

Backscattering limitation for fiber-optic quantum key distribution systems

Darius Subacius, Anton Zavriyev, and Alexei Trifonov^{a)}

MagiQ Technologies, Inc., 11 Ward Street, Somerville, Massachusetts 02143

(Received 29 June 2004; accepted 29 October 2004; published online 22 December 2004)

We characterized backscattering effects in optical fiber using a photon counting technique and considered its implications for quantum key distribution (QKD). We found that Rayleigh (elastic) backscattering can put strong limitations on a two-way QKD system's performance. Raman (inelastic) scattering can restrict the ability of wavelength multiplexing of a quantum channel with strong classical data channel(s). © 2005 American Institute of Physics. [DOI: 10.1063/1.1842862]

Advances in quantum key distribution (QKD) in fiber-optic networks dictate the necessity for system improvement to increase transmission distance and key transmission rate.¹ In a typical QKD setup, communication occurs between two parties, traditionally called Bob and Alice. Alice transmits single photons and encodes the information in their polarization or phase, while Bob randomly chooses predetermined coordinate bases to measure the photon's properties.^{1,2} This is followed by a public discussion on a classical light channel during which sifting, error correction, privacy amplification, and key generation occur (see, for example, BB84 protocol).^{2,3} To properly conduct this procedure, Bob and Alice need to be synchronized; this can be done by sending strong light pulses between them. To optimize the resource utilization, these classical channels should share the transmission fiber with the QKD photons. In addition, from the optical networking perspective there is a practical need to combine QKD with classical wavelength division multiplexing optical channels.⁴ Some of the photons from the classical channel can undergo spontaneous inelastic Raman scattering into the quantum channel bandwidth. This effect is characterized by wide frequency bandwidth, and is proportional to the total power of classical channels and depends on the fiber link length. Since QKD involves detecting single photons, very sensitive detectors are required,⁵ and any background light in the fiber increases the system noise level and limits its performance.

Yet another noise mechanism involves Rayleigh backscattering of the quantum channel itself. In a typical one-way QKD setup, Alice sends a signal to Bob. Any known implementation of a one-way system requires active interferometer stabilization. An elegant solution to this problem, so-called "plug-and-play system," has been proposed by Müller *et al.* in Ref. 6. It involves sending a light pulse from Bob to Alice and then reflecting it back to Bob by a Faraday mirror and signal encoding. Bidirectional pulse transmission compensates for fiber-induced polarization fluctuations, and removes the requirement of interferometer stabilization.^{1,6,7} While solving many practical problems associated with one-way interferometry, plug-and-play system introduces problems of its own: strong laser pulses propagating from Bob to Alice can suffer Rayleigh scattering by fiber refractive index inhomogeneities. A fraction of this scattered light is captured in the fiber spatial mode and propagates in the backward direction (i.e., back to Bob). Since this light is of the same fre-

quency as the initial pulses, it cannot be decoupled using optical filtering and ends up in the detectors. Because the effect can happen any place in the fiber, the scattering cannot be gated away by timing the detectors, resulting in an increased false click probability. This effect can be suppressed by sending the trains of pulses and using a storage line of corresponding length at Alice's station;⁸ however, this approach decreases an effective key rate.

In this work we studied how the Rayleigh and Raman light scattering in optical fibers affect QKD. A two-way system is more vulnerable to backscattering effects, and especially to Rayleigh scattering. Results of Raman scattering, meanwhile, can be applied to both systems.

We used the following simple model to estimate the scattering effects on QKD. Consider a QKD link of distance L [km] and fiber loss α_1 [dB/km]. We denote the channel transmission as $\eta_F = 10^{-\alpha_1 L/10}$ and total (round-trip) loss inside Alice as L_A [dB] ($\eta_A = 10^{-L_A/10}$). From a system performance point of view, L_A must be minimized; its lower limit is given by the choice of the components. At the same time, due to the risk of eavesdropper (Eve) using a Trojan horse attack,^{1,9} L_A can not be arbitrarily small. In the rest of the analysis we assume it to be 20 dB. If the experimental situation dictates a lower or higher loss value, results should be rescaled correspondingly.

Optical fiber Rayleigh backscattering can be characterized by a single coefficient β , which describes a fraction of cw forward propagated light backscattered into the fiber spatial mode. For optical time domain reflectometry applications, backscattering is usually defined for a single launched pulse. The actual level then depends on the pulse duration and acquisition time window. The cw limit corresponds to the infinite pulse duration and acquisition time.

Consider a two-way QKD system with a pulse repetition rate R . The number of photons per second launched by Bob can be given by

$$P_{\text{in}} = R \frac{\mu}{\eta_A \eta_F}, \quad (1)$$

where μ is a mean number of photons per pulse. If weak coherent pulses are used, the probability of finding n photons in a pulse follows the Poisson statistics:

$$p(n, \mu) = \frac{\mu^n}{n!} e^{-\mu}. \quad (2)$$

As μ increases, the probability of multiphoton pulses becomes significant and Eve can successfully conduct a photon

^{a)}Electronic mail: alexei@magiqtech.com

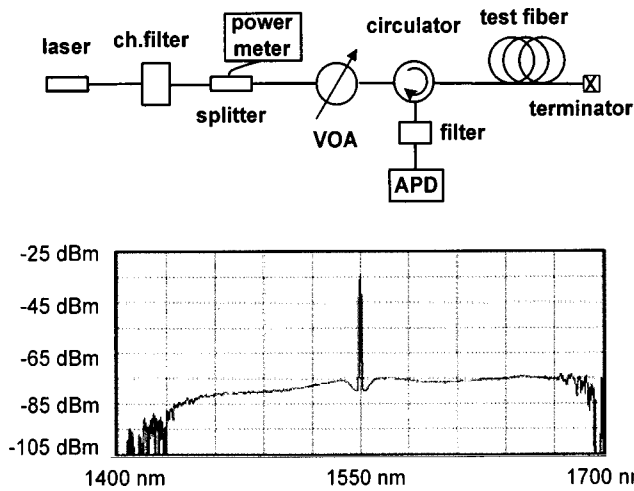


FIG. 1. Scattering experimental setup. Inset shows a typical Raman scattering spectrum.

number splitting attack.^{10,11} To reject this attack, Alice must decrease the value of μ as the channel loss increases. The ultimate security model states that all the multiphoton pulses can be eavesdropped by Eve.¹⁰ Making an assumption that Eve can change the channel loss but not the detector quantum efficiency (QE), we end up with a condition $\mu = \eta_F$.^{12,13} Eq. (1) can be then simplified to

$$P_{\text{in}} = \frac{R}{\eta_A}. \quad (3)$$

The backscattered light level (in photon/sec) is then given by

$$P_{\text{back}} = [1 - \exp(-2\alpha_2 L)] P_{\text{back}}^0, \quad (4)$$

where P_{back}^0 is the light backscattered from an infinite fiber:

$$P_{\text{back}}^0 = \beta P_{\text{in}} \quad (5)$$

and $\alpha_2 = \alpha_1 \times (\ln 10/10)$.

We further assume that the QKD signal is detected using gated avalanche photo diodes (APDs),^{5,13} with the following parameters: gate pulse width δt , dark current rate DCR, and quantum efficiency QE. The probability of getting a false click caused by Rayleigh scattering is

$$p_{\text{Rayleigh}} = [1 - \exp(-2\alpha_2 L)] \beta \frac{R}{\eta_A} \delta t \text{QE}. \quad (6)$$

In addition, if other optical (classical) channels are present, their Raman scattering contribution can be estimated by

$$p_{\text{Raman}} = [1 - \exp(-2\alpha_2 L)] \beta_R(\lambda) \delta t \text{QE} \cdot P_{\text{in}} \cdot \Delta\lambda, \quad (7)$$

where $\beta_R(\lambda)$ is a coefficient defining Raman backscattering into 1 nm bandwidth in a manner similar to that of the Rayleigh coefficient [Eq. (5)]. The Raman contribution depends on the wavelength of a classical channel, and on the bandwidth $\Delta\lambda$ of the filter in front of the receiver.

Figure 1 shows our experimental setup. The output of a pulsed [repetition frequency=600 KHz, full width at half-maximum (FWHM) ~ 50 ps] laser passed through a 100 GHz channel filter and a circulator, and was launched into a 26-km-long fiber spool standard single-mode fiber (SMF) or LEAF (® Corning). (Scattering from an infinitely long fiber spool should be roughly 10% higher.) The back-

TABLE I. Raman and Rayleigh backscattering test results for SMF fiber.

Type of scattering	Photons/pulse	Average power	False click probability
Rayleigh	1×10^4	-61 dBm	1.3×10^{-4}
Raman	5×10^7	-26 dBm	5.5×10^{-5}

scattered light was passed through a tunable filter and directed through a variable attenuator into a gated InGaAs/InP APD, cooled to -80 °C ($\delta t = 2$ ns, QE=10%, DCR $\approx 2 \times 10^{-6}$). An optical spectrum analyzer was used to monitor the scattering spectrum.

A typical Raman scattering spectrum is shown as an inset in Fig. 1. A 1538 nm laser was used in a Raman scattering photon-counting measurement. We measured the count rate when the receiver filter was set at $\lambda = 1549$ nm ($\Delta\lambda = 0.8$ nm). For the Rayleigh scattering characterization, we used a 1549 nm laser. Measurement results for the SMF fiber are summarized in Table I.

From these measurements we estimated the Rayleigh backscattering coefficient for the SMF as $\beta = -40.5$ dB. (Rayleigh backscattering for the LEAF fiber was slightly larger: $\beta = -39.5$ dB.)

We used our data to estimate the scattering effects in a bidirectional QKD setup. Figure 2 shows the detector false click probability as a function of the transmission distance. Contributions from imperfect interferometer visibility, and Rayleigh backscattering [for different repetition rates R as given by Eq. (6)] are shown on a graph. We assumed a standard fiber loss $\alpha_1 = 0.2$ dB/km, $\beta = -40$ dB, and a 20 dB round-trip loss inside Alice. The mean number of photons launched by Bob is equal to 100. We also assumed the following detector parameters: $\delta t = 1$ ns, DCR = 10^{-6} , and QE = 10%. As the figure shows, the Rayleigh backscattering contribution (at $R = 1$ MHz) becomes the dominant error contribution at distances larger than 90 km. This means, when ultimate security is desired, that Rayleigh scattering quickly becomes a limiting factor for longer transmission distances and higher pulse repetition rates. The only known solution is to reduce the repetition rate, which causes key distribution to be rather slow and inefficient. The idea of Bethune *et al.* to

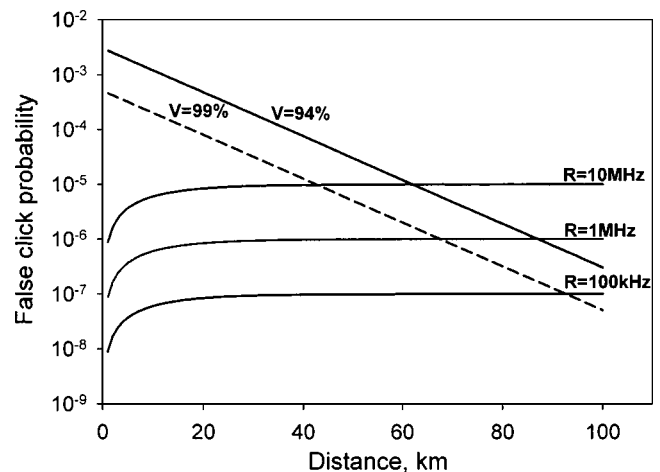


FIG. 2. Detector false click probability vs distance in ultimate security model: contribution from interferometer visibility ($V = 94\%$ and 99%), and Rayleigh backscattering noise for different pulse repetition rates R .

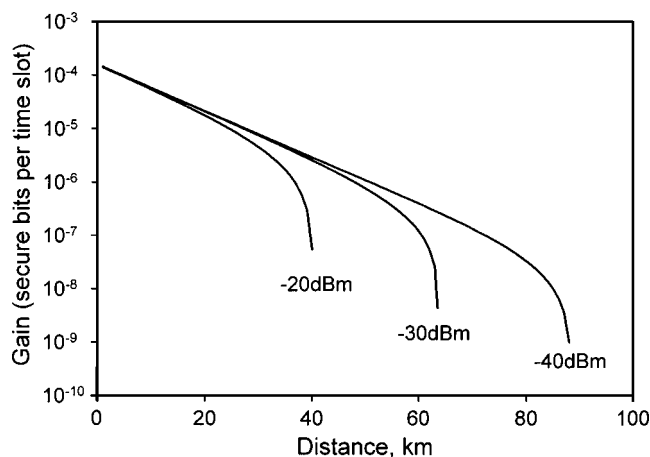


FIG. 3. Secure bit gain per time slot vs distance for different classical channel launch power. Quantum and classical channels are 10 nm apart, receiver filter bandwidth is 0.8 nm (100 GHz).

shift the frequency at Alice does not work well due to dispersion.¹⁴

When a weak quantum signal is forced to share the fiber with strong classical channels (synch or data), Raman scattering can become a limiting factor in a QKD system. Large Raman bandwidth (>240 nm) puts a limitation on the optical power of classical channels. The magnitude of this effect depends on the channel's wavelength and on the optical filter used in front of Bob's quantum detectors. Figure 3 shows secure bit gain as a function of QKD transmission distance for different average power launched into a classical channel. (Channel separation of 11 nm and a filter FWHM of 0.8 nm

were assumed.) We used a measured Raman scattering coefficient value.

In conclusion, backscattering can be a major limitation for bidirectional QKD. Even with improved detector performance (QE and DCR, afterpulsing, etc.), Rayleigh scattering can limit the key rate. Raman scattering, on the other hand, puts stringent power restrictions on additional optical channels sharing the same fiber.

¹N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).

²C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), pp. 175–179.

³C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *J. Cryptology* **5**, 3 (1992).

⁴M. S. Goodman, P. Toliver, R. J. Runser, T. E. Chapuran, J. Jackel, R. J. Hughes, C. G. Peterson, K. McCabe, J. E. Nordholt, K. Tyagi, P. Hiskett, S. Mcnown, N. Nweke, J. T. Blake, L. Mercer, and H. Dardy, *Conference Proceedings—Lasers and Electro-Optics Society Annual Meeting-LEOS, 2003*, Vol. 2, p. 1040.

⁵D. Stucki, G. Ribordy, A. Stefanov, H. Zbinden, J. G. Rarity, and T. Wall, *J. Mod. Opt.* **47**, 1967 (2001).

⁶A. Müller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, *Appl. Phys. Lett.* **70**, 793 (1997).

⁷D. S. Bethune and W. P. Risk, *IEEE J. Quantum Electron.* **36**, 340 (2000).

⁸G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinard, and H. Zbinden, *J. Mod. Opt.* **47**, 517 (2000).

⁹A. Trifonov, A. Zavriyev, D. Subacius, R. Alléaume, and J.-F. Roch, *Proc. SPIE* **5436**, 1 (2004).

¹⁰N. Lutkenhaus, *Phys. Rev. A* **61**, 052304 (2000).

¹¹G. Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders, *Phys. Rev. Lett.* **85**, 1330 (2000).

¹²G. Gilbert and M. Hamrick, arXiv: quant-ph/0009027.

¹³A. Trifonov, D. Subacius, A. Berzanskis, and A. Zavriyev, *J. Mod. Opt.* **51**, 1399 (2004).

¹⁴D. S. Bethune, M. Navarro, and W. P. Risk, *Appl. Opt.* **41**, 1640 (2002).