Security-Enhanced 10,118-km Single-Channel 40-Gbit/s Transmission Using PSK Y-00 Quantum Stream Cipher

Ken Tanizawa, Fumio Futami

Quantum ICT Research Institute, Tamagawa University, Japan, tanizawa@lab.tamagawa.ac.jp

Abstract *We demonstrate the first ultra-long haul transmission of Y-00 quantum-noise randomized stream cipher. 40-Gbit/s QPSK signal is encrypted by 2^{16}-level phase randomization with a key. Irreducible security based on signal masking by quantum (shot) noise and adequate signal quality after 10,118-km SMF transmission are achieved.*

Introduction

Eavesdropping is a potential security risk in a current fibre-optic transmission system. A typical attack has two steps: 1) tap optical signal and demodulate digital data, and 2) cryptanalyze the data by using computational resources. Digital-layer cipher implemented in layer 2 or higher, such as the advanced encryption standard, prevents step 2) because of high computation complexity. To achieve higher security, step 1) should be prevented as well. Such techniques are called physical layer encryption (PLE). PLE uses a pre-shared short key and directly hides data utilizing unique optical encoding or scrambling techniques[1-5]. Secure key exchange methods, e.g. quantum key distribution, are necessary before PLE, although they are not the scope of this paper. Here we focus on PLE based on secrecy realized by signal masking by quantum (shot) noise[4], called AlphaEta[5] or Y-00 quantum stream cipher[6]. The signal masking is achieved by converting a low-order data signal into an extremely high-order IM/PSK/QAM signals, e.g. 2^{18} PSK[7]. The conversion process using a seed key is based on a prescribed protocol[8]. Correct detection of such an extremely high-order signal is inherently disrupted by shot noise, while a legitimate receiver can detect the low-order data signal by using the seed key. The signal masking by shot noise provides irreducible security in practice, because shot noise is inherently inevitable and truly random. As this cipher system is compatible with optical amplification and WDM, 61.4 Gbit/s×165 λ transmission over 160-km fibre[9], 40-Gbit/s transmission over 800-km fibre[7], and 1.5-Gbit/s transmission over the longest 1,000-km fibre[10] were experimentally demonstrated.

Our previous study showed that OSNR penalty caused by the encryption and decryption was less than 0.5 dB in a PSK Y-00 cipher system[7]. This suggests that PSK Y-00 cipher is potentially capable of longer reach transmission with enhanced security at physical layer. This paper reports PSK Y-00 cipher transmission over a record-long transoceanic-distance fibre. Theoretical study shows that tradeoff between the reach and security is mitigated by increasing the number of phase levels. A transmission reach of 10,118 km, which is >10 times longer than the previous reports[5-10], is experimentally demonstrated in a single-channel 40-Gbit/s digital coherent DP-PSK Y-00 cipher system. The cipher has 2^{18} phase levels, and signal masking by shot noise for irreducible security as well as adequate signal quality are achieved. This cipher is applicable to a WDM system with a 37.5-GHz signal bandwidth[11], although this demonstration is a single-channel transmission.

Operating principles and system design

In a PSK Y-00 cipher system, secrecy against interceptions is achieved by randomly rotating the phase of *M*-ary PSK data modulation. Figure 1(a) shows the operation of phase rotation when a QPSK (*M* = 4) data signal is encrypted. The arrow on I axis indicates the basis of the phase data modulation. To encrypt the QPSK signal, the basis is rotated in a symbol-by-symbol manner. The rotation angle $\theta_{\mathrm{basis}}(i)$ for each symbol is determined randomly utilizing a seed key (typically 256 bits) that is securely pre-shared between legitimate users. As the phase

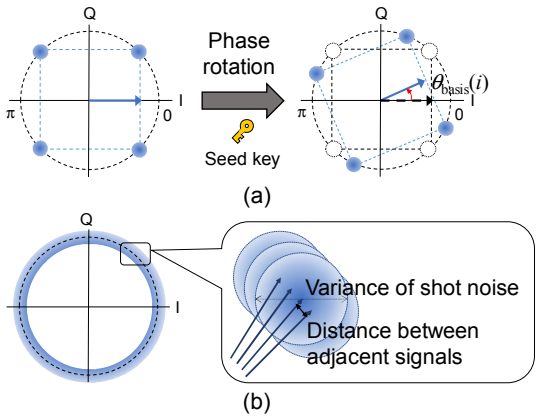

Fig. 1: Operating principles of PSK Y-00 cipher: (a) phase rotation of a QPSK symbol for the encryption, and (b) constellation diagram after the encryption.

rotation is random, a constellation diagram after the rotation is a shape like a donut, as shown in Fig. 1(b). When the resolution of the phase rotation is $\pi/2^{(m+1)}$ (m bits), the constellation corresponds to $2^{(m+2)}$ PSK. The resolution is set as finely as possible, e.g. m = 12 or more, such that variance of shot noise is wider than the distance of adjacent signals, as shown in the magnified image of Fig. 1(b). Then, correct detection of the high-order PSK is inherently prevented by shot noise. Thus, the cipher system achieves security against interception from the physical layer, or correct signal discrimination for subsequent cryptanalysis. A legitimate receiver with a seed key can recover the original QPSK signals by subtracting the angles of symbol-by-symbol phase rotation. The decryption is implemented as a part of digital signal processing (DSP) after detection[7].

The secrecy realized by the shot noise is called quantum-noise masking. As shot noise is proven to be inevitable at detection, quantum-noise masking is effective all along the fibre link. To evaluate the masking effects quantitatively, a quantum-noise masking number Γ_Q that indicates the number of phase levels covered by shot noise in $2^{(m+2)}$ PSK is introduced. Higher numbers are better for security, because uncertainty of detection by an eavesdropper is larger. The masking number Γ_Q is defined here assuming that an eavesdropper performs an ideal heterodyne detection at the input of a fibre link. The masking number is a function of the bit resolution of phase rotation m and average photon number of a symbol[12].

Here, assuming a simple long-haul fibre link in which each constant span loss is fully compensated by an Er-doped fibre amplifier (EDFA), we theoretically investigate relation between the masking number Γ_Q and reach in the cipher system. The fibre link consists of fibre spans of 50 km with a loss of 10 dB and EDFAs with a noise figure (NF) of 5 dB. The output OSNR of the link is estimated from the gain and NF of the EDFA, input optical power P_{in}, and wavelength[13]. When a required OSNR at the receiver is fixed, the relation between the masking number and reach is calculated using the output OSNR estimation and the definition of masking number. Figure 2 shows the results for 12-Gbaud DP-PSK Y-00 cipher with m = 12, 14, and 16. The required OSNR at the receiver was preliminarily measured and was set to 7.4 dB to satisfy a typical Q threshold of 6.4 dB for SD-FEC with 20 % overhead[14]. In a target reach of 10,000 km, a masking number Γ_Q > 430 is achievable when m = 16. We estimate from Γ_Q that a symbol error ratio (SER) of ideal heterodyne detection of the cipher ($2^{(m+2)}$ PSK) by an eavesdropper SER_{eve} is > 0.9980 (see the right vertical axis). Although a simple linear transmission is assumed, this result indicates that PSK Y-00 cipher system with m = 16 can achieve security based on the quantum-noise masking in a 10,000-km fibre transmission.

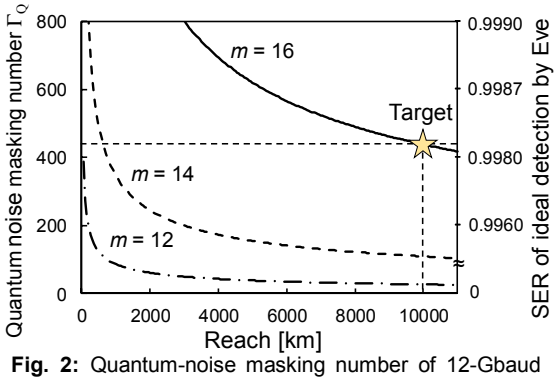

Fig. 2: Quantum-noise masking number of 12-Gbaud DP-PSK Y-00 cipher (left vertical axis) and SER of an eavesdropper (right vertical axis) in a long-haul link when the bit resolutions m are 12, 14, and 16.

Experiments

Ultra-long haul transmissions of PSK Y-00 cipher with 2^{18} phase levels (m = 16) are demonstrated using a recirculating loop system. Fig. 3 shows the experimental setup. Data stream of a pseudorandom binary sequence (PRBS) with a length of 2^{23}-1 and a pre-shared seed key are put into a Y-00 mathematical encryption box. In the box, the seed key is extended to a practically non-repeated PRBS (key stream) by using a pseudorandom number generator. Then, 16 bits is extracted for random phase rotation of each symbol. Besides, 2-bit data encoding for each time slot is determined based on the extracted key stream, such that data for QPSK modulation (2 bits) is randomized. Details of the algorithm can be found elsewhere[8]. The encoded 2 bits of data and 16 bits for the phase randomization are combined in the optical domain. First, coherent light at 1550.12 nm is modulated at 12 Gbaud by the 2-bit data in an IQ modulator. Next, two cascaded phase modulators are synchronously driven with two AWG outputs to achieve phase randomization with a nominal bit resolution of 16 bits[7]. Then, polarization-division multiplexing is emulated, and 48-Gbit/s (line rate) DP-PSK Y-00 cipher with 2^{18} phase levels is generated.

The DP-PSK Y-00 cipher is launched into the recirculating loop system consisting of two acousto-optic modulators and a 50.59×5 km standard single-mode fibre (MFD = 9.2 μm) link with EDFAs. An average span loss is 9.6 dB. Signal power launched into each span P_{in} is adjusted to be constant with a variable optical attenuator. After the transmission, Y-00 cipher is

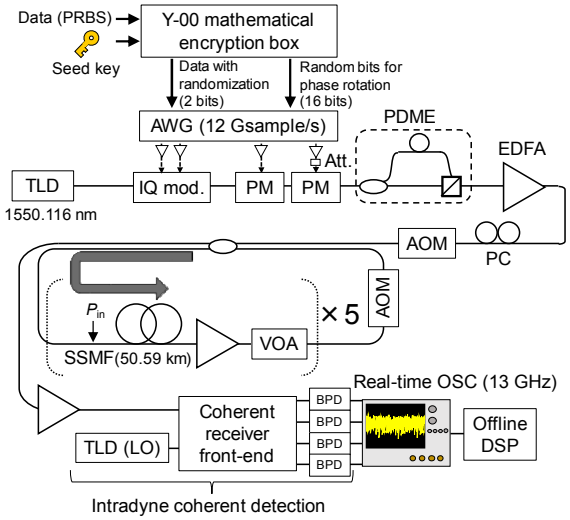

Fig. 3: Experimental setup of cipher transmission.

received by a conventional intradyne coherent detection setup. Digitization is achieved with a real-time oscilloscope with a bandwidth of 13 GHz. Finally, offline DSP for dispersion compensation, polarization demultiplexing, decryption, and carrier phase recovery is performed. The decryption is a unique process for the cipher. The phase rotation angles $\theta_{basis}(i)$ for each symbol are obtained by putting the seed key into the same encryption box. The complex amplitude of each received symbol is multiplied by $\exp(-j\theta_{basis}(i))$ for inverse phase rotation. Timing synchronization for the decryption is achieved by adding preamble bits in the offline processing. In a real-time DSP, synchronization protocol can be implemented prior to the start of communication.

Figure 4 shows the Q factors of decrypted signal when the transmission distance is 10,118 km. More than 1.1 million ($>2^{20}$) symbols were processed to measure BER. Q factors were calculated from BER. Signal power launched into the spans P_{in} was changed from −10 to −4 dBm. A Q factor higher than a typical Q threshold (SD-FEC with 20% overhead) of 6.4 dB[13] was achieved at an input power P_{in} of −7 dBm. The inset constellations show that QPSK signal is successfully recovered by the decryption. The black solid curve in Fig. 4 shows the SER of ideal detection of the cipher (2^{18} PSK) by an eavesdropper, SER_{eve}. When P_{in} = −7 dBm, SER_{eve} was more than 0.9965 (Γ_Q = 231). The SER was calculated assuming that only shot noise at highest power P_{in} affected the detection. This indicates that the detection contains inevitable many errors even if the eavesdropper taps all power at the input of the fibre link and performs ideal heterodyne detection without any additive noise. In other words, the SER shown here cannot be improved in practice. The masking by shot noise provides a lower bound of security in this system. Thus, appropriate signal quality above the Q threshold and irreducible security based on the masking by shot noise were achieved simultaneously in the cipher transmission over 10,118-km fibre. Moreover, if the cipher is tapped at a point of the fibre link after amplification, accumulated amplified spontaneous emission noise also works effectively for signal masking. Figure 5 shows the Q factors of the cipher and reference DP QPSK when the transmission distance changes. The signal input power P_{in} was −7 dBm. The difference of the Q factors was approximately 0.4 dB for all the transmission distances. The penalty to pay for the security was small, and hence security-enhanced ultra-long haul transmission was achieved.

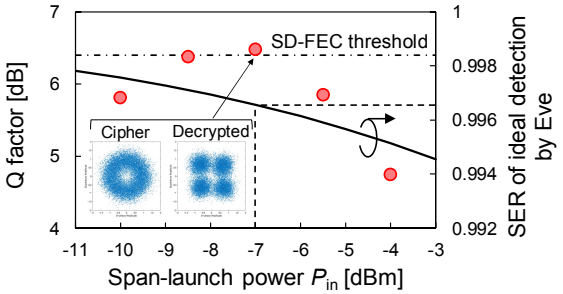

Fig. 4: Q factors and quantum-noise masking number for various span-launch optical power P_{in} in the cipher transmission over 10,118-km SSMF.

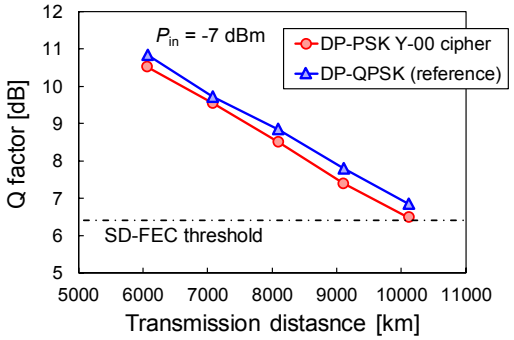

Fig. 5: Q factors vs. transmission distances when the span-launch optical power Pin is −7 dBm.

Conclusions

A single-channel 40-Gbit/s DP-PSK Y-00 quantum stream cipher transmission over 10,118 km fibre was experimentally demonstrated. Adequate signal quality after decryption and security enhancement at physical layer based on the quantum-noise signal masking were simultaneously achieved. PSK Y-00 cipher is applicable to transoceanic distance transmission systems.

Acknowledgements

This work was supported in part by JSPS KAKENHI Grant Number JP18K04290 and Research Grant of KDDI foundation.

References

[1] V. A. Lodi, S. Donati, and A. Scire, “Synchronization of chaotic injected-laser systems and its application to optical cryptography”, IEEE J. Quantum Electron., 32, (6), pp. 953–959, 1996.

[2] T. H. Shake, “Security performance of optical CDMA against eavesdropping”, IEEE/OSA J. Lightwave Technol., 23, (2), pp.665-670, 2005.

[3] Y. Huang, H. Chen, H. Huang, Q. Zhang, Z. Li, N. K. Fontaine, R. Ryf, and M. Wang, “Two-Level Optical Encryption for Secure Optical Communication”, Proc. Opt. Fiber Comm. Conf. (OFC 2020), 2020, M4A.2

[4] G. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, “Secure communication using mesoscopic coherent states”, Phys. Rev. Lett., 90, p.227901, 2003

[5] E. Corndorf, C. Liang, G. S. Kanter, P. Kumar, and H. P. Yuen, “Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks”, Phys. Rev. A, 71, (6), p.062326, 2005.

[6] O. Hirota, M. Sohma, M. Fuse, and K. Kato, “Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme”, Phys. Rev. A, 72, (2), p.022335, 2005.

[7] K. Tanizawa, and F. Futami, “Single channel 48-Gbit/s DP-PSK Y-00 quantum stream cipher transmission over 400- and 800-km SSMF”, Opt. Express, 27, (18), pp. 25357-25363, 2019.

[8] F. Futami, K. Guan, J. Gripp, K. Kato, K. Tanizawa, C. Sethumadhavan, and P. J. Winzer, “Y-00 quantum stream cipher overlay in a coherent 256-Gbit/s polarization multiplexed 16-QAM WDM system”, Opt. Express, 25, (26), pp.33338–33349, 2017.

[9] F. Futami, K. Tanizawa, and K. Kato, “Y-00 Quantum-Noise Randomized Stream Cipher Using Intensity Modulation Signals for Physical Layer Security of Optical Communications”, IEEE/OSA J. Lightwave Technol., 38, (10), pp. 2773-2780, 2020.

[10] M. Yoshida, T. Kan, K. Kasai, T. Hirooka, and M. Nakazawa, “10 Tbit/s QAM Quantum Noise Stream Cipher Coherent Transmission over 160 km”, Proc. Opt. Fiber Comm. Conf. (OFC 2020), 2020, T3D.2

[11] K. Tanizawa, and F. Futami, “Multi-Channel Simultaneous Encryption in WDM Systems of PSK Y-00 Quantum Stream Cipher”, Proc. 25th Optoelectronics and Communications Conference (OECC 2020), 2020, to be presented.

[12] K. Tanizawa, and F. Futami, “Quantum Noise-Assisted Coherent Radio-over-Fiber Cipher System for Secure Optical Fronthaul and Microwave Wireless Links”, IEEE/OSA J. Lightwave Technol., 38, (16), pp. 4244-4249, 2020.

[13] I. P. Kaminow, T. Li, and A. E. Willner, “Optical Fiber Telecommunications V B: Systems and Networks”, Elsevier, 2008

[14] T. Mizuochi, Y. Miyata, K. Kubo, T. Sugihara, K. Onohara, and H. Yoshida, “Progress in Soft-Decision FEC”, Proc. Opt. Fiber Comm. Conf. (OFC 2011), 2011, NWC2.