Securing an optical network by quantum noise

Osamu Hirota, Kenichi Ohhata, Makoto Honda, Shigeto Akutsu, Katsuyoshi Harasawa, and Kiichi Yamashita

A randomized stream cipher provides ultra-high-speed data encryption over long-distance channels.

Single-photon quantum communication exploits special properties of photon states to securely transfer information from place to place. An inherent drawback of this system, however, is that it is very sensitive to the so-called energy-loss effect during transit. Consequently, exchanging cryptographic keys, whether by fiber or satellite, is not fast enough to be practical. An alternative approach is the ‘Yuen protocol’ (Y-00), which works with multi-photon light and provides ultra-high-speed encryption of messages over long distances thanks to a randomized stream cipher (code) enabled by quantum noise from the transmitting signals. Here, at least theoretically, security is ensured by evaluating the length of the data string. This approach has the potential to protect information, albeit a finite amount, even if an attacker has unbounded computing power. A generalized Y-00 scheme with several randomizations can protect $2^M$ data, where $|K|$ is the secret key length. The challenge in developing such systems has been to achieve speeds of 2.5Gb/s for 200km fiber transmission using the techniques of multilevel phase shift key (M-ary PSK) modulation\(^1\,2\) or amplitude (intensity) shift key (M-ary ASK) modulation to scramble the transmission signal.\(^3\) This is something we recently achieved in our research.\(^4\)

In the real world, however, next-generation networks will require basic fiber links of 10Gb/s and very high power lasers for secure satellite-based communications. Here, we describe the performance of Y-00 by ASK at 10Gb/s using a high-speed digital to analog converter (DAC). We also report on the feasibility of several randomization circuits using this high-speed modulation.

Y-00 can be implemented in two ways. The first is a phase-modulation scheme\(^3\) that uses $M$ pairs of two coherent (pure) states of laser light $|\alpha e^{i\theta}|$ and $|\alpha e^{(i\theta+\pi)}|$, $j = 1, 2, \ldots M$. The log $M$ bit signals from the linear feedback shift register (LFSR) assign the basis for sending the information bit, which is then transmitted using the two coherent states that correspond to the basis selected. In practice, the differential phase (between two light pulses) is used for the pair states because it is resistant to channel disturbance. The legitimate receiver can assign the threshold for deciphering the information bit (consisting of the two coherent states) by using the sequence from the same LFSR as the transmitter. If the amplitude of the received signal is appropriate, the decision for the binary phase signals with $\pi$ phase difference is error free. An attacker who does not know the sequence of the LFSR must discriminate among the $2^M$ different phase signals, and will incur critical errors in his data owing to the quantum noise of the coherent state. However, a high-power laser requires a huge number of basis states ($M \gg 1$) to foil the attacker.

The second approach to Y-00 is amplitude modulation.\(^3\) This scheme does not require as many basis states even if a high-power laser is used because the maximum ($\alpha_{\text{max}}$) and minimum ($\alpha_{\text{min}}$) amplitudes are fixed, and the signal distance for the

Continued on next page
attacker is set by $|\alpha_{\text{max}} - \alpha_{\text{min}}|/2M$, which is independent of laser power. However, this technique has the disadvantage that the error distribution in the maximum and minimum amplitude’s neighborhood is non-uniform, which requires additional randomization to improve it.

Thus far, all of our experimental trials have been devoted to demonstrating the basic Y-00 system. But security depends critically on the randomizations, which are add-ons. Several ways of generating them have been proposed, such as using a nonlinear feedback shift register, enhancing the quantum noise effect, and introducing more noise. In general, however, it is very difficult to implement these schemes at Gb/s operation because they affect the legitimate user’s receiver.

Figure 1 shows our experimental system. The power of the laser diode is 1mW with a wavelength of 1500nm. (For the satellite application, our scheme also permits using a laser of 200mW and an 800nm wavelength without degradation of security.) To carry out the experiment, we developed a high-speed LFSR and a 10bit high-speed SiGe DAC (see Figure 2). The transmitter circuit basically consists of parallel LFSRs, a DAC, and an external optical modulator of lithium niobate. In addition, we installed overlapped selection keying, deliberate signal randomization by additional LFSRs, and irregular mapping, which are all randomizations intended to compensate for the imperfections of the system and devices.

The evaluation and design of security is obviously of crucial importance, and assumes the following: (1) The attacker requires an ultimate receiver (i.e., specified by the initial sender) to discriminate $2M$ signals for a ciphertext-only attack or $M$ signals for a known plaintext attack (i.e., the attacker has access to the usable source as well as the encrypted data). Even with an ultimate receiver, his data will have many errors. (2) The attacker performs a crypto-analysis based on received data that contains many errors. The accuracy of the data depends on the type of receiver employed in step (1). The security system is designed to invalidate any crypto-analysis by taking the steps (1) and (2) into account.

At present, it is difficult to achieve either quantum optimum, heterodyne, or direct detection for a large number of $M$ signals. Consequently, we measured the binary detection error between neighboring signals using conventional direct detection. At the initial setting, we designed an error probability of the attacker as $P_e = 0.35$, and confirmed that the eye pattern does not open (see Figure 3). By controlling $\Delta$ or $M$ of $\Delta/2M = |\alpha_{\text{max}} - \alpha_{\text{min}}|/2M$, we obtained an error probability of the attacker $P_e = 0.5$. This setting corresponds to that needed for real-world operation: the attacker is prevented from obtaining detailed information on ciphertext and cannot perform crypto-analysis. Finally, we applied our Y-00 encryption system to optical fiber transmission over 300km in the laboratory with 10 optical amplifiers. The legitimate receiver showed a bit error probability of $10^{-7}$, which is acceptable for practical applications. In the future, we plan to

Continued on next page
apply the quantum-stream cipher to a space-satellite communication system using a high-power laser.

In summary, we have implemented a quantum encryption system based on the Y-00 protocol working at 10Gb/s, and demonstrated transmission along a 300km fiber cable to verify performance. We have not yet achieved the theoretical target of security, though the system is more secure than any conventional mathematical cipher. These advances will require more sophisticated randomizations than are currently proposed.\textsuperscript{5–7} Finally, the control circuits of our present system are fabricated by field-programmable gate arrays, which makes them susceptible to temperature-related effects at very fast speeds. As a next step, we plan to integrate all the circuits to make them more stable.

This work was supported by National Institute of Information and Communication Technology, grant 119.

Author Information

Osamu Hirota, Makoto Honda, Shigeto Akutsu, and Katsuyoshi Harasawa
Research Center for Quantum Information Science
Tamagawa University
Tokyo, Japan

Osamu Hirota directs the Research Center for Quantum Information Science. He is the founder of the International Conference on Quantum Communication, Measurement, and Computing, and the Quantum Communication Award.

Kenichi Ohhata and Kiichi Yamashita
Kagoshima University
Kagoshima, Japan

References