# Long-Term Time Evolution Measurements of Polarization Drift in Optical Fibers

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

***Abstract*—We present a model for the quantum-bit error rate in a polarization-encoding system for transmission of quantum information, without compensation of polarization. The random evolution of the polarization along the fiber is induced by its polarization mode dispersion. An experimental setup able to measure the quantum-bit error rate in the transmission of the photons through several fiber lengths is proposed, and some experimental results are obtained. Our experimental scheme is designed to work on the 1550 nm telecom band.**

***Index Terms*—Quantum-Bit Error Rate, Optical Fiber, Photon Polarization, Single Photon, Avalanche Photodiode.**

## I. Introduction

THE need for highly secure systems for transmission of information, is one of the main goals in nowadays research on optical communications. Thus, the implementation of quantum key distribution (QKD) systems appears as a natural solution for helping solve this problem [1]. The quantum-bit error rate (QBER) can be used to measure the quality of the signal transmission in the QKD systems. In general it depends on several factors, such as the type of protocol used, the transmission impairments, the noise and imperfections of the fiber link, or the dark counts of the detection system [1].

In order to share secret keys between two entities, the need for quantum protocols is of utmost importance. The first QKD protocol was proposed in 1984 by Bennett and Brassard [2], and its implementation took place at IBM, in 1989 [3, 4]. This protocol makes use of two nonorthogonal sets of basis, *i.e.*, of four states of polarization (SOPs). Since then, many other QKD protocols were developed, like the E91 [5], the B92 [6], the six-state [7], the decoy-state [8], or the SARG04 [9]. Experimental implementations of these protocols, were presented for optical fibers [10–13], and free-space [14, 15]. The QBER of a system can be measured by comparing the right and wrong bits, whose codification can be performed in phase, polarization, frequency, among others [1].

In this paper, we present a simplified model for the QBER, in a system where we use the polarization of the photons to encode information. This model does not includes compensation of the random rotations of polarization due to transmission through the optical fiber, since that was already presented in [16]. We also propose an experimental setup able to measure the QBER in the system, and obtain some experimental results after propagation of the photons in different fiber links.

This paper is organized in four sections. In Section II, we present a simplified model for the QBER in a system that makes use of polarization-encoding, and its evolution with the fiber length and the time. An experimental setup used to measure the QBER, and the experimental results obtained after transmission through several optical fibers with different lengths, are presented in Section III. Finally, in Section IV we present our main conclusions.

## II. Simplified Model for QBER Evolution Without Compensation of Polarization

In order to obtain a theoretical model for the QBER in a polarization-encoding system without compensation of polarization, for transmission of quantum information, we assume the scenario presented in Fig. 1. If a linear SOP, *e.g.* vertical, is sent to an optical fiber, it will experience a random rotation due to the residual fiber birefringence. Then, after the fiber, we consider that it will be rotated of an angle $\theta$ in relation to the vertical. Next, it will reach a 50/50 beam splitter, and it can be detected in one of two detectors ($D_1$ or $D_2$), after passing through two linear analysers ($A_1$ and $A_2$), one horizontally set, and the other vertically aligned.

The probability of a photon to be detected in detector $D_1$ is given by,

$$P_h = \frac{1}{2}\Big[1 - \cos(\theta)^2\Big], \tag{1}$$

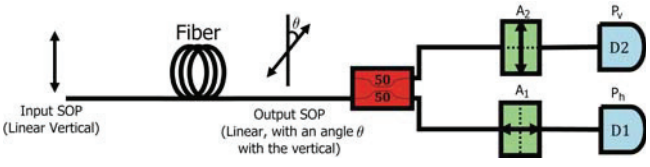


Fig. 1. Schematic draw of the evolution of a linear SOP after propagation through an optical fiber and its detection.

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, and the Instituto de Telecomunicações, University of Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal, Tel: +351 234 377 900, Fax: +351 234 377 901 (Emails: aalmeida@av.it.pt; pandre@av.it.pt).

Nelson J. Muga, Nuno A. Silva and Armando N. Pinto are with the Department de Electronics, Telecommunications and Informatics, University of Aveiro, and the Instituto de Telecomunicações, University of Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal, Tel: +351 234 377 900, Fax: +351 234 377 901 (Emails: muga@av.it.pt; nasilva@av.it.pt; anp@ua.pt).

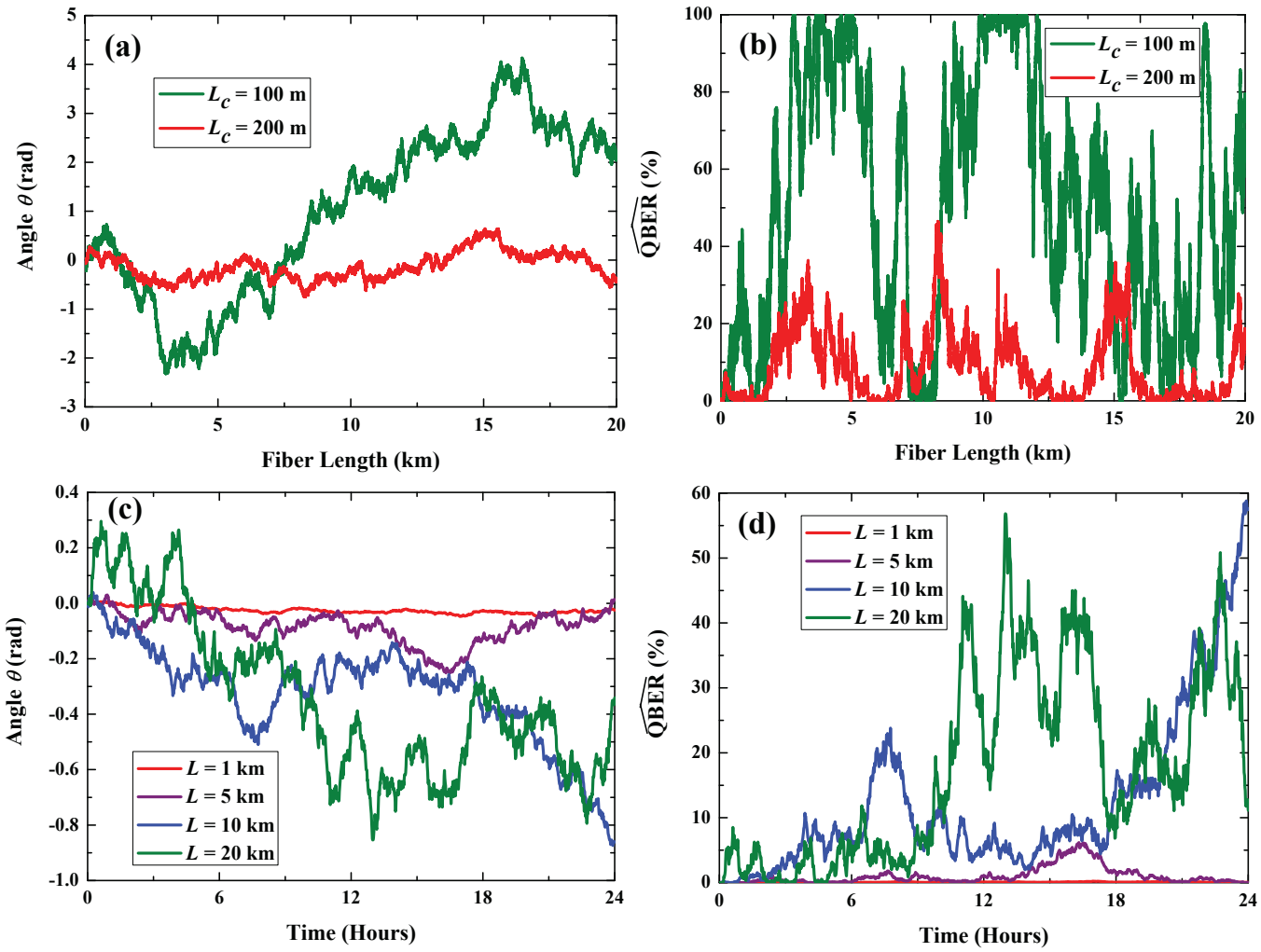


Fig. 2. (a)-(b) Evolution of the SOP and the $\widehat{\text{QBER}}$ along the fiber, for two different $L_c$ values. (c)-(d) Variation of the SOP and the $\widehat{\text{QBER}}$ as a function of time, for several fiber transmission lengths.

and the probability of being detected in $D_2$, by,

$$P_v = \frac{1}{2}\Big[\cos(\theta)^2\Big]\,, \tag{2}$$

where the $1/2$ is related with the coupler probability, and the term $1-\cos(\theta)^2$ gives the probability for the photons to pass through the polarizer.

The QBER can be defined as the rate between the wrong bits and the total number of bits received when $t \to \infty$, as [1, 17],

$$\text{QBER} = \lim_{t\to\infty} \frac{N_{\text{wrong}} \text{ in } [0,t]}{N_{\text{received}} \text{ in } [0,t]}\,. \tag{3}$$

Since we are measuring the QBER in a finite time interval $\Delta t = t_w - 0$, we will have,

$$\widehat{\text{QBER}} = \frac{N_{\text{wrong}} \text{ in } [0,t_w]}{N_{\text{received}} \text{ in } [0,t_w]}\,. \tag{4}$$

Assuming that the input photons have a vertical linear SOP, the number of wrong bits are given by the detections in $D_1$, *i.e.*, the number of received photons times $P_h$. Therefore, the $\widehat{\text{QBER}}$ can be written as,

$$\widehat{\text{QBER}}_{D_1} = \frac{N_{\text{received}} \text{ in } [0,t_w] \times P_h}{N_{\text{received}} \text{ in } [0,t_w] \times (P_h + P_v)} = 1 - \cos(\theta)^2\,. \tag{5}$$

In order to obtain the variation of the SOP along the fiber, we assume that the rate of change of the angle $\theta$ is a white-noise process [18],

$$\frac{d\theta}{dz} = g_\theta(z)|_{t=t_0}\,, \tag{6}$$

with,

$$\langle g_\theta(z)\rangle = 0\,, \tag{7}$$

and,

$$\langle g_\theta(z) g_\theta(z')\rangle = \sigma_z^2 \delta(z-z')\,, \tag{8}$$

where $\sigma_z^2 = 2/L_c$, being $L_c$ the correlation length, and $\delta(z-z')$ represents the Dirac delta function [19].

The variation of $\theta$ with time can be modeled as,

$$\frac{d\theta}{dt} = h_\theta(t)|_{z=z_0}\,, \tag{9}$$

with,

$$\langle h_\theta(t)\rangle = 0\,, \tag{10}$$

and,

$$\langle h_\theta(t)h_\theta(t')\rangle = \sigma_t^2\delta(t-t')\,, \tag{11}$$

where $\sigma_t^2 = 2/t_c$, and $t_c = 2t_f/(3\omega^2 D_p^2 z)$, where $t_c$ represents the drift time of the index difference between the fast and slow fiber axes, $\omega$ is frequency of the photons, and $D_p$ represents the polarization mode dispersion (PMD) coefficient [16].

A representation of the angle $\theta$ and the $\widehat{\text{QBER}}$ evolutions with the propagation along the fiber and the time is shown in Fig. 2. For these plots, we have used the following parameters: $L_c = 100$ and 200 m, $t_f = 5\times10^9$ s, $D_p = 0.2$ ps/km$^{1/2}$, and $\lambda = 1550$ nm [16].

From Fig. 2, we can see that the angle $\theta$ shows a random variation either with the fiber length and the time, which leads also to a random variation of the $\widehat{\text{QBER}}$ in both quantities. In the time evolution, we observe higher angle drifts for longer fiber distances. In the evolution with the distance, we observe that the drifts are highly dependent on the correlation length. As smaller the $L_c$, larger the SOP variations.

## III. Experimental QBER Measurement

In this section we focus on the experimental realization of our subject of study. First, we describe the experimental setup proposed, focusing on its main details. Next we show and analyse the experimental data that we have obtained.

### A. Experimental Setup

The schematics of the experimental setup that we used to measure the $\widehat{\text{QBER}}$ in a polarization-encoding system in optical fibers is presented in Fig. 3.

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 10 kHz. A variable optical attenuator (VOA) can be used to control the average number of photons per pulse that are generated. Then, the pulses are filtered using a flat-top dense wavelength-division multiplexing (DWDM) optical filter with a FWHM of 100 GHz, in order to eliminate its sidebands, and go into a 50/50 beam splitter, where two linear SOPs can be generated. Two acousto-optic modulators (AOM-1 and AOM-2) are used as switches, and are connected to a microcontroller, which can be used to send a binary pattern to the system. When the microcontroller sends a bit "0", the photon in AOM-1's arm can be sent, and if the microcontroller sends a bit "1", is the photon in AOM-2's that can be sent. The pattern uploaded to the microcontroller was a pseudorandom binary sequence (PRBS) with length 12, and with 131072 bits (16 kB). After the two AOMs, photons pass through a polarization-beam splitter (PBS), where the photon from channel 1 (CH1) outputs at 0° polarization, and the photon form channel 2 (CH2) outputs at 90° polarization. The two PCs (PC-2 and

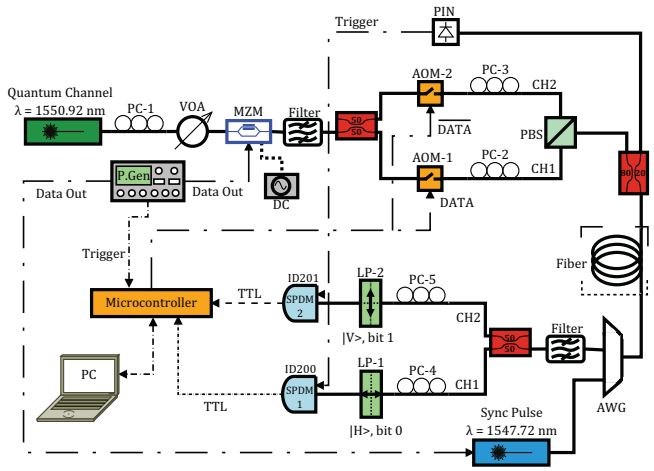


Fig. 3. Schematics of the experimental setup used to measure the $\widehat{\text{QBER}}$ in a polarization-encoding system in optical fibers. The synchronization laser is sent counter-propagating.

PC-3) are used to align the polarization of the photons with the axes of the PBS. After passing through the PBS, the quantum signal can be transmitted through different fibers links. Then, the photons enter in an arrayed-waveguide grating (AWG) with a 200 GHz channel separation, where a classical signal at $\lambda_s = 1547.72$ nm, that works as a synchronization pulse for the detectors, is inserted counter-propagating. The synchronization signal is externally modulated with the same frequency as the quantum signal, and is received by a PIN detector, which will give the trigger to both single-photon detector modules (SPDMs). The quantum signal passes through an optical filter which is used to eliminate some cross-talk from the synchronization channel to the quantum channel. Then, it reaches another 50/50 beam splitter where single photons can choose going up or down. In the lower arm, photons with 0° polarization can pass through the linear polarizer (LP-1) set at 0° and reach SPDM-1 (id200) [20, 21]. In the upper arm, photons with 90° polarization can pass through the linear polarizer (LP-2) set at 90° and reach the SPDM-2 (id201) [20, 22]. The TTL outputs of both SPDMs are connected to the microcontroller, which compares the bits received by the SPDMs with the ones the were sent, in order to calculate the $\widehat{\text{QBER}}$ according to (4).

### B. Experimental Data

In Fig. 4 we present the variation of the $\widehat{\text{QBER}}$ with time, for different fiber lengths.

The experimental results show that the $\widehat{\text{QBER}}$ in a back-to-back situation is almost constant with time, starting at a value of about 0.5%. This value is much close to the devices limit, and traduces an interference visibility of 99%, which is very good [1]. This behaviour for back-to-back also traduces proper alignment of polarization and good stability of the system. When we add an optical fiber for transmission of the photons, we can see for the case when $L = 5$ km, that the $\widehat{\text{QBER}}$ starts to increase due to random rotations of polarization in the fiber. Increasing even more the fiber length, i.e., when the

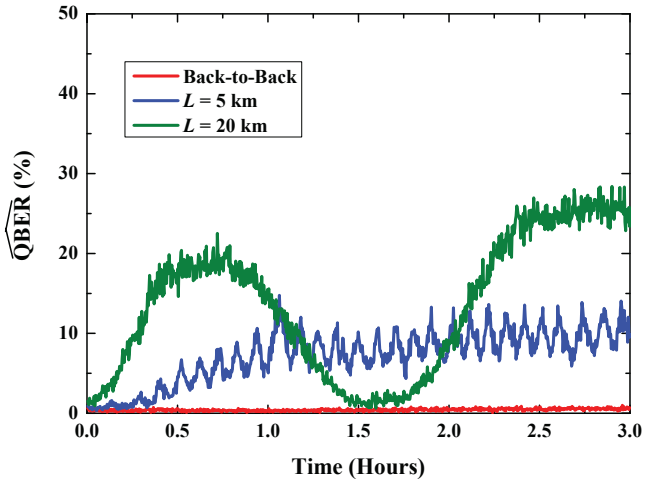


Fig. 4. $\widehat{\text{QBER}}$ as a function of time, for several propagation fiber lengths.

fiber length $L = 20$ km, the $\widehat{\text{QBER}}$ shows a more random behaviour, as we have seen in Fig. 2.

These results highly recommend the use of a polarization control scheme, in order to maintain the $\widehat{\text{QBER}}$ low, and to be possible to use this scheme in QKD experiments, guaranteeing the security of the transmission.

## IV. Conclusions

From the theoretical and the experimental results presented in this paper, we concluded that the $\widehat{\text{QBER}}$ is highly dependent on time, and also on the fiber length were the photons are transmitted. The background $\widehat{\text{QBER}}$, that is also achieved in a back-to-back situation, highly depends on the number of cross-talk photons from the synchronization channel to the quantum channel, and the alignment of polarization.

The counter-propagating scheme for sending the synchronization pulse allows to avoid largely the cross-talk photons, which decreases the need for high quality filters. The $\widehat{\text{QBER}}$ highly depends also on the stability of the system, with main attention to the lasers, the power source and the fiber.

We concluded that an active polarization control scheme is mandatory in order to assure small $\widehat{\text{QBER}}$ values, compatible with a real and efficient implementation of quantum cryptographic protocols.

## References


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

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

[3] ——, "Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working]," *SIGACT News*, vol. 20, pp. 78–80, November 1989.

[4] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental Quantum Cryptography," *Journal of Cryptology*, vol. 5, pp. 3–28, 1992.

[5] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters*, vol. 67, pp. 661–663, Aug. 1991.

[6] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, pp. 3121–3124, May 1992.

[7] D. Bruß, "Optimal Eavesdropping in Quantum Cryptography with Six States," *Physical Review Letters*, vol. 81, pp. 3018–3021, Oct. 1998.

[8] W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Physical Review Letters*, vol. 91, no. 5, p. 057901, Aug. 2003.

[9] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations," *Physical Review Letters*, vol. 92, no. 5, p. 057901, Feb. 2004.

[10] A. Muller, J. Breguet, and N. Gisin, "Experimental Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fibre over More than 1 km," *Europhysics Letters*, vol. 23, pp. 383–388, Aug. 1993.

[11] 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.

[12] F. A. Mendonça, D. B. de Brito, J. B. R. Silva, G. A. P. Thé, and R. V. Ramos, "Experimental Implementation of B92 Quantum Key Distribution Protocol," in *Telecommunications Symposium, 2006 International*, Sep. 2006, pp. 712–717.

[13] S. Ali and O. Mahmoud, "Implementation of SARG04 decoy state quantum key distribution," in *Telecommunication Systems, Services, and Applications (TSSA), 2011 6th International Conference on*, oct. 2011, pp. 86–90.

[14] Y.-C. Jeong, Y.-S. Kim, and Y.-H. Kim, "Weak-pulse implementation of B92 quantum cryptography protocol in free-space," pp. 1–4, 2007. [Online]. Available: http://qopt.postech.ac.kr/publications/B92_ver3.pdf

[15] Y.-C. Jeong, K.-Y. Hong, Y.-S. Kim, and Y.-H. Kim, "Weak-pulse implementation of SARG04 quantum cryptography protocol in free space," in *Lasers and Electro-Optics, 2008 and 2008 Conference on Quantum Electronics and Laser Science. CLEO/QELS 2008. Conference on*, may 2008, pp. 1–2.

[16] N. J. Muga, M. F. S. Ferreira, and A. N. Pinto, "QBER Estimation in QKD Systems With Polarization Encoding," *Journal of Lightwave Technology*, vol. 29, pp. 355–361, Feb. 2011.

[17] 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.

[18] P. K. A. Wai and C. R. Menyuk, "Polarization Mode Dispersion, Decorrelation, and Diffusion in Optical Fibers with Randomly Varying Birefringence." *Journal of Lightwave Technology*, vol. 14, p. 148, Feb. 1996.

[19] N. J. Muga, M. F. S. Ferreira, and A. N. Pinto, "Broadband polarization pulling using Raman amplification," *Optics Express*, vol. 19, p. 18707, Sep. 2011.

[20] 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.

[21] 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 May 17, 2012.

[22] ——, "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 May 17, 2012.