Auto-compensating Quantum Cryptosystem using Homodyne Detection

Q. Xu[a], M. B. Costa e Silva[a], P. Gallion[a], and F. J. Mendieta[a,b]
[a]*Ecole Nationale Supérieure des Télécommunications, Paris, 75013 France*
[b]*on leave from CICESE, km.107 Carr. Tijuana, Ensenada, Baja California 22800, México*
**Corresponding author: qing.xu@enst.fr*

Abstract: We implement an experimental quantum cryptosystem using standard 1550nm channel devices with auto-compensation for phase instabilities in which balanced homodyne detection employs a time-multiplexed strong reference. We use a dual-threshold to improve QBER.

OSC codes: 060.1660, 060.2920, 270.5568, 270.2500

1. Introduction

Quantum cryptography, as a system that guarantees unconditional security of communications [1], has been extensively studied recently in the search for high-speed, long distance operational scheme that is compatible with optical networks. The key issue in a quantum cryptosystem is the detection of quantum level Qbits, such as the reliable and inexpensive weak coherent pulses (WCP) that are widely used instead of the immature single photon sources.

Balanced homodyne detection (BHD) 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. It operates near the quantum limit, and it is potentially capable to overcome non-desirable effects such as afterpulses and "dark counts" characteristics of single photon detection measurement (SPDM) [2]. BHD, using high efficiency, high bandwidth and low cost PIN photodiodes operating at room temperature, is also sensitive to phase and polarization matching, this leads to a frequency selection scheme that is useful for background radiation rejection as for the compatibility with the current WDM networks. Optical phase and information recoveries are to be solved both by Bob and Eve, as well the higher-level electronic signals offer to implement a multilevel BHD decision process.

After receiver Bob's base selection, the detection of QPSK (2 symbols in each of the 2 bases) constellation turns to BPSK detection. For binary phase-shift keying (BPSK) signal, the two signal coherent states are $|\alpha_1\rangle = |\alpha\rangle$ and $|\alpha_2\rangle = -|\alpha\rangle$. The average signal photon number is $N_S = |\alpha|^2$, thus the signal overlap is $\langle\alpha_1|\alpha_2\rangle = e^{-|\alpha_1-\alpha_2|^2} = e^{-4N_S}$. When a strong local in phase field is used, the detected sum field using intensity detection in the absence of thermal noise results in the probability of error [3]: $BER = 1/2\,erfc\left(\sqrt{2N_S}\right)$.

Since a complete differentiation of the received states is not possible, an inherently finite error rate is obtained. This finite error rate is easy to calculate and can be as low as 8% for 0.1 average photon number pulses when an appropriate detection scheme. Such a result is obtained by the implementation of a double decision process with a compromise in inconclusive results, which reduces the efficiency of the key production, however it remains far above the photon counter efficiency at the telecom wavelengths.

2. System Implementation

We have implemented a QPSK one-way quantum key distribution (QKD) link. As shown in Fig.1(a), QPSK encoding is implemented in our system as 4 data representations of the 2 different symbols in 2 conjugated bases [4,5]. Alice (Φ_A: π/4 and -3π/4 in Base A_1; -π/4 and 3π/4 in Base A_2) and Bob (Φ_B: π/4 in Base B_1, -π/4 in Base B_2) establish a QKD link of 11km length in a standard telecom single mode fiber.

At Alice's end, the laser pulses are separated by a polarization-beam-splitter (PBS). The weak QPSK modulated Φ_A signal and the strong LO are time-multiplexed by a polarization-beam-combiner (PBC) after a delay Mach-Zehnder interferometer. At the receiver Bob's end, the signal and the LO pulses are separated again by a PBS, and then enter into a similar delay Mach-Zehnder interferometer. Bob introduces his base choice as Φ_B through the PM-B (phase modulator Bob) on the same arm. The symbol "clock" is provided by the direct detection of the strong LO pulses for the system synchronization at the Detector 3.

An unavoidable problem for such a configuration is the phase drift due to the fluctuations in the interferometer paths [6,7], such as 2 rad/min in our system typically. This phase drift $\Delta\Phi$ is compensated by an optical feedback sub-system using the phase shifter (PS) based on a piezoelectric transducer acting on the fiber. A periodical interval of *N* bits in quantum channel is used as "training frames" so as to compute the phase drift in the system and

978-1-55752-855-1/08/$25.00 ©2008 IEEE

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 a V_π=10V and an external driver of $V_{p\text{-}p}$=150V allowing a dynamic range of 15π and a response time of several milliseconds.

Using WCP, the individual outputs of the BHD with *N* independent samples, according to the central limit theorem, follow the normal distribution $N\left(\mu,\sigma/\sqrt{N}\right)$. Where an uncertainty in amplitude estimation less than error E, then the following condition must be met:

$$erfc\left(\sqrt{2N}/2\sigma\right)\approx 2\exp\left(-N/2\sigma^2\right)<E \tag{1}$$

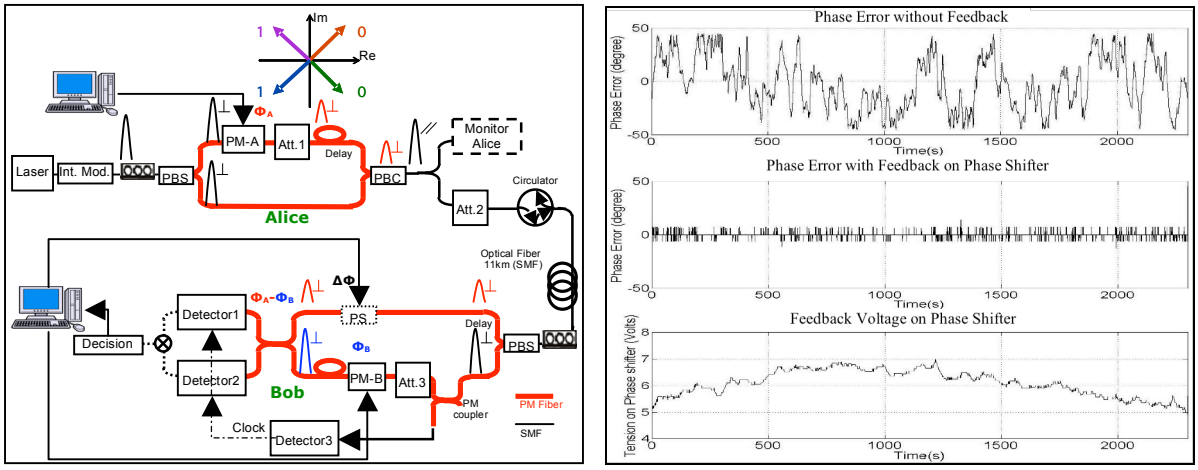

Fig. 1 (a) Experimental setup of quantum cryptosystem; Fig.1 (b) The system phase error: without feedback (up), with feedback (middle) and the applied voltages on the phase shifter (low) that keeps the phase error below 5°.

We use a high-speed 8-bit A/D converter for 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 $\Phi = \pi/2$ or $-\pi/2$. Since the BHD detects only one field quadrature at a given time, it is only possible to differentiate $\Phi = 0$ and π (conversion to BPSK), as shown in the histogram in Fig.2(a) (inset).

For the signal value $|\alpha|^2\cos(\Phi)$, the Heisenberg uncertainty principle gives a lower bound on the product of the standard deviations of coherent states $\Delta|\alpha|^2\Delta\Phi \geq 1/2$. 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 average photon number N_S. After the reconciliation process, only those BC bits would be retained, so the effective decision is made only for $\Phi = 0$ and π, we can obtain the standard bit error rate (BER), and the bit correct rate (BCR):

$$\begin{cases} BER_i = 1/2\,erfc\left[\left(2N_S\right)^{1/2}\left(X+1\right)\right] \\ BCR_i = 1/2\,erfc\left[\left(2N_S\right)^{1/2}\left(X-1\right)\right] \end{cases} \tag{2}$$

Hence the post-selection error rate is: $BER_p = BER_i/\rho = BER_i/\left(BER_i + BCR_i\right)$, where ρ is the detection efficiency.

3. Experimental results

We have performed the experiments with an ILM (integrated laser/modulator) electro-absorption modulated light source to generate laser pulses of 5ns at 8MHz. The phase compensation feedback loop allows free operation without manual adjustment; we have tested with signal pulse power of 0.2-1.5 photons/bit and the LO pulses power of $2.8\text{x}10^5$ photons/bit for different threshold parameters X. Fig.2(a) is a plot of post-detection efficiency ρ and the histogram of the detected QPSK signal with measured standard deviation close to ½. The measured BER_P as in Fig.2(b) is slightly higher than the theoretical values since the QPSK modulation signal constellation was difficult to be maintained with good precision and the interferometer visibility was imperfect due to residual polarization mismatch; the 8-bit A/D converter produced quantification errors as well. Hence a higher threshold is necessary and

beneficial for a weaker signal to obtain its optimal throughput as well as a more secured raw key with a tradeoff in the effective key generation rate.

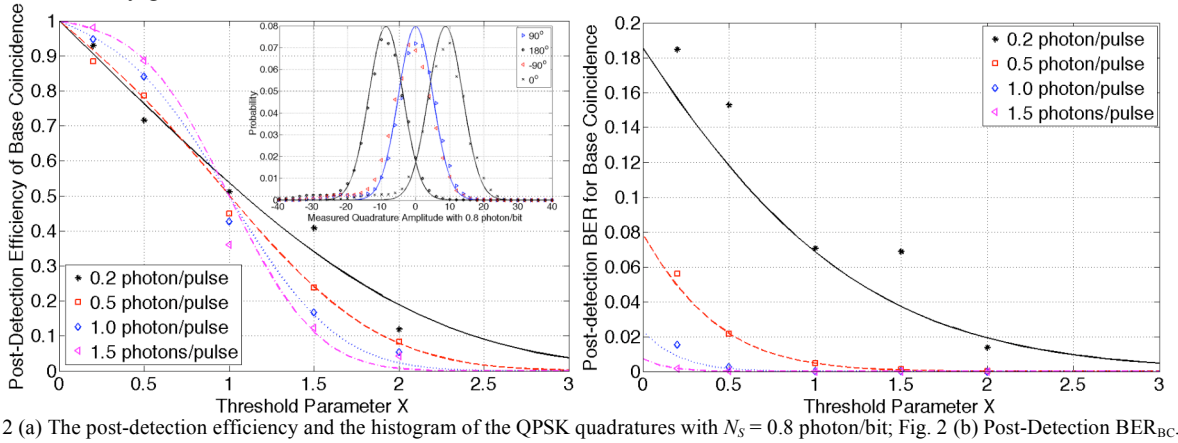

Fig. 2 (a) The post-detection efficiency and the histogram of the QPSK quadratures with N_S = 0.8 photon/bit; Fig. 2 (b) Post-Detection BER_{BC}.

4. Comparison between BHD and SPDM for QKD

We now compare the performance of the BHD receiver with the typical SPDM schemes that use cooled Geiger-mode avalanche photodiodes [8]. For example, when $N_s = 0.5$ and $X = 1$, the post-detection efficiency is $\rho = 0.5$ with $BER_P < 1\%$ with no constraints on the operational frequency. As for the SPDM schemes, the detection efficiency is below 0.1 and most reported *QBER* values are between 0.5% and 5%, and the operational frequency is limited to less than 4MHz by after-pulse effects. Besides, the inevitable problem in SPDM is the "dark counts" and the *QBER* is related directly to the fringe visibility of the interferometer that is more sensitive to the polarization variation. Hence our scheme outperforms in terms of cost, key generation rate as well as the system flexibility.

As a final comment, for an operational long-distance QKD system, the decoy-state protocol has been proposed [9] that allows signal states intensity close to 1 photon/bit on average. Our system can also be readily adapted for such method since it allows distinguishing the multi-photon coherent states.

5. Conclusion

We have implemented an experimental all fiber QPSK quantum key distribution system set-up at 1550 nm using balanced homodyne detection with interferometer path-length auto-compensation in which the phase errors are computed and compensated with small intervals of training frames.

A two-threshold decision scheme is used for the signal post-detection to enhance the system performance in term of bit error rate by discarding the inconclusive bits. The experimental results of ρ and BER_P for different thresholds X are close to the theoretical values and have proved the scheme's feasibility of a high-speed field operation. The optimal threshold values are to be found according to the transmission distance or WCP intensity.

This work was done with a grant from the French ANR, HQNET project.

6. References

[1] C. H. Bennett, G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", International Conference on Computers, Systems & Signal Processing, Bangalore, India, pp. 175-179, (1984)

[2] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, R. Namiki, "Quantum cryptography using pulsed homodyne detection", Phys. Rev. Lett, A 68, 042331-1 – 042331-7, (2003)

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

[4] M.B. Costa e Silva, Q. Xu, S. Agnolini, P. Gallion, F. J. Mendieta, "Integrating a QPSK Quantum Key Distribution Link", ECOC 2006 Conference Proceeding, Cannes, France, (2006)

[5] 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)

[6] 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)

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

[8] Q. Xu, M. B. Costa e Silva, J-L. Danger, S. Guilley, P. Bellot, P. Gallion, F. Mendieta, "Towards Quantum Key Distribution System using Homodyne Detection with Differential Time-Multiplexed Reference", 5th IEEE Int. Conf. on Information & Comm. Tech. RIVF (2007)

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