Implementation of a High-Speed Quantum Key Distribution System for Metropolitan Networks

Akihisa Tomita[1, 3], Akihiro Tanaka[2], Ken-ichiro Yoshino[3], Seigo Takahashi[2], Yoshihiro Nambu[3], and Akio Tajima[2]
[1]Quantum Computation and Information Project, JST ERATO-SORST, Miyukigaoka 34, Tsukuba Ibaraki 305-8501, Japan
[2]System Platforms Research Laboratories, NEC Corporation, 1753, Shimonumabe, Nakahara-ku, Kawasaki, Kanagawa 2111-8666, Japan
[3]Nano Electronics Research Laboratories, NEC Corporation, 34, Miyukigaoka, Tsukuba, Ibaraki 305-8501, Japan
a-tomita@az.jp.nec.com

Abstract: Improvement of QKD performance, particularly on key generation rate, has been required to meet current network traffic. A high-speed QKD system should be equipped with low loss receivers with high visibility, highly efficient photon detectors with small dark count probability, and a stable clock synchronization system with low stray light to the quantum signals, because the key generation rate is determined by photon detection rate and error rate. High speed post processing is also required to improve key generation through-put. A solution for these issues will be discussed.

OCIS codes: (270.5568) Quantum cryptography

1. Introduction

Recent development of optical communication technology stimulates the growth of the information traffic. Vast variety of information flows through the optical communication networks. Extremely important messages, such as national defense information or financial transactions, are carried through current optical communication links. Moreover, the current internet carries crucial sensing and control information for the social infrastructures, such as traffic networks and electric power supply networks. The society is getting vulnerable to the malicious attacks on the networks. Small latency will be required rather than wide bandwidth. Another issue on the security lies in the network itself. Networks have the control-plane over the data-plane for routing. The routing information is also to be protected from the attacks. Requirement on the security on the control plane is the integrity of the routing information with small latency. The solution to the above challenges is cryptography. However, it has been pointed out that advanced computation may break the conventional crypto-systems, because the security is guaranteed by the computational complexity. It means endless updating of the public crypto-system is necessary to ensure the security. Since the systems are optimized to the current specifications, the updating will cost considerable resources. Moreover, the updating may not be useful for some of the important information concerning diplomatic negotiations or military operations, which should be kept secret for a long time. A message encrypted with obsolete cryptography would be decrypted with a future powerful computer.

One-time-pad cipher has been used for highly secure communication to obtain information theoretical security. However, the one-time-pad cipher, as suggested by its name, requires single-use cryptographic key of the same length as the message sent. Quantum key distribution (QKD) is expected to provide a solution to the problem on refueling keys. One of the practical issues on QKD is key generation speed, which should meet the requirement from the application. If we were satisfied to replace a 1024-bit password or seed key every one minute, the system would only need to generate a key at 17 bps. Higher key generation will be necessary to extend applications of one-time-pad. We here set our target key generation speed at 1 Mbps, which enables to encrypt compressed video signals. Since we consider applications on metropolitan networks, we assume transmission loss as 10 dB. This value corresponds to 50-km transmission in a good fiber link (fiber loss of 0.2 dB/km.) In a real fiber network, however, allowed transmission length would be much small, because the link constructed with a number of short fibers, and splicing causes excess loss.

2. Key generation rate

Key generation in a QKD system consists of two processes. One is quantum communication to share random bits (sift key) between two parties. The other is key distillation to create the final (secure) key by post-processing on the sift key. The key distillation process is made up with two processes: error correction and privacy amplification. The former corrects the difference in the sift key between the sender and receiver. Privacy amplification erases eavesdropper's information on the final key by randomly reducing key length with a universal hash function. The amount of key reduction is determined from the error rate, which measures the eavesdropper's information on the sift key. After collecting a designed number of sift key, the quantum communication process forwards the sift key to the key distillation process. The time to generate the final key is given by the collection time of the sift key and distillation time of the final key. These two processes can be performed with pipeline processing, so that the slower process determines the key generation time.

After weak laser light of mean photon number μ is transmitted through an optical fiber of loss $\alpha l + \gamma$ [dB], the sift key will be obtained at the rate of

$$\begin{aligned} R_{sift} =& \frac{1}{2} f_c \left[1 - \exp\left(-\mu 10^{(\alpha l+\beta+\gamma)/10} \eta \right) + 1 - \left(1 - 10^{-\beta/10} \eta \right)^{N_{ext}} + P_d \right] \\ \approx& \frac{1}{2} f_c \left[\mu 10^{(\alpha l+\beta+\gamma)/10} \eta + N_{ext} 10^{-\beta/10} \eta + P_d \right] , \end{aligned} \tag{1}$$

where the factor 1/2 comes from the sift operation. We employ a system with the clock frequency f_c, the receiver loss β [dB], and the detector of detection efficiency η and the dark count probability P_d. Stray photons enter the receiver at the rate of N_{ext} photons per gate in addition to the signal photons. The three terms in Eq. (1) represent the signal photon detection, the stray photon detection, and the dark counts, respectively. Only the first term will yield the correct bit values, whereas the others cause errors. The detection rate of the signal photon is order of 10^{-3} for a typical system with α=0.2 dB/km, β =5 dB, γ =0, l=50 km, η =0.1, and μ =0.4. As suggested in Eq. (1), the sift key rate can be improved by increasing efficiency of the detector, reducing receiver loss, and increasing clock frequency. The clock frequency is limited by the electronics for clock synchronization and signal processing in the receiver. Dead time of the photon detector also limits the clock frequency. We have designed a QKD system with the clock frequency of 1.25 GHz.

The error rate also affect the final key rate, since the final key rate is given by the product of sift key rate and key distillation rate. The key distillation rate, defined by the ratio of the number of the final key to that of the sift key, is a decreasing function of the error rate, because the key distillation process regards the error as a result of eavesdropping. In asymptotic case (*i.e.*, infinite code length,) the key distillation rate is given by [1]

$$R_{dist} = f_{EC} \left[1 - H\left(p_e\right) - Q^{(1)} H\left(p_e^{(1)}\right) \right] , \tag{2}$$

where $Q^{(1)}$ denotes the fraction of photon detection events due to the pulses containing only a single photon, and $p_e^{(1)}$ represents the error rate in the single photon detection. The values of $Q^{(1)}$ and $p_e^{(1)}$ are to be estimated with decoy method. The quantum bit error rate (QBER) p_e is given by

$$p_e = \frac{\frac{1}{2}(1-\nu)\mu_n 10^{-(\alpha l+\beta+\gamma)/10}\eta + \frac{1}{2} N_{ext} 10^{-\beta/10}\eta + \frac{1}{2} P_d}{\mu_n 10^{-(\alpha l+\beta+\gamma)/10}\eta + N_{ext} 10^{-\beta/10}\eta + P_d}, \tag{3}$$

where the imperfection in the receiver is described by visibility ν of the interferometer. Though this QBER may result from noise of the transmission line and the receiver, we need to regard it as a result of eavesdropping in order to guarantee the security of the protocol. Therefore, it is important to decrease the QBER to obtain high key distillation rate by improving the visibility and reducing the stray photons and dark counts.

Another important issue is stability. We estimate channel parameters $Q^{(1)}$ and $p_e^{(1)}$ from the performance of the quantum communication, which are characterized by the photon detection rate and the QBER. Since the photon detection rate is limited, it is necessary to take a long period for collecting enough number of the photon detection events and the error events. If the performance of the system components, such as visibility of the interferometers and/or detection efficiency and dark count of the photon detectors, fluctuates, the channel parameters contain large estimation errors, which require larger key reduction to ensure the security. To summarize, the receiver in a high-speed QKD system should be composed of low-loss interferometers with high visibility and efficient photon detectors with a low dark count probability. .

In the following section, we will explain two key technologies to realize high speed QKD. One is one-way quantum communication system based on planar lightwave circuits, and the other is a logic board for key distillation.

3. One-way QKD systems with Planar Lightwave Circuit

One-way QKD systems have been expected to be suited to high-speed transmission. The main difficulty with the one-way system is to provide two identical interferometers at remote nodes in a fluctuating environment. This problem with phase and polarization fluctuations can be eliminated by using an asymmetric Mach-Zehnder interferometer (AMZI) based on planar lightwave circuit (PLC) technology. Stable and reliable QKD operation over 100 km has been demonstrated [2], where stable and polarization insensitive interference was achieved by precise temperature regulation (0.01 K,) attaining the total extinction ratio as high as 20 dB.

QKD systems based on the BB84 protocol exploit four states. In optical fiber system, time-bin qubit is often used, where information is encoded on amplitudes and/or relative phase of coherent double-pulses. We employ phase-time coding, which exploits two orthogonal states used in the phase coding (either X basis or Y basis,) and two orthogonal states in time-basis (Z basis) in which a photon exists in only one of the two time-bin pulses. A fully passive receiver without any optical modulators has been proposed and demonstrated using a two inputs and four outputs (2×4) PLC-based optical circuit followed by four photon detectors [2]. Photon detection at each photon detector implies the detection of corresponding BB84 state. The passive receiver scheme greatly simplifies the receiver construction, and also eliminates optical loss due to the modulator, leading to a higher key-generation rate. Although a transmitter can be constructed without modulators by using the same PLC and four light sources, these four light sources should be operated with precisely controlled timing and emission wavelength for security.

We developed modulation scheme of dual-drive Mach-Zehnder interferometer modulator to generate BB84 states, and demonstrated the encoder/decoder operation with 625 MHz repetition [3].

4. Hardware logic board for key distillation

It is required to reduce the execution time of the key distillation process, along with improvement on the sift-key generation. In our previous system, the distillation process was done with software worked on CPU, and the execution time was almost comparable to the quantum communication time. Since the developing system will work with 1.25-GHz clock, which is 20 times faster than the previous system, a high-speed hardware logic board will thus be required. The requirement of the logic board for QKD differs from conventional signal processing in optical communication. First, the bit value and basis should be kept with time stamp during key transmission. Since classical communication uses a part of secure key for authentication, the block of key transmission should be as large as possible. It implies the hardware for sift operation should equip memory of high-speed (1.25-GHz read/write frequency) and large capacity. Second, the code length for error correction should be long (100 kbits or more) to obtain good coding rate against relatively high error rate about several percents. We need to construct error correction code for quantum communication, because conventional one assumes shorter code length. Third, code length for privacy amplification should be at least 1 Mbits to maintain key distillation rate [4]. Since the operations in the key distillation are matrix multiplication, the operations require resource as large as the square of the code length. We have developed hardware for key distillation, which consists of FPGAs connected to high-speed memories.

5. Conclusion

We have discussed engineering issues in a high-speed QKD system, and presented two important technologies. We have also developed the components that are essential for high-speed transmission, such as capacity enhancement in QKD using WDM technique [5], and an APD module and detection circuit for single photon detection [6]. The high-speed QKD system should begin an era of highly secure commercial telecommunication networks in metropolitan areas.

Acknowledgments

This work was partly supported by the National Institute of Information and Communication Technology.

References

[1] D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill, “Security of quantum key distribution with imperfect devices,” Quantum Inf. Comput. **4,** 325-360 (2004).

[2] Y. Nambu, K. Yoshino, and A. Tomita, “Quantum encoder and decoder for practical quantum key distribution using a planar lightwave circuit,” J. Mod. Optics **55**, 1953-1970 (2008).

[3] A. Tanaka, M. Fujiwara, S. W. Nam, Y. Nambu, S. Takahashi, W. Maeda, K. Yoshino, S. Miki, B. Baek, Z. Wang, A. Tajima, M. Sasaki, and A. Tomita, “Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization,” Optics Express **16,** 11354-11360 (2008).

[4] J. Hasegawa, M. hayashi, T. Hiroshima, and A. Tomita, “Security analysis of decoy state quantum key distribution incorporating finite statistics,” arXiv:0407.3541v1 (2007).

[5] A. Tanaka, A. Tajima, and A. Tomita, “Colourless Interferometric Technique for Large Capacity Quantum Key Distribution Systems by use of Wavelength Division Multiplexing,” Technical Digest of ECOC2009, (Wien, 2009) paper 1.4.2.

[6] S. Takahashi, A. Tajima, and A. Tomita, “High-efficiency single photon detector combined with an ultra-small APD module and a self-training discriminator for high-speed quantum cryptosystems,” The13th Microooptics Conference, Takamatsu, Japan, PD-1 (2007).