INTEGRATED DIRECT-MODULATION BASED QUANTUM CRYPTOGRAPHY SYSTEM

Johann Cussey[1], Matthieu Bloch[2], Jean-Marc Merolla[1] and Steven.W McLaughlin[2]
[1] *GTL-CNRS Telecom UMR 6174, 2-3 rue Marconi 57070 Metz, France,*
jcussey@georgiatech-metz.fr
[2] *Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, Georgia, USA,*
mbloch@georgiatech-metz.fr

Abstract: We report a new quantum key distribution scheme using direct-modulation method associated with single sideband detection (SSB). Experiments were carried out at 850 nm using standard electronic and optical components.

1. INTRODUCTION

Quantum cryptography or quantum key distribution (QKD) has known an increasing interest because it offers higher security than public-key based key transfer systems [1]. Several systems [1-4] have been developed to exchange quantum keys via optical fibres, achieving key distribution up to 100km [5]. In a recent experiment [6], a 23km key transmission was performed in free space, hence demonstrating the feasibility of QKD for ground-to-ground or space application. However, only one method based on polarization-coded quantum states has been explored to realize free-space key distribution.

We report a new free-space transmission quantum key distribution method, using a direct-modulation technique associated to a single sideband detection method [7]. The use of directly modulated laser diodes and standard electronical components at the emitter enables suitable integration and thus offers potential

satellite-to-ground applications. The experimental prototype operates at 850nm using off-the-shelf components.

2. PRINCIPLE

Figure 1 shows the proposed system.

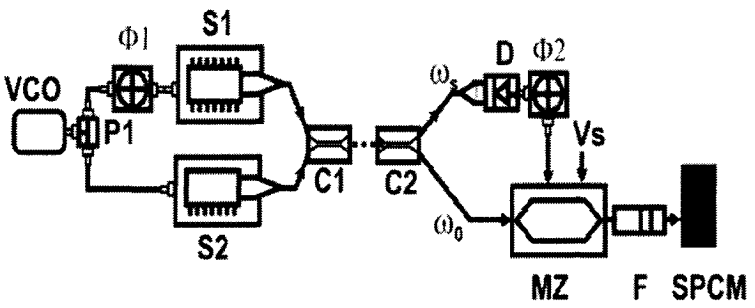

Figure 1. Schematic diagram of the direct modulation scheme.

The source (S1) is an attenuated laser diode operating at optical frequency ω_0 (quantum signal). S1 is directly modulated at $\Omega << \omega_0$ with a modulation depth $m<<1$. The modulating signal is produced by a voltage controlled oscillator (VCO) that drives simultaneously a second laser diode S2 operating at optical frequency ω_s. Both optical signals are transmitted thanks to a WDM coupler (C1). Their optical spectra are composed of a central peak and two sidebands at frequencies $\omega_0 \pm \Omega$ ($\omega_s \pm \Omega$) with phase Φ_1 *(0)* relative to the central peak. The phase Φ_1 is introduced by a phase shifter. At the receiver, a WDM demultiplexer (C2) separates the transmitted signals. The synchronisation signal is converted by a detector (D) that generates an electrical signal at frequency Ω. The amplitude of the electrical signal is matched to the emitter modulation depth m and drives an unbalanced integrated Mach-Zehnder modulator (MZ). An additional phase shift Φ_2 is introduced thanks to a second phase shifter. The bias voltage Vs is matched to the chirp value of the source S1 such that the probability P_1 and P_2 of detecting one photon in the lower and the upper sidebands of the quantum signal are respectively governed by a sine-squared and a cosine-squared function of the phase difference (Φ_1-Φ_2). The sidebands are separated by an optical filter (F) and photons are counted by a single photon counting module (SPCM). The BB84 protocol can then be implemented with only one detector as shown in [8].

3. EXPERIMENT

The experimentals circuits are shown in figure 2 and 3. The actual prototype size emitter (fig.2) is 15x10 cm .The quantum signal is generated by a 1mW, 852nm DBR laser diode. The modulation amplitude is set to $m \approx 0.3$V thanks to an integrated VCO and amplifier (RF circuit). Calibrated attenuators attenuate the light so that with the chosen value of m, the average photon number sent in the fibre is approximately 0.21 photon per pulse in each modulation sideband. The operating frequency is 2GHz. The synchronisation signal at 2GHz is produced by the same VCO and modulates a standard CATV DFB laser (DMDFB) emitting at 1310 nm.

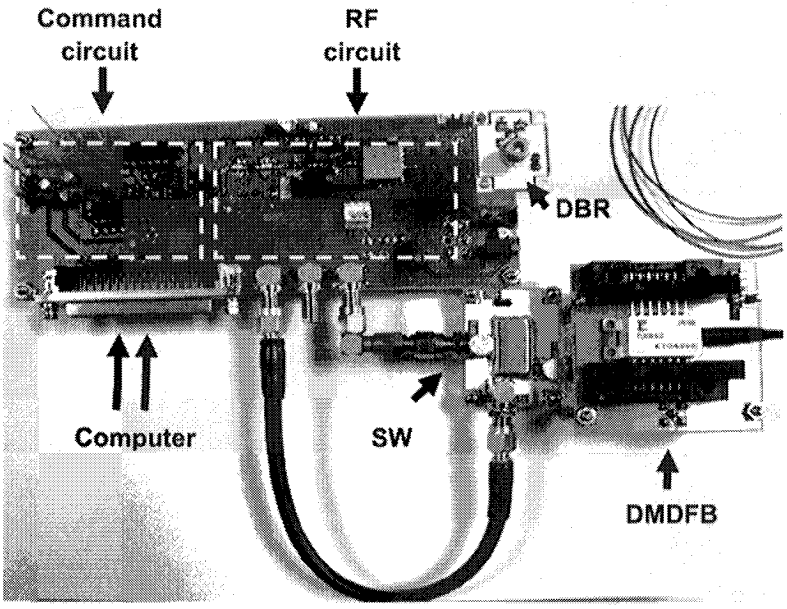

Figure 2. Prototype of the emitter.

Its average power was set to 10 μW to avoid crosstalk with the quantum signal. At the emitter a computer controls a quadrature phase-shift-keying (QPSK) modulator (including in the RF circuit) to introduce a phase variation Φ_l , randomly chosen among four possible values. An additional square-modulation at 1MHz is mixed with the synchronization signal to be used as a clock thanks to an external RF switch (SW). The command circuit converts the digital signal generated by the computer into the required analog signal.

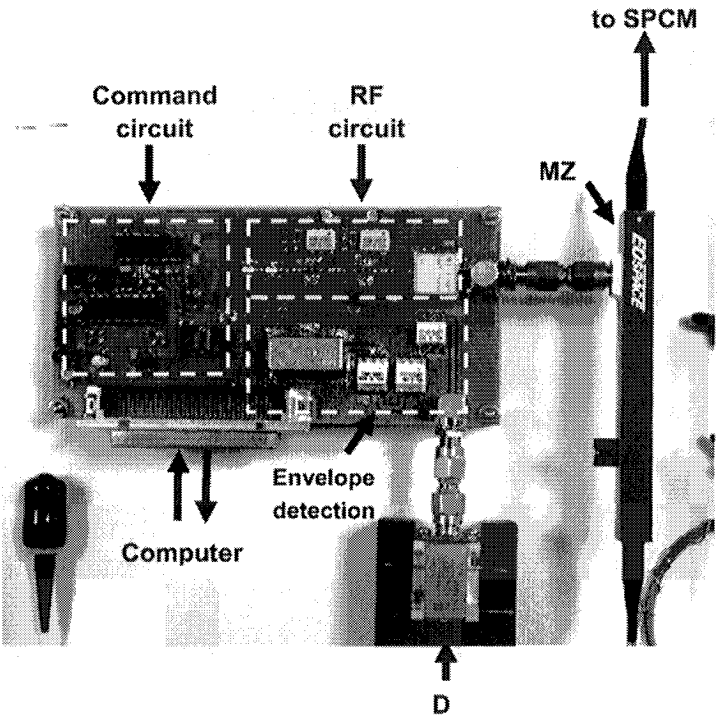

Figure 3. Prototype of the receiver.

At the receiver (fig.3), the quantum and the synchronization signal are separated by a 30dB isolating WDM demultiplexer (not shown in fig 3). The synchronisation signal is first converted into an electrical signal by a standard detector (D). The resulting electrical signal is then split and filtered in two different ways to obtain in one case the plain 2GHz frequency and in the other case the 1MHz square envelope. This 1MHz clock is used to switch randomly and synchrounously the phase Φ_2 among four possible values and generates a 50ns duration gate that allows the EGG single photon counting module to be gated. In these conditions the quantum efficiency and the dark count per gate are 50% and 1.10^{-6}. We use a customized $LiNbO_3$ intensity modulator (MZ) and fibre Fabry-Pérot interferometer (composed of two bragg gratings, not shown in fig 3) with a FSR of 10GHz and a finesse of 100 to select only one sideband. Quantum signal was detected by a SPCM. Key distributions have been performed with a 100m single mode fibre at 850nm. The reconciliation process [9,10] uses a LAN connection as the public channel. The global attenuation of the receiver was around

6dB at 850nm. The quantum bit error rate (QBER) measured was thus found to be around 1% for a raw bit rate of 5Kc/s.

4. CONCLUSION

We have reported a new direct modulation method using a SSB detection scheme. Unlike a recent free space polarization based QKD experiment [11], the synchronisation and quantum signal used the same transmission channel. The first results obtained show the possible used of our method in free space transmission. Finally, the laser diodes can be replaced by VCSEL sources allowing future on-chip integration of the emitter with hybrid CMOS VLSI [12] electronic circuits. This work is under progress.

ACKNOWLEDGMENTS

I wish to thank Samuel Moec for his invaluable help during the design of electronic circuits. This work was supported by FRANCE TELECOM under contrat N°: 991B489 and is protected under patent number : WO 02/049267 A1.

REFERENCES

[1] C.H.Bennett, F.Bessette, G.Brassard, L.Salvail and J.Smolin, "Experimental quantum cryptography", *Journal of Cryptology*, 5 (1992), 3.

[2] A. Muller, H. Zbinden and N. Gisin, "Quantum cryptography over 23 km in installed under-lake telecom fibre", *Europhysics Letters*,33 (1996), 335-339.

[3] P.D. Townsend, J.G. Rarity and P.R. Tapster, "Single photon interference in 10 km long optical fibre interferometer", *Electronics Letters*, 29 (1993), 634-635.

[4] R.J. Hughes, G.L. Morgan and C.G. Peterson, "Quantum key distribution over a 48-km optical fiber network," *Journal of Modern Optics*, 47 (2000), 533-547.

[5] H.Kosaka, A.Tomita, Y.Nambu, T.Kimura and K.Nakamura, "Single-photon interference experiment over 100 Km for quantum cryptography system using balanced gated-mode photon detector", *Electronics letters*, 39 (2003), 1199-1201.

[6] C. Kurtsiefer, P. Zarda, M. Halder, P.M. Gorman, P.R. Tapster, J.G. Rarity and H. Weinfurter, "Long distance free-space quantum cryptography", *Proceedings of the SPIE*, 4917 (2002), 25-31.

[7] O.L. Guerreau, J.-M. Merolla, A. Soujaeff, F. Patois, J.-P. Goedgebeur, F.J. Malassenet, "Long-distance QKD transmission using single-sideband detection scheme With WDM synchronization", *Journal of Selected Topics in Quantum Electronics*, 9 (2003), 1533-1540.

[8] P. Moller, C. Schori, J.L. Sorensen, L. Salvail, I. Damgard and E. Polzik, " Experimental quantum key distribution with proven security against realistic attacks", *Journal of Modern Optics*, 48 (2001), 1921-1942.

[9] G. Gilbert and M. Hamrick, " Secrecy, Computational Loads and Rates in Practical Quantum Cryptography " , *Algorithmica*, 34 (2002), 314.

[10] D. Gottesman and H.-K. Lo, "Proof of security of quantum key distribution with two-way classical communications", *IEEE Transactions on Information Theory*, 49 (2003), 457.

[11] J.C. Bienfang, A.J. Gross, A. Mink, B.J. Hershman, A. Nakassis, X.Tang, R.Lu, D.H. Su, C.W.Clark, C.J. Williams, E.W. Hagley, J. Wen "Quantum key distribution with 1.25 Gbps clock synchronization", *Optics Express*, 12 (2004), 2011-2016.

[12] A.V. Krishnamoorthy and D.A.B. Miller, "Scaling optoelectronic-VLSI circuit into the 21st century: a technologiy roadmap" , *Journal of Selected Topics in Quantum Electronics*, 2 (1996), 55-76.