Photonic Generation of Quantum Noise Assisted Cipher at Microwave Frequencies for Secure Wireless Links

Ken Tanizawa* and Fumio Futami
Quantum ICT Research Institute, Tamagawa University, 6-1-1 Tamagawa-gakuen, Machida, Tokyo, 194-8610, Japan
**tanizawa@lab.tamagawa.ac.jp*

Abstract: We propose novel wireless physical layer encryption utilizing signal masking by truly random quantum noise. 12-Gbit/s cipher with sufficient masking is generated in 30-GHz band by optical heterodyne, and secure microwave wireless transmission is achieved.
OCIS codes: (060.0060) Fiber optics and optical communications; (060.4785) Optical security and encryption

1. Introduction

In communication networks, signal interceptions at the physical layer are one of the security risks. Wireless transmissions are particularly vulnerable to interception as the microwave signals are broadcasted into open air. Although conventional ciphers based on computational complexity are implemented at the higher layers, interception at the physical layer should be directly protected against for higher security of transmission systems. Security measures for the physical layer in wireless systems based on advanced coding [1] or direct-data encryption have been demonstrated. The latter approach utilizes unique signal encoding or scrambling [2]-[5].

Here, we focus on symmetric-key direct-data encryption utilizing signal masking by quantum (shot) noise [6] and aim for the first realization of quantum noise enhanced security in high-speed microwave wireless links. The cipher system was first demonstrated in the AlphaEta [7] or Y-00 quantum stream cipher [8] for fiber-optic transmission. Recently, high-speed transmission at 10 Gbit/s or more [9], [10], and compatibility with WDM systems [11], [12] were experimentally demonstrated. Secrecy is achieved by converting data (plain text) into an extremely high-order optical signal, such as a 2^{17} (=131,072) PSK signal [9], with a pre-shared short seed key. Doing so makes the signal distance of the high-order signal smaller than the uncertainty due to quantum noise at detection. This prevents an eavesdropper without the key, from measuring the encrypted signal correctly. Quantum noise is an ideal mask to realize secrecy because of its truly random and inherently unavoidable nature, which confers security which can neither be modified nor avoided by external parties. On the other hand, to exploit the technique for microwave wireless transmissions is difficult because the masking effect is proportional to the square root of the signal frequency. The secrecy in microwave frequencies (1 to 100 GHz), which are three to five orders of magnitude lower than optical ones (~200 THz), is only 1/500 to 1/50 of the secrecy in optical frequencies. Although the addition of artificial noise using a pseudorandom noise generator has been demonstrated [4], [5], the artificial noise, unlike quantum noise, is not truly random. Hence, its secrecy cannot be theoretically proved in a strict sense.

Here, we propose the seamless conversion of the quantum noise masking effect from optical to microwave frequencies by utilizing microwave photonics. The quantum noise masking cipher is first generated in the optical domain. Frequency conversion, based on optical heterodyne with local oscillator (LO) light, is then performed. Quantum noise in the optical domain is *naturally* added to a microwave difference frequency in the process. This generates a microwave cipher with sufficient masking due to the truly random quantum noise. We experimentally demonstrate the generation and transmission of 12-Gbit/s wireless cipher at a center frequency of 30 GHz. Adequate signal quality is achieved while retaining the secrecy conferred by the quantum noise masking.

2. Operating principle

M-ary PSK data signals (*M* is an order of data modulation) are encrypted by randomly rotating the phase using a pre-shared short key. Figure 1 shows the operating principle when QPSK ($M = 4$) is used for data modulation. The QPSK data signal is rotated for encryption, as shown in Fig. 1 (a). The arrow on the I axis indicates the basis of the phase modulation. The basis is rotated by $\theta_{\mathrm{basis}}(i)$. Here i is the identification of a symbol. The rotation angle $\theta_{\mathrm{basis}}(i)$ ranges from $-\pi/4$ to $\pi/4$ and is determined randomly, using the pre-shared seed key (typically 256 bits). The phase rotation is performed in a symbol-by-symbol manner. After the encryption, the constellation becomes an extremely high-order PSK signal, as shown in Fig.1 (b). Provided that the resolution of the rotation angle is $\pi/2^{(m+1)}$, the order of the PSK signal becomes $2^{(m+2)}$. The bit resolution m is set at the largest achievable value for maximal secrecy. It can be intuitively understood that noise prevents eavesdropping attempts from accurately detecting the high-order PSK, e.g. 16,384 PSK for $m = 12$. On the other hand, a legitimate receiver who has a seed key can detect the original QPSK signal by subtracting $\theta_{\mathrm{basis}}(i)$ in a symbol-by-symbol manner. As shown in the magnified image of Fig. 1 (b),

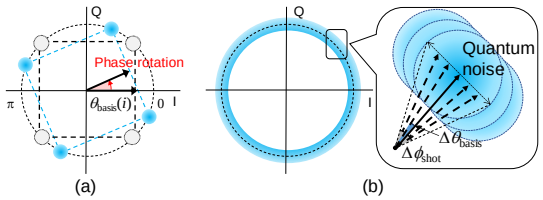

Fig. 1. Signal encryption based on quantum noise masking: (a) phase rotation of a QPSK signal for the encryption and (b) constellation after the encryption.

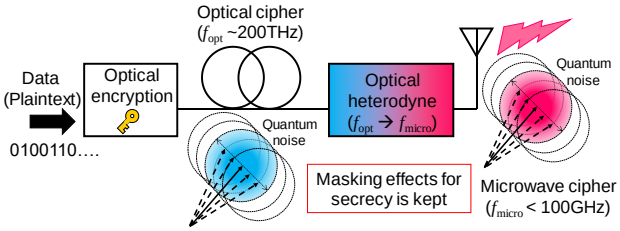

Fig.2. Seamless conversion of the quantum noise masking effect from optical to microwave frequencies with optical heterodyne.

m is set at a large number such that the adjacent signals are masked by quantum noise. The security provided by quantum noise masking can neither be modified nor avoided, because quantum noise is truly random and is inherently inevitable at detection. The masking effect for secrecy is quantified by defining a masking number Γ as $\Gamma = \Delta\phi_{shot}/\Delta\theta_{basis}$. The masking number, which indicates the number of signal phase levels falling within the variance of quantum noise, is proportional to the square root of the signal frequency [10]. This relation diminishes the effectiveness of quantum noise masking at microwave frequencies.

We propose to utilize microwave photonics in order to achieve quantum noise masking at microwave frequencies (< 100 GHz). Figure 2 shows the basic configuration for the conversion of the quantum noise masking effect from optical to microwave frequencies. First, the cipher is generated at an optical frequency f_{opt} (~200 THz) by a prescribed encryption protocol. The optical frequency is high enough to provide a sufficient effect of quantum noise masking for secrecy. Then, optical heterodyne technique is employed to shift f_{opt} to the target microwave frequency f_{micro}. An LO light which has a frequency $f_{opt} + f_{micro}$ or $f_{opt} - f_{micro}$ is mixed with the optical cipher, generating the cipher at the microwave difference frequency of f_{micro}. Here, the quantum noise in the optical domain is added *naturally* to the microwave frequency f_{micro}, and the secrecy level realized by the quantum noise masking effect is maintained. This cipher generation integrates well with analog radio-over-fiber (RoF) systems because the basic configuration using heterodyne technique with LO is consistent. A distinct advantage of the system is that both the wireless and fiber-optic links can be simultaneously secured against interception.

3. Experiments

We demonstrate a quantum noise assisted 12-Gbit/s cipher system based on QPSK data signals for 30-GHz wireless transmission. Figure 3 illustrates the experimental setup. A data stream consisting of PRBS 2^{23}-1 and a pre-shared seed key are put into a mathematical encryption box. The encryption box, which is implemented offline, includes pseudorandom number generators and a mapper. Random phase rotation angles $\theta_{basis}(i)$ with 16-bit resolution (m = 16) and polarity randomized data (2 bits) are generated according to the prescribed protocol [12]. These outputs are used for driving optical modulators, via a 6 Gsample/s arbitrary waveform generator. An IQ modulator is driven by the polarity randomized data for QPSK data modulation. Then, the rotation angles with 16-bit resolution are divided into coarse (6-bit resolution) and fine (10-bit resolution) angles, and two cascaded phase modulators are synchronously driven by them for the encryption with high bit resolution beyond a single DAC [9]. Thus, the cipher with $2^{(2+6+10)} = 2^{18}$ phase levels is generated at 1550.116 nm. Next, the cipher is combined with an LO light at 1549.872 nm which is approximately 30 GHz apart from the cipher wavelength. The two wavelengths have not been locked to 30 GHz because this is a simple, proof-of-concept setup. Precise locking is, however, necessary in practice. The cipher and LO are detected by a photo detector (PD) with 50 GHz bandwidth, and the cipher with the quantum noise masking is generated at a center frequency of 30 GHz. Then, the cipher is amplified and transmitted over (i) a short RF cable (back-to-back condition) or (ii) a 0.3 m wireless link, using a pair of horn antennas and an amplifier. The wireless link distance is limited by the size of our microwave shielding. At the receiver, the cipher is down-converted with an IQ mixer and an LO at 30 GHz, and digitized by an oscilloscope with 6-GHz bandwidth. Digital signal processing (DSP) for the decryption and demodulation is performed offline.

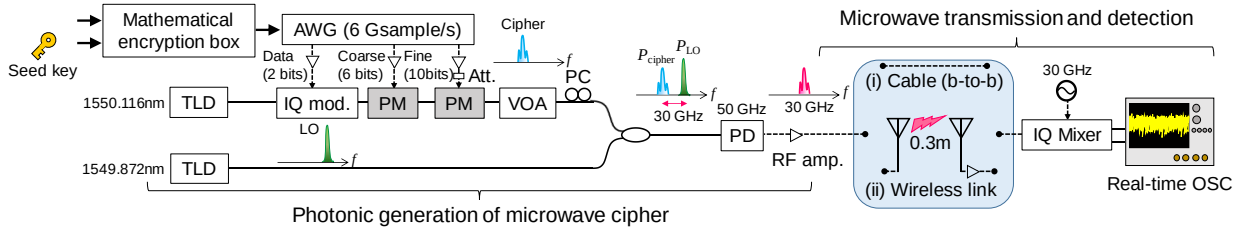

Fig. 3. Experimental setup of the generation and transmission of wireless cipher at a center frequency of 30 GHz.

We first demonstrate encryption and decryption in (i) back-to-back condition. The optical powers of the cipher P_{cipher} and LO P_{LO} at the input of the PD are set to −9.0 and 6.3 dBm, respectively. Figure 4 (a) shows the electrical spectrum after the heterodyne. The cipher is successfully generated at the center frequency of approximately 30 GHz. Figure 4 (b) shows the constellations before and after the decryption. The QPSK constellation is successfully recovered by the DSP with decryption, and no bit errors are observed. Figure 4 (c) shows the Q values after the decryption when P_{cipher} changes from −9 to −23 dBm. P_{LO} is maintained at a constant value of 6.3 dBm. The Q values after the decryption are more than 16.5 dB. A large Q margin from a SD-FEC Q threshold (7.3 dB) is achieved. A reference curve of a non-cipher QPSK signal is also plotted. The maximum Q penalty is 0.6 dB, which indicates that the encryption and decryption are achievable without significant negative impacts on the signal quality.

The RF cable is replaced with the pair of antennas and an amplifier to demonstrate wireless transmission of the cipher over (ii) a 0.3-m wireless link. Figure 5 shows the Q values after the decryption (red curve) when P_{cipher} changes from −9 to −17 dBm. Even after the wireless transmission, Q values of more than 15 dB, and Q margin of more than 7.5 dB from the SD-FEC threshold are achieved for measured P_{cipher}. In the current setup, the RF power of the cipher at the output of the antenna is limited to less than 0.5 mW by the gain of the amplifier we used. A larger margin for a practical lossy wireless link can be achieved using an amplifier with a higher gain. The quantum noise masking number of the microwave cipher Γ is co-plotted (black curve) in Fig. 5. The masking number increases with the decrease of P_{cipher}. The number is kept above 50 for measured P_{cipher}. Here, practical security realized by the masking is briefly discussed. We focus on a typical attack on a seed key where an eavesdropper intercepts the cipher with 2^{18} phase levels. The first step of the attack is the discrimination of the 2^{18} phase levels for subsequent computational analysis. As an example, 103 phase levels were masked due to quantum noise (Γ = 103) at P_{cipher} of −15 dBm. Then, the probability of pinning down the correct phase levels of l consecutive symbols is approximately $(1/103)^l$. The symbol length l, required to deduce a seed key by the analysis, depends on the procedure in the mathematical encryption box. It is typically large, and the probability of success is extremely low in practice, e.g. 3.9×10^{-65} for l = 32. Since the quantum noise masking is proved to be irreducible, the probability for a given value of l remains unchanged. Thus, good signal quality and high security against signal interception are simultaneously achieved in this wireless cipher system.

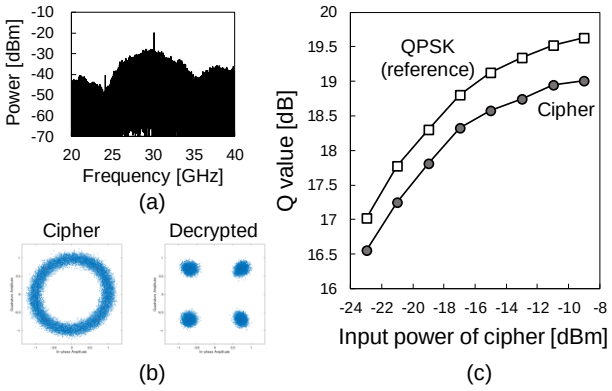

Fig. 4. Experimental results in a back-to-back condition: (a) electrical spectrum after optical heterodyne, (b) constellation diagrams, and (c) Q values when P_{cipher} changes.

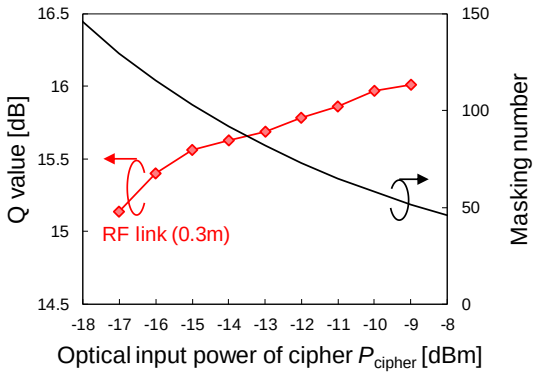

Fig. 5. Q values and quantum noise masking numbers for various optical input powers of the cipher P_{cipher}.

4. Conclusions

We proposed a photonic-assisted microwave cipher system that realizes quantum noise enhanced security. Heterodyne optical-to-microwave frequency conversion was utilized to achieve sufficient effects of quantum noise masking for secrecy. 12-Gbit/s wireless cipher at a center frequency of 30 GHz was successfully generated and transmitted. Adequate signal quality and high security were achieved simultaneously.

5. References

[1] H. V. Poor, et al., *PNAS*, **114**, pp.19-26 (2017).
[2] M. A. Khan, et al., *Proc. ICIAS*, pp. 484–488 (2007).
[3] A. Morales, et al., *Opt. Express* **26**, pp. 22296-22306 (2018).
[4] D. Reilly, et al., *IEEE RWS2009*, TU2P-28.
[5] R. Ma, et al., *IEEE Trans. Consum. Electron.*, **56**, pp. 1328–1332 (2010).
[6] G. Barbosa, et al, *Phys. Rev. Lett.* **90**, 227901 (2003).
[7] E. Corndorf, et al., *Phys. Rev. A*, 71, (6), p.062326 (2005).
[8] O. Hirota, et al., *Phys. Rev. A*, 72, (2), p.022335 (2005).
[9] K. Tanizawa, et al., *Opt. Express* **27**, pp. 1071-1079 (2019).
[10] K. Tanizawa, et al., *Opt. Express* **27**, pp. 25357-25363 (2019).
[11] F. Futami and O. Hirota, *OECC2014*, MO1A2.
[12] F. Futami, et al., *Opt. Express* **25**, pp. 33338-33349 (2017).