Time-cost analysis of a quantum key distribution system clocked at 100 MHz

X. F. Mo,[1] I. Lucio-Martinez,[1,*] P. Chan,[2] C. Healey,[1] S. Hosier,[3] and W. Tittel[1]

[1]*Institute for Quantum Information Science, and Department of Physics and Astronomy, University of Calgary, Calgary, Alberta, T2N 1N4, Canada*
[2]*ATIPS Labs, Department of Electrical and Computer Engineering, University of Calgary, Calgary, Alberta, T2N 1N4, Canada*
[3]*Southern Alberta Institute of Technology, Calgary, Alberta, T2M 0L4, Canada*
**ilucio@qis.ucalgary.ca*

Abstract: We describe the realization of a quantum key distribution (QKD) system clocked at 100 MHz. The system includes classical post-processing implemented via software, and is operated over a 12 km standard telecommunication dark fiber in a real-world environment. A time-cost analysis of the sifted, error-corrected, and secret key rates relative to the raw key rate is presented, and the scalability of our implementation with respect to higher secret key rates is discussed.

OCIS codes: (060.2330) Fiber optics communications; (060.5565) Quantum communications; (270.5568) Quantum cryptography.

References and links

1. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, pp. 175–179 (1984).
2. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden,"Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
3. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Duek, N. Ltkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301 (2009).
4. B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, "Time-shift attack in practical quantum cryptosystems," Quantum Inf. Comput. **7**, 73–82 (2007).
5. A. Lamas-Linares and C. Kurtsiefer, "Breaking a quantum key distribution system through a timing side channel," Opt. Express **15**, 9388 (2007).
6. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," Nat. Photonics **4**, 686–689 (2010).
7. N. Jain, C. Wittman, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, "Device calibration impacts security of quantum key distribution," *arXiv*: 1103.2327v2, (2011).
8. 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).
9. Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz quantum key distribution with InGaAs avalanche photodiodes," Appl. Phys. Lett. **92**, 201104 (2008).
10. A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Continuous operation of high bit rate quantum key distribution," Appl. Phys. Lett. **96**, 161102 (2010).
11. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legre, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Langer, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD network," *arXiv*:1103.3566 (2010).

#147765 - $15.00 USD Received 19 May 2011; revised 23 Jun 2011; accepted 23 Jun 2011; published 25 Aug 2011

12. M. Peev, C. Pacher, R. Allaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Frst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hbel, G. Humer, T. Lnger, M. Legr, R. Lieger, J. Lodewyck, T. Lornser, N. Ltkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," N. J. Phys. **11**, 075001 (2009).
13. G. Brassard and L. Salvail, "Lecture notes in computer science," in *Advances in Cryptology EUROCRYPT '93* (Springer, 1994), vol. 765, pp. 410–23.
14. D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quantum Inf. Comput. **4**, 325 (2004).
15. W. Hwang "Quantum key distribution with high loss: toward global secure communication," Phys. Rev. Lett. **91**, 057901 (2003).
16. X. Wang "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**, 230503 (2005).
17. X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A **72**, 012326 (2005).
18. M. Dŭsek, O. Haderka, and M. Hendrych, "Generalized beam-splitting attack in quantum cryptography with dim coherent states," Opt. Commun. **169**, 103–108 (1999).
19. G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders,"Limitations on practical quantum cryptography," Phys. Rev. Lett. **85**, 1330–1333 (2000).
20. I. Lucio-Martinez, P. Chan, X. Mo, S. Hosier, and W. Tittel, "Proof-of-concept of real world quantum key distribution with quantum frames," N. J. Phys. **11**, 095001 (2009).
21. In the current setup, the number of sifted key bits to be processed in one execution of error correction is fixed to 10 kb. The time required to collect this data is setup dependent.
22. C. Healey, I. Lucio-Martinez, M. R. E. Lamont, X. F. Mo, and W. Tittel, "Characterization of an InGaAs/InP single-photon detector at 200 MHz gate rate," in preparation.
23. Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, "High speed single photon detection in the near-infrared," Appl. Phys. Lett. **91**, 041114 (2007).
24. A. R. Dixon, J. F. Dynes, Z. L. Yuan, A. W. Sharpe, A. J. Bennet, and A. J. Shields, "Ultrashort dead time of photon-counting InGaAs avalanche photodiodes," Appl. Phys. Lett. **94**, 231113 (2009).
25. D. J. Rogers, J. C. Bienfang, A. Nakassis, H. Xu, and C. W. Clark, "Detector dead-time effects and paralyzability in high-speed quantum key distribution," N. J. Phys. **9**, 319 (2007).
26. R. G. Gallager, "Low-density parity-check codes," IRE Trans. Inf. Theory **8**(1), 21–28 (1962).
27. D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," Electron. Lett. **33**(6), 457–458 (1997).
28. D. Pearson, "High-speed QKD reconciliation using forward error correction," Quantum Commun. Meas. Comput. **734**(1), 299–302 (2004).
29. R. C. Agarwal and C. S. Burrus, "Number theoretic transforms to implement fast digital convolution," Proc. IEEE **63**(4), 550–560 (1975).
30. N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," Phys. Rev. A **61**, 052304 (2000).
31. P. Rice and J. Harrington, "Numerical analysis of decoy state quantum key distribution protocols," *arxiv*:0901.0013 (2009).
32. R. Y. Q. Cai and V. Scarani, "Finite-key analysis for practical implementations of quantum key distribution," N. J. Phys. **11**, 045024 (2009).
33. C.-H. F. Fung, X. Ma, and H.-F. Chau, " Practical issues in quantum-key-distribution processing," Phys. Rev. A **81**(1), 012318 (2010).
34. J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, "UMAC: fast and secure message authentication," *Advances in Cryptology CRYPTO 99*, Lecture Notes in Computer Science, **1666**, 79 (1999).
35. Y. Bo, R. Karri, and D. A. McGrew, "A high-speed hardware architecture for universal message authentication code," IEEE J. Sel. Areas Commun. **24**(10), 1831–1839 (2006).
36. B. Levine, R. Reed Taylor, and H. Schmit, "Implementation of near Shannon limit error-correcting codes using reconfigurable hardware," *IEEE Symposium on Field-Programmable Custom Computing Machines*, 217–226 (2000).
37. M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generator," Opt. Express **18**(12), 13029–13037 (2010).
38. Two bits are required to determine each polarization state, and four bits allow a random choice of vacuum, decoy and signal states with the desired distribution. Furthermore, some randomness is required for privacy amplification. Note that no random numbers are required at the receiver end due to the passive basis choice.
39. T. Honjo, A. Uchida, K. Amano, K. Hirano, H. Someya, H. Okumura, K. Yoshimura, P. Davis, and Y.

#147765 - $15.00 USD Received 19 May 2011; revised 23 Jun 2011; accepted 23 Jun 2011; published 25 Aug 2011

Tokura,"Differential-phase-shift quantum key distribution experiment using fast physical random bit generator with chaotic semiconductor lasers," Opt. Express **17**(11), 9053–9061 (2009).

1. Introduction

Quantum Key Distribution (QKD) takes advantage of the peculiar quantum properties of single photons to distribute secret keys [1–3]. When implemented correctly [4–7], QKD, in combination with the One-Time Pad, allows two distant parties to communicate in an information-theoretic secure way over an untrusted but authenticated channel.

A QKD system requires a quantum and a classical channel to distribute quantum information, here in form of quantum bits (qubits), and classical information, respectively. To obtain a secret key, a QKD system must complete the following steps: (1) Generation, faithful transmission, and measurement of qubits, yielding the *raw key*. (2) Sifting of the raw key, i.e. comparison of the bases used by the sender and receiver to generate and detect each individual qubit. This is done over the classical channel. Only detection events where the bases match are kept, resulting in the *sifted key*. (3) Error correction. The purpose of this step is to remove all errors in the sifted key due to a noisy channel or eavesdropping. This procedure requires communication over the classical channel. It yields information about the quantum bit error rate (QBER) of the sifted key and results in the *error-corrected key*. (4) Privacy amplification. The final step in QKD shortens the error-corrected key and thereby removes all information that Eve might have obtained while eavesdropping. The result is the *secret key*. Furthermore, all classical communication required for the establishment of the secret key has to be authenticated to corroborate the identity of the authorized parties and to avoid a man-in-the-middle attack.

For given loss in the quantum channel, the relevant figure of merit characterizing a QKD system is the secret key rate. Significant effort has been devoted over the past several years to increase this rate [8–10]. However, with a few notable exceptions reporting actual rates up to 1 MHz [11, 12], the secret key rate is often calculated from the sifted key rate assuming a reasonable efficiency for error correction as compared to the Shannon limit [13], and taking into account a reduction of the error-corrected key during privacy amplification [14]. While this leads to a rate that has some predictive power, it states an upper bound that can only be attained if qubits are distributed continuously, key sifting, error correction and privacy amplification can keep up with the rate at which the raw key is obtained, and if the memory of the processor(s) in use can cope with the amount of data involved. These conditions may be difficult to satisfy in an actual system, in particular in the case of systems clocked at high rates.

In this paper we analyze the performance of our QKD system in view of a high secret key rate. The goal of the analysis is to determine the limitation on the key rate based on the time-cost of each of the steps mentioned above. We also propose improvements that we will pursue in the near future. The bottlenecks revealed in this analysis, while obtained using our QKD system, are likely to be relevant for other implementations as well. Hence, we believe that this study will help other research groups to develop high-rate QKD systems.

2. Our QKD System

2.1. Hardware

Our test took place between the Quantum Cryptography and Communication Research Laboratory (QCCRL) at SAIT, where Alice is placed, and the Quantum Cryptography and Communication (QC2) Laboratory at the University of Calgary (UofC), where Bob is located. As usual, Alice and Bob denote the sender and receiver of quantum data, respectively. The transmission loss of the communication channel, a 12 km-long standard telecommunication fiber featuring many splices, is 6.5 dB. Our QKD system is fiber-based, implements the BB84 protocol sup-

#147765 - $15.00 USD Received 19 May 2011; revised 23 Jun 2011; accepted 23 Jun 2011; published 25 Aug 2011

plemented with two decoy states [3, 15–17] to detect photon number splitting attacks [18, 19], and employs polarization encoding. Furthermore, it is characterized by the use of quantum frames, which consist of alternating sequences of high-intensity laser pulses (forming classical control frames) and faint laser pulses (encoding quantum data), see figure 1. The classical control frames contain frame number and polarization information; the latter is used to assess and compensate time-varying birefringence in the communication channel [20]. The frames also contain information for clock synchronization and, in view of future integration into network environments, sender and receiver address to allow for routing.

Figure 2 shows a schematic of the optical and electronic components of our QKD system; a more detailed description of the optical part is given in [20]. Optical pulses of 500 ps duration and 1550 nm wavelength are generated by the *quantum laser diode* and are attenuated using a variable attenuator (ATT). To create the required signal and two decoy states, we use an intensity modulator (IM), generating weak pulses of light with mean photon numbers of μ, 0.2μ, 0.01μ, respectively (the fixed relation between these three values is due to the way the attenuator and intensity modulator are used to generate loss). To encode the required polarization states, $\pm$ 45^o linear polarized, and right- and left-circular polarized states, we use a polarization modulator (PM). Both modulators are configured to ensure passive compensation of temperature-dependent birefringence and polarization mode dispersion. On the receiver side, a photodiode is placed behind a 90/10 beamsplitter; it allows detecing the strong optical pulses, generated by the *classical laser diode*, that form the control frames. Next, a 50/50 beamsplitter is placed to randomly select one of the two polarization bases for qubit measurement. Per basis, a voltage-controlled polarization controller (PC) and an optical detector (a low-bandwidth powermeter in the current system, not shown) are used to compensate for time-varying polarization changes in the transmission line. This procedure relies on feedback from the classical control frames.

Polarization compensation executes whenever the QBER exceeds a certain threshold (between 3% and 4.5%, setup dependent). We have previously shown that the polarization stability over our real-world fiber link can vary greatly over time [20]. Thus, for this feedback to work, the QBER must be updated sufficiently often, i.e. error correction must run on sifted key bits collected over a sufficiently short time [21]. In this case the feedback will ensure that the QBER is kept low when the channel is unstable (then generating only a small amount of raw key bits), while allowing key generation to run without interruption over several minutes during extended periods of stability. The time needed for polarization compensation is determined by the reaction time of the powermeter, which limits the number of detectable voltage changes per second to one.

Qubit detection is either accomplished using four commercially available single photon detectors (SPDs) gated at 1 MHz, or using one high-rate, home-made detector [22] that utilizes the self-differencing technique [23, 24] and allows photon detection up to 100 MHz. Note that qubit generation is clocked at 100 MHz in both cases. Currently, our QKD system is vulnerable to fake-state attacks [6], but preventive measures against detector vulnerabilities and potential loopholes arising from control information being sent between Alice and Bob [6, 7] or high-rate operation [25] will be implemented in the near future.

2.2. Software

All data is transferred via National Instruments digital I/O cards into or out of the CPUs with the following specifications; Alice: AMD 64 X2 Dual Core 4600+, 2.4 GHz, 2 GB RAM, WinXP 32-bit; Bob: Intel Core2 Quad CPU Q8300, 2.5 GHz, 4 GB RAM, Windows Vista 32-bit. Our system uses Field Programmable Gate Arrays (FPGAs) to control all active components. The clock rate, 100 MHz, is limited by the rate with which electronic signals are currently generated

#147765 - $15.00 USD Received 19 May 2011; revised 23 Jun 2011; accepted 23 Jun 2011; published 25 Aug 2011

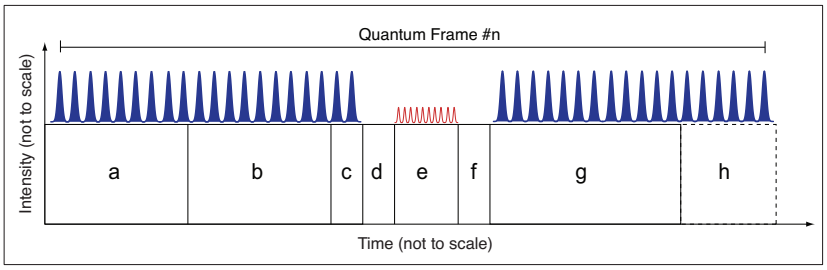

Fig. 1. Structure of the quantum frames. a: generation of bit and basis information to encode qubits; b: data transfer; c: generation of the classical control frame; d: deadtime, e: generation and transmission of quantum data (qubits); f: deadtime, g: processing time, h: time for polarization control (when required).

by the FPGA and can be transmitted to, and converted by our home-made drivers that control the laser diodes and modulators. However, the optical components can generate qubits at a maximum rate of 980 MHz. Our system also includes classical post-processing (sifting, error correction and privacy amplification) implemented via software. Error correction is performed using low-density parity check codes (LDPC) [26–28], and privacy amplification founds on Toeplitz matrices [29].

Our QKD software is responsible for frame generation (Alice), data acquisition (Bob), key sifting, error correction, controlling polarization compensation, and writing collected data to the hard drives. The classical communication required for these tasks is performed using a TCP/IP connection established between the two computers over the public Internet. Each of the post-processing tasks can run independently, and both Alice and Bob run their tasks on one computer each. The data gathered by the system is analyzed later on a computer with an Intel i5 CPU 760 @ 2.8GHz, where decoy state analysis and privacy amplification is performed.

The software is implemented primarily in National Instruments LabVIEW, with more time-intensive tasks being implemented in C++ libraries that are called as appropriate by the LabVIEW code. These libraries may execute in parallel with any LabVIEW code that is not directly involved in controlling their execution. Hence, as more than one task may be executing at the same time, the elapsed times that we measure for processing tasks do not necessarily represent the required execution time. In particular, some tasks such as polarization compensation are not computationally intensive, but currently require significant time for the hardware to act. During this time, computationally intensive tasks such as error correction may execute if there is data available to be processed.

3. System Performance

To determine the performance of our QKD system, we increase the raw key rate from 0.2 to 120 kbps, and monitor the sifted and error-corrected key rates. As we will argue below, the secret key rate is simply related to the error-corrected rate by a factor described in [14]. As an example, the reduction assuming a QBER of 2.6%, μ=0.5 photons per pulse (with Poissonian photon number distribution), and no PNS attack is 23.5% (see also [20]).

In a first set of experiments, we employ four commercial single photon detectors gated at 1 MHz. This effectively limits the clock rate of our QKD system to the same value. To change the raw key rate, we vary μ between 0.40 and 7.0 photons per pulse. Given the loss of 6.5 dB in the quantum channel, a detector efficiency of $\sim$10%, as well as additional attenuation of $\sim$3.5 dB in Bob's device, this yields raw key rates between $\sim$0.2 and 4.8 kbps. This calculation

#147765 - $15.00 USD Received 19 May 2011; revised 23 Jun 2011; accepted 23 Jun 2011; published 25 Aug 2011

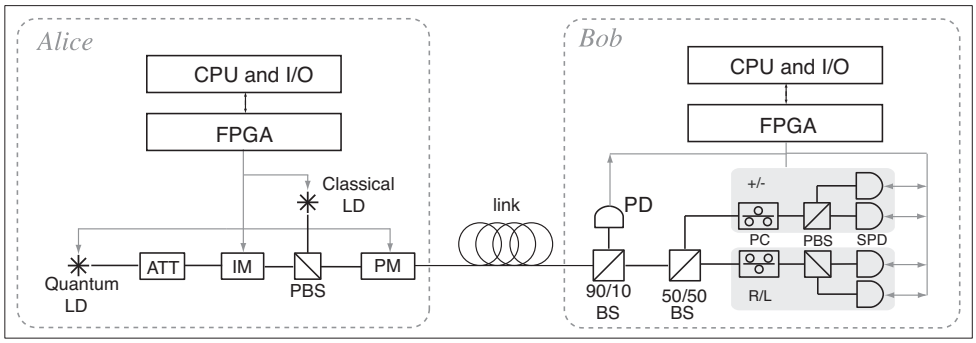

Fig. 2. Schematics of the optical and some electronic components of our QKD system. LD: laser diode; ATT: attenuator; IM: intensity modulator; PBS: polarization beam splitter; PM: phase modulator; BS: beam splitter; PD: photo diode; PC: polarization controller; SPD: single photon detector; CPU: central processing unit (personal computer); FPGA: field programmable gate array; I/O: input/output interface. See text and [20] for more details.

also takes into account that quantum data is sent only during $\sim$10% of the system operation time; this is further discussed below. While this procedure does not deliver secret keys for large values of μ (e.g. $\mu > 1$), it does allow us to gauge how the system responds in the event of large raw key rates. However, we point out that there is a limit to this procedure. Indeed, as μ increases, the probability that multiple detectors detect photons simultaneously also increases. This leads to larger processing requirements as only one, randomly selected detection is kept for subsequent steps [30]. In turn, this leads to an underestimation of the sifted key, and hence error-corrected key rates (this effect was, however, not noticeable for $\mu \leq 7$).

To obtain higher raw key rates, we perform a second set of measurements using a single, home-made SPD [22] that is gated at 100 MHz. We vary μ from 0.30 to 20 photons per pulse. Obviously, using only one detector does not allow distributing a secret key. Nevertheless, this setup allows increasing the raw key rate, and hence assessing the system performance in the event of large rates. More precisely, it delivers one quarter (i.e. 2.24 to 121 kbps) of the raw key rate we expect in a fully implemented QKD system with four high-rate detectors while providing a similar QBER. All key rates listed below and in Fig. 3 refer to the actually detected (not extrapolated) rates.

Figure 1 shows the execution flow and frame structure in our system from Alice's perspective. This perspective was chosen since Alice's timing currently limits the maximum frame rate. First, the state of all qubits within a quantum frame is determined by a software-based pseudo-random number generator (a, 225 ms). Note that this solution is temporary - our final QKD system will employ true (if possible quantum) random number generators for improved security; this will be discussed in section 4. This data is then transferred to a digital I/O card (b, 225 ms), which, along with an FPGA, controls our hardware. These devices generate the classical control frame (c, 960 ns), which includes a frame number, control information for polarization compensation, and a sender and receiver address that will be used for quantum packet routing in future work. The header is followed by a deadtime (d, 50 ms), after which the qubits are generated and transmitted (e, 100 ms). A second deadtime (f, 50 ms) follows. These deadtimes exist to avoid accidentally exposing the single photon detectors to strong light, which is generated at all times outside of the deadtimes and 'qubit time' (e). The second deadtime is followed by an idle time for the hardware, which is used by the computer for software post-processing and data logging (g, 55-130 ms, depending on the raw key rate). This time is determined by

#147765 - $15.00 USD Received 19 May 2011; revised 23 Jun 2011; accepted 23 Jun 2011; published 25 Aug 2011

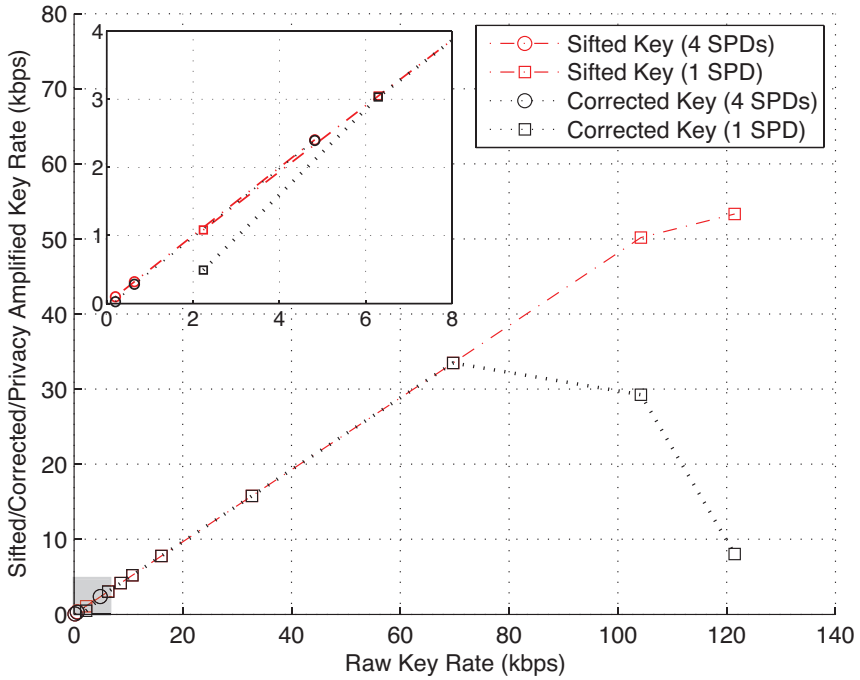

Fig. 3. Sifted and error corrected key rates as a function of the raw key rate. The inset shows the shaded area in more detail.

when the processor becomes available to generate the data for the next quantum frame. In particular, when the error rate has exceeded a certain threshold, the overall idle time is extended and then also comprises compensation for time-varying birefringence of the communication channel (h, averaging to 140 ms per frame). To summarize, qubits are transmitted on average during 100 ms out of 845-920 ms, i.e. during 10.9-11.8% of the system operation time.

The sifted and error corrected key rates obtained over the total system operation time are shown in Fig. 3 as a function of the raw key rate. From Fig. 3 we see that the error-corrected key rate peaks at 33.488 kbps at a raw key rate of 69.720 kbps, and that the sifted key rate does no longer increase linearly with respect to the raw key rate once the latter exceeds 114.160 kbps. This is due to the fact that the post-processing software is run on the same computers as the data generation and collection software, and once processing resources are at their limit, the error correction, and subsequently key sifting, will get less execution time than is required to process all available data. To show the impact of this effect, error correction was run independently with simulated data, yielding a maximum error-corrected key rate of 53.213 kbps at an average QBER of 3.5%. This average QBER is consistent with what is experienced during operation of the QKD system with the four commercial single photon detectors and $\mu = 1$. The QBER obtained using the high-rate detector is lower due to a better ratio between detection efficiency and dark count probability. In addition, the QBER decreases as μ is increased since the higher detection rates make dark counts less significant. Thus, the 33.488 kbps rate obtained in the actual system is due to limited computational resources. Similarly, we also conclude that the sifted key rate is affected by process competition.

We have also performed the decoy state analysis (according to the methodology described in

#147765 - $15.00 USD Received 19 May 2011; revised 23 Jun 2011; accepted 23 Jun 2011; published 25 Aug 2011

[17]) on the data recorded by our QKD system to establish the maximum amount of information that may have leaked to an eavesdropper. The execution time to process the data collected over 15 hours (enough to ignore finite key effects [31,32]) was found to be less than a minute, and is thus negligible. Privacy amplification using the Toeplitz matrix approach has also been shown to require insignificant computational time if a number theoretic transform is used [11,29]. Hence, the time required to establish and remove the eavesdropper's information does not need to be considered in our time-cost analysis. In addition, authenticated communication is needed for all classical post-processing steps to prevent a man-in-the-middle attack [33]. Yet, the impact of authentication on the secret key rate is negligible as well. Indeed, authentication of Gbps messages in real-time has been reported [34,35].

4. Proposed Improvements

The secret key rate of our QKD system can be improved by increasing the proportion of time spent transmitting quantum data. Three simple modifications to our close to sequential execution of tasks stick out. First, the deadtimes (d, f) can be shortened. In principle, these times can be less than a millisecond. However, as our system is still under development, we have chosen to maintain a large safety margin in case changes are made that alter the relative timing at the sender and receiver. Second, we write more information to the hard drives than is necessary to perform decoy state analysis, privacy amplification, and authentication. This increases the hardware idle time (g), but allows for a thorough analysis of the system. The secret key rate can thus be improved by writing only necessary information to file, or by replacing our current approach with a more efficient method of data transfer. Third, the powermeters used for polarization compensation have a response time on the order of a second, and multiple measurements are required to determine the necessary adjustments to the polarization controller. As such, the polarization compensation time (h) can be reduced to a few ms by using fast photodetectors in conjunction with a fast polarization controller.

In addition, we note that the 100 ms time interval for qubit transmission in each frame (e) is determined by the clock rate of 100 MHz and by the available memory in the digital I/O card, which allows generating 10^7 qubits per frame. This limitation is present in our system for both detector setups, as Alice's system generates qubits at 100 MHz even when the detector gate rate is limited to 1 MHz. While reducing Alice's clock frequency in the case of the commercial detectors would bring the time used for qubit transmission much closer to 100% of the system operation time, this would ideally provide only a 8-9 fold increase in the raw key rate. In comparison, using the fast detector provided more than a 60 fold increase in raw key rate. In the case of the fast detector setup, it is possible to add more memory to the I/O card. However, this would result in a proportional increase in the time required for the data preparation (a), data transfer (b), and key sifting plus error correction (g) steps. This suggests that the following needs to be explored: a faster interface to the computer, faster random number generation, as well as more efficient post-processing, for instance using dedicated hardware that may also take care of authentication.

As used in QKD, LDPC encoding is not computationally intensive, requiring only a series of parity calculations [28]. Decoding, however, is an iterative process that uses the received data, parity information, and an initial estimate of the error rate (derived from previous executions of the protocol) in order to compute better estimates of the probability that each bit is in error [26, 27]. This iterative process ends successfully when the most likely result for the corrected data is consistent with the parity information, and failure is declared if a set maximum number of iterations is reached without meeting this condition. In order to improve the throughput of the error correction in our system, two approaches are possible. The computations required for LDPC decoding algorithm are well suited to parallel implementations. Thus CPU utilization

#147765 - $15.00 USD Received 19 May 2011; revised 23 Jun 2011; accepted 23 Jun 2011; published 25 Aug 2011

can be improved in our software implementation by taking advantage of this fact. Moreover, LDPC decoding is well suited to hardware implementation [36], and performing the decoding using specialized hardware, whether in an FPGA or custom integrated circuit, can yield error-corrected key rates of Mbps error-corrected key rates, as we have shown in [20]. It should also be noted that the error correcting code used in our experiment was originally designed for use with the commercial detectors. Since these detectors only provide a small key rate, a short block length of 10^4 bits was used for the LDPC code in order to evaluate the QBER, and hence provide feedback to initiate the polarization control procedure in a timely fashion. The block length of the code can be increased significantly when using fast detectors, leading to better performance relative to the Shannon limit. This, in turn, translates to a higher secret key rate since less information is revealed to the eavesdropper in this process.

Similarly, one should investigate hardware-based key sifting. In particular, executing sifting, error correction, privacy amplification and authentication within the same FPGA would avoid time-consuming data transfer into and out of a CPU.

Another concern in our current implementation is the generation of random qubit states using a software-based, pseudo-random number generator. For a secure system, a true (possibly quantum) random number generator (RNG) is required. A lot of progress has been obtained over the past years, and the highest rate for a quantum RNG reported to date is 50 Mbps [37]. Hence, two RNGs operated in parallel would suffice for our current system as only $\sim 10^6$ qubits are generated per second, and each qubit is determined by six random bits with uniform distribution of zeros and ones [38]. Yet, to improve the clock rate to 1 GHz, or the fraction of time during which qubits are generated, or both, the amount of RNGs that have to be operated in parallel would constitute a major challenge. Nevertheless, given recent progress in high-rate single photon detectors [24], better quantum RNGs may become available in the near future and allow for high-rate QKD. Another possibility, which would already constitute a significant improvement over pseudo-random numbers, is the use of physical (non-quantum) RNGs for which Gbps rates have been reported [39].

5. Conclusions

We have demonstrated a QKD system that implements the BB84 protocol supplemented with decoy states and quantum frames. The system executes software-based key sifting and error correction in real-time over a real-world fiber optic channel. We have done a time-cost analysis of all steps required in the generation of a secret key, and proposed improvements to our current implementation. Furthermore, we have analyzed the scalability of the sifted, error corrected and privacy amplified key rate with respect to the raw key rate, finding them to be determined by the sequential execution of the different steps in the key distribution protocol. Consequently, all processes that take significant time despite optimization have to be executed parallel to the distribution of qubits using dedicated, possibly custom hardware. Ignoring communication time, transmission loss and detector efficiency, the secret key rate would then be limited by the clock rate and the detector gate rate, i.e. 100 MHz in our current implementation with high-rate detectors.

Acknowledgments

The authors thank V. Kiselyov for technical support. This work is supported by General Dynamics Canada, Alberta's Informatics Circle of Research Excellence (iCORE, now part of Alberta Innovates Technology Futures), the National Science and Engineering Research Council of Canada (NSERC), QuantumWorks, Canada Foundation for Innovation (CFI), Alberta Advanced Education and Technology (AET), and the Mexican Consejo Nacional de Ciencia y Tecnología (CONACYT).

#147765 - $15.00 USD Received 19 May 2011; revised 23 Jun 2011; accepted 23 Jun 2011; published 25 Aug 2011