Quantum Key Distribution System using Dual-threshold Homodyne Detection

Qing Xu, Manuel Sabban, Philippe Gallion
Ecole Nationale Supérieure des Télécommunications
(TELECOM ParisTech, CNRS LTCI)
75013 Paris, France
qing.xu@enst.fr

Francisco Mendieta
on sabbatical leave from CICESE
km.107 Carr. Tijuana, Ensenada, Baja California 22800,
México

Abstract— **In this work we present the principles of a flexible quantum key distribution (QKD) system using quadrature-phase-shift-keying (QPSK) base and symbol encoding and dual-threshold balanced homodyne detection (BHD) scheme. We give its security proofs and we compare its performance experimentally with a photon counting detection scheme.**

Keywords- quantum key distribution, quantum cryptography, balanced homodyne detection, QPSK modulation, BB84 protocol, photon counting, phase shift keying, unconditional security

I. INTRODUCTION

The ongoing boom of information technology (IT) and telecommunications infrastructure is a main driving force of the technological and social changes in the late 20th and early 21st centuries. The confidentiality of the IT based applications and communications systems, i.e. the information security is becoming one of the biggest concerns in governments, military, homeland security, financial institutions, hospitals, and private businesses.

The security of the conventional public-key cryptosystems such as Data Encryption Standard (DES), Advanced Encryption Standard (AES) relies on the computational difficulty of certain mathematical functions, and can provide neither any indication of eavesdropping nor guarantee of key security. It is threatened by the calculation capacity potential improvement of super computer, or eventually quantum computer. On the other hand, information theory shows that traditional private-key (secret-key) cryptosystems cannot be totally secure unless the key is used once only, being at least as long as the enciphered text. This algorithm is also called one-time pad (OTP) [1].

Based on the laws of quantum mechanics, in contrast to traditional public key cryptography, quantum cryptography (QC), as a system that guarantees unconditional security of communications [2], has been extensively studied recently in search for high-speed, long distance operational scheme that is compatible with the today's optical networks.

An important point is that QC is only used to produce and distribute a key, not to transmit any message data itself. In such a quantum key distribution (QKD) system the security is checked *a posteriori* and the key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel. The algorithm most commonly associated with QKD is OTP, as it is up to now considered as unbreakable when used with a perfectly secret, random key.

QC is now moving from the promise of physics to the hard reality of electrical engineering world and is obviously handling with the full quantum nature of light. Optical QKD system is based on the use of single-photon Fock states in which any state of the Fock space is with a well-defined number of particles. Unfortunately, these states are up to now difficult to realize experimentally. A more practical choice of our days is faint laser pulses [3-5], i.e. weak coherent states (WCP) or entangled photon pairs [6,7], in which both the photon and the photon-pair number distribution, obey Poisson statistics [8].

Then the key issue in a QKD system turns to be the detection of quantum level Qbits, such as the reliable and inexpensive WCP. Today, the Geiger gated-mode avalanche diode, also called photon counter (PC), is widely used. PC works under low and precise temperature control, i.e. around -30ºC, and exhibits inherent low quantum efficiency around 0.1 and the inevitable residual after-pulse noise due to the macroscopic avalanche [9,10] at the C band, i.e. 1550nm widely used in optical communications. Moreover its operational frequency is limited to 4-8MHz due to the necessary quenching process.

On the other hand, coherent optical communication is one of the most promising ways to achieve highest receiver sensitivity, excellent spectral efficiency and longest transmission distance for the next generation of optical communication systems. Already in the late 1980s and early 1990s coherent systems attracted a lot of attention [11-20] as it was a promising way to improve the receiver sensitivity.

Balanced homodyne detection (BHD), using high efficiency, high bandwidth and low cost positive-intrinsic-negative diode (PIN) operating at room temperature, is also sensitive to phase and polarization matching. It allows a noise free single quadrature measurement of the optical field. This leads to a frequency selection scheme that is useful for background radiation rejection as for the compatibility with the current WDM networks. It allows signal phase encoding more suitable for optical fiber communications than polarization encoding in one-way systems because it benefits from the mixing with a strong local optical field. Operating near the quantum limit, it is potentially capable of overcoming the non-desirable effects such as afterpulses and "dark counts" characteristics of the single photon detection measurement (SPDM). Optical phase encoding is well known to overcome the fiber impairments of the historical polarization encoding. Optical phase and information recoveries are to be solved both by the receiver Bob and the eavesdropper Eve.

Post-detection, threshold and symbol synchronization stages must be properly designed as in BHD the decision process is carried out *a posteriori* [21,22], in opposite to photon counting that inherently performs built-in decision [9,10], making a compromise between detection efficiency and bit error rate (BER).

In this paper we first recall the principles of the BB84 QKD protocol [2], and then we discuss the homodyne detection using both photon counting and BHD. Next we analyze the security issues of the BHD QKD system under the "intercept-resend" attack and the "intermediate base" attack. Furthermore we present the experimental setup of a one-way BB84 QKD system using weak coherent pulses (WCP) QPSK format encoding at Alice's end and BPSK base switching at Bob's end. Photon counting and dual-threshold BHD are performed with optical synchronization for phase drift compensation. Finally we compare the system performance of the two receivers in terms of detection efficiency and BER.

II. HOMODYNE QKD SYSTEM

A. BB84 protocol and unconditional security

Charles H. Bennett and Gilles Brassard proposed the first protocol for QC in 1984, as usually referred as BB84 [2]. In this protocol, the two protagonists Alice and Bob use two channels of communications: one quantum channel and another classical channel. The quantum channel allows the transmission of quantum objects that have to be very weak so that quantum effects are measurable. The eavesdropper, namely Eve, is supposed to have full access to this quantum channel although the quantum channel nature limits her actions. These quantum objects are prepared in such a way that Eve's tentative of acquiring the information will induce, in accordance with the quantum mechanics, by a perturbation of the signals that Alice and Bob could measure by comparing the communications through the classical channel.

The classical channel that permits Alice and Bob to communicate can be a standard telephone line, cable, radio frequency, or even the same fiber link as quantum channel. Eve can listen to the conversation between Alice and Bob, but she will not modify the information. In other terms, this classical channel should be authenticated, which is possible by the classical cryptography algorithm, since Alice and Bob share *a priori* some secret key.

The protocol BB84 is a group of strict rules that is indispensable for a QKD system to be implemented as an unconditionally secure communication. From two orthogonal bases chosen randomly by Alice, four quantum eigen states can be generated separately (the symbols 0 and 1 in two different bases), constituting a QPSK constellation. At Bob's end, the base coincidences turn to a BPSK constellation; base anti-coincidences are not considered since their results are discarded and do not contribute to the bit error rate (BER).

Alice's choices of bases and symbols and Bob's choices of bases, as well as the key coincidence/anti-coincidence are shown in Table I.

TABLE I. QPSK BB84 PROTOCOL

Alice					Bob			
Base	Bit	Φ_1	Φ_2	Φ_A	**Base**	Φ_B	Φ_A-Φ_B	Key
A1	0	0	π/2	π/4	**B1**	π/4	0	0
					B2	-π/4	π/2	?
	1	π	-π/2	-3π/4	**B1**	π/4	π	1
					B2	-π/4	-π/2	?
A2	0	0	-π/2	-π/4	**B1**	π/4	-π/2	?
					B2	-π/4	0	0
	1	π	π/2	3π/4	**B1**	π/4	π/2	?
					B2	-π/4	π	1

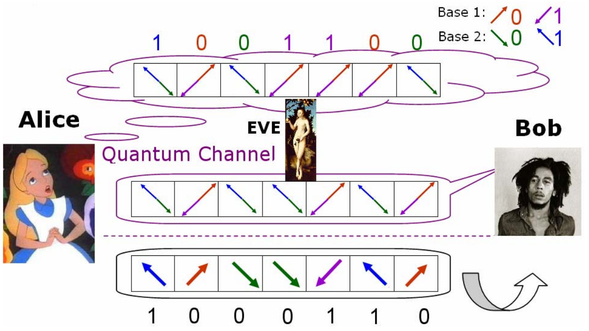

Figure 1. BB84 Protocol in quantum channel

The steps of BB84 protocol in quantum channel are: 1 - Alice chooses a random series of bits; 2 - Alice sends each bit with a random base choice (base 1 or base 2); 3 - Bob detects each bit using another random choice of the base (base 1 or base 2).

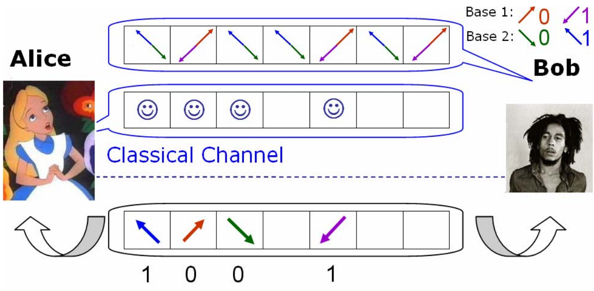

Figure 2. BB84 Protocol classic channel

The steps of BB84 protocol in classical channel are: 4 - Bob publicly announces his series of base choices (but not the measurement result!); 5 - Alice publicly announces the base coincidences, i.e. the bits correctly detected by Bob; 6 - Bob and Alice use this bit sequence as the key, a raw key is thus generated through this "reconciliation" process.

When there is base coincidence between Bob and Alice, the bit is correctly detected and when there is base anti-coincidence, the result of the measurement is random. Only those bits of base coincidence are kept, which will then be used for the generation of the keys.

As a matter of fact, in the quantum channel, the raw BER is 0.25 since the base coincidence and base anti-coincidence are equal-probable. After the communications in the classical channel and the "reconciliation" process, the theoretical post-detection BER should be 0 since bits of anti-coincidence are discarded.

Eve's presence can only be perceived when the noise induced by the experimental imperfections and the system impairments is below the level of perturbation issued from Eve's intervention. In this case Alice and Bob can effectively evaluate the quantity of information gained by Eve, and a procedure of "privacy amplification" can be used to extract a secret key, rending Eve's intervention (attacks) useless [23,24]. Oppositely, if Alice and Bob acknowledge that Eve has obtained more information than Bob, they can simply abandon the generated keys, or counter-attack by giving false information to Eve.

B. *Homodyne detection for phase coding signals*

Coherent optical transmission of the telecommunications wavelength has been studied for more than three decades, 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 post-detection BER. And the standard quantum limited (SQL) reception is attainable when a strong local oscillator (LO) field is used. Furthermore, the use of the constant envelope formats, in opposition to the traditional intensity modulation with direct detection (IM/DD), is more tolerant to the non-linear impairments.

C. *Photon Counting for QKD*

In telecom applications, the coherent detection process consists of mixing the signal field E_S and the LO field E_{OL} in a 2X2 coupler at the receiver's end.

Photon counting scheme, 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 above the breakdown voltage. This kind of operation is also called Geiger mode and an indispensable quenching process limits its operation frequency to 4-8MHz. Also its quantum efficiency is limited to approximately 0.1 at telecom band. When $|E_{LO}|=|E_S|$, the photon arrives on the output D1 if $\Phi_A-\Phi_B=0$ or arrives on the output D2 if $\Phi_A-\Phi_B=\pi$. There is no intrinsic BER due to the built-in decision of the PC. However it is also limited by the interferometer contrast, i.e. the interferometer fringe visibility and the after-pulses induced by the precedent avalanche.

D. *Dual-threshold balanced homodyne detection*

BHD consists of mixing the weak signal filed with the strong LO field before intensity detection, i.e. $|E_{LO}|>>|E_S|$. BHD technique is potentially capable of overcoming the non-desirable effects of PC. However, 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 [12,25,26].

The output of a BHD receiver is proportional to the E_S and its additional quantum noise $|\Delta E_S|$. This input signal is found to be amplified by the deterministic part of the in-phase LO quadrature on the detectors that act as a noise free mixing gain. Since only one quadrature is measured, there is no additional noise to the zero-point fluctuation. As reported by Yuen [13], the input signal quantum noise is therefore the only noise limitation since the LO noise has a negligible influence and the output noise is only dominated by the vacuum fluctuation entering into the signal port. Consequently, BHD is only limited by the quantum fluctuation of the signal. The output noise quantum limitation level of a homodyne detector has been experimentally proved by Machida [27].

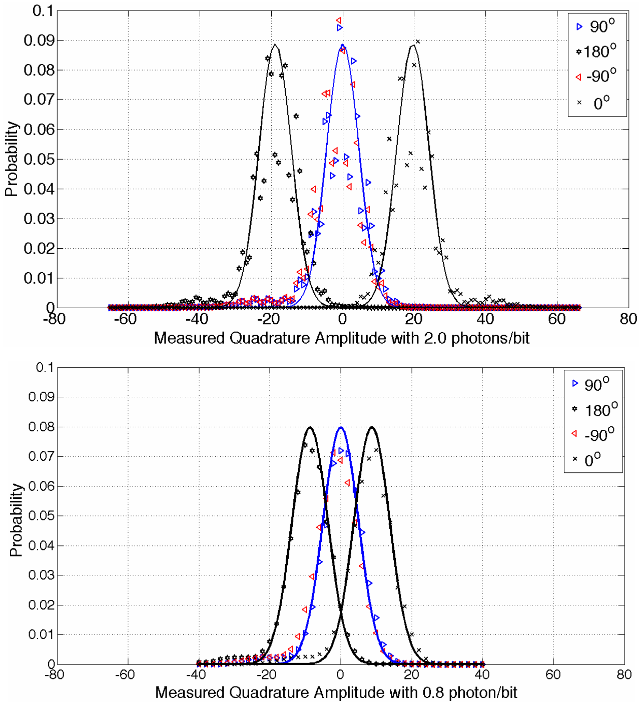

Figure 3. Histogram of the detected signals a) $N_S = 2.0$, a) $N_S = 0.8$

In Figure 3, we depict the theoretical probability density function (PDF) and the experimental histogram: it is only possible to differentiate $\Phi=0$ and $\Phi=\pi$. Given the signal average photon number per bit N_S, the detected sum field using intensity detection in the absence of thermal noise results in the probability of error [12]:

$$BER=1/2\,erfc\left(\sqrt{2N_S}\right) \quad (1)$$

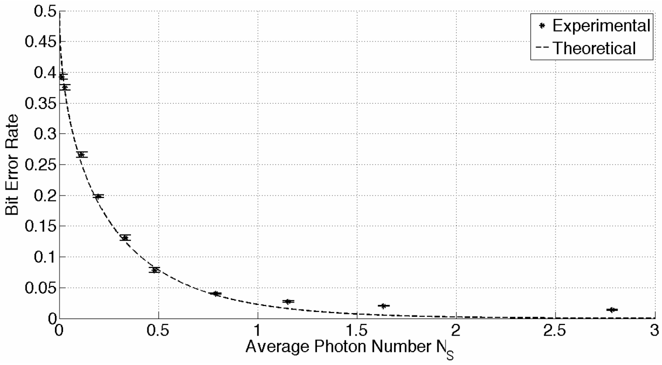

Figure 4. Experimental BER compared with the theoretical values

In digital communications the information loss due to the channel erasure must be processed by the forward error coding (FEC) techniques. However it differs significantly from the QKD situation in which the signal erasure (i.e. empty pulses) can be easily managed during the *a posteriori* reconciliation process [5] by decision abandonment, and mainly be turned into reduction of the key generation rate. In this way BHD can also permit the accurate implementation of a dual-threshold decision process on the post-detection high-level electronic signals, allowing the possibility of inconclusive measurements to lower the BER, with a trade-off in the reduced key generation efficiency. Therefore Eve's attack turns more to a Bob's signal degradation than a substitution since the corresponding information can be suppressed during the reconciliation.

For the signal discrimination Bob sets up two symmetrical thresholds ±X (normalized to the average photon number per bit N_S) for the detected value x, with the selection rule:

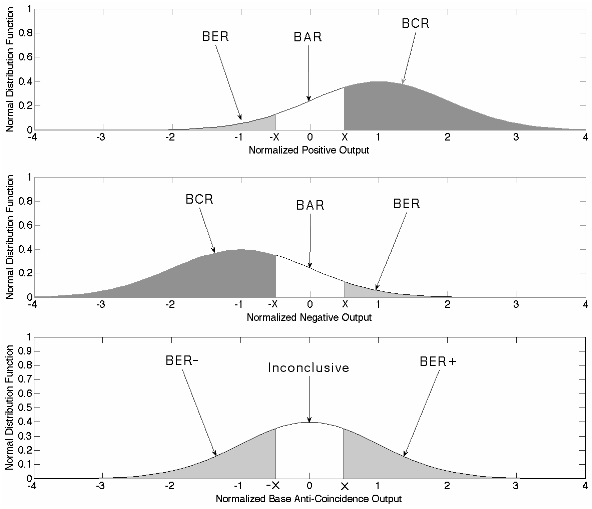

Figure 5. Dual-threshold BHD decision

$$Judgement = \begin{matrix} 1 & if\left(x > X\right) \\ 0 & if\left(x < -X\right) \\ Abandon & otherwise \end{matrix} \qquad (2)$$

We assume equally probable symbols; hence we obtain the bit error rate (BER), and the bit correct rate (BCR):

$$BER_i = 1/2\, erfc\left[\left(2N_S\right)^{1/2}\left(X+1\right)\right] \qquad (3)$$

$$BCR_i = 1/2\, erfc\left[\left(2N_S\right)^{1/2}\left(X-1\right)\right] \qquad (4)$$

In order to dispose of a parameter to compare with photon counting, we introduce the post-detection efficiency ρ, which is defined as the probability of a conclusive judgment:

$$\rho\left(X, N_S\right) = BER_i + BCR_i \qquad (5)$$

In order to compare with the QBER of photon counting, we introduce the BHD post-detection BER_P as:

$$BER_p = BER_i/\rho = \left(1/2\rho\right) erfc\left[\left(2N_S\right)^{1/2}\left(X+1\right)\right] \qquad (6)$$

E. Security of dual-threshold BHD

In the section we analyze the security issues of the BHD QKD system under the "intercept-resend" attack and the "intermediate base" attack, provided that the guarantee of security lies either on the mutual information gain or the perception of the eavesdroppers' intervention.

In order to investigate the security of a quantum cryptosystem, we have to take into account the action of Eve, and we analyze the amount of information accessible to her. We represent the information entropy of Alice, Bob and Eve by *H(A)*, *H(B)* and *H(E)*, respectively. The mutual information *I(A,B)*, *I(A,E))* are defined as the estimation of the information shared by Alice and Bob, and that shared by Alice and Eve, respectively.

$$\begin{aligned} I(A,B) &= H(A) - H(A|B) \\ I(A,E) &= H(A) - H(A|E) \end{aligned} \qquad (7)$$

The key is secure if *I(A,B)* is higher than *I(A,E)* [32]. Therefore we define the amount of the obtainable security *S*:

$$S = I(A,B) - I(A,E) = H(A|E) - H(A|B) \qquad (8)$$

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 abandon randomly a portion of the obtained key sequence to decrease Eve's useful information [28-30]. Otherwise the key must be dropped as long as no algorithm could guarantee the unconditional security. In this case, Bob should be capable to detect Eve's intervention.

1) Intercept-Resend attack

Namiki and Hirano [31] have given some specific contributions with respect to Eve's intervention. We define $\mathrm{P}_{+}=\frac{1}{4}\left(\mathrm{erfc}\left(-(N_S/2)^{1/2}\right)\right)^2$ as the probability that Eve resends the correct bit state on the correct base; $\mathrm{P}_{-}=\frac{1}{4}\left(\mathrm{erfc}\left((N_S/2)^{1/2}\right)\right)^2$ as the probability that Eve resends the wrong bit state on the correct base; and $\mathrm{P}_{\perp}=\frac{1}{4}\mathrm{erfc}\left((N_S/2)^{1/2}\right)\mathrm{erfc}\left(-(N_S/2)^{1/2}\right)$ as the probability that Eve resends the bit state on the wrong base. Hence the modified post-detection efficiency and the BER at Bob's end is given by:

$$\rho'(X,N_s)=(\mathrm{P}_{+}(N_s)+\mathrm{P}_{-}(N_s))\rho(X,N_s)+2\mathrm{P}_{\perp}\,\mathrm{erfc}\left((2N_s)^{1/2}X\right) \quad (9)$$

$$BER_{Bob}'=\frac{\mathrm{P}_{+}(N_s)BER_i+\mathrm{P}_{-}(N_s)BCR_i+\mathrm{P}_{\perp}(N_s)\mathrm{erfc}\left((2N_s)^{1/2}X\right)}{\rho'(X,N_s)} \quad (10)$$

Eve's BER can simply be obtained as if she performs the measures on half the signal power, hence

$$BER_{Eve}'=BER_i(0,N_s/2)=1/2\bullet erfc\left(\sqrt{N_S}\right) \quad (11)$$

As we have mentioned in equation (8), we can obtain the differential mutual information by calculating Alice-Bob, Alice-Eve mutual information, and $S=H(A|E)'-H(A|B)'$.

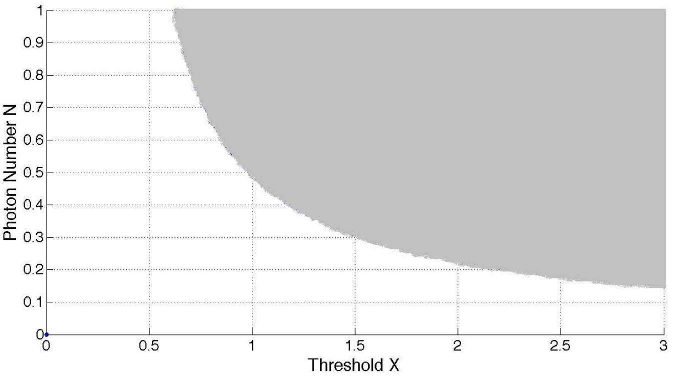

Figure 6. The security zone under intercept-resend attacks

As a higher threshold X could allow Bob to obtain a lower BER, we conclude 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 shown in Figure 6.

2) Intermediate-base attack

In this attack Eve's loss 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 equations (3), (4) that $BER_{Eve}''=BER_i(0,N_s/2)$ and Eve's BCR is: $BCR_{Eve}''=BCR_i(0,N_s/2)$.

Consequently Bob's incoming BER and BCR are modified: $BER_i''=BER_i(X,N_S/2)$ and $BCR_i''=BCR_i(X,N_S/2)$. 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:

$$BER_{Bob}''(X,N_s)=\frac{BER_{Eve}''BCR_i''+BCR_{Eve}''BER_i''}{\rho''(X,N_s)} \quad (12)$$

Under intermediate-base attack, Eve could always obtain more information than Bob, thus this quantum link is not unconditionally secure. Therefore, Bob should be capable of detecting the Eve's intervention and tell Alice.

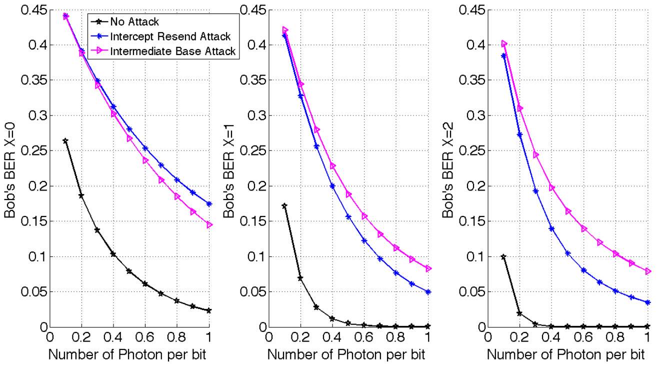

Figure 7. The post-detection BER evaluations with different X=0, 1, 2

In Figure 7 we give the theoretical comparison of the post-detection 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 more evident to disern Eve's attacks by comparing the operating post-detection BER with the original post-detection BER.

Although Eve's mixed strategies can be diversified, including individual, joint and collective attacks, if she doesn't manage to gain the mutual information and maintain Bob's incoming BER_i and post-detection BER_P to cover up her action at the same time, the attack will be detected.

At Bob's side, in order to guarantee the security he needs to set a high dual-threshold so as to lower BER_i and BER_P to make Eve's intervention detectable. This is consistent with the parameters choice for a higher performance system.

III. EXPERIMENTAL ARRANGEMENT

We have implemented an experimental one-way quantum key distribution (QKD) system with QPSK modulation. 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 Figure 8, we use a 1550nm electro-absorption modulated light source to generate laser pulses of 5ns width with 25dB extinction ratio.

In the PC detection scheme, the operational repetition frequency is limited to 4MHz. As for the BHD scheme, we chose to use the same rate 4MHz for the performance comparison. Our balanced amplified photo-detector has a flat response passband from DC to 150MHz.

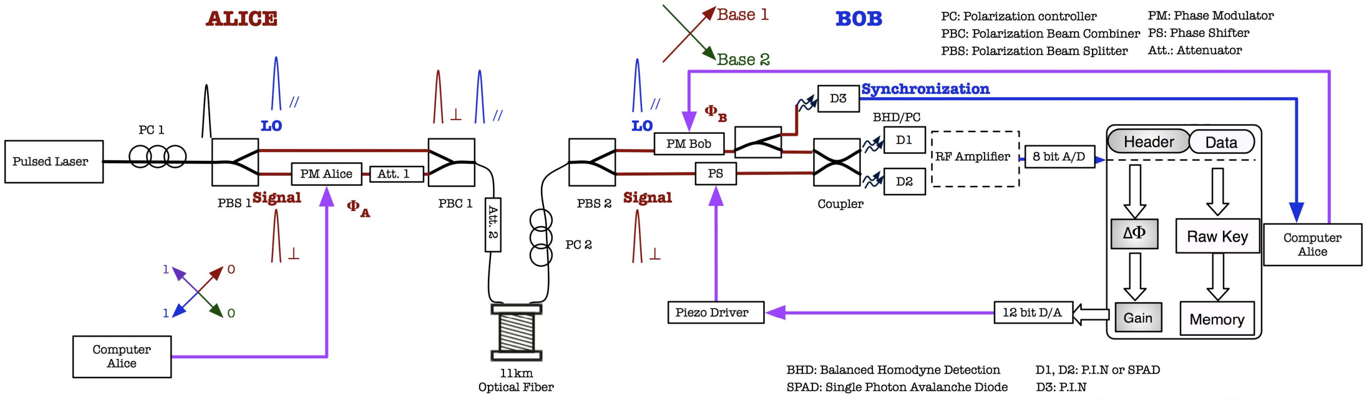

Figure 8. Experimental setup of QKD system using photon counting/BHD

Alice's laser pulses are separated by a polarization-beam-splitter (PBS), then the horizontal component passes through the upper arm and the vertical component passes through the lower arm of a Mach-Zehnder interferometer constructed with polarization maintaining (PM) components. Alice encodes the vertical component of her signal pulses (Φ_A: $\pi/4$ and $-3\pi/4$ in base A1; $-\pi/4$ and $3\pi/4$ in base A2) on a Lithium Niobate phase modulator [21,22], constituting a QPSK modulation. The weak signal and the un-modulated LO pulses are time-multiplexed by a polarization-beam-combiner (PBC). The delay between the two components is set to be 20ns. Since the signal and LO are orthogonally polarized, they propagate with a high degree of isolation despite an extinction ratio of only 30dB. Attenuator 1 is used to generate the weak coherent states (WCS) signal pulses and attenuator 2 is used only in the PC scheme to match the signal and LO relative power levels.

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

Bob's receiver has a similar Mach-Zehnder interferometer structure. He performs the phase shift on the upper arm horizontal LO component on a Lithium Niobate phase modulator to apply his base choice (Φ_B: $\pi/4$ in Base B1, $-\pi/4$ in Base B2), constituting a BPSK conversion. The delay between the signal and LO pulses is also 20ns so that they arrive precisely the same time on the PM coupler and with the same state of polarization (SOP).

A. Phase error compensation

As in all the coherent systems, the phase drift is a main problem caused by the drift in the optical paths of the Mach-Zenhder interferometers. To keep the system unconditionally secured, the QBER threshold must remain under the range of 11% to 17%: with reduced key generation rates, the corresponding phase error is ΔΦ ≈ 27°~41° [32,33].

The phase drift ΔΦ 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 to feedback on the PS. The training frames contain predetermined sequences that Alice and Bob agree on the symbols and bases. The piezo-driver fiber actuator allows a dynamic range $[-8\pi,8\pi]$ for the PSs and a response time of few milliseconds.

1) Phase error compensation for photont counting

In the photon counting scheme, we use two single photon detection modules (SPDM) as D1 and D2 in Figure 8. A short gate operation of 2.5ns is selected, and the output of the SPDM is a pulse of 100ns width when a detection event occurs. We have implemented an 8-bit analogue/digital converter (ADC) for the pulses detection and to record the arrival time of the detected events. A 12-bit digital/analogue converter (DAC) outputs the voltage to be applied on the PS that compensates the phase error. Figure 9 shows our experimental results of the long-term measured real-time phase error and the residual QBER when the mean photon number per pulse N_S is 0.5.

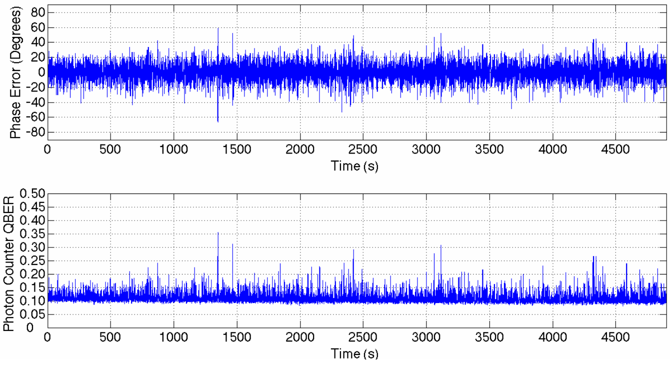

Figure 9. Photon counting system residual phase error and its QBER

2) Phase error compensation for BHD

In the BHD scheme, the LO level is fixed, and the signal level is strongly attenuated with the Attenuator 1. We use a balanced photo-detector together with a flat passband voltage amplifier to obtain an optimized resolution for the high-speed 8-bit ADC PCI transient recorder.

We have performed the measurements of the signal pulses of N_S = 0.02-3.0 photons per bit with strong LO pulses of 2.8x10^5 photons per bit so that the quantum noise is at least 10dB above the thermal noise. We have set 5% of the received bits as the "training frame header" and 95% as the "Data". In Figure 10 we show the comparison of the long-term phase error without phase compensation and with phase compensation feedback when N_S = 0.8.

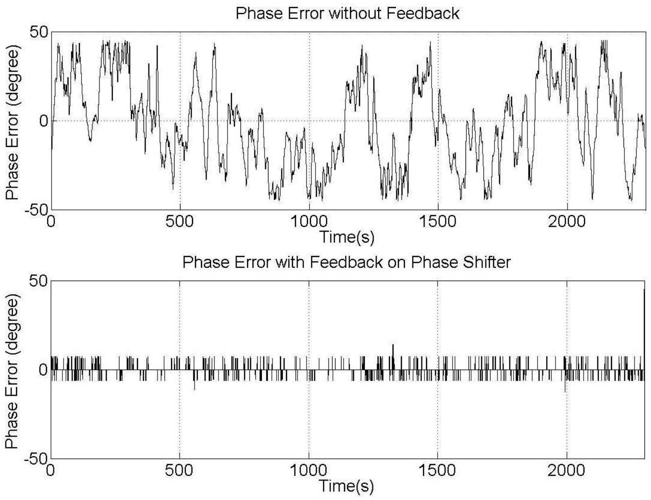

Figure 10. The BHD QKD system real-time phase error

B. Detection effiency measurements

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

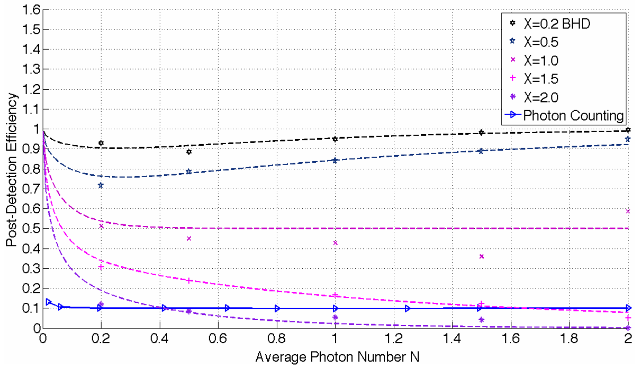

Figure 11. Experimental measurements of the detection efficiency

The experimental results in Figure 11 show that the post-detection efficiency ρ can be higher than the photon counting detection efficiency with appropriate parameters selection. As a matter of fact, even if the selection of a high threshold X decreases the detection efficiency, a high key generation rate is attainable since BHD can potentially operate at much higher speed than PC.

C. Bit error rate measurements

We also measure the post-detection BER for different thresholds ±X, the obtained BER_P as shown in Figure 12 is slightly higher than the theoretical value due to the system quantification errors and the other impairments such as residual polarization mismatch. (Note that when X = 0, it is a standard decision as depicted in equation (1)).

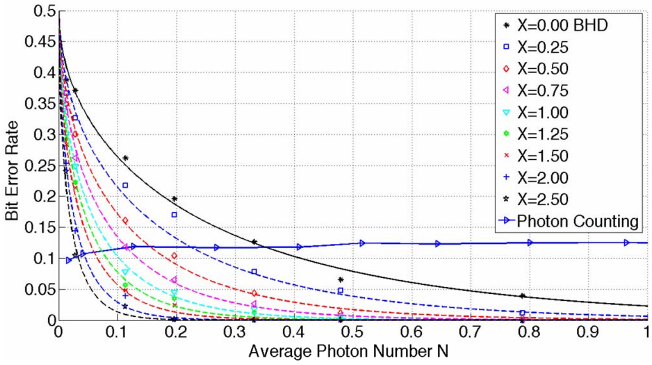

Figure 12. BHD post-detection BER and photon-counting QBER

As for the photon counting (also shown in Figure 12), the QBER is almost constant when the signal photon number N_S is below than 1. 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 attribute to the erroneous detection events are the imperfect coupler visibility and the dark counts. The QBER increases slightly with the average photon number probably due to the after-pulses effects.

Exhibiting higher detection efficiency with no constraints on operation bit rates, the dual-threshold decision BHD can use decoy states in which the signal state intensity can be chosen to be up to one photon per bit on average thanks to a sophisticated reconciliation process [34-38]. The BHD system is readily adaptable for such a protocol since it allows distinguishing the multi-photon coherent states for its higher detection efficiency and its dual-threshold is adjustable according to the quantum key signal levels and the transmission distance.

IV. CONCLUSION

We have implemented an all fiber one-way QPSK optical encoding quantum key distribution system at 1550nm using dual-threshold decision BHD scheme in which the transmission of a strong LO reference is time-multiplexed with key symbols. We have also investigated the security issues of the BHD QKD system under two main individual attacks: intercept-resend attack and intermediate-base attacks. We compared experimentally the performance of photon counting and BHD in terms of detection efficiency and BER. The advantages of BHD QKD scheme over photon counting consist of cost, flexibility, quantum efficiency, potential key generation rate, as well as selective flexibility in the operation regions.

ACKNOWLEDGMENT

We thank for the grant of ANR RNRT HQNET project from French government, we also thank AVANEX for providing laser source that used in our QKD system.

REFERENCES

[1] G. Vernam, "Ciper printing telegraphe systems for secret wire and radio telegraphic communications", Journal American Institute of Electrical Engineering, 1926, Volume XLV, page 109—113.

[2] C.H. Bennett, G. Brassard, "Quantum Cryptography: Public key distribution and coin tossing", Proceeding of IEEE International Conference on Computers, systems, and Signals Processing, 1984, pp. 175-179.

[3] J-M. Mérolla, Y. Mazurenko, J-P. Goedgebuer, H. Porte, W. T. Rhodes, "Phase-Modulation Transmission System for Quantum Cryptography", Optics Letters, Volume 24, No. 2, January 15, 1999.

[4] F. Grosshans, P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States", Physical Review Letters, Vol. 88, Number 5, February 4, 2002.

[5] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, "Quantum cryptography using pulsed homodyne detection", Physical Review A 68, 042331, 2003.

[6] S. Gasel, N. Gisin, G. Ribordy, and H. Zbinden, "Quantum key distribution over 30km of standard fiber using energy-time entangled photon pairs: a comparison of two chromatic dispersion reduction methods", European Phys. J. D 30, 143—148 (2004), March 22, 2004.

[7] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin "Quantum Cryptography Using Entangled Photons in Energy-Time Bell States" Physical Review Letters Volume 84, Number 20, May 15, 2000.

[8] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, "Quantum Cryptography", Reviews of Modern Physics, Vol. 74, January, 2002.

[9] Id Quantique, "Single-photon detection with InGaAs/InP avalanche photodetectors", Single-Photon detector Module: Application note, http://www.idquantique.com.

[10] MagiQ Technologies, Inc., "MagiQ quantum cryptography test bed: uncompromising research results", http://www.magiqtech.com, 2005.

[11] R. J. Glauber, "Coherent and Incoherent States of the Radiation Field", Phys. Rev. vol. 131, no. 6, 1963.

[12] C. W. Helstrom, "Quantum Detection and Estimation Theory, Mathematics in science and Engineering", vol. 123, Academic Press, New York, 1976.

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

[14] T. Okoshi, "Recent advances in coherent optical fiber communication systems", Journal of Lightwave Technology, Volume 5, Issue 1, 44 – 52, Januray 1987.

[15] T. Okoshi and K. Kikuchi, "Coherent Optical Fiber Communications", KTK Scientific, 1988.

[16] J. R. Barry, E. A. Lee, "Performance of Coherent Optical Receivers", Proceedings of the IEEE Vol. 78, NO.8 August 1990.

[17] B. Glance, "Performance of Homodyne Detection of Binary PSK Optical Signals", Journal of Lightwave Technology, Vol. LT-4, No. 2, February 1996.

[18] C. XU, X. Liu, X. Wei, "Differential Phase-Shift Keying for High Spectral Efficiency Optical Transmissions", Invited Paper, IEEE Journal of Selected Topics in quantum electronics, Vol. 10, No. 2, March/April 2004.

[19] K-P Ho, "Phase-Modulated Optical Communication Systems", Springer, 1 edition, 2005.

[20] A. H. Gnauck, and P. J. Winzer, "Optical Phase-Shift-Keyed Transmission", Journal of lightwave technology, Vol. 23, No. 1, January 2005.

[21] Q. Xu, M. B. Costa e Silva, P. Gallion, F. Mendieta, "One Way Differential QPSK Quantum Key with Channel Impairment Compensation", CLEO/Europe-IQEC, JSI-3, 2007.

[22] Q. Xu, M. B. Costa e Silva, P. Gallion, F. Mendieta, "Auto-compensating quantum Crypto-system using homodyne detection". Optical Fiber Communication Conference, OFC 2008, Paper JWA49, San Diego, California, 2008.

[23] J.-P. Marc, G. Brassard, C.H. Bennett, "How to Decrease Your Enemy's Information," in Advances in Cryptology: Proc of Crypto 85, Hugh C. Williams ed., Lecture Notes in Computer Science 218, Springer (Berlin) pp 468-476, 1986.

[24] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert "Privacy Amplification by Public Discussion" S.I.A.M. Journal on Computing 17, 210-229, 1988.

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

[26] R. L. Cook, Paul J. Martin and J. M. Geremia, "Optical coherent state discrimination using a real-time closed-loop quantum measurement", Nature, in press, 2007.

[27] S. Machida; Y. Yamamoto. "Quantum-limited operation of balanced mixer homodyne and heterodyne receivers", IEEE Journal of Quantum Electronics (ISSN 0018-9197), vol. QE-22, p. 617-624, May 1986.

[28] , C. H. Bennett, G. Brassard, J-M. Robert, "Privacy amplification by public discussion", SIAM Journal on Computing, vol. 17, no. 2, pp. 1919 – 1923, 1988.

[29] C. H. Bennett, G. Brassard, C. Crépeau, U. M. Maurer, "Generalized privacy amplification", IEEE Transactions on Information Theory, vol. 41, no. 6, 1995.

[30] M. Koashi, "Unconditional Security of Coherent State Quantum Key Distribution with a Strong Reference Phase Pulse", Phys. Rev. Lett., 93, 120501-1 – 120501-4, 2004.

[31] R. Namiki, T. Hirano, "Security of quantum cryptography using balanced homodyne detection", Phys. Rev. A 67, 022308, 2003.

[32] B. B. Elliott, O. Pikalo, J. Schlafer, G. Troxel, "Path-length control in an interferometric QKD link", Quantum Information and Computation, Proceedings of the SPIE, 5105, pp. 26-38, 2003.

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

[34] W-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication", Phys. Rev. Lett., 91, 057901, 2003.

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

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

[37] H-K. Lo, "Decoy state quantum key distribution", Phys. Rev. Lett., 94, 230504-1-4, 2005.

[38] D. Rosenberg, "Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber", Phys. Rev. Lett., 98, 010503, 2007.