One-way quantum key distribution in the frequency domain

Paulo Vinícius Pereira Pinheiro and Rubens Viana Ramos

***Abstract*—This works brings an optical setup for one-way quantum key distribution in the frequency domain. The optical setup and the quantum protocol are described and the security analysis is performed.**

Keywords— Quantum key distribution, security analysis, frequency modulation.

I. INTRODUÇÃO

Quantum key distribution is the part of quantum cryptography that promises to provide a perfect secure key exchange [1-3]. However, in practical implementations, the non-ideality of optical and optoelectronic devices opens the possibility of some efficient attacks. An important attack that can be successfully implemented by an eavesdropper in QKD setups that employ non-ideal single-photon sources, like weak coherent states, is the photon number splitting attack (PNS). The PNS attack limits the reachable distance between users of a QKD system. In order to transform a QKD setup resistant to PNS attack, a smart trick was proposed: QKD employing decoy states [4-8]. On the other hand, differential phase shift QKD setups (DPS-QKD) can be naturally resistant to PNS attack [9-10]. Besides this advantageous property, when compared to setups that run BB84, DPS-QKD setups are easier to implement since Alice is the only active part, that is, the optical modulators are placed only in Alice; Bob, by its turn, has only passive components. Thereat, sometimes DPS-QKD is also named one-way QKD [11-12], in the meaning that only Alice's action defines the bits values.

There are already different optical implementations of the main quantum key distribution protocols. In particular, there are some optical setups for implementation of the BB84 and B92 quantum protocols using single-photon interference in sidebands of phase or amplitude-modulated light (hereafter we call it QKD in the frequency domain) [12-13] but there is not such implementation for one-way QKD protocols. In this direction, this work presents a setup for one-way QKD in the frequency domain. Its implementation, the quantum protocol and its security analysis are discussed.

II. OPTICAL SETUP FOR ONE-WAY QKD IN THE FREQUENCY DOMAIN

Paulo Vinicius Pereira Pinheiro and Rubens Viana Ramos are with the Laboratory of Quantum Information Technology, Department of Teleinformatic Engineering, Federal University of Ceara, Fortaleza, Brasil, E-mails:paulovpp@gmail.com,rubens@deti.ufc.br.

The proposed setup is shown in Fig. 1.

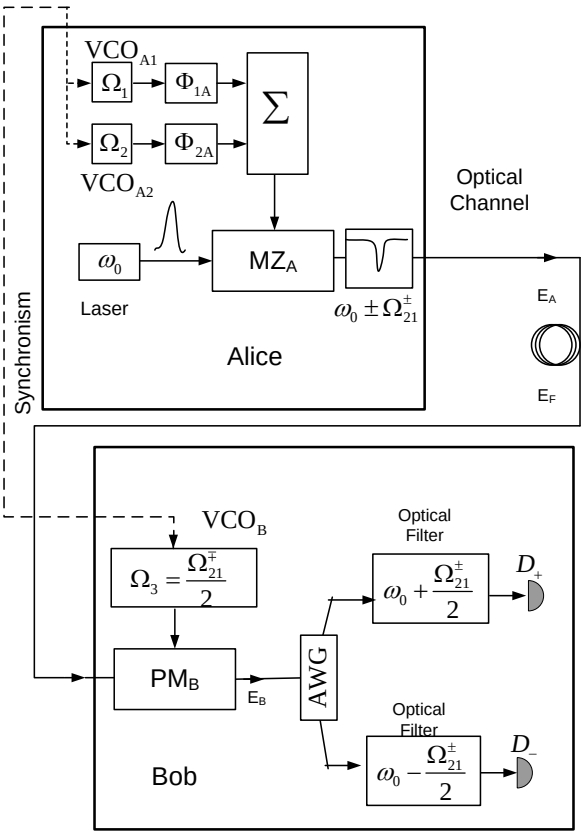

Fig. 1. Optical setup for one-way QKD in the frequency domain.

As can be seen in Fig. 1, Alice has a weak coherent light source operating at ω_0, two voltage controlled oscillator (VCO), operating at the frequencies Ω_1 and Ω_2, two phase shifters, Φ_{1A} and Φ_{2A}, an amplitude modulator, MZ_A (Mach_Zehnder), and reject band filters at the frequencies $\omega_0 \pm \Omega_{21}^{\pm}$, where $\Omega_{21}^{\pm} = \Omega_2 \pm \Omega_1$. Bob, by its turn, has an optical phase modulator PM_B, a VCO that can operate at the frequencies $\Omega_3 = \Omega_{21}^{\mp}/2$, and an AWG filter able to separate the frequencies $\omega_0 + \Omega_{21}^{+}/2$ and $\omega_0 - \Omega_{21}^{+}/2$ if Bob uses $\Omega_3 = \Omega_{21}^{-}/2$, and $\omega_0 + \Omega_{21}^{-}/2$ and $\omega_0 - \Omega_{21}^{-}/2$ if Bob uses $\Omega_3 = \Omega_{21}^{+}/2$. At last, D_+ and D_- are single-photon detectors.

Following the electric field propagation through the optical setup [15], if Bob uses $\Omega_3 = \Omega_{21}^{-}/2$ one gets for the quantum state after Bob's optical phase modulator the states

$$\left|\alpha_{\omega_0+\Omega_{21}^{+}/2}\right\rangle = \left|0.5\alpha_{\omega_0} t m_A m_B \sin\left[\left(\Phi_{2A}-\Phi_{1A}\right)/2\right]\right\rangle \quad (1)$$

$$\left|\alpha_{\omega_0-\Omega_{21}^{+}/2}\right\rangle = \left|0.5\alpha_{\omega_0} t m_A m_B \cos\left[\left(\Phi_{2A}-\Phi_{1A}\right)/2\right]\right\rangle \quad (2)$$

if the following conditions are satisfied

$$\left(\beta_1^{-}-\beta_2^{-}\right)L = \left(2k+1\right)\pi \quad (3)$$

$$\left(\beta_1^{+}-\beta_2^{+}\right)L = 2k'\pi. \quad (4)$$

In (1) and (2) m_A and m_B are, respectively, the modulation indexes used by Alice and Bob; $\left|\alpha_{\omega_0}\right\rangle$ is the quantum state generated by Alice and t is the total transmission coefficient that takes into account the losses at channel and Alice and Bob's devices. In (3) and (4) one has $\beta_{1(2)}^{\pm} = \left(n/c\right)\left(\omega_0 \pm \Omega_{1(2)}\right)$, L is the length of the channel and k and k' are natural numbers.

On the other hand, if Bob uses $\Omega_3 = \Omega_{21}^{+}/2$ one gets for the quantum state after PM_B the states

$$\left|\alpha_{\omega_0+\Omega_{21}^{-}/2}\right\rangle = \left|0.5\alpha_{\omega_0} t m_A m_B \sin\left[\left(\Phi_{2A}+\Phi_{1A}\right)/2\right]\right\rangle \quad (5)$$

$$\left|\alpha_{\omega_0-\Omega_{21}^{-}/2}\right\rangle = \left|0.5\alpha_{\omega_0} t m_A m_B \cos\left[\left(\Phi_{2A}+\Phi_{1A}\right)/2\right]\right\rangle \quad (6)$$

if the following conditions are satisfied

$$\left(\beta_2^{+}-\beta_1^{-}\right)L = \left(2k+1\right)\pi \quad (7)$$

$$\left(\beta_1^{+}-\beta_2^{-}\right)L = 2k'\pi. \quad (8)$$

Now, aiming to implement a one-way QKD in the frequency domain using the setup presented in Fig. 1, Alice and Bob agree with the bit codification shown in Table I.

TABLE I. Bit codification for implementation of one-way QKD in the frequency domain.

Ω_3	Detection	Bit
$\Omega_{21}^{-}/2$	D_+	1
$\Omega_{21}^{-}/2$	D_-	0
$\Omega_{21}^{+}/2$	D_+	1
$\Omega_{21}^{+}/2$	D_-	0

In order to implement the codification presented in Table I, the set of phases used by Alice are shown in Table II.

TABLE II. Phase codification for one-way QKD in the frequency domain.

	Φ_{2A}	Φ_{1A}	$\Delta\Phi_{21}^{-}$	$\Delta\Phi_{21}^{+}$
S_1	$\pi/2$	$\pi/2$	0	π
	$3\pi/2$	$\pi/2$	π	0
S_2	$5\pi/4$	$3\pi/4$	$\pi/2$	0
	$3\pi/4$	$\pi/4$	$\pi/2$	π
	$3\pi/4$	$3\pi/4$	0	$3\pi/2$
	$5\pi/4$	$\pi/4$	π	$3\pi/2$

In Table II, the first two rows, set S_1, are the phases used for data codification. On the other hand, the last four rows, set S_2, are the decoy states employed to force an eavesdropper to cause an error in Bob's detection. Now the one-way QKD in frequency domain protocol is described as follows:

1. For each pulse produced by Alice, she chooses, with probability f, Φ_{2A} and Φ_{1A} from S_1 and, with probability (1-f), Φ_{2A} and Φ_{1A} from S_2.
2. For each pulse that arrives at Bob's apparatus, he chooses randomly with probability 1/2 between $\Omega_3 = \Omega_{21}^{-}/2$ (photons are detected in $\omega_0 \pm \Omega_{21}^{+}/2$) and $\Omega_3 = \Omega_{21}^{+}/2$ (photons are detected in $\omega_0 \pm \Omega_{21}^{-}/2$).
3. Bob informs publically to Alice the time slots in which he used $\Omega_3 = \Omega_{21}^{+}/2$ (or when he used $\Omega_3 = \Omega_{21}^{-}/2$).
4. Alice informs publically to Bob the time slots in which she used a decoy state and which decoy states were used.

III. SECURITY ANALYSIS

In order to make the security analysis, we are going to consider the PNS and the intercept-resend attacks. We also consider that Eve attacks the pulse at the beginning of the channel, as soon as it leaves Alice's setup. Firstly, one can see that if Eve tries to make a photon number measurement, the phase relation between the pulses at different frequencies is destroyed. This is equivalent to the PNS attack in the QKD protocol discussed in [11]. Hence, the PNS attack is not useful since it will introduce errors in the data bits.

There are two possible intercept-resend attacks to be considered. In the first type, Eve uses the same apparatus used by Bob. She makes a measurement and, according to her results, she prepares a suitable state to be sent to Bob. In the second type, Eve uses a cascade of high trasmissivity beam splitters to try to separate the photons of a multi-photon pulse

sent by Alice. If the pulse sent by Alice has two or more photons and Eve succeeds in separate them in two no empty pulses, she can realize two measurement (one using $\Omega_3 = \Omega_{21}^{-}/2$ and the other using $\Omega_3 = \Omega_{21}^{+}/2$) and trying to guess correctly the two phases sent by Alice. On the other hand, if Eve does not get two no empty pulses, she stops the pulse sent by Alice and sends an empty pulse to Bob. Since this second type is more powerful, this is the one that we are going to consider. One can note that

1. When Alice sends a state from S_1, Eve, after the measurements, will be completely sure about the phases sent by Alice and she will be able to reproduce the correct state. Hence, no error will be introduced in Bob's measurement. In this case, Eve sends the correct state to Bob through an ideal quantum channel in order to maximize the probability of Bob having detection.
2. When Alice sends a state from S_2 (a decoy state), Eve, after the measurements, will be only 50% sure about the phases sent by Alice. Hence, she can produce a wrong state causing an error in Bob's measurement that will reveal her presence. For example, let us assume that Alice used the phases $5\pi/4$ and $3\pi/4$. In this case, Eve will have detection in D_- for the measurement using $\Omega_3 = \Omega_{21}^{+}/2$ and she will obtain detection in D_+ (50%) or D_- (50%) for the measurement using $\Omega_3 = \Omega_{21}^{-}/2$. Considering each possibility one gets the results shown in Table 3.

TABLE III – Possible results of Eve's attack when Alice used the phases $5\pi/4$ and $3\pi/4$.

$\Omega_3 = \Omega_{21}^{+}/2$	$\Omega_3 = \Omega_{21}^{-}/2$	$\Delta\Phi_{21}^{-}$	$\Delta\Phi_{21}^{+}$	Eve's guess	Error probability
D_-	D_+	π	2π	$(3\pi/2, \pi/2)$	0
D_-	D_-	0	2π	$(5\pi/4, 3\pi/4)$ or $(3\pi/4, 3\pi/4)$	0.5

As it can be seen in the second row of Table 3, if Eve has detections at D_- and D_+ she will think that Alice used the phases $(3\pi/2, \pi/2)$. This set of phases will cause detection in Bob at the correct places and, hence, none error will take place. On the other hand, if Eve has detections in D_- and D_-, she will be sure that Alice used a decoy state but she cannot be sure about which decoy states were used since the two set of phases $(5\pi/4, 3\pi/4)$ and $(3\pi/4, 3\pi/4)$ are compatible with Eve's measurement results. If Eve sends to Bob optical pulses with phases $(5\pi/4, 3\pi/4)$ none error will be introduced in Bob's measurement. On the other hand, if Eve sends to Bob optical pulses with phases $(3\pi/4, 3\pi/4)$, there will be a probability of 50% of Bob getting detection in D_+ if he uses $\Omega_3 = \Omega_{21}^{+}/2$. Bob will know that this result is an error when Alice reveals to him that she used $(5\pi/4, 3\pi/4)$ at that time slot. Considering all the cases, the probability of Eve to produce and error in Bob's measurement, per state sent by Alice, is

$$p_e = (1-f)/8. \quad (9)$$

As explained before, Eve has probability of 50% of identifying the presence of a decoy state. She may introduce an error in Bob exactly in the cases she knows that Alice sent a decoy state. Hence, Eve can adopt the following strategy: If a decoy state was identified an empty pulse is sent to Bob with probability q. In the other cases, Eve acts as explained before. With this strategy, the error probability is $p_e=(1-q)(1-f)/8$.

The count rate of decoy states when Eve is present is $t_B\eta(1-q/2)$ while the count rate of decoy states without Eve's attack is $[1-\exp(-\mu t t_B \eta)]$. Eve's action on decoy states will not be perceived if the two count rates are equal and q=1.

IV. CONCLUSÕES

We have proposed an optical setup able to run a one-way QKD protocol in the frequency domain. Three relevant points for the implementation of the setup proposed are: 1) as any other QKD protocol in the frequency domain, it requires synchronization between the voltage-controlled oscillators in Alice and Bob. 2) In order to have a low error rate the conditions (3)-(4) and (7)-(8) must be satisfied in the best way. 3) Since the probability of Eve being detected is low, a large amount of decoy states has to be used.

ACKNOWLEDGMENTS

This work was supported by CNPq, Grant no. 303514/2008-6. Also, this work was performed as part of the Brazilian National Institute of Science and Technology for Quantum Information.

REFERENCES

[1] C. H. Bennett and G. Brassard, Quantum cryptography: public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, pp. 175–179, 1984.

[2] A. K. Ekert, "Quantum cryptography based on Bell's theorem", Phys. Rev. Lett., v. 67, no. 6, pp. 661-663, 1991.

[3] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication", Phys. Rev. Lett., vol. 91, pp. 057901/1-4, 2003.

[4] H.-K. Lo, X. Ma and K. Chen, "Decoy state quantum key distribution", Phys. Rev. Lett., vol. 94, pp. 230504/1-4, 2005.

[5] Q. Wang, X.-B. Wang and G.-C. Guo, "Practical decoy-state method in quantum key distribution with a heralded single-photon source", Phys. Rev. A., vol. 75, pp. 012312/1-5, 2007.

[6] Q. Wang and A. Karlsson, "Performance enhancement of a decoy-state quantum key distribution using a conditionally prepared down-conversion source in the Poisson distribution", Phys. Rev. A., vol. 76, pp. 014309/1-4, 2007.

[7] Q. Wang, W. Chen, G. Xavier, M. Swillo, T. Zhang, S. Sauge, M. Tengner, Z.-F. Han, G.-C. Guo and A. Karlsson, "Experimental decoy-state quantum key distribution with sub-Poissonian heralded single-photon source", Phys. Rev. Lett., vol. 100, pp. 090501/1-4, 2008.

[8] Y. Zhao, B. Qi, X. Ma, H.-K. Lo and L. Qian, "Simulation and Implementation of decoy state quantum key distribution over 60 km Telecom fiber", In Proc. IEEE Int. Symp. Inf. Theor., pp. 2094–2098, 2006.

[9] K. Inoue, E. Waks and Y. Yamamoto,"Differential phase shift quantum key distribution", Phys. Rev. Lett., vol. 89, pp. 037902/1-3, 2002.

[10] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue, and Y. Yamamoto, "Differential phase shift quantum key distribution over 105 km fibre", New J. Phys., vol. 7, pp. 1-12, 2005.

[11] N. Gisin, G. Ribordy, H. Zbinden, D. stucki, N. Brunner, V. Scarani, "Towards practical and fast quantum cryptography", xxx.lanl.gov quant-ph/0411022, 2004.

[12] D. stucki, N. Brunner, N. Gisin, V. Scarani and H. Zbinden, "Fast and simple one-way quantum key distribution", Appl. Phys. Lett., 87, pp. 194108/1-3, 2005.

[13] J.-M. Mérolla, Y. Mazurenko, J. P. Goedgebuer and W. T. Rhodes, "Single-photon interference in sidebands of phase-modulated light for quantum cryptography", Phys. Rev. Lett., vol. 82, pp. 1656-1659, 1999.

[14] J.-M. Mérolla, 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.

[15] J. Capmany, A. Ortigos-Blanch, J.Mora, A. Ruiz-Alba, W. Amaya and A. Martínez, "Analysis of subcarrier multiplexed quantum key distribution systems: signal, intermodulation and quantum bit error rate", IEEE Journal of Selected Topics in Quantum Electronics, vol. 15, no. 6, pp. 1607-16212, 2009.