Experimental Investigation of the Performance Limits for First Telecommunications-Window Quantum Cryptography Systems

Paul D. Townsend

Abstract—**Quantum cryptography offers the unique possibility of certifiably secure key distribution between remote locations. Practical systems require efficient, low noise, single photon avalanche photodiodes (SPAD's) to achieve this goal. This letter reports experimental results from a polarization-encoded system utilizing a state-of-the-art silicon SPAD. The system is used to investigate the performance limits of quantum cryptography systems operating in the first optical fiber communication window at wavelengths around 0.8 μm. The results demonstrate the potential for secure quantum key distribution at Mb·s^1 rates over fiber LAN's also carrying conventional high-speed (Gb·s^1) data channels at a wavelength of 1.3 μm.**

Index Terms—**Cryptography, data security, optical fiber communications, optics, quantum cryptography, quantum processing.**

QUANTUM cryptography [1]–[3] solves one of the central problems in secure communications by exploiting the laws of quantum mechanics in order to achieve certifiably secure key distribution between two or more [4] locations. The scheme developed by Bennett and Brassard [1] uses a single-photon-based quantum communication channel to establish shared random bit strings that are encoded using pairs of conjugate quantum observables such as the linear and circular photon polarization states (BB84 protocol). These observables are incompatible in the sense that a measurement of one necessarily changes the value of the other. The BB84 coding scheme is designed to force an eavesdropper into frequently performing an incompatible quantum measurement on the channel and thereby generating an error. An insecure classical channel is subsequently used for a public exchange of information that allows the number of such errors to be estimated and, hence, the secrecy of the transmission tested. In real systems noise from sources such as detector, dark counts will generate errors in the transmission even when no eavesdropper is present. Nevertheless, the measured error rate can be used to provide a conservative upper limit on the potential information leakage present on the channel. If the error rate is sufficiently low (typically of the order of a few percent in practice), then error correction [2] and "privacy amplification" [5] can be employed to generate a final error-free and certifiably secret key. This key can then be safely used together with an appropriate algorithm for data encryption purposes.

To date there have been a number of practical demonstrations of secure quantum key distribution over multikilometer distances on optical fiber point-to-point links [6]–[9] and multiuser passive optical networks [4] with recent experiments extending the achievable span to around 50 km at a wavelength of 1.3 μm [10], [11]. A key component in such a system is the single photon detector in the receiver which is usually an avalanche photodiode biased beyond breakdown and operating in the Geiger mode (SPAD) [12]. In previous work, we have employed germanium SPAD's because of their ability to count photons at a wavelength of 1.3 μm where optical fiber loss is low and the achievable transmission distances are, therefore, large (up to 50 km). However, these detectors require cryogenic cooling to 77 K in order to reduce their effective dark count rate to about 10^4 s^{-1}, which is still a relatively large value. In comparison, silicon SPAD's are currently at a much more advanced stage of development. For example, the EG&G SPCM-AQ module used in this study is a compact Peltier-cooled device with a dark count rate of about 50 s^{-1} and a high quantum efficiency of 50% at a wavelength of 0.83 μm. The relatively high-fiber loss and dispersion in the 0.8-μm wavelength region do not favor long distance applications. However, as will be demonstrated, for short span applications in LAN's, for example, silicon SPAD's may be the detectors of choice for high-performance quantum cryptography systems.

Fig. 1 shows a schematic diagram of the experimental setup. The transmitter contained an 0.83-μm-wavelength semiconductor laser that was gain-switched at a clock rate of 400 MHz to provide a train of 80-ps duration pulses. These pulses were attenuated to a mean photon number $\mu \ll 1$, and then encoded with a random bit sequence using a polarization coding scheme where vertical polarization represents binary 1 ($V = 1$) and horizontal polarization represents binary 0 ($H = 0$). Encoding was achieved using a 1×2 LiNbO$_3$ modulator driven by a 400 Mb·s^{-1} ($2^{23}-$ 1) pseudorandom bit sequence (PRBS), with path-to-polarization conversion performed by means of static polarization controllers and a polarization combiner at the modulator output ports. Note that the BB84 protocol also requires the use of the right and left circular polarization states, however, the current scheme is adequate for testing most of the basic performance parameters. In a fully implemented BB84 system the receiver must switch randomly between linear and circular polarization measurements in each data period. However, the simplified single polarization basis

Manuscript received February 2, 1998.

The author is with BT Laboratories, Martlesham Heath, Ipswich, IP5 3RE, U.K.

Publisher Item Identifier S 1041-1135(98)04701-6.

1041–1135/98$10.00 © 1998 IEEE

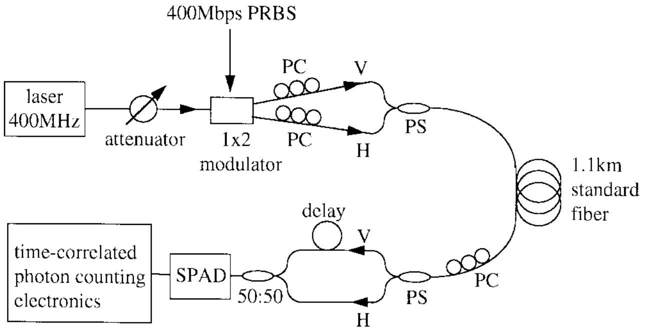

Fig. 1. Schematic diagram of the experiment. PC: Polarization controller. PS: Polarization splitter/combiner. V: Vertical polarization state = 1. H: Horizontal polarization state = 0.

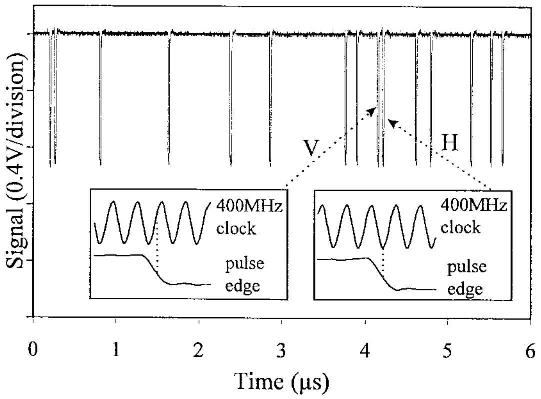

Fig. 2. Silicon SPAD output pulses representing a random bit sequence received at a mean rate of 2.4 Mb·s^{-1}. The insets show how counts arising from the $H = 0$ and the $V = 1$ photons can be distinguished from their different positions in the 400-MHz clock cycle.

scheme used here only required a static polarization controller to compensate for polarization evolution in the fiber and a polarization splitter to separate the $H = 0$ and the $V = 1$ photons. A single EG&G silicon SPAD was connected to the polarization splitter via a 50:50 fiber coupler and counts arising from the $H = 0$ and the $V = 1$ photons were distinguished by means of the 1.25-ns differential time-delay introduced by a fiber delay loop in one of the paths. The transmission link was a 1.1-km length of standard single-mode telecommunication fiber. The system also contained a pair of wavelength-division multiplexers (WDM's) so that a conventional 1.3-μm data channel, simulated by a 1.2 Gb·s^{-1} (2^{23}− 1) PRBS, could be propagated through the fiber at the same time as the 0.83-μm quantum channel. Apart from the transmission fiber, all components in the experiment had fiber pigtails that were single-moded (SM) at 0.83 μm.

Since standard fiber can support more than one spatial mode at the chosen operating wavelength it was necessary to control the fiber launch conditions to obtain stable SM behavior. The modal behavior was characterized using time-resolved photon counting measurements of pulse propagation through the fiber. The photocount distributions contained peaks due to both the LP_{01} and LP_{11} modes [13], and the relative magnitudes of the peaks were used to determine the proportion of photons propagating in each mode. When the transmitter and receiver SM pigtails were fusion-spliced to the transmission fiber only 0.4% of the photons were launched into the LP_{11} mode compared with 99.6% in the LP_{01} fundamental mode. Furthermore, no additional coupling could be induced either by breaking and resplicing the transmission fiber, or by submitting the fiber to thermal and mechanical strain. The small proportion of LP_{11} photons were further reduced at the receiver by the spatial filtering effect of the SM pigtail. Hence, stable SM behavior was readily attained with no observable instabilities or errors due to modal interference or dispersion.

Fig. 2 shows an oscilloscope trace of a typical sequence of photon-generated SPAD output pulses, obtained with a μ-value of 0.1 at the input to the transmission fiber. The insets to the figure illustrate how the time-correlated photon counting electronics in the receiver use leading-edge discrimination to determine the arrival times of the individual photons and to distinguish the $H = 0$ and $V = 1$ detection events by means of their different positions within the 400-MHz clock cycle. In the case of the small sample shown in the figure, the receiver detected photons in clock periods: 76, 101, 319, 647, 948, 1141, 1500, 1555, 1656, 1681, 1840, 1913, 2108, 2204, and 2259, representing the random bit sequence: 101 101 101 001 111. In a BB84 quantum cryptography system the list of "successful" clock periods would be publicly revealed (along with the type of measurement performed by the receiver in each successful period i.e., circular or linear) to enable the transmitter and receiver to establish a shared subset of bits from the initial random sequence. As is always the case in a practical quantum cryptography system, the mean count rate in the experiment was significantly less than the laser clock rate. This was due to the fiber loss (~3 dB), loss in the receiver components and connectors (not shown in Fig. 1) (~8 dB), SPAD quantum efficiency (50%) and the low mean photon number ($\mu = 0.1$) per input pulse (the low μ-value ensures that the probability for an eavesdropper to undetectably split a pulse is small [2]). Because of these inefficiencies, the mean count rate of 2.4×10^6 counts s^{-1} was comfortably below the maximum value of 2×10^7 counts s^{-1} set by the SPAD deadtime. Since about half of the bits are discarded in the public discussion stage of the quantum cryptographic protocol the measured count rate translates to a maximum potential key distribution rate of about 1.2 Mb·s^{-1}. This is some 3 orders of magnitude higher than in previous experiments with germanium SPAD's [4], [6]. The improvement is due to the silicon SPAD's high quantum efficiency, fast avalanche quenching and recovery, and negligible after-pulsing. All of these properties favor high-speed photon counting with negligible noise or saturation penalties.

Perhaps the most important parameter for a quantum cryptography system is the quantum channel bit-error rate (QBER), since this determines the security of the system. The design aim is to achieve background QBER's of a few percent or less so that error correction and privacy amplification procedures can be used to generate certifiably secret keys [2], [5]. QBER measurements were performed by gating the receiver electronics with 550-ps-wide windows centred on the $V = 1$ and $H = 0$ photocount peaks and monitoring the number of $V = 1$ photons falling in the $H = 0$ window

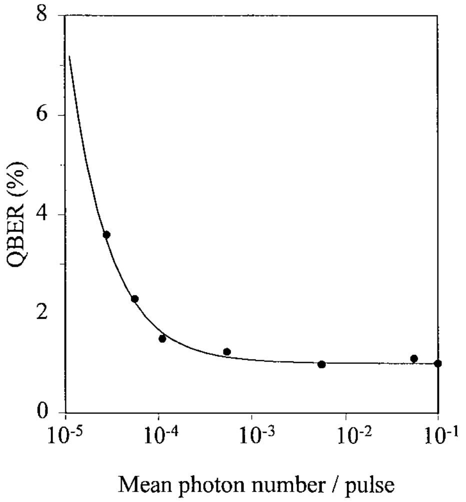

Fig. 3. QBER as a function of input photon number. Filled circles: Experimental points. Solid line: Prediction based on measured SPAD dark count and measured depolarization factor.

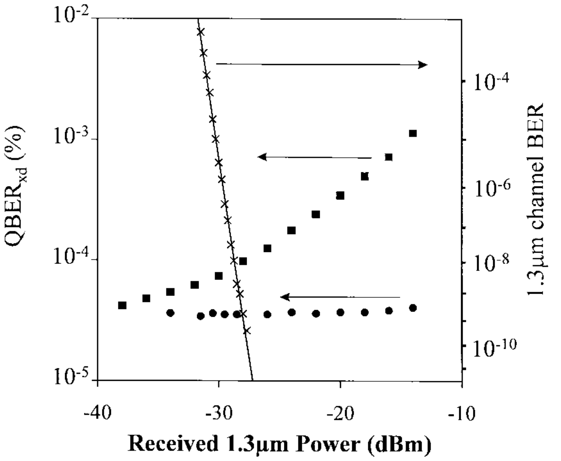

Fig. 4. $QBER_{xd}$ contribution from dark counts and 1.3-μm crosstalk for co- (squares) and counterpropagating (circles) cases and conventional channel BER (crosses) as a function of received 1.3-μm power. The crosstalk induced contribution to the *total* QBER ($= 10^{-2}$) is negligible at all power levels.

and vise versa. The photocount peaks showed FWHM values of 450 ps due to the intrinsic timing jitter associated with the avalanche buildup in the SPAD. Note that the differential delay for the $V = 1$ and $H = 0$ photons (1.25 ns) and the laser clock period (2.5 ns) were both chosen to be large compared with this resolution time so that timing errors in which a photon is misregistered in an adjacent clock period were minimized. The QBER data is shown in Fig. 3 together with a fit based on the SPAD dark count and the measured depolarization factors in the system. For μ values in the range $10^{-1} - 10^{-4}$ the QBER has a constant value of about 1% that is dominated by depolarization-induced errors. These errors arise from dynamic depolarization due to the nonflat frequency response of the modulator and from static depolarization that results from the finite extinction ratios of the various polarizing components in the system. For $\mu < 10^{-4}$ the QBER rises as the dark counts falling within the 550–ps-wide photocount windows start to become the dominant contribution to the noise. Since the fiber loss is 2.5 dB·km^{-1} at 0.83 μm, these results suggest that systems with spans of up to about 10 km could also operate with low QBER's of ~1% with $\mu = 0.1$. Fig. 4 shows the results of further experiments performed with the 1.3-μm conventional data channel turned on. The contribution to the QBER from dark counts and 1.3-μm crosstalk $QBER_{xd}$ is plotted in the graph as a function of received 1.3-μm power for both copropagating and counterpropagating channels. The effects of crosstalk are only observable in the copropagating case and the contribution to the overall QBER ($= 1\%$) is negligibly small. For example, when the conventional channel is operating essentially error-free at a received power level of -27 dBm the QBER value due to crosstalk and dark counts is only ~0.01%. This excellent isolation is due to the WDM's (>50 dB) and the very low quantum efficiency of the silicon SPAD at 1.3 μm, which was measured to be $\sim 10^{-7}$.

In conclusion, quantum cryptography systems based on silicon SPAD's may be good candidates for applications on LAN's and short-span links up to about 10 km in length. WDM techniques may be used to add a 0.8-μm quantum key distribution channel to a fiber system carrying conventional high data channels at 1.3 or 1.5 μm. In this case, keys distributed securely over th e quantum channel can then be used for encrypting the traffic carried by the conventional channel.

Acknowledgment

The author would like to thank G. Buller for useful discussions and K. Blow for advice and support for this work.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public-key distribution and coin tossing," in *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing*, Bangalore, India, 1984, pp. 175–179.

[2] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, pp. 3–28, 1992.

[3] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, 1991.

[4] P. D. Townsend, "Quantum cryptography on multi-user optical fiber networks," *Nature*, vol. 385, pp. 47–49, 1997.

[5] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion, *SIAM J. Comput.*, vol. 17, pp. 210–229, 1988.

[6] C. Marand and P. D. Townsend, "Quantum key distribution over distances as long as 30 km," *Opt. Lett.*, vol. 20, pp. 1695–1697, 1995.

[7] J. D. Franson and B. C. Jacobs, "Operational system for quantum cryptography," *Electron. Lett.*, vol. 31, pp. 232–234, 1995.

[8] R. J. Hughes, G. G. Luther, G. L. Morgan, and C. Simmons, "Quantum cryptography over 14 km of installed optical fiber," in *Proc. 7th Rochester Conf. Coherence and Quantum Optics*, J. H. Eberly, L. Mandel, and E. Wolf, Eds. New York: Plenum, 1996, pp. 103–112.

[9] A. Muller, H. Zbinden, and N. Gisin, "Underwater quantum coding," *Europhys. Lett.*, vol. 378, p. 449, 1996.

[10] R. J. Hughes, W. T. Butler, P. G. Kwiat, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Quantum cryptography over 48 km of underground optical fiber," presented at Opt. Soc. Amer. Annu. Meet., 1997, paper MG3.

[11] P. D. Townsend, "Quantum cryptography on fiber networks," presented at Opt. Soc. Amer. Annu. Meet., 1997, paper ThJJ1.

[12] A. Lacaita, P. A. Francese, F. Zappa, and S. Cova, *Appl. Opt.*, vol. 33, pp. 6902–6918, 1994.

[13] P. D. Townsend, C. Marand, S. J. D. Phoenix, K. J. Blow, and S. M. Barnett, "Secure optical communication systems using quantum cryptography," *Phil. Trans. R. Soc. Lon. A*, vol. 354, pp. 805–817, 1996.