Quantum Communication Using Polarization-Encoded Photons in Optical Fibers

Álvaro J. Almeida, Daniel L. Macedo, Nuno A. Silva, Nelson J. Muga, Paulo S. André and Armando N. Pinto

***Abstract*—A theoretical description for the quantum-bit error rate (QBER) in a polarization-encoded system in optical fibers is presented. Two orthogonal quantum states are used. The description takes into account the number of bits transmitted and received in the system. The model is experimentally verified.**

***Index Terms*—Quantum Communication, Quantum Cryptography, Polarization Encoding, Quantum-Bit Error Rate.**

I. Introduction

SINCE the initial proposal by Stephen Wiesner for the use of quantum mechanics to make banknotes [1], quantum cryptography have seen a rapid progress in both theory and experiment [2, 3]. With the proposal of the first quantum cryptographic protocol (widely known as BB84) [4], quantum key distribution (QKD) have became the most developed application of quantum cryptography, and thus probably the first application of quantum mechanics at the single-quantum level [2].

The quantum-bit error rate (QBER) is used to measure the quality of the signal transmission in QKD systems [2, 5]. This quantity depends on several factors, such as the type of protocol used, the transmission impairments, or the noise and imperfections of the fiber link [2]. The QBER of a system can be measured by comparing the rate of right and wrong bits which arrive at the receivers, whose codification can be performed by using the phase, polarization, frequency, among others [2, 5]. Regarding the light state of polarization (SOP), it is well known that it changes during propagation through an optical fiber, due to polarization-mode dispersion or polarization dependent losses [6]. A general model for the QBER, considering systems implementing the BB84 protocol is presented in [2]. Despite the majority of the protocols use nonorthogonal quantum states, orthogonal states can also be used [7, 8].

We present a theoretical description of the QBER in a polarization-encoded system over optical fibers. The model is verified experimentally, through the measurement of the number of bits received as a function of transmitted bits.

This paper is organized in four sections. In Section II, we present a theoretical description for the QBER, which accounts for the number of bits used in the measurement. In Section III, we propose and implement an experimental setup suitable to test our model. Finally, in Section IV the main conclusions are presented.

II. QBER Theory

In contrast to classical communications, where the bit error rate (BER) is of the order of 10^{-9}, in quantum communications, the so-called QBER is normally on the order of a few percent [2].

In terms of the frequency of bits received in the detectors, the QBER can be defined as the ratio of wrong bits, R_{wrong}, to the total frequency of bits (wrong and right),

$$\text{QBER} = \frac{R_{\text{wrong}}}{R_{\text{total}}}\,, \tag{1}$$

where $R_{\text{total}} = R_{\text{right}} + R_{\text{wrong}}$, with R_{right} being the rate of right bits [2, 9].

In order to describe the QBER in a two-state polarization encoding system, we can start from the scheme presented in Fig. 1.

By using an attenuated laser source, the photon distribution at its output will follow a Poissonian statistics. Then, the probability of a pulse to carry n photons is given by,

$$P(n,\mu) = \frac{\mu^n}{n!}\exp(-\mu)\,, \tag{2}$$

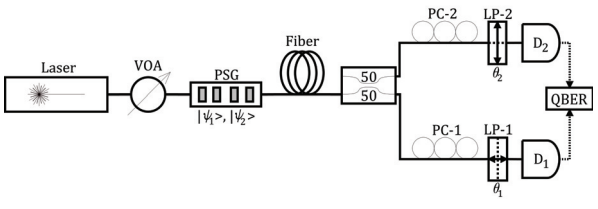

Fig. 1. Schematic draw of a two-state polarization-encoded system. VOA: Variable Optical Attenuator; PSG: Polarization State Generator; PC: Polarization Controller; LP: Linear Polarizer; D: Single-Photon Detector.

This work was supported in part by the FCT - Fundação para a Ciência e a Tecnologia, through the PhD Grants SFRH/BD/79482/2011 and SFRH/BD/63958/2009, and the Post Doctoral Grant SFRH/BPD/77286/2011, by the FCT and European Union FEDER - Fundo Europeu de Desenvolvimento Regional, through project PTDC/EEA-TEL/103402/2008 (QuantPrivTel), and by the FCT and the Instituto de Telecomunicações, under the PEst-OE/EEI/LA0008/2011 program, project 'P-Quantum'.

Álvaro J. Almeida and Paulo S. André are with the Department of Physics, University of Aveiro, Aveiro, Portugal and the Instituto de Telecomunicações, Aveiro, Portugal (E-mails: aalmeida@av.it.pt, pandre@av.it.pt).

Daniel L. Macedo is with the Instituto de Telecomunicações, Aveiro, Portugal (E-mail: djlmacedo@av.it.pt).

Nuno A. Silva, Nelson J. Muga and Armando N. Pinto are with the Department of Electronics, Telecommunications and Informatics, University of Aveiro, Aveiro, Portugal and with the Instituto de Telecomunicações, Aveiro, Portugal (E-mails: nasilva@av.it.pt, muga@av.it.pt, anp@ua.pt).

where μ is the average number of photons per pulse [2]. At the laser source output, the two SOPs can be represented as,

$$|\psi_1\rangle = \cos(\psi_1)|H\rangle + \sin(\psi_1)|V\rangle\,, \tag{3}$$

and

$$|\psi_2\rangle = \cos(\psi_2)|H\rangle + \sin(\psi_2)|V\rangle\,, \tag{4}$$

where $|H\rangle$ and $|V\rangle$ are the horizontal and vertical SOPs, respectively, and ψ_1 and ψ_2 are the initially generated SOPs [10].

These two states are now sent to an optical fiber, i.e., the quantum channel. After the photons pass through the optical fiber, the probability of a pulse to carry at least one photon can be written as,

$$P = 1 - \exp(-\eta_{\text{F}}\mu)\,, \tag{5}$$

where $\eta_{\text{F}} = 10^{-\alpha L/10}$ is the transmission coefficient of the fiber, α is the attenuation of the fiber (in dB/km) and L is the fiber length (in km) [11].

Next, the beam passes through a 50/50 beam splitter, Fig. 1, and two beams will be generated with independent Poissonian statistics. Then, we will have in each arm,

$$P_i = 1 - \exp\left(-\frac{\eta_{\text{F}}\mu}{2}\right), \tag{6}$$

where $i = 1, 2$ indicates the detector number [12].

The photon will reach one of two linear polarizers (LPs), set at angles θ_1 and θ_2, and have a probability of transmission given by,

$$P_{\text{t}}^{ij}(\psi_i \pm \phi_i, \theta_j) = |\langle \psi_i \pm \phi_i | T_{\theta_j}\rangle|^2\,, \tag{7}$$

where

$$|T_{\theta_j}\rangle = \cos(\theta_j)|H\rangle + \sin(\theta_j)|V\rangle \tag{8}$$

represents the SOP after the polarizer, with $i = 1, 2$ and $j = 1, 2$, and $|\psi_i \pm \phi_i\rangle = \cos(\psi_i \pm \phi_i)|H\rangle + \sin(\psi_i \pm \phi_i)|V\rangle$, where ϕ_i represents the rotation of the photon in relation to the initial SOP ψ_i, between the coupler and the LP [13]. The polarization controllers (PC) are used to adjust the polarization of the photons with the axes of the linear polarizers, and thus, to compensate for the polarization rotation inside the optical fiber.

Substituting (3)-(4) and (8) in (7), we obtain that [14],

$$\begin{aligned} &P_{\text{t}}^{ij}(\psi_i \pm \phi_i, \theta_j) = \\ &\quad \cos(\theta_j)^2 \cos(\psi_i \pm \phi_i)^2 + \sin(\theta_j)^2 \sin(\psi_i \pm \phi_i)^2 + \\ &\qquad 2\cos(\theta_j)\cos(\psi_i \pm \phi_i)\sin(\theta_j)\sin(\psi_i \pm \phi_i)\,, \end{aligned} \tag{9}$$

where P_{t}^{11} and P_{t}^{21} represent the probability of transmission of a photon in the states $|\psi_1 \pm \phi_1\rangle$ and $|\psi_2 \pm \phi_1\rangle$, respectively, through the LP-1, and P_{t}^{12} and P_{t}^{22} represent the probability of transmission of a photon in the states $|\psi_1 \pm \phi_2\rangle$ and $|\psi_2 \pm \phi_2\rangle$, respectively, through the LP-2.

From (6) and (9) we can write the probability of detection as,

$$P_{\text{d}}^{ij} = \left[1 - \exp\left(-\frac{\eta_{\text{F}}\eta_{\text{Bi}}\eta_{\text{Di}}\mu}{2}\right)\right] P_{\text{t}}^{ij}\,, \tag{10}$$

where P_{d}^{11} and P_{d}^{21} represent the probability of detection in detector 1 (D_1), with P_{d}^{21} being the probability of the state $|\psi_2\rangle$ to be detected in D_1, and P_{d}^{12} and P_{d}^{22} is the probability of detection in detector 2 (D_2), with P_{d}^{12} being the probability of the state $|\psi_1\rangle$ to be detected in D_2, $\eta_{\text{B}i} = 10^{-L_{\text{B}i}/10}$, with $L_{\text{B}i}$ representing the total losses in each arm (in dB) between the beam splitter and the detector, and η_{D} is the detection efficiency [14].

The probability of a detector to click can be denoted by [11],

$$P_{\text{click}}^{ij} = P_{\text{d}}^{ij} + P_{\text{dc}}^{ij} - P_{\text{d}}^{ij} P_{\text{dc}}^{ij}\,, \tag{11}$$

where the probability of click of each detector is written as,

$$P_{\text{click}}^{\text{D}_1} = P_{\text{click}}^{11} + P_{\text{click}}^{21}\,, \tag{12}$$

and

$$P_{\text{click}}^{\text{D}_2} = P_{\text{click}}^{12} + P_{\text{click}}^{22}\,. \tag{13}$$

In terms of a detector counting rate, (12)-(13) results in,

$$C_{\text{D}_i} = f_{\text{r}} P_{\text{click}}^{\text{D}_i}\,, \tag{14}$$

where f_{r} is the pulse repetition rate [11]. The number of bits received, N_{r}, in the detectors can be obtained from,

$$N_{\text{r}}^{\text{D}_i} = C_{\text{D}_i}\tau\,, \tag{15}$$

where τ is the measurement time, which is given by,

$$\tau = \frac{N_{\text{s}}}{f_{\text{r}}}\,, \tag{16}$$

with N_{s} being the number of bits sent. Substituting (14) and (16) in (15), we obtain

$$N_{\text{r}}^{\text{D}_i} = P_{\text{click}}^{\text{D}_i} N_{\text{s}}\,. \tag{17}$$

Then, the total number of bits received is given by,

$$N_{\text{r}}^{\text{total}} = N_{\text{r}}^{\text{D}_1} + N_{\text{r}}^{\text{D}_2}\,. \tag{18}$$

The probability to obtain right clicks in both detectors is written as,

$$P_{\text{click}}^{\text{right}} = P_{\text{click}}^{11} + P_{\text{click}}^{22}\,, \tag{19}$$

and the probability to obtain a wrong click is given by,

$$P_{\text{click}}^{\text{wrong}} = P_{\text{click}}^{12} + P_{\text{click}}^{21}\,, \tag{20}$$

which represents the bits that are detected in the wrong detector. In terms of frequencies, (19) and (20) can be written as,

$$R_{\text{click}}^{\text{right}} = f_r P_{\text{click}}^{\text{right}}\,, \tag{21}$$

$$R_{\text{click}}^{\text{wrong}} = f_r P_{\text{click}}^{\text{wrong}}\,, \tag{22}$$

where the frequency of total counts is written as,

$$R_{\text{click}}^{\text{total}} = R_{\text{click}}^{\text{right}} + R_{\text{click}}^{\text{wrong}}\,. \tag{23}$$

By using (22) and (23), (1) is finally written as,

$$\text{QBER} = \frac{P_{\text{click}}^{\text{wrong}}}{P_{\text{click}}^{\text{right}} + P_{\text{click}}^{\text{wrong}}}\,. \tag{24}$$

Considering, for instance, a quantum channel with a length of 50 km, we can plot the probability of click as a function of the rotation angles, ϕ_1 and ϕ_2, according to (11), Fig. 2, for $\psi_1 = \theta_1 = 0$ and $\psi_2 = \theta_2 = 0$.

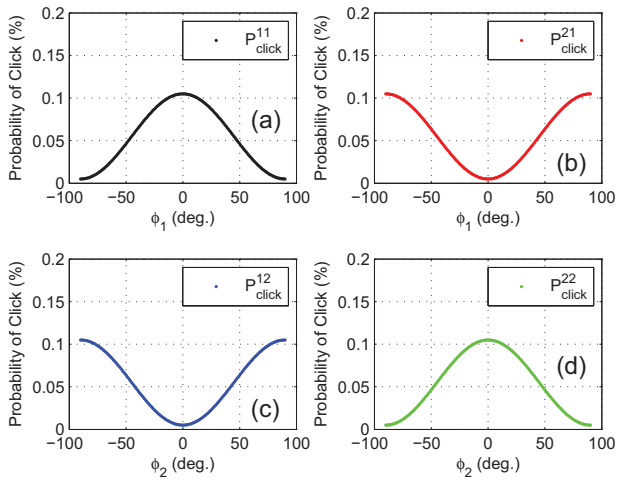

Fig. 2. Probability of click as a function of the rotation angles, ϕ_1 or ϕ_2, after propagation of two states through a system which includes an optical fiber with 50 km in length. The maximum values are obtained for perfect alignment with the linear polarizers.

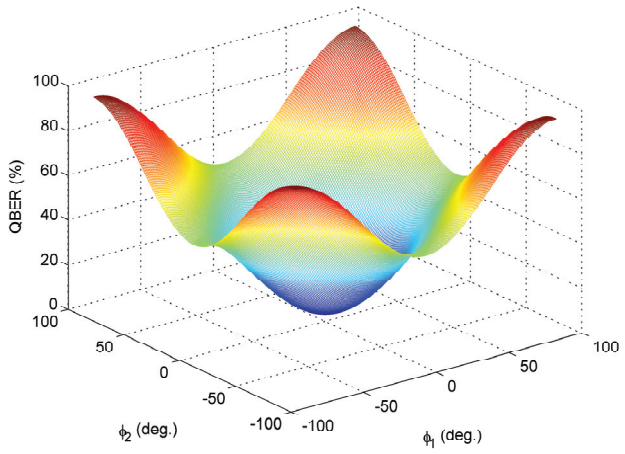

Fig. 3. QBER as a function of the rotation angles ϕ_1 and ϕ_2 after propagation of two states through a system, which includes an optical fiber with 50 km in length.

Looking at the results shown in Fig. 2, we can see that only a max of 0.1% of the bits sent are detected, considering the scheme presented (Fig. 1). Also, it can bee seen that the probability of click is maximum when the photon's polarization is aligned with the transmission axis of the LP. In that case, the probability of a photon to click in the wrong detector (P^{12}_{click} and P^{21}_{click}) is minimum. The QBER as a function of the angles ϕ_1 and ϕ_2 is shown in Fig. 3. The parameters used to plot Figs. 2-3 are presented in Table I.

A behavior similar to the one presented in the probability of click is observed.

III. Experimental Validation

A. Experimental Setup

In order to validate the proposed model for the number of bits transmitted and received, we have implemented the experimental setup presented in Fig. 4. The setup works as follows: a pump at $\lambda_p = 1550.92$ nm from a tunable laser source (TLS) passes through a polarization controller (PC-1), and is externally modulated, using a Mach-Zehnder modulator (MZM), to produce optical pulses with a full-width at half maximum (FWHM) of approximately 1 ns, and a repetition rate of 100 kHz. Then, the pulse is filtered in order to reduce its sidebands, and goes into a 50/50 beam splitter. After the beam splitter, two accousto-optic modulators (AOM-1 and AOM-2), which are connected to a microcontroller, work as a switch. In the lower arm, it will be defined the $|\psi_1 = 0°\rangle$ SOP, and in the upper arm, the $|\psi_2 = 90°\rangle$ SOP. The polarization controllers, PC-2 and PC-3, are used to adjust the input light with the axes of a polarization-beam splitter (PBS). Next the photons are attenuated with a variable optical attenuator (VOA), in order to obtain an average number of photons per pulse, $\mu \ll 1$, enter in a 5/95 coupler, and reach an optical fiber that works as a quantum channel, with 1 km long. Next, the photons pass through an arrayed-waveguide grating (AWG), reach a 50/50 beam splitter, and find one of two analyzers, composed of a PC and a linear polarizer (LP), set at $|\theta_1 = 0°\rangle$ and $|\theta_2 = 90°\rangle$ SOPs. The photons are detected using two avalanche photodiodes (APD1 and APD2). The two APDs are InGaAs/InP avalanche photodiodes, operating in a gated Geiger mode [15]. APD1 (id200) has a dark count probability per time gate $t_g = 5$ ns of $P_{\text{dark}} = 6 \times 10^{-5}$, and a quantum detection efficiency $\eta_D \approx 10\%$ [16]. APD2 (id201) has a dark count probability per time gate $t_g = 5$ ns of $P_{\text{dark}} = 2.58 \times 10^{-5}$, and a quantum detection efficiency $\eta_D \approx 10\%$ [17]. Both

TABLE I
Parameters used to plot the graphics in Fig. 2-3.

Parameter	Value
η_D	10 [%]
α	0.2 [dB/km]
L_B	0 [dB]
P_{dc}	5×10^{-5} [gate^{-1}]
μ	0.2 [photons/pulse]

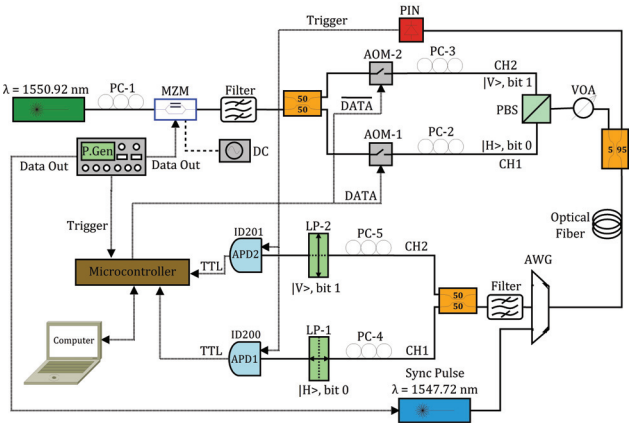

Fig. 4. Schematics of the experimental setup.

APDs are connected to the microcontroller through a TTL output, and then the microcontroller calculates the QBER of the system.

A synchronization pulse at $\lambda_s = 1547.72$ nm from a distributed feedback laser (DFB) is sent counter-propagating through the AWG, the EPC and the fiber, and is used to give the trigger to the APDs, through the photodiode (PIN).

B. Experimental Results

By using an optical fiber with a length equal to 1 km, we have sent patterns with different sizes to the system, i. e., PatternSize = $[2^{17}; 2^{16}; 2^{15}; 2^{14}; 2^{13}]$ bits, and recorded the number of bits that were detected with no errors, $P_{\text{click}}^{\text{right}}$, and in the wrong detector, $P_{\text{click}}^{\text{wrong}}$. The results are presented in Fig. 5.

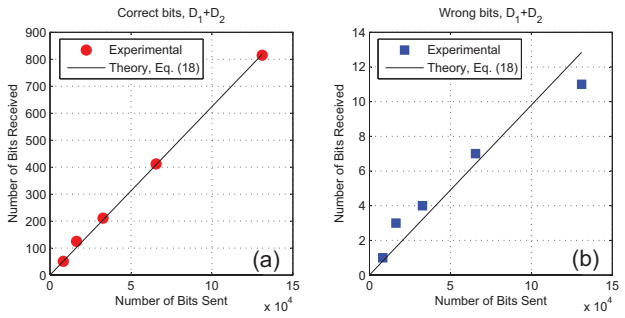

Fig. 5. (a) Number of correct bits received by the detectors as a function of the number of bits sent. The theoretical fit uses (18) and (19). (b) Number of wrong bits received by the detectors as a function of the number of bits sent. The theoretical fit uses (18) and (20). The transmission length was 1 km.

The parameters used to fit (18) in Fig. 5 are presented in Table II.

TABLE II
PARAMETERS USED TO FIT (18) IN FIG. 5.

Parameter	Value
$\eta_{D_1} = \eta_{D_2}$	10 [%]
η_F	0.16
$\eta_{B_1} = \eta_{B_2}$	0.14
P_{dc_1}	6×10^{-5}
P_{dc_2}	2.58×10^{-5}
μ	0.5 [photons/pulse]
ϕ_1	2°
ϕ_2	3°

From the results plotted in Fig. 5(a), we can see a good agreement between theory and experiment. The efficiency of the system is around 0.6%. This means that only 0.6% of the total bits sent are detected by the correct basis detector. From Fig. 5(b), it can be seen a rougher adjustment, mainly because the rate of wrong bits was very low, thus being close to the system fluctuations.

The rotation angles ϕ_1 and ϕ_2 are misalignment angles, due to experimental imperfections between the PC and the LP.

IV. CONCLUSIONS

We have presented a theoretical description for the QBER in a two-state polarization encoding system in optical fibers. The description takes into account all the components used in the experiment, verifying that every one has a particular role in the final result. The number of bits received as a function of the bits transmitted in the system was also described. For the case of quantum communications, where the detection efficiency is particularly low, the average number of bits received is quite low, which indicates that we should send a large number of bits to the system in order to calculate the QBER. It was also verified that the alignment in the system plays a crucial role. The experimental validation shows that our system can be used to share quantum information encoded into polarization.

REFERENCES

[1] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, no. 1, pp. 78–88, 1983.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, pp. 145–195, Jan. 2002.

[3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, pp. 1301–1350, Jul. 2009.

[4] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*. Bangalore, India, 1984, vol. 175, pp. 175–179.

[5] H. Zbinden, N. Gisin, B. Huttner, A. Muller, and W. Tittel, "Practical aspects of quantum cryptographic key distribution," *J. Cryptology*, vol. 13, pp. 207–220, 2000.

[6] J. Breguet, A. Muller, and N. Gisin, "Quantum Cryptography with Polarized Photons in Optical Fibres: Experiment and Practical Limits," *Journal of Modern Optics*, vol. 41, pp. 2405–2412, Dec. 1994.

[7] L. Goldenberg and L. Vaidman, "Quantum Cryptography Based on Orthogonal States," *Physical Review Letters*, vol. 75, pp. 1239–1243, Aug. 1995.

[8] G. P. He, "Quantum key distribution based on orthogonal states allows secure quantum bit commitment," *Journal of Physics A Mathematical General*, vol. 44, p. 5305, Nov. 2011.

[9] P. D. Kumavor, A. C. Beal, S. Yelin, E. Donkor, and B. C. Wang, "Comparison of Four Multi-User Quantum Key Distribution Schemes Over Passive Optical Networks," *Journal of Lightwave Technology*, vol. 23, pp. 268–276, Jan. 2005.

[10] J. N. Damask, *Polarization Optics in Telecommunications*, J. N. Damask, Ed. Springer Science+Business Media Inc., 2005.

[11] A. Trifonov, D. Subacius, A. Berzanskis, and A. Zavriyev, "Single photon counting at telecom wavelength and quantum key distribution," *Journal of Modern Optics*, vol. 51, pp. 1399–1415, Sep. 2004.

[12] P. D. Townsend and I. Thompson, "A Quantum Key Distribution Channel Based on Optical Fibre," *Journal of Modern Optics*, vol. 41, pp. 2425–2433, Dec. 1994.

[13] E. J. Galvez, C. H. Holbrow, M. J. Pysher, J. W. Martin, N. Courtemanche, L. Heilig, and J. Spencer, "Interference with correlated photons: Five quantum mechanics experiments for undergraduates," *American Journal of Physics*, vol. 73, pp. 127–140, Feb. 2005.

[14] A. J. Almeida, N. A. Silva, N. J. Muga, and A. N. Pinto, "Single-Photon Source Using Stimulated FWM in Optical Fibers for Quantum Communication," in *Proc. SPIE 8001*, May 3, 2011, p. 80013W.

[15] G. Ribordy, N. Gisin, O. Guinnard, D. Stucki, M. Wegmuller, and H. Zbinden, "Photon counting at telecom wavelengths with commercial InGaAs/InP avalanche photodiodes: current performance," *Journal of Modern Optics*, vol. 51, pp. 1381–1398, Sep. 2004.

[16] id Quantique, "id 200-Single-Photon Detection Module: Operating Guide, Version 2.2," http://www.idquantique.com/images/stories/PDF/id201-single-photon-counter/id200-operating.pdf, accessed September 5, 2012.

[17] ——, "id 201-Single-Photon Detection Module: Operating Guide, Version 4.0," http://www.idquantique.com/images/stories/PDF/id201-single-photon-counter/id201-operating-guide.pdf, accessed September 5, 2012.