Experimental study of high speed polarization-coding quantum key distribution with sifted-key rates over Mbit/s

Xiao Tang, Lijun Ma, Alan Mink, Anastase Nakassis, Hai Xu, Barry Hershman, Joshua C. Bienfang, David Su, Ronald F. Boisvert, Charles W. Clark and Carl J. Williams

National Institute of Standards and Technology, 100 Bureau Dr., Gaithersburg, MD 20899
xiao.tang@nist.gov; alan.mink@nist.gov

Abstract: We present a quantitative study of various limitations on quantum cryptographic systems operating with sifted-key rates over Mbit/s. The dead time of silicon APDs not only limits the sifted-key rate but also causes correlation between the neighboring key bits. In addition to the well-known count-rate dependent timing jitter in avalanche photo-diode (APD), the faint laser sources, the vertical cavity surface emission lasers (VCSELs) in our system, also induce a significant amount of data-dependent timing jitter. Both the dead time and the data-dependent timing jitter are major limiting factors in designing QKD systems with sifted-key rates beyond Mbit/s.

OCIS codes: (060.4510) Optical communication; (060.2330) Fiber optics communications; (030.5260) Photon counting; (270.5570) Quantum detectors

References and links

1. C. H. Bennet and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (Institute of Electrical and Electronics Engineers, Bangalore, India,1984), pp. 175-179.
2. C. H. Bennett, “Quantum cryptography using any two nonorthogonal states,” Phys. Rev. Lett. **68**, 3121-3124 (1992).
3. N.Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” Rev. Mod. Phys. **74**, 145-195 (2002).
4. J.C. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lum D. H. Su, C. W. Clark, “Quantum key distribution with 1.25 Gbps clock synchronization,” Opt. Express. **7**, 2011-2016 (2004).
5. J. G. Rarity, P. R. Tapster and P. M. Gorman, “Secure Free-space key-exchange to 1.9 km and beyond,” J. Mod. Opt. **48**, 1887-1901 (2001).
6. C. Elliott, D. Pearson, and G. Troxel, “Quantum cryptography in practice,” in SIGCOMM’ 03: Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (ACM Press, New York, 2003), pp. 227-238.
7. D. S. Bethune, M. Navarro, and W. P. Risk, “Enhanced autocompensating quantum cryptography system,” Appl. Opt. **41**, 1640-1648 (2002).
8. J. Breguet, A. Muller, and N. Gisin, “Quantum cryptography with polarized photons in optical fibers, experiment and practical limits,” J. of Mod. Opt., **41**, 2405-2412 (1994).
9. P. D. Townsend, “Experimental investigation of the performance limits for first telecommunication-window quantum cryptography system,” IEEE Photon. Technol. Lett. **10**, pp. 1048-1050 (1998).
10. K. J. Gordon, V. Fernandez, P. D. Townsend, and G. S. Buller, “A Short Wavelength GigaHertz Clocked Fiber-Optic Quantum Key Distribution System,” IEEE J. of Quantum Electron. **40**, 900-908 (2004).
11. X. Tang, L. Ma, A. Mink, A. Nakassis, B. Hershman, J. Bienfang, R. F. Boisvert, C. Clark, and C. Williams, “High Speed Fiber-Based Quantum Key Distribution using Polarization Encoding,” in Optics and Photonics 2005: Quantum Communications and Quantum Imaging III, Proc. SPIE 5893, 1A-1-1A-9 (2005)
12. A. Nakassis, J. Bienfang, and C. Williams, “Expeditious reconciliation for practical quantum key distribution,” in Defense and Security Symposium: Quantum Information and Computation II, Proc. SPIE **5436,** 28-35 (2004).
13. D. S. Pearson and C. Elliott, “On the optimal mean photon number for quantum cryptography,” Eprint quant-ph/0403065 (2004), http://arxiv.org/fpt/quant-ph/papers/0403/0403064.pdf

#10264 - $15.00 USD Received 11 January 2006; revised 6 March 2006; accepted 15 March 2006

14. J. K. Guenter and J. A. Tatum, “Modulating VCSELs,” (Honeywell), http://www.adopco.com/publication/documents/ModulatingVCSELs.pdf.
15. K. J. Gordon, V. Fernandez, G. S. Buller, I. Rech, S. D. Cova, and P. D. Townsend, “Quantum key distribution system clocked at 2 GHz,” Opt. Express **13:** 3015-3020 (2005).

1. Introduction

A quantum key distribution (QKD) system can create a shared, secret cryptographic key over an unsecured optical link [1−3]. These systems use the fundamental quantum properties of single photons to guarantee the security of the shared key, which is commonly called the net key. The net keys generated in this manner, and at sufficiently high rates, enable use of a one-time-pad cipher for encryption of broadband communications links. A number of groups have developed experimental QKD systems operating in both free-space [4, 5] and optical fiber [6, 7]. The first study of a fiber-based polarization coding QKD system with silicon detectors was reported in 1994 [8]. Townsend [9] and Gordon *et al.* [10] reported similar systems in the 800-nm wavelength region using standard single-mode fiber (SMF). More recently, we reported a fiber-based polarization coding QKD system operating at a sifted-key rate of 1.1 Mbit/s [11].

In this work, we implemented the B92 protocol [2]. Although it is well known that the B92 protocol is less secure than the BB84 protocol, it is widely used in the laboratory study of the physical-layer limitations of a QKD system, such as timing jitter, dead time, and polarization leakage. By adding two additional APDs and faint laser sources, a B92 QKD test-bed could be converted to BB84.

Based on the B92 high-speed experimental test-bed we present a quantitative study of various effects that limit further improvements. In comparison with Ref. [11], we increased the sifted-key rate to 2.1 Mbit/s by doubling the bit repetition rate to 625 Mbit/s. At such higher rate, several limiting factors become more significant.

Currently, in most high-speed QKD systems the APDs for detection of different bases and key bit values operate independently in free-running mode. By this means, the highest sifted-key rate achievable equals twice of the inverse of the dead time of the APDs. Moreover, even one could sufficiently increase the quantum channel transmission rate (QCTR) to approach this ultimate limit, the dead time could also induce significant correlation between neighboring sifted-key bits.

The system timing jitter dominates the quantum bit error rate (QBER) causing an increased QBER when it approaches or exceeds the detection time window (i.e., quantum channel transmission period). When the jitter is less than the detection time window, the QBER is dominated by polarization leakage. It is well known that APD could induce the timing jitter in the detected photon signal [15]. In this work, we found that the timing jitter from faint laser sources, VCSELs in our system, is also non-negligible. The timing jitter induced by the VCSELs is data dependent while the jitters from APDs include both data independent part and data dependent part. In APD, the data independent part of the jitter is caused by the statistical fluctuation in the depth, where the photon is absorbed, from the device surface, and the data-dependent part of the jitter is caused by the tails of previous avalanche currents. This paper is organized as follows. In Section 2 we describe the configuration of our system. In Section 3 we present the limiting factors to the performance of the system on the sifted-key rate, QBER and security issue.

2. System configuration

The experimental configuration is shown in Fig. 1. Alice and Bob are PC-based commercial off the shelf computers running a Linux operating system. A pair of custom high-speed data handling printed circuit boards were designed and implemented at NIST. The boards communicate with Alice and Bob via their PCI bus. On each board, there is a field-programmable gate array (FPGA) and gigabit Ethernet serializers/deserializers (SerDes): one for the classical channel and four for the quantum channel. A 1.25 Gbit/s coarse wavelength

Received 11 January 2006; revised 6 March 2006; accepted 15 March 2006

division multiplexer transceiver at each end of 1 km of SMF-28 fiber is used to form the bi-directional classical channel: from Alice to Bob at 1510 nm and from Bob to Alice at 1590 nm. Alice generates classical and quantum data-streams at a synchronized 1.25 GHz. Bob recovers and synchronizes to that clock from the received classical channel data-stream, which uses a standard 8B/10B encoding scheme.

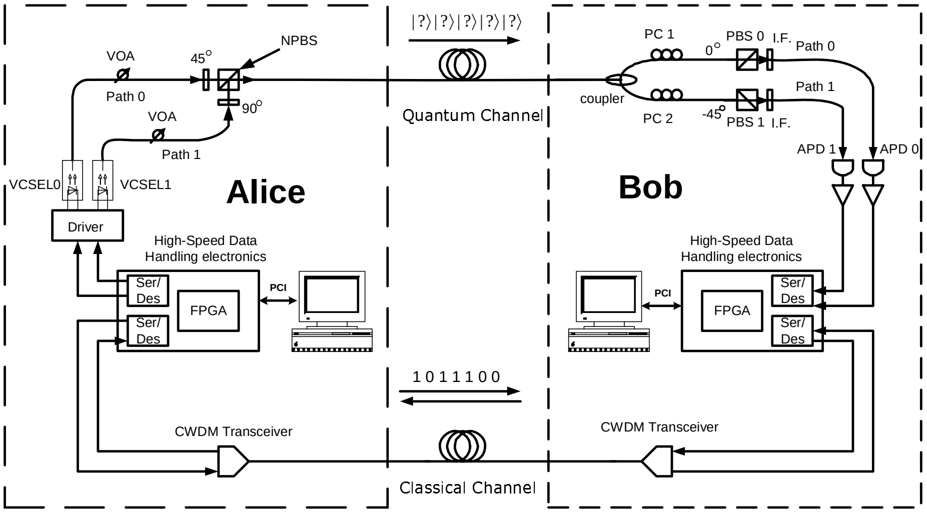

Fig. 1. Configuration of the NIST fiber-based QKD System

Alice and Bob are also connected via a uni-directional quantum channel that is parallel to the classical channel. In order to take advantage of the high-speed 10 GHz multimode vertical-cavity surface-emitting lasers (VCSELs, Advanced Optical Components, HFE6190-561P) and the high speed, high detection efficiency of Si-APDs (PerkinElmer, SPCM-AQR-14), a wavelength of 850 nm is used for the quantum channel. When executing the B92 protocol, Alice randomly fires pulsed light polarized at either +45 degrees (path 0) or +90-degrees (path 1), see Fig. 1. In each path the light from the VCSELs is coupled into a multimode fiber and then attenuated by a variable optical attenuator (VOA). The attenuation is carefully adjusted to yield a mean photon number $\mu = 0.1$ at Alice's output. The attenuated light is then coupled into a single mode 850 nm fiber patchcord and collimated into free-space. The polarization is set by a linear polarizer at +45 degrees (path 0) or +90 degrees (path 1). The paths are combined via a non-polarizing beam-splitting cube (NPBS) and then coupled into a 1 km, single mode fiber (Corning HI780). At the receiver, a 1 x 2 non-polarizing single mode fiber coupler randomly directs photons to one of two paths (path 0 and path 1). A fiber polarization controller (P.C.) is installed in each path to recover the photon's polarization state. To recover the polarization state of the photons, the polarization controllers are adjusted so that photons from VCSEL0 (+45 degrees) have a minimal probability of reaching APD1 and photons from VCSEL1 (+90 degrees) have a minimal probability of reaching APD0. After the P.C., photons pass through a polarizing beam-splitting cube (PBS). The photons from VCSEL0 that reach PBS0 only have 50% probability to pass the PBS0 and the photons from VCSEL1 that reach PBS1 have 50% probability to pass the PBS1. Following the PBS, an interference filter (I.F.) is used to remove noise from other wavelengths. Finally, the photons are coupled into a 62.5 μm multi-mode fiber and focused onto the surface of the Si-APD for detection. This results in a 25% probability of a photon reaching the correct APD, 50% at the coupler and 50% at the PBS.

Received 11 January 2006; revised 6 March 2006; accepted 15 March 2006

Alice generates and stores a non return-to-zero (NRZ) pseudo random data-stream at rates up to 1.25 Gbit/s. Every 2048 clock periods of data is grouped into a packet. In this work, we studied the system with different quantum channel transmission rates (QCTRs), as shown in Table 1. Alice sends a synchronizing message to Bob on the classical channel at the beginning of each quantum packet. Bob searches for the rising edge of the photon detection signals from the APDs. The photon arrival time is influenced by a variety of effects, and the rising edge (as well as the registration of the photon) has a degree of uncertainty in time. It is important to note that when the rising edge falls into another detection time window, a quantum-bit error may be generated. We discuss these effects in the next section. For each detection event, the packet number and bit position within the packet but not the bit value, of the detected photons are returned to Alice over the classical channel. By this means, both Alice and Bob acquired the sifted key. With the similar setup one can also implement BB84 protocol by adding two additional faint lasers and APDs. In BB84, the detection basis of Bob will be also returned to Alice, who will compare it with her basis and send the result back to Bob. According to this result, Bob will sift off those bits with wrong basis. After acquiring the sifted key, both Bob and Alice send these sifted key values to their CPUs for reconciliation and privacy amplification [12] to generate their shared net keys. The QBER can be measured in real time from the sifted key before reconciliation. For convenience, we list the quantum channel transmittance rate (QCTR) performed and corresponding numbers of clock period in Table 1.

Table 1. QCTRs and the corresponding numbers of clock period

Number of clock period	2	4	8	16	32
QCTR (Mbit/s)	625.0	312.5	156.3	78.1	39.1

3. Results and discussion

In this work we focus on increasing the sifted-key rate and reducing the QBER since these quantify system performance for a given transmission distance and mean photon number. Using B92 we transmitted random quantum streams and performed key generation, measuring sifted-key rate and error rates. When the QCTR is set to 625 Mbit/s, we obtained a sifted-key rate of 2.1 Mbit/s. This doubles our previous sifted-key rate [11]. By using the reconciliation and privacy amplification algorithms in ref. [12], we achieved a net key rate of approximately 1 Mb/s for this QCTR setting. With this net key rate we performed a QKD-secured high-speed video transmission over the Internet using one-time pad encryption. This experiment will be discussed further in a later publication. Our focus here is the limiting effects on the sifted key rate and the QBER.

3.1 Sifted-key rate

A major limitation to the sifted-key rate is imposed by the APD. After the APD receives a photon, the avalanche process generates an electrical output signal. The device then needs a certain amount of time (dead time, t_{dead}) to recover its initial operation state for detection of the next photon. During this period, the bias voltage across the p-n junction of the APD is below the breakdown level and no photon can be detected. Moreover, in most high-speed QKD system, the APDs operate in free-running mode and different APDs works independently from each other so that when one APD is in the dead time the other APD can still detect a photon. In this case, the sifted-key rate can be calculated by

$$R = 2/(t_{dead} + 1/R_1) \tag{1}$$

where t_{dead} is 50 ns in this experiment and R_1 is the detection count rate for each APD. In B92,

$$R_1 = \mu \times v \times L_{\mathrm{f}} \times L_{\mathrm{o}} \times L_{\mathrm{c}} \times L_{\mathrm{P}} \times P_{\mathrm{d}}, \tag{2}$$

#10264 - $15.00 USD Received 11 January 2006; revised 6 March 2006; accepted 15 March 2006

where μ is the mean photon number per pulse sent by Alice. There are some discussions [13] that choose a mean photon number greater than 0.1 for a higher sifted-key rate without adverse affects on system security. If we increase the mean photon number our system can run at higher data rate. However, we set it to 0.1 for our experiment as most QKD experimental systems do in practice. The quantity ν is the QCTR. The photon detection efficiency P_d of the APDs is 45% at 850 nm according to the manufacturer's specifications. The quantity L_f represents the optical loss in the transmission fiber and connectors, which is measured to be −3.0 dB. Other optical devices have an additional loss L_o of approximately −2.0 dB. For a given path, the coupler causes 3-dB loss of power (L_c), *i.e.*, photon numbers. The polarization beam splitter further induces 6-dB loss (L_p) for a given path. Ideally, in the B92 protocol the polarization beam splitter blocks all photons in the incompatible bits (bits 1 for PBS in Path 0 and bits 0 for PBS in Path 1), and causes 3-dB loss in average numbers of photons per bit. The photons in incompatible bits could leak though a real PBS but this probability is small and has negligible effect on the sifted key rate. For example a typical PBS has more than 20 dB extinction ratio. In comparison, such imperfect extinction ratio has an important effect on the quantum bit error rate and we will discuss it in the next section.

Most of current 850-nm QKD systems operate with a relative low QCTR so that $t_{dead} << 1/R_1$. In this case, one can approximate R by $2R_1$ and therefore, R increases linearly over QCTR. As one further increases QCTR to achieve sifted-key rate beyond Mbit/s, the increase of the sifted-key rate gradually deviates from the linear growth and, at sufficient high QCTRs, the sifted-key rate is ultimately limited by $2/t_{dead}$. Figure 2 shows our measured sifted-key rate and QBER for different QCTRs. The solid line represents the sifted-key rate calculated with Eq. (1) and the dash line represents the sifted-key rate with the linear approximation (t_{dead}=0). As shown in the figure, the sifted-key rate agrees well with Eq. (1). The figure also shows that our system is operated at the edge of the linear region. The sifted-key rate will be gradually saturated as the QCTR further increases.

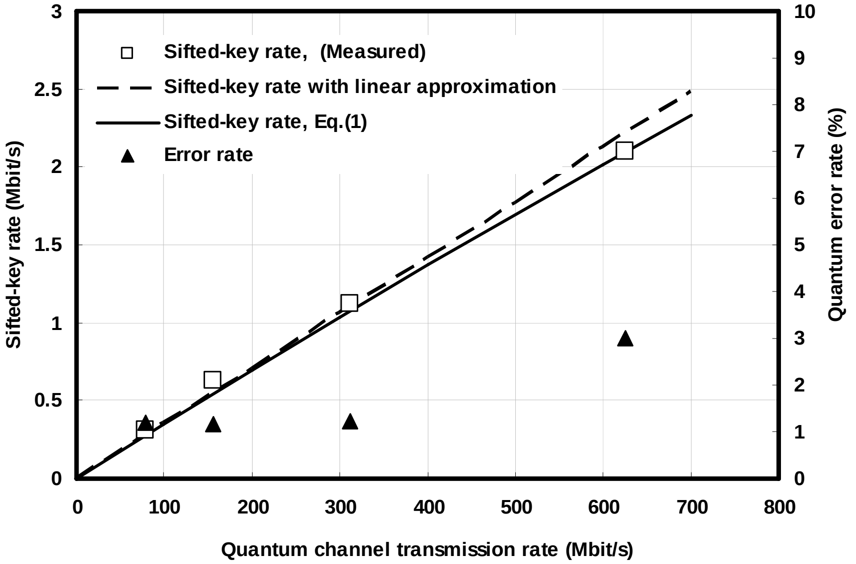

Fig. 2. Sifted-key rate as a function of QCTRs in experiment (open square) and the sifted-key rate calculated with Eq. (2) (dashed line for $t_{dead} = 0$ and solid line for t_{dead} = 50 ns). We also show the QBER at these QCTR (solid triangle).

Moreover, even though we could eventually realize a sifted-key rate of $2/t_{dead}$ with sufficiently high QCTR, the dead time could induce a strong correlation between neighboring sifted key bits. In this region, when one APD is in the dead time, photons can only be detected by the other APD, which generate key bits with different value. Thus the sifted key is not

Received 11 January 2006; revised 6 March 2006; accepted 15 March 2006

completely random and the security could be potentially degraded. When the QCTR is so high that the sifted-key rate is saturated to $2/t_{\text{dead}}$, the firing order of the two APDs can become self-synchronized. In that case, the APDs will come out of their dead time in the same order they entered. When an APD comes out of its dead time there is a high probability of it firing again before any of the other APDs come out of their dead times. This self-synchronized sequence can continue for some time resulting in a burst of non-random sifted keys. One heuristic way to inhibit such events would be disabling all APDs when one fires, until the dead time is over so that detections only occur when all APDs are available. Nevertheless, as can be seen from Fig. 2, our system is currently operating in the linear region and the potential degradation of security is negligible.

3.2 QBER

Quantum-bit errors are mainly caused by the following: (1) Spontaneous triggering of the APDs (dark counts) ; (2) Polarization leakage caused by the imperfect polarization extinction ratio; (3) Timing jitter of the system. The first effect exists in all polarization coding QKD systems and has been widely discussed [3]. Because dark counts and light leakage are independent from the system clock and the data transmission rate, their influences are negligible when the sifted-key rates are near the order of Mb/s.

To achieve a QBER below 1%, the system polarization extinction ratio, the ratio of photons detected by the APDs in compatible and incompatible paths, must be higher than 20 dB. In this experiment, we use polarization controllers to recover the linear polarization states. The highest polarization extinction ratio that we achieved is 25 dB. Due to the drifting birefringence of the quantum-channel fiber, the optimal setting of the polarization controllers is not constant over time. Under the environment of the laboratory, we can keep the extinction ratio above 20 dB for 2−3 hours without need of further adjustment of PCs. As a result, the QBER induced by polarization leakage is approximately 1.2% for QCTRs of 312.5 Mbit/s and below, as shown in Fig. 2, where timing jitter is not a major factor, see below. Such high performance over longer time would require an active polarization compensation sub-system that automatically traces the random fiber drift. Currently we are developing such sub-systems.

Figure 3 shows a “pulse” stream, which is the histogram of the photon detection events from one APD measured for two seconds with a time-correlated photon-counting system as we transmitted a repetitive quantum data stream at a QCTR of 625 Mbit/s. The width of each “pulse” in this histogram serves as a measure of the overall timing jitter in the system. The “pulse” width is influenced by the DC bias of the VCSELs. We selected a proper value of the VCSEL bias to achieve the narrowest “pulse” width and best intensity extinction ratio shown in Fig. 3. Also as can be seen, each “pulse” of the histogram has a non-negligible tail that extends into neighboring detection time windows. Detection events occurring in the wrong time window cause quantum bit errors.

#10264 - $15.00 USD Received 11 January 2006; revised 6 March 2006; accepted 15 March 2006

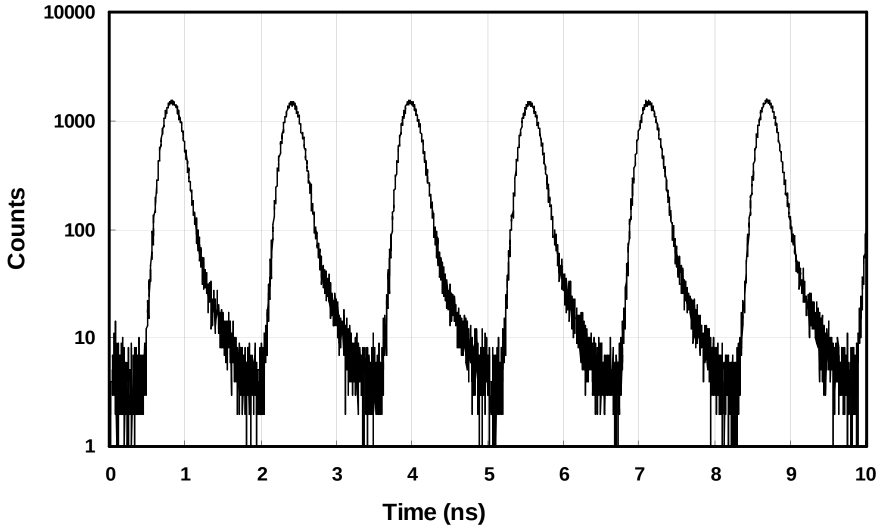

Fig. 3. This “pulse” steam represents a histogram of detection events collected from one APD over 2 seconds using the SPC-600 photon-counting card. The data was measured with a return-to-zero repetitive bit sequence at 625 Mbit/s. The detection time window, or the bit period, is 1.6 ns.

As the QCTR increases, the timing jitter becomes dominating factor for the QBER. For example, as shown in Fig. 2, for QCTR of 312.5 Mbit/s and below, the detection time window (transmission period) is much larger than the timing jitter and therefore the measured QBERs almost remains the same (≈ 1.2%). In these cases, the QBER is mainly due to polarization leakage since the dark counts are negligible at the high data rate in our system. In comparison, at 625 Mbit/s, the QBER increases to 3.08%, (as shown in Fig. 2), as the duration of the detection window (1.6 ns) is about the same as our system jitter, which is shown in Fig. 3.

There are two types of timing jitter, some of which are independent of the data pattern, and some of which are data dependent. We characterized the overall data-dependent effect in the entire system by measuring the histogram of different data patterns, i.e., a “1” bit following different numbers of ”0” bits. The triangle points in Fig. 4 show the relative delays of the five repetitive data streams. The first stream transmits a quantum bit every 1.6 ns (2 clock cycles), the second stream does every 3.2 ns (4 clock cycles) and so on. The fifth stream does every 25.6 ns (32 clock cycles). As shown in the insertion in Fig. 4, different patterns have significantly different time delays. Since a pseudo random data stream contains all these patterns with certain weight, its histogram is the weighted sum of these histograms.

Received 11 January 2006; revised 6 March 2006; accepted 15 March 2006

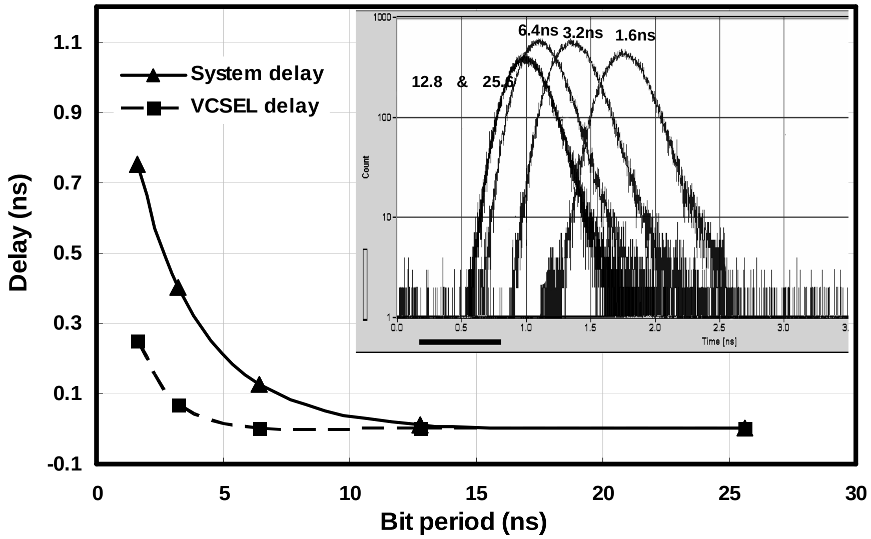

Fig. 4. The solid triangle points show relative delays of the histogram of repetitive data streams with different bit periods for the entire system including that caused by APD and VCSEL. The insertion shows the measured histograms for the system. The solid square points show relative delay of repetitive data with different bit periods at the output of VCSEL at the bias applied in the system.

The timing jitter can be caused by many effects. The data-independent part is induced by the non-zero optical pulse width and intrinsic timing jitters of the devices in the system. The influence of this data-independent part can be obtained by measuring the histogram of a repetitive data stream. The data-dependent part is induced by device properties that are dependent on the history of the signals. For example, for a bit value of “1”, both the turn-on delay of the VCSEL [14] and the count-rate delay of the APD [15] depend on how many “0”s were transmitted before this “1” bit. The count-rate dependent delay of APDs has been studied intensively. Here we observed the timing jitter due to turn-on delay of the VCSELs in QKD at near Gbit/s range.

In Ref. [13], it is revealed that VCSEL shows a significant turn-on delay when the zero-level of the pulse is below its threshold. On the other hand, it is desirable to set the zero-level below the threshold in order to achieve a high intensity extinction ratio. In this work we adjust the bias of VCSELs to set the zero-level below its threshold and thus to achieve the narrowest “pulse” width and higher intensity extinction ratio. Meanwhile, the turn-on delay is also introduced. The solid square points in Fig. 4 show relative delay of repetitive data with different bit periods at the output of VCSELs. . The measurement was carried out with a high-speed photo-receiver (New Focus, 12-GHz). One can see that there is non-negligible delay of the peak position at the repetition rate of 312 Mbit/s and above. Particularly, at 625 Mbit/s the delay can be as high as 250 ps. Consequently, the timing jitter from VCSELs is also important for QKD systems with a QCTR at 625 Mbit/s and higher. Since a pseudo random data stream contains components with certain weights of different data rate, its histogram is the weighted sum of the histograms of these components. A simulation for the histogram of pseudo random data has been made by superposition of these histograms with their own delay value and weights in pseudo random data. Figure 5 shows histograms of photon counts at a QCTR of 625 Mbit/s: (a) measured with a repetitive data stream, (b) measured with a pseudo random data stream, and (c) simulated with a random data stream. For the repetitive data stream, the width of the histogram at 5% of the maximum is measured to be 0.76 ns. In comparison, for the random quantum channel stream, this width is as high as 1.16 ns for measured and 1.17 ns for simulated. The width of the histogram base is broadened by about 50% for random data.

Received 11 January 2006; revised 6 March 2006; accepted 15 March 2006

The results show good agreement between the measured and the simulated values. We are currently investigating this effect. Nevertheless, the simulation accurately describes the broadening of the histogram due to the data-dependent timing jitter. These results show that the data-dependent timing jitter will become much more serious when the quantum bit period is reduced into the sub-nanosecond range causing the delay, shown in Fig. 4, to increase rapidly.

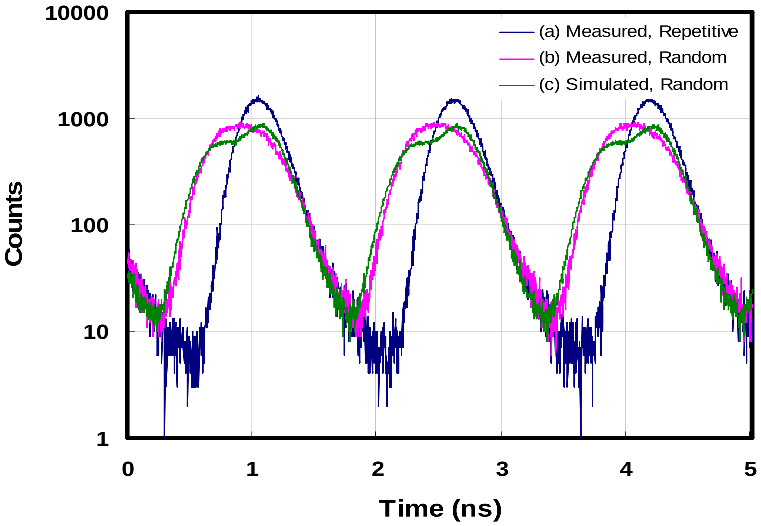

Fig. 5. The histogram of (a) measured repetitive data stream, (b) measured random data stream, and (c) simulated random data stream.

From our experimental and theoretical studies, we have shown that data-dependent timing jitter imposes a major limitation to the QBER at high quantum channel transmission rates. A modified VCSEL driving circuit that can reduce the turn-on delay of VCSEL is under study. It is also reported that the count-rate delay of APD can be reduced by an improved circuit [15]. The data-dependent jitter could be reduced obviously by these improvements and the reduction of jitter in quantum channel hardware will help the development of higher speed QKD system.

4. Conclusion

We have implemented a polarization encoding quantum key distribution system over 1 km of optical fiber. To our knowledge, as a complete system, the NIST fiber based polarization encoding QKD testbed currently runs at the highest sifted-key rate, more than 2 Mbit/s with the mean photon number $\mu = 0.1$ and an error rate of 3.08%. With QCTR below 1 Gbit/s in our system, the sifted-key rate increases approximately linearly over the QCTR. In comparison, at higher QCTR, the dead time can saturate the sifted-key rate and degrade security performance as well. Our results also show that the data-dependent system timing jitter has the major effect on the QBER in a QKD system operating around 1 GHz and beyond. A higher speed system requires a further reduction of both APD dead time and the data-dependent system timing jitter.

Acknowledgments

This work was supported in part by the Defense Advanced Research Projects Agency under the DARPA QuIST program.

Received 11 January 2006; revised 6 March 2006; accepted 15 March 2006