i.2030).

Four registers $\mathrm{R}_0, \mathrm{R}_{\pi/2}, \mathrm{R}_\pi, \mathrm{R}_{3\pi/2}$ store and update the estimated values for the four possible phase states. The detected values of the M bits are $\{\mathrm{a}_1, \mathrm{a}_2, \ldots, \mathrm{a}_\mathrm{M}\}$, in which $\{\mathrm{a_{i1}}, \mathrm{a_{i2}}, \ldots, \mathrm{a_{i(M/4)}}\}, \{\mathrm{a_{j1}}, \mathrm{a_{j2}}, \ldots, \mathrm{a_{j(M/4)}}\}, \{\mathrm{a_{m1}}, \mathrm{a_{m2}}, \ldots, \mathrm{a_{m(M/4)}}\}, \{\mathrm{a_{n1}}, \mathrm{a_{n2}}, \ldots, \mathrm{a_{n(M/4)}}\}$ correspond respectively to the bits that carry phase information $0, \pi/2, \pi$ and $3\pi/2$.

The normalized quadrature amplitude of the detected signal is proportional to $\cos(\Phi) = \cos(\Phi_\mathrm{A} - \Phi_\mathrm{B})$. Base coincidence (BC) occurs when $\Phi = 0$ or π; base anticoincidence (AC) occurs when $\Phi = \pi/2$ or $3\pi/2 (-\pi/2)$.

We can approximately obtain (8), shown at the bottom of the page, where $A_0, A_{\pi/2}, A_\pi$ and $A_{3\pi/2}$ are the envelope amplitudes, and we have

$$\begin{cases} A_0 \approx A_{\pi/2} \approx A_\pi \approx A_{3\pi/2} \\ \Delta\Phi_0 \approx \Delta\Phi_{\pi/2} \approx \Delta\Phi_\pi \approx \Delta\Phi_{3\pi/2} \end{cases}. \tag{9}$$

We can thus obtain the estimated envelope amplitude and the phase error

$$\begin{cases} A \cong \left[\left(R_0^2 + R_{\pi/2}^2 + R_\pi^2 + R_{3\pi/2}^2\right)/2\right]^{1/2} \\ \Delta\Phi \cong \left(\Delta\Phi_0 + \Delta\Phi_{\pi/2} + \Delta\Phi_\pi + \Delta\Phi_{3\pi/2}\right)/4 \end{cases}. \tag{10}$$

We have performed the measurements of the signal level $N_S = 0.02$–3.0 photons/bit with strong LO level 2.8×10^5 photons/bit so that the quantum noise is at least 10 dB above the thermal noise. For each measurement we have taken 5%

$$\begin{cases} R_0 = \overline{a_{ik}} = \left(\sum_{k=1}^{M/4} a_{ik}\right)/(M/4) = A_0\cos(\Delta\Phi_0) \\ R_{\pi/2} = \overline{a_{jk}} = \left(\sum_{k=1}^{M/4} a_{jk}\right)/(M/4) = A_{\pi/2}\cos(\Delta\Phi_{\pi/2} + \pi/2) \\ R_\pi = \overline{a_{mk}} = \left(\sum_{k=1}^{M/4} a_{mk}\right)/(M/4) = A_\pi\cos(\Delta\Phi_\pi + \pi) \\ R_{3\pi/2} = \overline{a_{nk}} = \left(\sum_{k=1}^{M/4} a_{nk}\right)/(M/4) = A_{3\pi/2}\cos(\Delta\Phi_{3\pi/2} + 3\pi/2) \end{cases} \tag{8}$$

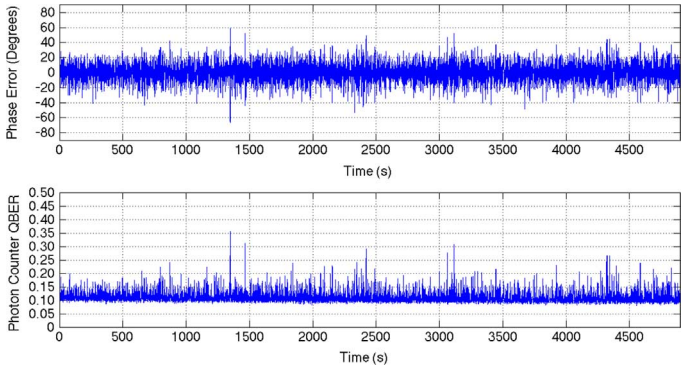

Fig. 2. Photon counting system residual phase error and its QBER.

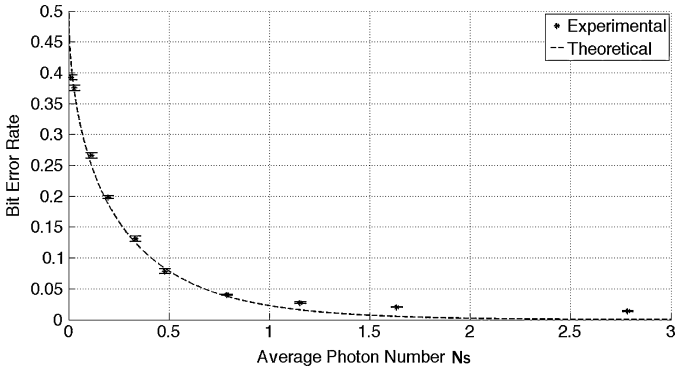

Fig. 4. Experimental BER compared with the theoretical values.

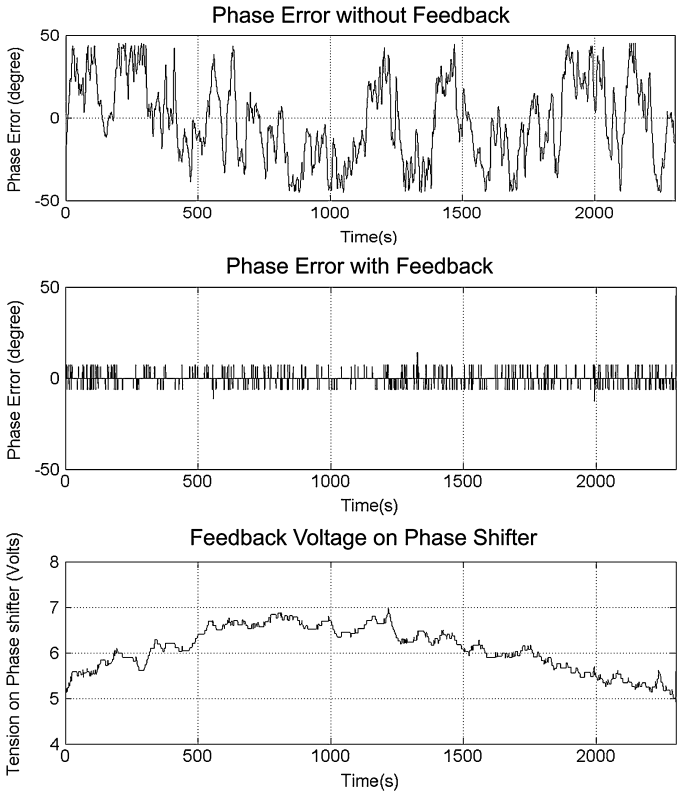

Fig. 3. BHD QKD system real-time phase error.

of the received bits as the "training frame header" and 95% as the "Data." In Fig. 3, we show the comparison of the long-term phase error without phase compensation and with phase compensation feedback for $N_S = 0.8$. The residual phase error is well controlled under 5°. Also the experimental BER with different signal powers is shown in Fig. 4.

IV. System Performance

A. The Dual-Threshold Decision of BHD

In digital communications the information loss due to the channel erasure must be recovered by the forward error coding (FEC) techniques using signal overhead. It differs significantly from the QKD situation in which the signal erasure (i.e., empty pulses) can be managed during the *a posteriori* reconciliation process [14] by decision abandonment, and mainly be turned only into efficiency reduction in the key generation rate. In this way BHD can also permit the implementation of a dual-threshold decision process on the postdetection electronic signals: allowing the possibility of inconclusive measurements to improve the BER, with a trade-off in the key generation rate. In spite of this, the resulting efficiency remains higher than the photon counter efficiency. Additionally, we will demonstrate later in the Section V that the eavesdropper Eve's attack leads more to a Bob's signal degradation than a substitution since the corresponding information can be suppressed during the reconciliation.

Since in QKD systems BHD measures only one optical field quadrature at one time, it is obviously easier to differentiate the antipodal phase states 0 and π. In Fig. 5, we depict the theoretical probability density function (pdf) and the experimental histogram.

For the signal discrimination Bob sets up two symmetrical thresholds $\pm X$ (normalized to N_S) for the detected value x, with the selection rule

$$\text{Judgement} = \begin{cases} 1 & \text{if } (x > X) \\ 0 & \text{if } (x < -X) \\ \text{Abandon} & \text{otherwise.} \end{cases} \tag{11}$$

Assuming equally probable symbols, we obtain from (3) the BER and the bit correct rate (BCR)

$$\text{BER}_i = 1/2\text{erfc}[(2N_S)^{1/2}(X+1)] \tag{12}$$

$$\text{BCR}_i = 1/2\text{erfc}[(2N_S)^{1/2}(X-1)]. \tag{13}$$

In order to compare with photon counting, we introduce the postdetection efficiency ρ, which is defined as the probability of getting a conclusive judgment

$$\rho(X, N_S) = \text{BER}_i + \text{BCR}_i. \tag{14}$$

In photon counting, the quantum efficiency of PC is determined by the built-in decision circuit. For comparison we have measured the BHD postdetection efficiency with different threshold parameters X and the photon counting efficiency at the same repetition rate of 4 MHz.

We observe from Fig. 6 that the postdetection efficiency ρ can be better than PC detection efficiency with appropriate selection of parameters, such as N_S and X. As a matter of fact, even though the selection of a high threshold X decreases ρ, a

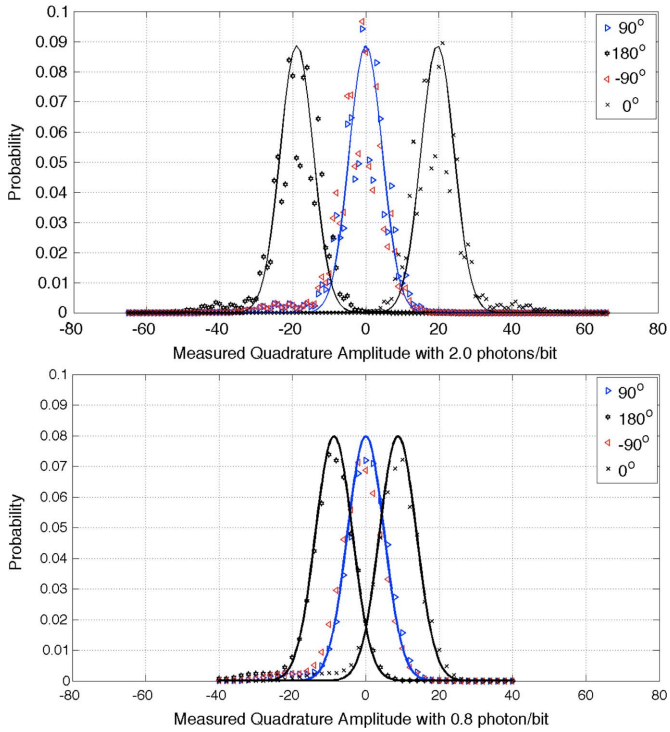

Fig. 5. Histogram of the detected QPSK signals when (a) $N_S = 2.0$ photon/bit, (b) $N_S = 0.8$ photon/bit.

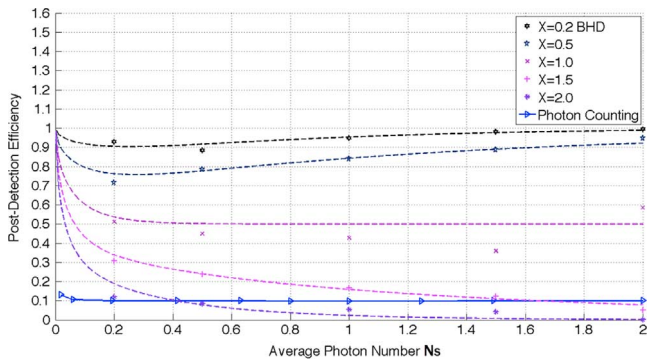

Fig. 6. Experimental measurements of the detection efficiency.

high key generation rate is attainable since BHD can potentially operate at much higher speed than PC.

B. QBER and postDetection BER

In order to continue the comparison with the QBER of photon counting, we also introduce the BHD postdetection BER_p as

$$\mathrm{BER}_p = \mathrm{BER}_i/\rho = (1/2\rho)\mathrm{erfc}[(2N_S)^{1/2}(X+1)]. \quad (15)$$

We measured the BER_P for different thresholds $\pm X$, the obtained values as shown in Fig. 7 is slightly higher than the theoretical value due to the system quantification errors and other impairments such as residual polarization mismatch. (Note that when $X = 0$, it is the standard single-threshold decision as depicted in Fig. 4).

As for the photon counting (also shown in Fig. 7), the QBER is almost constant when the signal photon number $N_S < 1$.

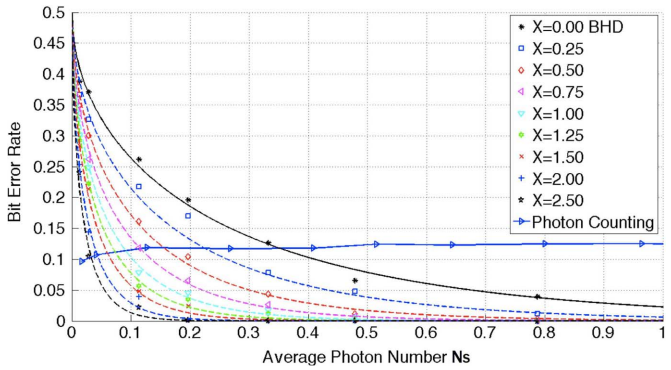

Fig. 7. BHD postdetection BER and photon-counting QBER.

Erroneous detection events occur when only one of the signal and LO photons arrives at the coupler while the other is absorbed in the optical fiber (quantum channel). The other facts that may contribute to the false detection events are the imperfect coupler contrast, i.e., the interferometer visibility, and the dark counts. The QBER increases slightly with N_S probably due to the afterpulses effects.

The observed QBER in the PC scheme in our phase encoding system appears as high as 0.1 due to the residual phase errors since the phase correction is calculated by counts of detected photon, hence less precise than the BHD scheme as a consequence of the limited counting events, unequal PC detection efficiency, as well as the dark counts. It appears constant over a wide range of signal level since errors are mainly produced by the phase fluctuations and the limited extinction ratio that are in principal independent of the signal level. QBER can be improved by a more accurate phase and polarization control, such as polarization stabilizer, special pulsed laser source with narrower spectral lineswidth and wider coherent time, as well as higher extinction ratio optical devices. Meanwhile BHD scheme can also take advantage of these improvements, still making it a more efficient detection scheme.

In Table I, we show the different characteristics of the two receiver configurations. As a matter of fact, in PC the inherent threshold parameter is adjusted as a trade-off between quantum efficiency and dark count rate, and is independent of the received signal so as to offer a wide operation range for single photon measurements; while in BHD the dual-threshold can be more flexibly adjusted as a trade-off between BER_P and key exchange rate. Furthermore, the dual-threshold BHD scheme has three main advantages over photon counting scheme: a) the quantum efficiency of PIN photodiodes is near unity; b) ultrahigh speed QKD system is achievable since no quenching process is required; and c) the cost of telecom wavelength PIN photodiodes is much lower and the supply requirements are much simpler.

Recently a decoy-state protocol has been proposed [29] and extensively studied by some research groups [30]–[33]. The signal state intensity can be chosen to be up to one photon on average thanks to a sophisticated reconciliation process. The BHD system is readily adaptable for such a protocol since it allows distinguishing the multiphoton coherent states.

TABLE I
PHOTON COUNTING VERSUS DUAL-THRESHOLD BHD

Photon Counting	Dual-threshold BHD
Low speed Geiger mode APD	High speed PIN photodiodes
Low quantum efficiency< 10%	High quantum efficiency > 90 %
Equal amplitude reference	Strong reference LO
Signal independent threshold	Signal dependent threshold
Dark count limited QBER	Shot noise limited BER_P
Delicate phase synchronization	Efficient phase synchronization

V. SECURITY OF HOMODYNE QKD SYSTEM

Having demonstrated the advantages of the dual-threshold BHD over photon counting, we now proceed to present the security analysis.

In order to investigate the security of a quantum cryptosystem, we have to take into account the action of the eavesdropper, namely Eve, and analyze the amount of information accessible to her.

We represent the information entropy of Alice by $H(A)$. The conditional entropies of Bob and Eve are defined as $H(A|B)$ and $H(A|E)$ given that Alice's information is known. The mutual information $I(A,B), I(A,E)$ are defined as the estimation of the information shared between Alice and Bob, and that shared between Alice and Eve, respectively. Note that Eve is supposed limited only by the physical laws.

$$\begin{cases} I(A,B) = H(A) - H(A|B) \\ I(A,E) = H(A) - H(A|E) \end{cases}. \tag{16}$$

The key is said to be secure if the $I(A,B)$ is higher than $I(A,E)$ [34]. Therefore, we define the amount of the obtainable security S

$$S = I(A,B) - I(A,E) = H(A|E) - H(A|B). \tag{17}$$

According to information theory, if S is positive, it is theoretically possible to decrease the amount of information gained by Eve through the process of "privacy amplification," i.e., Alice and Bob scarify the key length of the obtained key sequence to decrease Eve's useful information [35], [36]. Otherwise, i.e., when S is negative, Bob must be capable of detecting Eve's intervention [37].

We have analyzed the security issues in view of two potential individual attacks, along with a mixed power attack strategy.

A. Intercept-Resend Attack

In order to evaluate the differential mutual information S, we calculate Bob's BER under Eve's intercept-resend attack in which she performs five main steps:

1. Eve listens to the quantum channel and steals all the Q-bits.
2. She splits the signal in two equal parts.
3. She performs a measurement of the two equal parts on the two bases (as Bob's bases); accordingly she obtains two measured values x_1 and x_2.
4. As she makes the decision, she chooses the most likely value from the two measures and resends it to Bob. For example, if $x_1 > |x_2|$, then Eve resends to Bob the bit "1" on the base A1. Nevertheless she stores the two measured values until the reconciliation process.
5. During the reconciliation process, Eve listens carefully to the divulgation of the bases used by Alice and Bob. To improve her information, she switches those wrong decisions made in step 3.

Namiki and Hirano [38] have given some specific contributions with respect to Eve's intervention. We define $\mathrm{P}_+ = (1/4)[\mathrm{erfc}(-(N_S/2)^{1/2})]^2$ as the probability that Eve resends the correct bit state on the correct base; $\mathrm{P}_- = (1/4)[\mathrm{erfc}((N_S/2)^{1/2})]^2$ as the probability that Eve resends the wrong bit state on the correct base; and $\mathrm{P}_\perp = (1/4)\mathrm{erfc}[(N_S/2)^{1/2}]\mathrm{erfc}[-(N_S/2)^{1/2}]$ as the probability that Eve resends the bit state on the wrong base.

Hence, the modified postdetection efficiency and the BER at Bob's end is given by

$$\begin{aligned} &\rho'(X,N_s) \\ &\quad = [\mathrm{P}_+(N_s) + \mathrm{P}_-(N_s)]\rho(X,N_s) \\ &\qquad + 2\mathrm{P}_\perp[(2N_S)^{1/2}X] \end{aligned} \tag{18}$$

$$\begin{aligned} &\mathrm{BER}'_{\mathrm{Bob}}(X,N_s) \\ &\quad = \frac{1}{\rho'(X,N_s)} \\ &\qquad \cdot (\mathrm{P}_+(N_s)\mathrm{BER}_i + \mathrm{P}_-(N_s)\mathrm{BCR}_i \\ &\qquad + \mathrm{P}_\perp(N_s)\mathrm{erfc}[(2N_S)^{1/2}X)]. \end{aligned} \tag{19}$$

Eve's BER can simply be obtained as if she performs the measures on half the signal power, hence $\mathrm{BER}'_{\mathrm{Eve}} = \mathrm{BER}_i(0, N_s/2) = 1/2 \cdot \mathrm{erfc}(\sqrt{N_S})$.

As we have mentioned in (17), we can obtain the differential mutual information by calculating Alice--Bob, and Alice--Eve mutual information, shown in (20) at the bottom of the page.

As a higher threshold X can allow Bob to obtain a lower BER, we conclude from Fig. 8 that with properly selected parameters (X, N_S) Alice and Bob can guarantee the unconditional security wherever the differential mutual information S is above 0, as we will precise later in the Section V.C.

B. Intermediate Base Attack

In the intermediate base attack Eve performs the four main steps:

1) Eve steals all the Q-bits.
2) She performs the measurements of all the Q-bits with the intermediate base $\Phi = \pi/4$.

$$\begin{cases} H(A|B)' = -[\mathrm{BER}'_{\mathrm{Bob}}\log_2(\mathrm{BER}'_{\mathrm{Bob}}) + (1-\mathrm{BER}'_{\mathrm{Bob}})\log_2(1-\mathrm{BER}'_{\mathrm{Bob}})] \\ H(A|E)' = -[\mathrm{BER}'_{\mathrm{Eve}}\log_2(\mathrm{BER}'_{\mathrm{Eve}}) + (1-\mathrm{BER}'_{\mathrm{Eve}})\log_2(1-\mathrm{BER}'_{\mathrm{Eve}})] \end{cases} \tag{20}$$

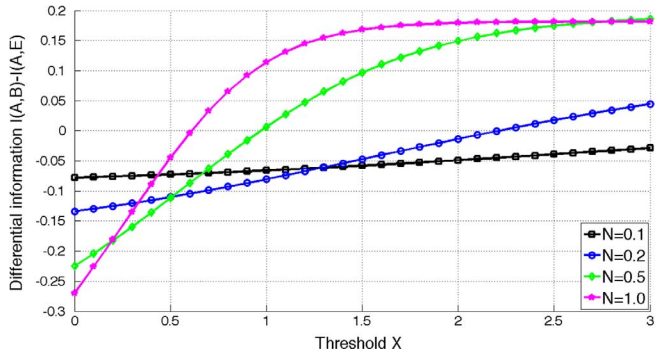

Fig. 8. Differential mutual information under intercept resend.

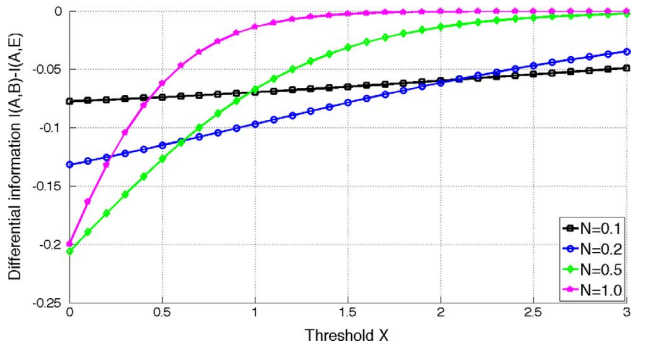

Fig. 9. Differential mutual Information under intermediate base attack.

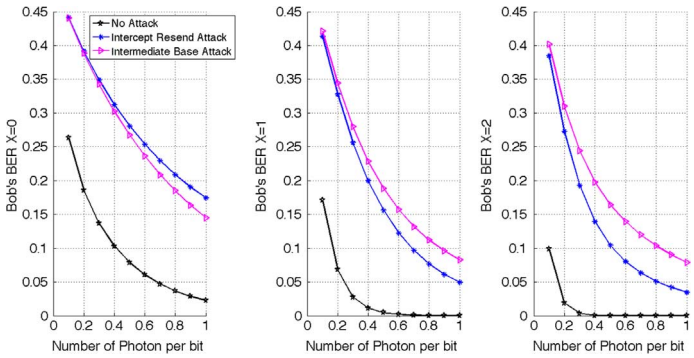

Fig. 10. Postdetection BER evaluations with different $X = 0$, $X = 1$, $X = 2$.

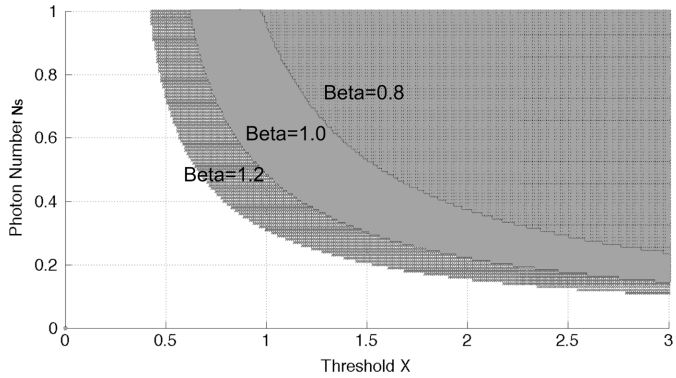

Fig. 11. Security zone under intercept resend attacks with different β.

3) She resends to Bob the bits she has obtained on the intermediate base, and stores the bit values until the reconciliation process.
4) During the reconciliation process, she uses the base revelation to discriminate the bit states (0 or 1) that Alice has sent.

The loss of Eve in the step 2 is 3 dB due to the intermediate base projection. Thus, Eve's BER is the same as under the intercept-resend attack. Furthermore, we can deduce from (12), (13) that $\mathrm{BER}''_{\mathrm{Eve}} = \mathrm{BER}_i(0, N_s/2)$ and Eve's BCR is: $\mathrm{BCR}''_{\mathrm{Eve}} = \mathrm{BCR}_i(0, N_s/2)$.

Consequently Bob's incoming BER and BCR are modified: $\mathrm{BER}''_i = \mathrm{BER}_i(X, N_S/2)$ and $\mathrm{BCR}''_i = \mathrm{BCR}_i(X, N_S/2)$. And Bob's modified efficiency is given by $\rho''(X, N_s) = \rho(X, N_s/2)$.

Thus the modified Bob's BER is given by

$$\mathrm{BER}''_{\mathrm{Bob}}(X, N_s) = \frac{1}{\rho''(X, N_s)} \cdot(\mathrm{BER}''_{\mathrm{Eve}}\mathrm{BCR}''_i + \mathrm{BCR}''_{\mathrm{Eve}}\mathrm{BER}''_i) \quad (21)$$

Fig. 9 shows that Eve could always obtain more information than Bob, thus this quantum link is not unconditionally secure under the intermediate base attack. Therefore, Bob must be capable of detecting the Eve's intervention and tell Alice.

In Fig. 10, we give the theoretical comparison of the postdetection BER evaluation when $X \in \{0, 1.0, 2.0\}$ are used: the BER is largely modified under the two attacks. When we chose to use a higher threshold X, it will be even more evident to find out Eve's attacks by comparing the operating postdetection BER with the original postdetection BER, the generated keys must be rejected.

C. Attacks and Power Analysis

It has been proven in the precedent chapters that Eve could not obtain useful information by using the two types of attack, in that when she gains more mutual information than Bob, the key will be discarded. Now we investigate on Eve's mixed attack strategy: using power modification to hide her intervention.

When Eve makes the decision and resends the key sequence to Bob, she can actually modify the signal power so as to circumvent Bob's vigilance. She will seek to lower $I(A, B)$ and maintain Bob's postdetection BER to conceal her attacks. In this regard, we replaced the signal level N_S by βN_S (β is a power factor). If Eve resends the signal at the same power level as she has received, $\beta = 1$. If $\beta > 1$ she amplifies the signal power and if $\beta < 1$ she resends the signal bit with attenuation. We note that the "beam-splitter attack" can be considered as a special operation in which $\beta = 1$.

Under the intercept-resend attack, we illustrate the security zone in Fig. 11 for $\beta \in \{0.8; 1; 1.2\}$. Secure zone stands for positive differential mutual information S. First we can see that amplifying the signal will not be a wise choice for Eve, since doing so she lowers Bob's postdetection BER but increases $I(A, B)$, as well as a larger security zone. In the other hand, if she attenuates the signal, Bob will be aware of her presence since the incoming BER_i will increase and the detection efficiency will drop in consequence.

Under the intermediate base attack, if Eve amplifies the signal power, Bob will also have a lower postdetection BER, however this β has to be very high to hide her presence. In this case, by comparing the incoming BER_i, the detection efficiency and the postdetection BER, Bob can still find out that Eve has been attacking the quantum channel. And if she attenuates the signal, the increasing postdetection BER and incoming BER_i, together with the decreasing detection efficiency will reveal her presence.

In conclusion, Eve's mixed strategies can be diversified, including individual, joint and collective attacks. However, if she doesn't manage to gain the mutual information and maintain Bob's incoming BER_i and postdetection BER to cover up her action at the same time, the attack will be discerned.

At Bob's side, in order to guarantee the security he needs to set a high threshold so as to lower the incoming BER_i and the postdetection BER to make Eve's intervention detectable. This is consistent with the parameters choice of a higher performance system thanks to BHD's high-potential operation rates.

VI. Conclusion

We have implemented an all fiber one-way QPSK QKD system at 1550 nm using both photon counting and BHD configuration. An automatic optoelectronic feedback loop is implemented for the interferometric phase drift compensation.

We have developed a dual-threshold decision scheme for the BHD signal postdetection. We compared experimentally the performance of photon counting and BHD in terms of detection efficiency and BER (or QBER). We point out that BHD is potentially more effective in terms of quantum key generation rate and system flexibility.

We have also investigated the security issues of the BHD QKD system under two main individual attacks: intercept-resend attack and intermediate-base attacks. A mixed attack strategy of signal power modification has also been analyzed. We have proved that Eve's intervention cannot be effective with appropriate parameter pair choice of (X, N_S).

Acknowledgment

We thank for all the technical supports from the Département Communications et Electronique, we also thank AVANEX for providing laser source that is used in our QKD system.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. Int. Conf. Comput., Syst. & Signal Process.*, Bangalore, India, 1984, pp. 175–179.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phy.*, vol. 74, pp. 145–195, 2002.

[3] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, p. 057902, 2002.

[4] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "'Plug and play' systems for quantum cryptography," *Appl. Phys. Lett.*, vol. 70, pp. 793–795, 1997.

[5] H. Zbinden, J.-D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, "Interferometry with Faraday mirrors for quantum cryptography," *Electron. Lett.*, vol. 33, pp. 586–588, 1997.

[6] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," *Phys. Rev. A*, vol. 73, p. 022320, 2006.

[7] J.-M. Merolla, Y. Mazurenko, J. P. Goedgebuer, H. Porte, and W. T. Rhodes, "Phase-modulation transmission system for quantum cryptography," *Opt. Lett.*, vol. 24, pp. 104–106, 1999.

[8] T. Okoshi, "Recent advances in coherent optical fiber communication systems," *J. Lightw. Tech.*, vol. 5, pp. 44–52, Jan. 1987.

[9] L. G. Kazovsky, "Balanced phase-locked loops for optical homodyne receivers," *J. Lightw. Tech.*, vol. 4, pp. 182–195, Feb. 1986.

[10] T. Chikama, T. Naito, S. Watanabe, T. Kiyonaga, M. Suyama, and H. Kuwahara, "Optical heterodyne image-rejection receiver for high-density optical frequency division multiplexing system," *IEEE J. Sel. Areas Commun.*, vol. 8, no. 6, pp. 1087–1094, Aug. 1990.

[11] C. Xu, X. Liu, and X. Wei, "Differential phase-shift keying for high spectral efficiency optical transmissions," *IEEE J. Sel. Topics Quantum Electron.*, vol. 10, no. 2, pp. 281–293, Mar./Apr. 2004.

[12] A. H. Gnauck and P. J. Winzer, "Optical phase-shift-keyed transmission," *J. Lightw. Tech.*, vol. 23, pp. 115–130, 2005.

[13] H. P. Yuen and V. W. S. Chan, "Noise in homodyne and heterodyne detection," *Opt. Lett.*, vol. 8, pp. 177–179, 1983.

[14] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, "Quantum cryptography using pulsed homodyne detection," *Phys. Rev. A*, vol. 68, p. 042331, 2003.

[15] J. R. Barry and E. A. Lee, "Performance of coherent optical receivers," *Proc. IEEE*, vol. 78, no. 8, pp. 1369–1393, 1990.

[16] H. P. Yuen and J. H. Shapiro, "Optical communication with 2-photon coherent states. 3. Quantum measurements realizable with photo-emissive detectors," *IEEE Trans. Inf. Theory*, vol. 26, no. 1, pp. 78–82, Jan. 1980.

[17] R. J. Glauber, "Coherent and incoherent states of the radiation field," *Phys. Rev.*, vol. 131, pp. 2766–2788, 1963.

[18] C. W. Helstrom, *Quantum Detection and Estimation Theory, Mathematics in Science and Engineering*. New York: Academic Press, 1976, vol. 123.

[19] J. G. Webb, T. C. Ralph, and E. H. Huntington, "Homodyne measurement of the average photon number," *Phys. Rev. A*, vol. 73, p. 033808, 2006.

[20] R. L. Cook, P. J. Martin, and J. M. Geremia, "Optical coherent state discrimination using a real-time closed-loop quantum measurement," *Nature*, vol. 446, pp. 774–777, 2007.

[21] B. B. Elliott, O. Pikalo, J. Schlafer, and G. Troxel, "Path-length control in an interferometric QKD link," *Quantum Information and Computation, Proc. SPIE*, vol. 5105, pp. 26–38, 2003.

[22] V. Makarov, A. Brylevski, and D. R. Hjelme, "Real-time phase tracking in single-photon interferometers," *J. Appl. Opt.*, vol. 43, pp. 4385–4392, 2004.

[23] Q. Xu, M. B. Costa e Silva, P. Gallion, and F. Mendieta, "One way differential QPSK quantum key with channel impairment compensation," *CLEO/Europe-IQEC JSI-3*, 2007.

[24] Q. Xu, M. B. Costa e Silva, P. Gallion, and F. Mendieta, "Auto-compensating quantum Crypto-system using homodyne detection," in *Opt. Fiber Commun. Conf. 2008*, San Diego, California, Paper JWA49.

[25] "Single-photon detection with InGaAs/InP avalanche photodetectors," Single-Photon Detector Module: Application Note [Online]. Available: http://www.idquantique.com Id Quantique

[26] *MagiQ Quantum Cryptography Test Bed: Uncompromising Research Results*, , 2005 [Online]. Available: http://www.magiqtech.com, MagiQ Technologies, Inc.

[27] K.-P. Ho, *Phase-Modulated Optical Communication Systems*, 1st ed. New York: Springer, 2005.

[28] P. Agrawal, *Fiber-Optic Communication Systems*, 3rd ed. New York: Wiley-Interscience, 2002, ch. 10.

[29] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, p. 057901, 2003.

[30] X.-F. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A*, vol. 72, p. 012326, 2005.

[31] X.-B. Wang, "Beating the photon pulse-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. 94, pp. 230503-1–230503-4, 2005.

[32] H.-K. Lo, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, p. 230504, 2005.

[33] D. Rosenberg, "Long-distance decoy-state quantum key distribution in optical fiber," *Phys. Rev. Lett.*, vol. 98, p. 010503, 2007.

[34] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pp. 379–423, 623–656, Jul./Oct. 1948.

[35] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM J. Comput.*, vol. 17, pp. 1919–1923, 1988.
[36] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.
[37] M. Koashi, "Unconditional security of coherent state quantum key distribution with a strong reference phase pulse," *Phys. Rev. Lett.*, vol. 93, p. 120501, 2004.
[38] R. Namiki and T. Hirano, "Security of quantum cryptography using balanced homodyne detection," *Phys. Rev. A*, vol. 67, p. 022308, 2003.

Qing Xu was born in Shanghai, China, on November 15, 1979. He received the B.E. degree in information engineering from Shanghai Jiaotong University, Shanghai, in 2002, and the M.E. degree in telecommunications from the Ecole Spéciale de Mécanique et d'Electricité, Paris, France, in 2005. He is currently working toward the Ph.D. degree in electrical engineering at the Ecole Nationale Supérieure des Télécommunications (TELECOM ParisTech), Paris.

From 2002 to 2003, he was a code division multiple access (CDMA) R&D Engineer in Wide Telecom, Inc. He joined the Département Communications et Electronique, Ecole Nationale Supérieure des Télécommunications, in 2005.

Mr. Xu received a French Government Research Fellowship. His current research interests include the experimental phase encoding quantum key distribution system and the coherent detection technologies with the group of optical communications.

Manuel Sabban was born in Strasbourg, France, on September 5, 1981. He received the Master's degree in digital telecommunication systems from the École Nationale Supérieure des Télécommunication (TELECOM ParisTech), Paris, France, and the Université Paris VI, Paris, in 2005.

He was with the French École Normale Supérieure de Cachan. His current research interests include security in quantum cryptography.

Marcia B. Costa e Silva was born in Recife, Brazil. She received the B.A. degree from the Federal University of Pernambuco, Recife, Brazil, in 1998, the M.S. degree from the University of Campinas (UNICAMP), Campinas, Brazil, in 2000 and the Ph.D. degree from the Pontifical Catholic University, Rio de Janeiro, Brazil, in 2004.

In 2004, she was a Fellow with Physical Departments, Federal University of Pernambuco, Recife, Brazil. Since 2005, she has been a Postdoctoral Researcher with the Ecole Nationale Supérieure des Télécommunications (TELECOM ParisTech), Paris, France. She has authored or coauthored several technical papers in optical communications area.

Philippe Gallion (SM'83) received the Doctorat de Troisième Cycle degree from the University of Rheims, Rheims, France, in 1975 and the Doctorat d'Etat degree from the University of Montpellier, Montpellier, France, in 1986. In 1978, he was enrolled at the Ecole Nationale Supérieure des Télécommunications (ENST), also called TELECOM ParisTech, Paris, France, where he is currently a Full Professor.

He is engaged in research at the Laboratoire de Traitement et Communication de l'Information, LTCI, joint research laboratories between ENST and the Centre National de la Recherche Scientifique (CNRS), where he is in charge of research activities in the fields of communications, electronics, radiofrequencies and optoelectronics. He has made pioneering contributions on laser noise, injection locking, semiconductor laser modulation chirp and tuning, coherent systems and optical devices, digital optical communications systems and networks. His current research interests include include theory, design, modeling, and characterization of functional devices, advanced optical digital communication systems and networks, radio over fiber systems and quantum cryptography systems. He has authored or coauthored more than 200 technical papers and communications and he has served as an advisor for more than 40 Ph.D. degree thesis.

Dr. Gallion is a Member of the Optical Society of America. He is the Chairman of the IEEE Laser and Electro Optics Society (LEOS) French Chapter. He serves on the Editorial Board and Scientific Committee of several technical publications and as member of program or steering committee of international scientific meetings.

Francisco J. Mendieta (M'80) obtained his Bachelor's degree in mechanical and electrical engineering from the National University of Mexico, Mexico City, Mexico, the Master's and Ph.D. degrees in the field of coherent optical communications from the National Superior School of Telecommunications (ENST, TELECOM ParisTech), Paris, France.

In the Institute for Electrical Research (IIE), Cuernavaca, Morelos, Mexico, he was engaged in development projects on applications of optical fibers to electrical power systems. In the National University of Mexico he led a continuous education program on telecommunications systems. During a leave in the Utah State University, Logan, UT, he participated in a project on instrumentation for space experiments. At CICESE, Ensenada B.C., Mexico, he formed the Optical Communications group, where he has led several research projects on telecommunications and sensing; he is a lecturer in the graduate program on optical and digital telecommunications, and has been adviser for diverse Master's and Doctor's thesis. During a sabbatical leave at ENST, he participated in a project on quantum communications. He has authored or coauthored diverse journal papers and conference papers in the field of optical communications and sensing.