$$\gamma_{n1} = 2z_{n-1} - (z + z') \quad \text{(A5)}$$

$$\gamma_{n2} = (z + z') - 2z_n \quad \text{(A-6)}$$

$$\gamma_{n3} = 2d_n + (z - z') \quad \text{(A-7)}$$

$$\gamma_{n4} = 2d_n - (z - z') \quad \text{(A-8)}$$

$$D^p_n = 1 - \vec{\Gamma}^p_n \vec{\Gamma}^p_n t_n \quad \text{(A-9)}$$

$$\vec{\Gamma}^p_n = \frac{\vec{\Gamma}^p_{n-1,n} + \vec{\Gamma}^p_{n-1} t_{n-1}}{1 + {}^p_{n-1,n} \vec{\Gamma}^p_{n-1} t_{n-1}} \quad \text{(A-10)}$$

$$\vec{\Gamma}^p_n = \frac{\vec{\Gamma}^p_{n+1,n} + \vec{\Gamma}^p_{n+1,n} t_{n+1}}{1 + \vec{\Gamma}^p_{n+1,n} \vec{\Gamma}^p_{n+1} t_{n+1}} \quad \text{(A-11)}$$

$$t_n = e^{-j2k_{zn}d_n} \quad \text{(A-12)}$$

$$d_n = z_{n-1} - z_n \quad \text{(A-13)}$$

$$\vec{\Gamma}^p_{ij} = \frac{Z^p_j - Z^p_i}{Z^p_j + Z^p_i} \quad \text{(A-14)}$$

Here, Z^p_j denotes the characteristic impedance in the media j, the details is in Ref. 2.

Case 2: $m < n$
where

$$V^p_{v,i}(m,z|n,z') = V^p_{v,i}(n,z_{n-1}|n,z')[1 + \vec{\Gamma}^p_m \exp(-2jk_{zm}d_m)]^{-1} \prod_{k=m+1}^{n-1} \vec{T}^{vp}_k \{\exp[-jk_{zm}(z - z_m)] + \vec{\Gamma}^p_m \exp[-jk_{zm}(d_m + z_{m-1} - z)]\} \quad \text{(A-15)}$$

$$I^p_{v,i}(m,z|n,z') = I^p_{v,i}(n,z_{n-1}|n,z') \quad \text{(A-16)}$$

$$[1 - \vec{\Gamma}^p_m \exp(-2jk_{zm}d_m)]^{-1} \prod_{k=m+1}^{n-1} \vec{T}^{ip}_k$$

$$\{\exp[-jk_{zm}(z - z_m)] - \vec{\Gamma}^p_m \exp[-jk_{zm}(d_m + z_{m-1} - z)]\}$$

$$\vec{T}^{vp}_k = \frac{(1 - \vec{\Gamma}^p_k)\exp(-jk_{zk}d_k)}{1 - \vec{\Gamma}^p_k \exp(-2jk_{zk}d_k)} \quad \text{(A-17)}$$

$$\vec{T}^{ip}_k = \frac{(1 - \vec{\Gamma}^p_k)\exp(-jk_{zk}d_k)}{1 - \vec{\Gamma}^p_k \exp(-2jk_{zk}d_k)} \quad \text{(A-18)}$$

Case 3: $m > n$

$$V^p_{v,i}(m,z|n,z') = V^p_{v,i}(n,z_n|n,z')[1 + \vec{\Gamma}^p_m \exp(-2jk_{zm}d_m)]^{-1} \prod_{k=n+1}^{m-1} \vec{T}^{vp}_k \left\{ \begin{array}{c} \exp[-jk_{zm}(z_{m-1} - z)] \\ + \vec{\Gamma}^p_m \exp[-jk_{zm}(d_m + z - z_m)] \end{array} \right\} \quad \text{(A-19)}$$

$$I^p_{v,i}(m,z|n,z') = I^p_{v,i}(n,z|n,z')[1 - \vec{\Gamma}^p_m \exp(-2jk_{zm}d_m)]^{-1} \prod_{k=n+1}^{m-1} \vec{T}^{ip}_k \left\{ \begin{array}{c} \exp[-jk_{zm}(z_{m-1} - z)] \\ - \vec{\Gamma}^p_m \exp[-jk_{zm}(d_m + z - z_m)] \end{array} \right\} \quad \text{(A-20)}$$

where

$$\vec{T}^{vp}_k = \frac{(1 + \vec{T}^p_k)\exp(-jk_{zk}d_k)}{1 + \vec{\Gamma}^p_k \exp(-2jk_{zk}d_k)} \quad \text{(A-21)}$$

$$\vec{T}^{ip}_k = \frac{(1 - \vec{T}^p_k)\exp(-jk_{zk}d_k)}{1 - \vec{T}^p_k \exp(-2jk_{zk}d_k)} \quad \text{(A-22)}$$

REFERENCES

1. J.R. Mosig, Arbitrarily shaped microstrip structures and their analysis with a mixed potential integral equation, IEEE Trans Microwave Theory Tech 36 (1988), 314–323.
2. K.A. Michalski and J.R. Mosig, Multilayered media Green's functions in integral equation formulations, IEEE Trans Antennas Propag 45 (1997), 508–519.
3. F. Ling and J.M. Jin, Discrete complex image method for Green's functions of general multilayer media, IEEE Trans Microwave Guided Wave Lett 10 (2000), 400–402.
4. S.A. Teo, S.T. Chew, and M.S. Leong, Error analysis of the discrete complex image method and pole extraction, IEEE Trans Microwave Theory Tech 51 (2003), 406–413.
5. A.G. Polimeridis, T.V. Yioultsis, and T.D. Tsiboukis, An efficient pole extraction technique for the computation of Green's functions in stratified media using a sine transformation, IEEE Trans Antennas Propag 55 (2007), 227–229.
6. R.R. Boix, F. Mesa, and F. Medina, Application of total least squares to the derivation of closed-form Green's functions for planar layered media, IEEE Trans Microwave Theory Tech 55 (2007), 268–280.
7. Y. Hua and T.K. Sarkar, Generalized pencil-of-function method for extracting poles of an EM system from its transient response, IEEE Trans Antennas Propag 37 (1989), 229–234.
8. I.G. Damousis, A.G. Bakirtzis, and P.S. Dokopoulos, Network-constrained economic sispatch using real-coded genetic algorithm, IEEE Trans Power Syst 18 (2003), 198–205.
9. K.A. Michalski and D. Zheng, Electromagnetic scattering and radiation by surfaces of arbitrary shape in layered media. I. Theory, IEEE Trans Antennas Propag 38 (1990), 335–344.
10. D.C. Wittwer and R.W. Ziolkowski, The effect of dielectric loss in FDTD simulations of microstrip structure, IEEE Trans Microwave Theory Tech 49 (2001), 250–262.

© 2009 Wiley Periodicals, Inc.

HOMODYNE DETECTION OF WEAK COHERENT OPTICAL PULSE: APPLICATIONS TO QUANTUM CRYPTOGRAPHY

Qing Xu, Manuel Sabban, and Philippe Gallion
Ecole Nationale Supérieure des Télécommunications, TELECOM ParisTech, CNRS, LTCI UMR 5141, 46 rue Barrault Paris, 75013 France; Corresponding author: qing.xu@enst.fr

Received 13 November 2008

ABSTRACT: *We propose a quantum key distribution system using balanced homodyne detection, in which strong reference pulses are time-multiplexed with weak signal pulses by means of fiber interferometer.*

We use a dual-threshold decision scheme for postdetection to improve the system performance in terms of BER, with a trade-off in effective key generation rate. We conduct experimental measurements at 64 km SMF fiber at 1550 nm wavelength, and we prove that the system security can also be enhanced with properly selected threshold parameters. © 2009 Wiley Periodicals, Inc. Microwave Opt Technol Lett 51: 1934–1939, 2009; Published online in Wiley InterScience (www.interscience.wiley.com). DOI 10.1002/mop.24471

Key words: *homodyne detection; quantum cryptography; QKD; optical phase-encoding; weak coherent pulses*

1. INTRODUCTION

Quantum cryptography (QC), as a protocol proposed by Bennett and Brassard in 1984 (BB84), is based on the quantum mechanics of single photon and promise unconditional security [1]. QC is also referred as quantum key distribution (QKD) because in the exchange process only the keys can be mutually obtained between Alice and Bob, while no information is divulged.

As the most critical part of a QKD system is the single photon detection, the receiver should not only detect the photon and record the information that it carries but also operates under an almost noise-free condition to minimize the false detection events. A widely used detection scheme at 1550 nm wavelength is photon-counting (PC) using InGaAs/InP APDs that operate in Geiger gated-mode, also called single photon avalanche diode (SPAD). However, SPAD's quantum efficiency is as low as 0.1 at telecom wavelength and the operational frequency is limited to 4–8 MHz due to the quenching process after the macroscopic avalanche.

In search of a high-speed and high-performance QKD system, balanced homodyne detection (BHD) using PIN photodiodes is an ideal alternative to the SPADs for the detection of quantum level signals that consist of weak coherent pluses (WCP), since it allows unity quantum efficiency and potential GHz operation rate [2, 3]. Facilitated by a strong local oscillator (LO) whose noise has only negligible influence compared with the signal quantum noise [4, 5], BHD technique can overcome the nondesirable effects such as after-pulses and dark counts characteristics of SPAD. Furthermore, BHD measures only one signal quadrature at a time and there is no additional noise to the zero-point fluctuation of the signal field. The output noise is thus dominated only by vacuum fluctuation entering in the signal port and a standard quantum limited (SQL) reception is attainable.

From a system perspective, optical WCP can be easily produced by inexpensive and reliable light sources at wavelength 1550 nm where we can take advantage of the low fiber attenuation of the telecom infrastructure, as well as the stable low-cost integrated telecom devices. As for the WCP detection, the coherent BHD receivers can allow lower optical signal-to-noise ratio (OSNR) for a given postdetection bit-error-rate (BER), as well as a better frequency selection efficiency for background radiation rejection in the current WDM networks, since it is also sensitive to phase and polarization matching.

2. DUAL-THRESHOLD QPSK QKD SYSTEM

Homodyne detection allows signal phase encoding more suitable for optical fiber communications than polarization encoding in one-way systems, in which the optical phase and information recoveries are to be solved both by Bob and Eve who have the access to the link. However, a decision process is mandatory at the receiver's end: since the different coherent states transmitted by conventional light sources are not orthogonal, a simple Von Neumann projective measurement cannot conclusively distinguish the different states, thus leading to an inherently finite error rate. In a QKD system bit erasure by empty pulses or more generally by decision abandonment can be managed during the reconciliation process and mainly be turned into reduced key generation rate. In this way homodyne detection can also offer to implement a multilevel decision process on high-level electronic signals [6].

For a symmetric binary phase-shift keying (BPSK) signal, the two signal coherent states can be represented by $|\alpha_1\rangle = |\alpha\rangle$ and $|\alpha_2\rangle = -|\alpha\rangle$. Hence the average signal photon number is $N = |\alpha|^2$, and the signal overlap is $\langle\alpha_1|\alpha_2\rangle = e^{-|\alpha_1-\alpha_2|2} = e^{-4N}$. When a strong local field in phase is used, the detected sum field in the absence of thermal noise results in the following BER [7]:

$$\mathrm{BER} = \frac{1}{2}\mathrm{erfc}(\sqrt{2N}) \tag{1}$$

A phase-encoding QKD system using BHD receiver is first proposed by Hirano's group [2], we have also reported in [6] a dual-threshold BHD system using PIN photodiodes for QPSK signal detection. For signal discrimination Bob sets up two thresholds $-X$ and X for the detected value x. Bob judges the bit as 1 when $x > X$ and as 0 when $x < -X$; otherwise the decision over that bit is abandoned. We assume that all symbols are equally probable, and X is normalized to the root of the average signal photon number $\sqrt{N_s}$. After the reconciliation process, we can obtain the bit error rate BER_i and the bit correct rate BCR_i:

$$\begin{cases} \mathrm{BER}_i = 1/2\mathrm{erfc}[(2N_s)^{1/2}(X+1)] \\ \mathrm{BCR}_i = 1/2\mathrm{erfc}[(2N_s)^{1/2}(X-1)] \end{cases} \tag{2}$$

The postdetection efficiency ρ as the probability of getting a conclusive judgment is:

$$\rho = \mathrm{BER}_i + \mathrm{BCR}_i = 1/2\mathrm{erfc}[(2N_s)^{1/2}(X+1)] + 1/2\mathrm{erfc}[(2N_s)^{1/2}(X-1)] \tag{3}$$

Hence the postselection $\mathrm{BER_P}$ is given by:

$$\mathrm{BER}_P = \mathrm{BER}_i/\rho = \mathrm{BER}_i/(\mathrm{BER}_i + \mathrm{BCR}_i) \tag{4}$$

The implementation of a dual-threshold decision process allows inconclusive results that lower the $\mathrm{BER_P}$ and reduce the key generation efficiency but it still remains far above the SPAD efficiency at the telecom wavelength. In fact, Eve's attack leads more to a Bob's signal degradation than a substitution, making the inclusive bit erasure more efficient than the simple suppression of symbols with base anti-coincidence [1] that is independent of Eve intervention.

3. SYSTEM IMPLEMENTATION

We have implemented a QPSK one-way quantum key distribution (QKD) link for long distance transmission. As shown in Figure 1, QPSK encoding is implemented in our system as four data representations of the two different symbols in two conjugated bases. Alice (Φ_A: $\pi/4$ and $-3\pi/4$ in Base A_1; $-\pi/4$ and $3\pi/4$ in Base A_2) and Bob (Φ_B: $\pi/4$ in Base B_1, $-\pi/4$ in Base B_2) establish a QKD link of 64 km standard telecom single mode fiber (SMF).

The system passively compensates the polarization fluctuations using polarization-maintaining Mach-Zehnder interferometers, and actively cancels out the slow phase drift due to the physical interferometer paths variation using "training frames" that compensates on the receiver Bob's side by an optoelectronic feedback using a phase shifter (PS) in the lower arm. In this system, the

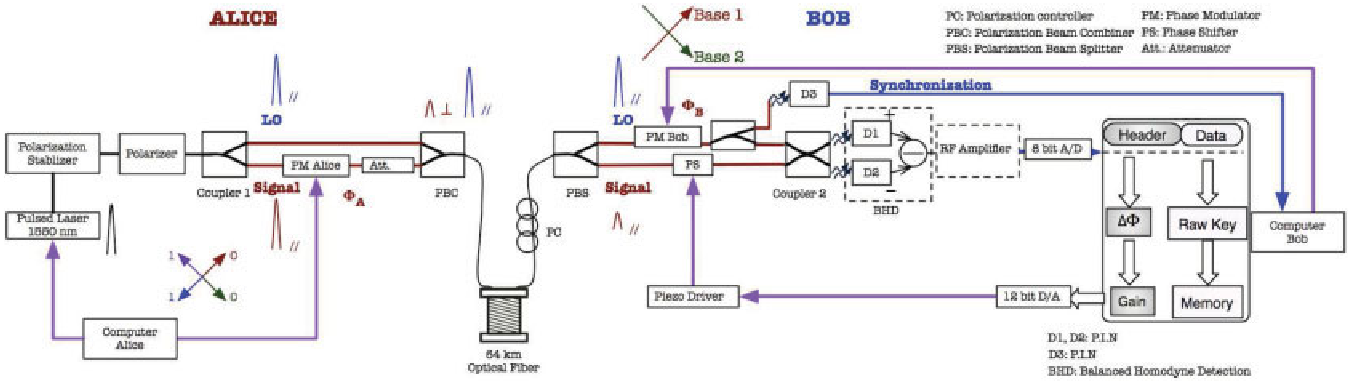

Figure 1 Experimental setup of QPSK QKD system using BHD. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com]

high-level electronic signals allow the implementation of a multi-level BHD decision process.

At Alice's end, we use a 1550 nm externally modulated laser (EML) which combines a distributed feed back (DFB) laser diode with an electro-absorption modulator to generate short pulses of 5 ns width with 25 dB intensity extinction ratio. We also use a polarization stabilizer followed by a polarizer to actively maintain a stable output state of polarization (SOP) with less than 0.1 dB fluctuation and to eliminate polarization fading. Alice's laser pulses are separated by a polarization-maintain coupler, and propagate through the upper and lower arms of a Mach-Zehnder interferometer constructed with polarization maintaining fiber. The weak QPSK modulated Φ_A signal and the strong LO are time-multiplexed with a 20 ns delay by a polarization-beam-combiner (PBC) with 30 dB polarization extinction ratio, before entering into the 1550 nm SMF link. At the receiver Bob's end, the signal and the LO pulses are separated again by a polarization-beam-splitter (PBS), and then enter into a similar delay Mach-Zehnder interferometer. Bob introduces his base choice as Φ_B through another phase modulator (PM Bob) on the upper arm. A portion of the strong LO pulses is used to provide the symbol clock for the system synchronization from the Detector 3. The advantage of this polarization-splitting scheme is to avoid weak signal loss at the receiver's end and to improve the overall extinction ratio in the transmission.

We use a high-speed 8-bit A/D converter for the data acquisition. The normalized quadrature amplitude of the detected signal is proportional to $\cos(\Phi) = \cos(\Phi_A - \Phi_B)$. Base coincidence (BC) occurs when $\Phi = 0$ or π; base anti-coincidence (AC) occurs when $\Phi = \pm\pi/2$.

We compensate the system phase drift $\Delta\Phi$ via an optical feedback on an optical phase shifter (PS) based on piezoelectric transducer acting on the fiber [8]. A periodical interval of M bits in the quantum channel is used as training frames, so as to compute the phase drift in the system and feedback on the PS. The training frames contained predetermined sequences that Alice and Bob agree on the symbols and bases choices prior to the QKD process. We use a phase shifter with $V_\pi = 10V$ and an external driver of $V_{p-p} = 160V$ that allows a dynamic range of $[-8\pi, 8\pi]$ and a response time of several milliseconds. The system auto-resets the PS to zero point when attaining the range limits. As we show in Figure 2, the residual phase error is well controlled below 5 degrees even with very weak signal levels, allowing a stable free-run operation.

4. EXPERIMENTAL RESULTS

4.1. Experimental Measurements at 0 km

We have conducted our first experiments at 0 km in order to compare the system performances of the PC detection scheme using SPAD and the BHD scheme using PIN photodiodes in terms of BER and detection efficiency.

4.1.1. QPSK Signal Histograms. In Figure 3, we depict the experimental histograms of detected QPSK signals; it is only possible to differentiate the phase states 0 and π, since the histograms of $\pm\pi/2$ overlap with each other. Given the signal average photon number per bit N_S, the standard deviations of the 3 histograms are very close to the lower bound given by the phase-number uncertainty principle, i.e. the quadrature amplitude standard deviation is

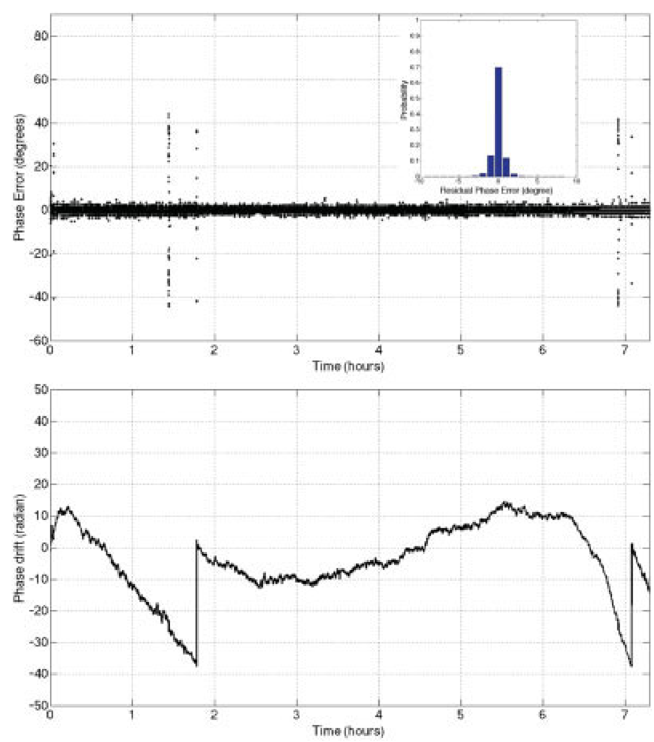

Figure 2 BHD QKD system residual phase error. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com]

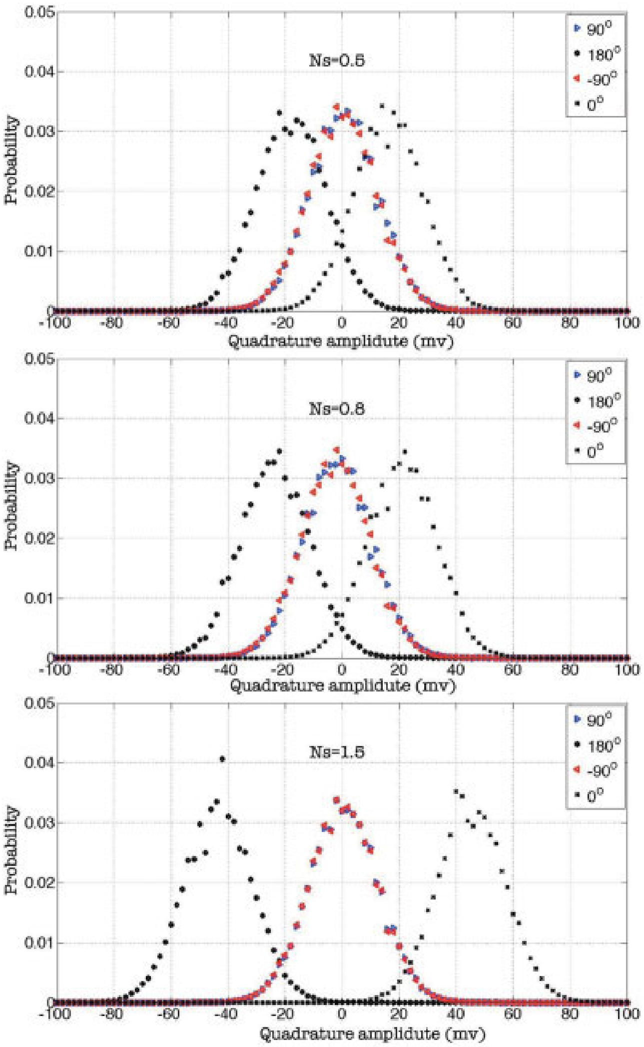

Figure 3 Histogram of the detected QPSK signals with different photon number N_s. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com]

limited by $\Delta N \Delta \Phi \geq 1/2$. Moreover we have obtained uniform histograms of different phase states since quasi-coherent laser source is used.

4.1.2. Experimental BER and Detection Efficiency at 0 km. In the PC scheme, the built-in decision circuit determines the quantum efficiency of SPAD. For comparison we have measured the BHD postdetection efficiency ρ with different threshold parameters X, and the PC detection efficiency at the same repetition rate 4 MHz.

We show in Figure 4 that the postdetection efficiency ρ can be higher 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 high key generation rate is attainable since BHD can potentially operate at much higher speed than PC.

The measured $\mathrm{BER_P}$ values as we show in Figure 5 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 for the photon counting (also shown in Fig. 5), the quantum BER (QBER) is almost constant when the signal photon number

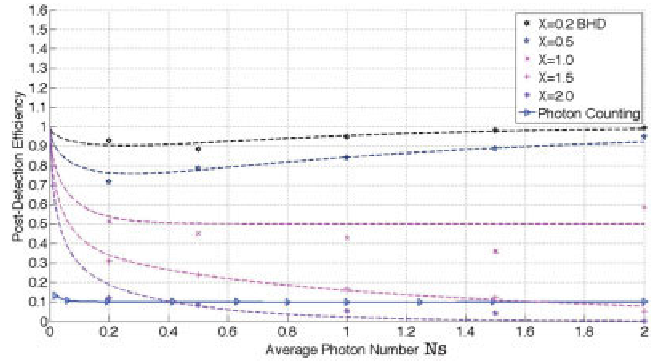

Figure 4 Experimental measurements of the detection efficiency. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com]

N_S is below 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 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 after-pulses 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.

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 $\mathrm{BER_P}$ 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) ultra-high speed QKD system is achievable since no quenching process is required; (c) the cost of telecom wavelength PIN photodiodes is much lower and the supply requirements are much simpler.

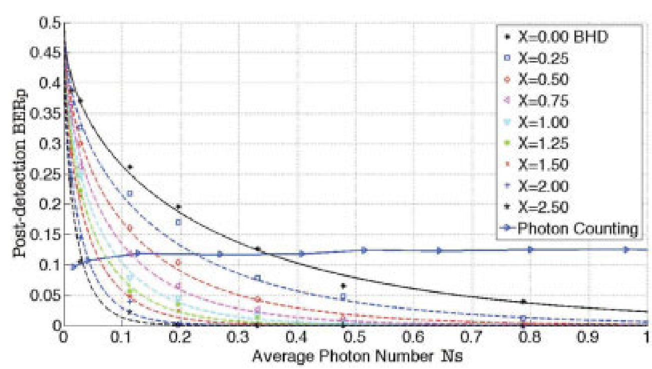

Figure 5 BHD postdetection BER and photon-counting QBER. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com]

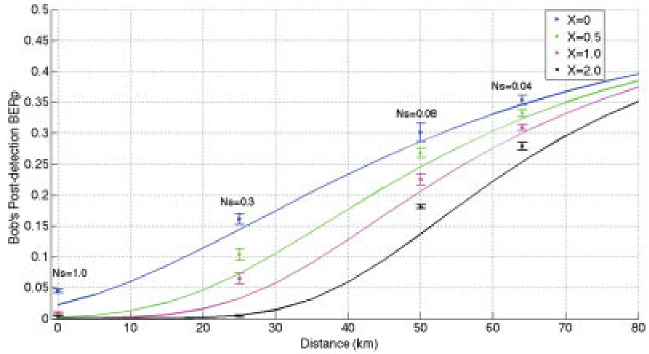

Figure 6 Bob's BER_P evaluation with distance. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com]

4.2. Experimental BER Measurements at Long Distance

Long distance transmission in optical fiber is subject to impairments such as fiber loss of 0.2 dB/km and dispersion of 17 ps/km nm at 1550 nm wavelength, which are the issues that a QKD system has to overcome in a practical and constant field operation. We have performed the experiments with strong LO pulses containing more than 5×10^7 photons, and the inline attenuator at Alice's end is used to adjust the weak signal pulses to mean energy below 1 photon, with a repetition rate of 16 MHz. We have successfully evaluated the system performance with SMF links of 0 km, 25 km, 50 km, and 64 km with different threshold parameters *X*: 0, 0.5, 1, and 2. In Figure 6 we show the experimental postdetection BER_P as compared to the theoretical values. The measured BER_P is slightly higher than the theoretical values due to the connection loss, residual phase fluctuations, and the quantification errors issued from the 8-bit A/D converter. Indeed, the LO pulses attenuate meanwhile with the weak signal pulses in the SMF link, e.g., at 64 km we have measured a transmission loss of 16.5 dB, i.e., the signal mean photon number is actually attenuated to $N_S = 0.04$. In principle the quantum noise is lower than the thermal noise from 90 km, which imposes a transmission limit. Hence, setting a higher dual-threshold is necessary and beneficial to obtain its optimal throughput as a tradeoff in the effective key generation rates, which is still much higher than that of SPDM since there is no operation frequency limit for BHD.

5. SECURITY ANALYSIS

In order to investigate the security of a quantum cryptosystem, we have to take into account the action of Eve and 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 conditional entropies of Bob and Eve are defined as $H(A|B)$ and $H(A|E)$, assuming that Alice's information is known. The mutual information *I(A,B)*, *I(A,E)* are defined as the estimation of the amount of information shared by Alice and Bob, and that shared by Alice and Eve, respectively. Note that Eve is assumingly only limited by the physical laws.

$$\begin{cases} I(A,B) = H(A) - H(A|B) \\ I(A,E) = H(A) - H(A|E) \end{cases} \quad (5)$$

The key is said to be secure if *I(A,B)* is higher than *I(A,E)* [9, 10]. However, under attacks such as photon-number-splitting (PNS) [11], the eavesdropper (Eve) can theoretically have the full information of Bob's sifted key, hence at Bob's side the detection of Eve is critical especially for long distance transmission. During the key exchange process, Bob must discern the real-time BER_P variations so as to detect Eve's attacks and to guarantee the security.

In Figure 7 we show that Bob's BER_P is largely modified under the intercept-resend, intermediate base and PNS attacks. As we have pointed out in [6, 12], under intercept-resend attack Bob can select a higher *X* value to maintain the information gain over Eve, while no information gain can be obtained under intermediate base and PNS attacks. In this case Bob can discern Eve's attacks by comparing the operating BER_P with the theoretical BER_P at the receiver's Bob end. Under a more advanced extended PNS attack proposed by Lütkenhaus and Jahma[13] in which Eve hides her presence by stealing only multi-photon pulses, a multi-states protocol similar to decoy states [14, 15] can be used to observe the detection efficiency ρ variations using higher photon number pulses and single photon pulses.

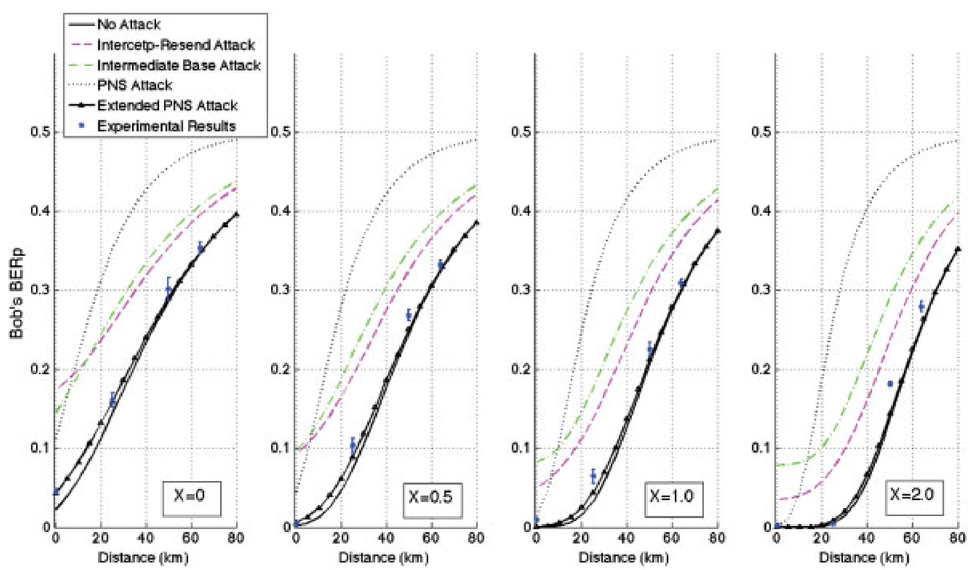

Figure 7 Bob's postdetection BER under divers attacks. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com]

6. CONCLUSION

We have implemented an experimental 1550 nm QPSK QKD system using BHD scheme for long distance transmission, with automatic polarization and phase fluctuation compensations. We have used a dual-threshold decision for the signal postdetection to enhance the system performance in term of BER by discarding the inconclusive bits. The experimental results have well conformed to the theoretical values and have proved the scheme's feasibility of a high-speed field operation.

We have also measured the postdetection efficiency ρ, BER_p, and conducted the security analysis under divers attacks for different threshold parameters X at 0 km, 25 km, 50 km, and 64 km. The trade-off is between the system security tolerance and the key generation rate: use a higher threshold when the transmission distance is longer or when the WCP is weaker. Accordingly, we have proposed the strategies to detect Eve's attacks by BER_p evaluations.

REFERENCES

1. C.H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, In: International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, pp.175–179.
2. T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, Quantum cryptography using pulsed homodyne detection, Phys Rev Lett A 68 (2003), 042331.
3. Q. Xu, M.B. Costa e Silva, J.L. Danger, S. Guilley, P. Bellot, P. Gallion, and F. Mendieta, Towards quantum key distribution system using homodyne detection with differential time-multiplexed reference, In: Fifth IEEE International Conference on Information and Communication Technologies, RIVF, Vietnam, 2007.
4. H.P. Yuen and V.W.S. Chan, Noise in homodyne and heterodyne detection, Opt Lett 8 (1983), 177–179.
5. P. Gallion, F.J. Mendieta, and S. Jiang, Signal and quantum noise in optical communcation and in cryptography, Prog Optics 52, 2008.
6. Q. Xu, M. Sabban, P. Gallion, and F.J. Mendieta, Quantum key distribution system using dual-threshold homodyne detection, In: Sixth IEEE International Conference on Information and Communication Technologies, RIVF, Vietnam, 2007.
7. C.W. Helstrom, Quantum detection and estimation theory, mathematics in science and engineering, Vol. 123, Academic Press, New York, 1976.
8. Q. Xu, M.B. Costa e Silva, P. Gallion, and F.J. Mendieta, Auto-compensating quantum crypto-system using homodyne detection, OFC 2008, JWA49, San Diego, CA, 2008.
9. M. Koashi, Unconditional security of coherent state quantum key distribution with a strong reference phase pulse, Phys Rev Lett 93 (2004), 120501.
10. R. Namiki and T. Hirano, Security of quantum cryptography using balanced homodyne detection, Phys Rev A: At Mol Opt Phys 67 (2003), 022308.
11. G. Brassard, N. Lütkenhaus, T. Mor, and B.C. Sanders, Limitations on practical quantum cryptography, Phys Rev Lett 85 (2000), 1330.
12. Q. Xu, M. Sabban, M.B. Costa e Silva, P. Gallion, and F.J. Mendieta, Dual-threshold balanced homodyne detection in 1550nm optical fiber quantum cryptography system, submitted.
13. N. Lütkenhaus and M. Jahma, Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack, New J Phys 4 (2002), 44.
14. W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, Phys Rev Lett 91 (2003), 057901.
15. D. Rosenberg, Long-distance decoy-state quantum key distribution in optical fiber, Phys Rev Lett 98 (2007), 010503.

© 2009 Wiley Periodicals, Inc.

COMPACT PLANAR MONOPOLE ANTENNA FOR 3G AND UWB APPLICATIONS

Mohamed Nabil Srifi,[1] Vamsi Krishna Palukuru,[2] Mohamed Essaaidi,[1] and Heli Jantunen[2]

[1] Electronics And Microwaves Group, Abdelmalek Essaadi University, Tetuan, Morocco; Corresponding author: essaaidi@ieee.org

[2] Microelectronics and Materials Physics Laboratories, and EMPART Research Group of Infotech Oulu,University of Oulu, Finland

Received 18 November 2008

ABSTRACT: *This article presents a compact printed monopole antenna for 3G and UWB mobile and wireless communication systems. The antenna consists on printed microstrip arms on a Rogers' substrate with a slotted partial ground plane. The size of the antenna is only 16 mm × 36 mm × 0.83 mm. The simulated and measured results show very good agreement.* © 2009 Wiley Periodicals, Inc. Microwave Opt Technol Lett 51: 1939–1942, 2009; Published online in Wiley InterScience (www.interscience.wiley.com). DOI 10.1002/mop.24462

Key words: *multiband antenna; monopole antenna; partial ground plane; 3G; ultra wideband*

1. INTRODUCTION

During the last few years, interest in internal antennas, such as Microstrip Patch antenna (MSA), has rapidly increased in mobile communication systems due to its attractive features as follows: small size and compact, low specific absorption rate (SAR), low cost, and easily integrated into planar circuit [1–5].

Design of antennas operating in multiband [6–9] allows the wireless devices to be used with only a single antenna for multiple wireless applications, and thus permits to reduce the size of the space required for antenna on the wireless equipment. The MSA plays an important role in the development of the new generation of wireless and mobile communication systems.

Ultra-Wide Band (UWB) wireless communication systems are defined as any radio system that has a −10 dB bandwidth larger than 25% with respect to the center frequency [10]. Due to the attractive advantages of wide frequency bandwidth, these communication systems have recently received great attention in the wireless technology domain.

Telecommunications-2000 (IMT-2000) standard was developed by the International Telecommunications Union (ITU). The 3G frequencies for the IMT-2000 mobile system were identified by the ITU at the 1992 World Administrative Radiocommunications Conference (WARC 92) [11]. The 1885–2025 MHz and 2110–2200 MHz bands are intended for use by administrations wishing to implement the IMT-2000 system. Terrestrial IMT-2000 services will operate in the frequency-division duplex (FDD) mode in the 1920–1980 MHz bands paired with 2110–2170 MHz for mobile stations transmitting in the lower sub-band and base stations transmitting in the upper sub-band [12]. It is suitable for the 3G mobile handset antennas to satisfy the bandwidth (BW) in the range of the proposed 1885–2025 MHz uplink and 2110–2200 MHz downlink (15.4% impedance BW if the frequency spectra from 1885 to 2200 MHz are fully covered).

The main benefit of the IMT-2000 is that it offers high-end service capabilities, which include substantially enhanced capac-