ISSN 2186-6570

Tradeoffs Between Quantum Noise Masking and Transmission Reach in PSK Y-00 Quantum Stream Cipher

Ken Tanizawa and Fumio Futami

Quantum ICT Research Institute, Tamagawa University
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan

Tamagawa University Quantum ICT Research Institute Bulletin, Vol.8, No.1, 9-12, 2018

Tradeoffs between Quantum Noise Masking and Transmission Reach in PSK Y-00 Quantum Stream Cipher

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

***Abstract*—This paper reports theoretical analysis of tradeoffs between the amount of masking by quantum noise and the maximum fiber transmission distance in phase-shift keying (PSK) Y-00 quantum stream cipher. We derive an analytical formula that shows the tradeoffs when a fiber link configuration is given. The tradeoffs are independent of a baud rate of PSK Y-00 cipher. We show numerical simulations using the formula in two scenarios of ultra-long-haul (< 12,000 km) and long-haul (< 3,000 km) transmission systems.**

***Index Terms*— Y-00 quantum stream cipher, digital-coherent transmission, secure fiber-optic communication system.**

I. Introduction

To support various IoT applications, security of communication systems is increasingly important recently. Fiber-optic transmission which composes the physical layer of the system faces a potential threat of eavesdropping such as tapping. A promising countermeasure is to use a symmetric-key direct data encryption utilizing physical properties. A Y-00 quantum stream cipher that utilizes signal masking by quantum or shot noise inevitable at optical detection [1] is particularly prospective since the security is promised by the inevitable effects of the shot noise. Y-00 cipher is achievable at a high data rate of over 10 Gbit/s and is compatible with wavelength-division-multiplexing systems [2]-[4]. The quantum noise masking, or Y-00 encryption, is implemented by high-order modulation of phase [5], [6], intensity [7], [8], or quadrature amplitudes [9], [10].

Among the three modulation formats, phase-based or phase-shift keying (PSK) Y-00 cipher is promising for long-reach transmission since the tolerance of optical signal-to-noise ratio (OSNR) is the highest. Recently, we have demonstrated introduction of digital-coherent technology to PSK Y-00 cipher for stable coherent detection with decryption [11], [12]. The experimental results indicate that transmission performances of PSK Y-00 cipher could be comparable with those of conventional binary PSK signals. A challenge of PSK Y-00 cipher was to achieve an extremely high modulation order to realize security promised by the effects of the shot noise. A resolution of a digital-to-analog converter (DAC) practically limits the order of the phase modulation at a high baud rate. We have proposed coarse-to-fine phase modulation that multiplexes two DAC outputs in an optical domain using two cascaded phase modulators [13]. A record 2^{17} phase-level 10-Gbuad Y-00 cipher was achieved, and the security was guaranteed by the effect of the shot noise at a practical optical power for fiber-optic transmission.

One of security measures in Y-00 cipher is a quantum-noise masking number that indicates the number of signal levels masked by the shot noise. The masking number is inversely proportional to the square root of optical power in PSK Y-00 cipher. Hence, higher masking number is achieved at lower optical power. On the other hand, in order to keep high signal-to-noise ratio (SNR), higher optical power is desirable in fiber-optic transmission. The tradeoffs are analytically discussed in this paper. First, quantum-noise masking number in PSK Y-00 cipher is derived as a function of average optical power. Then, the relation between transmission reach and average optical power launched into a fiber span is obtained assuming an ideal fiber link which consists of regularly repeated loss and gain. Using the two relations, we derive a formula of theoretical tradeoffs between the quantum-noise masking number and transmission reach. We confirm that the formula is independent of a baud rate of PSK Y-00 cipher. Numerical simulations using the formula in two different scenarios of ultra-long-haul (< 12,000 km) and long-haul (< 3,000 km) transmission systems are shown.

II. Theoretical Analysis

High-order phase modulation is employed for the generation of PSK Y-00 cipher. Fig. 1 shows the mapping of bases in PSK Y-00 cipher based on binary data modulation. Total 2^m bases are prepared, and one of them is selected randomly for one-bit modulation: the phase of coherent light is modulated to 0 or π on a bit-by-bit basis phase between 0 and π. First, we discuss signal masking by the shot noise in the PSK Y-00 cipher. Fig. 2 shows the magnified image of signals. The phase uncertainty caused by the shot noise $\Delta\phi_{\text{shot}}$ is expressed as

$$\Delta\phi_{\text{shot}} = \frac{1/2}{\sqrt{n}} \tag{1}$$

where n is the average number of photons of a symbol. When the data is modulated by M-ary PSK, n is obtained as

$$n = \frac{P_0}{R \cdot h\nu_0} \tag{2}$$

where P_0, R, h, and ν_0 are the signal average power, baud rate,

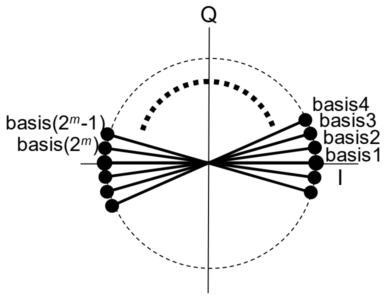

Fig. 1. Signal mapping of PSK Y-00 cipher in an IQ plane.

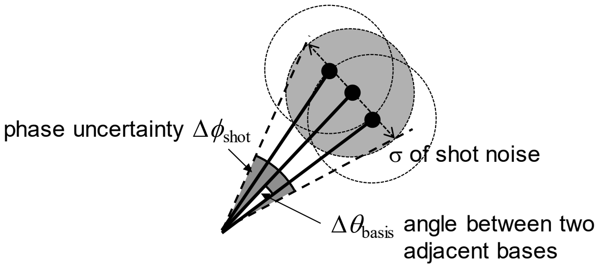
phase uncertainty $\Delta\phi_{\text{shot}}$
σ of shot noise
$\Delta\theta_{\text{basis}}$ angle between two adjacent bases

Fig. 2. Magnified image of the signals in PSK Y-00 cipher.

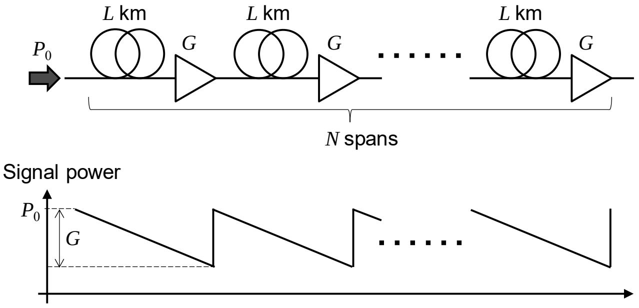

Fig. 3. Fiber link configuration and power diagram.

Planck constant, and signal frequency, respectively. When the PSK Y-00 cipher is based on binary data modulation (M=2), quantum-noise masking number Γ, which is a security measure of PSK Y-00 cipher, is defined as

$$\Gamma = \frac{\Delta\phi_{\text{shot}}}{\Delta\theta_{\text{basis}}} = \frac{2^{(m-1)}}{\pi}\sqrt{\frac{R\cdot h\nu_0}{P_0}} \tag{3}$$

where $\Delta\theta_{\text{basis}} = \pi/2^m$ is the angle between adjacent bases shown in Fig. 2. The masking number Γ indicates the number of signal phase levels covered by the standard deviation of the shot noise. A higher number is better for the security. The masking number is inversely proportional to the square root of the signal average power P_0. While higher signal power is better for transmission performance, it is not good for the security in PSK Y-00 cipher.

Next, we investigate the tradeoffs between the masking number and transmission reach of PSK Y-00 cipher. Fig. 3 shows the transmission fiber link and power diagram we assume in this analysis. The link consists of L km fiber spans and EDFAs, and loss and gain are regularly repeated. The number of spans is N, and the span loss is equal to the gain of the amplifier G. When the signal input power is P_0, OSNR of the output signal for a single polarization $OSNR_{\text{out}}$ is calculated as

$$\begin{aligned} OSNR_{\text{out}} &= \frac{P_0}{N\cdot 2n_{sp}h\nu_0\Delta\nu_{\text{noise}}(G-1)} \\ &\approx \frac{P_0}{N\cdot 2n_{sp}h\nu_0\Delta\nu_{\text{noise}}G} \end{aligned} \tag{4}$$

where n_{sp} is the spontaneous emission factor or population inversion factor of an EDFA, and $\Delta\nu_{\text{noise}}$ is the noise bandwidth of the definition of OSNR [14]. $\Delta\nu_{\text{noise}}$ is typically set at 12.5 GHz. Provided that a required OSNR at the output is $OSNR_{\text{req}}$, the achievable maximum number of spans N_{max} is obtained from the Eq. (4) as follows.

$$N_{\text{max}} = \left\lfloor \frac{P_0}{2n_{sp}h\nu_0\Delta\nu_{\text{noise}}G\cdot OSNR_{\text{req}}} \right\rfloor \tag{5}$$

Since the number of span is an integer, floor function is used. The maximum reach is obtained by multiplying N_{max} by L.

PSK Y-00 cipher has a relation between the signal average power and masking number shown in Eq. (3). Hence, tradeoffs between the masking number and maximum number of spans is obtained by substituting Eq. (3) into Eq. (5).

$$N_{\text{Y00\_max}} = \left\lfloor \frac{2^{2(m-1)}R}{2n_{sp}\pi^2\Delta\nu_{\text{noise}}G\cdot OSNR_{\text{req}}}\cdot\frac{1}{\Gamma^2} \right\rfloor \tag{6}$$

This equation indicates the tradeoffs as a function of the number of bases m, provided that a signal baud rate and a target OSNR are fixed. Since the target OSNR is practically determined in experiments, Eq (6) is useful for designing a secure fiber link using PSK Y-00 cipher.

Then, we discuss theoretical limit of the tradeoffs between the masking number and reach when a target BER P_{b} and a number of bases m are given. BER of binary signal P_{b} is expressed as

$$P_{\text{b}} = \frac{1}{2}erfc\left(\sqrt{\frac{E_b}{N_0}}\right) \tag{7}$$

where E_{b}/N_0 is a bit energy to noise power density ratio or SNR per bit. Provided that signal-ASE beat noise is dominant, the SNR per bit and OSNR have the following relation [14]:

$$OSNR = \frac{E_b}{N_0}\cdot\frac{R}{2\Delta\nu_{\text{noise}}} \tag{8}$$

We substitute Eq. (8) into Eq. (6) and obtain the theoretical limit of the tradeoffs as follows.

$$N_{\text{Y00\_max}} = \left\lfloor \frac{2^{2(m-1)}}{n_{sp}\pi^2 G\cdot\left(\frac{E_b}{N_0}\right)_{\text{req}}}\cdot\frac{1}{\Gamma^2} \right\rfloor \tag{9}$$

Using Eq. (7) and Eq. (9), we can obtain the theoretical limit of the tradeoffs when a target BER, a bit number of bases m, and a link configuration are given. It is worth noting that the tradeoffs are independent of a baud rate of PSK Y-00 cipher. We assume here that the nonlinear effects of the fiber transmission are negligible. Span-launch optical power increases as the baud rate increases, and nonlinear effects must be taken into account for a high baud rate in practice.

III. Numerical Simulations

We perform numerical simulations to show tradeoffs between the masking number and reach in two specific scenarios. The first scenario is ultra-long-haul transmission (< 12,000 km) such as submarine cable systems. A fiber link consists of 60-km span low-loss SMF with a fiber loss of 0.155 dB/km and low-noise EDFAs with a noise figure of 5.0 dB. Table I summarize the parameters for the simulation. The amplifier gain G, which is the product of the span length and fiber loss, is 9.3 dB. We set a target BER at 3.8×10^{-3} which is a threshold of hard-decision forward error correction (HD-FEC) with 7% overhead.

Fig. 4 shows the tradeoffs between the quantum noise masking number and reach in the ultra-long-haul transmission. The bit number of bases m is set to 15, 16, and 17. Larger m relaxes the tradeoffs. These curves are simple indicators to design secure fiber links utilizing PSK Y-00 cipher. In this scenario, a typical target of the reach is 10,000 km. Masking numbers of 233 and 116 are achieved when m are 17 and 16, respectively. From the masking number Γ, we can estimate a probability that an eavesdropper successfully discriminates the high-order signal via an ideal measurement limited only by the shot noise. The probability is expressed as $\{\mathrm{erf}(1/\sqrt{2}/\Gamma)\}^n$ for consecutive n bits in PSK-Y00 cipher. The masking numbers of 233 and 116 correspond to very low probabilities of 3.6×10^{-40} and 2.5×10^{-35} for consecutive 16 bits, respectively. The number of consecutive bits required for eavesdropping is much higher in practical cases, and the probability would be further reduced.

TABLE I
Simulation Parameters in Ultra-long-haul Transmission

Item	Value
Fiber span length: L	60 km
Fiber loss	0.155 dB
Amplifier gain: G	9.3 dB
Noise figure of amplifier: $2n_{sp}$	5.0 dB
Target BER (HD-FEC threshold)	3.8×10^{-3}

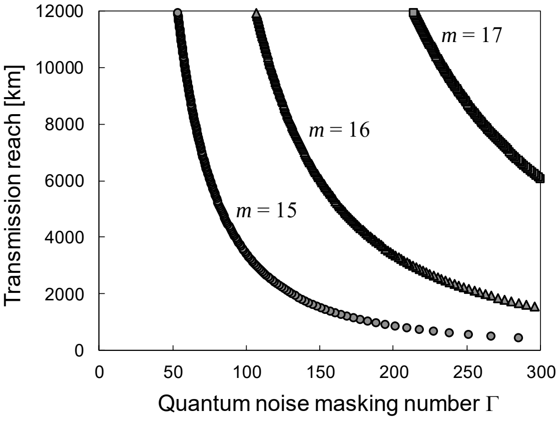

Fig. 4. Tradeoffs between quantum noise masking number and reach in ultra-long-haul transmission when m = 15, 16, and 17.

The second scenario is long-haul transmission (< 3,000 km) such as terrestrial cable systems. A fiber link consists of 100-km span standard SMF with a fiber loss of 0.18 dB/km and EDFAs with a noise figure of 5.5 dB. Table II summarize the parameters for the simulation. The amplifier gain G is 18 dB. The target BER is 3.8×10^{-3}.

Fig. 5 shows the calculated tradeoffs in the long-haul transmission when the number of bases m is set to 15, 16, and 17. Provided that a target reach is 1,500 km, masking numbers of approximately 270 and 135 are achieved when m are 17 and 16, respectively. We can also estimate a case of metro-area transmission whose reach is 500 km. Masking number reaches more than 233 and 116 when m = 16 and 15, respectively. The two case studies indicate that the design tradeoffs shown as Eq. (9) should be considered carefully when PSK Y-00 cipher is used for secure fiber-optic communication systems.

TABLE II
Simulation Parameters in Long-haul Transmission

Item	Value
Fiber span length: L	100 km
Fiber loss	0.18 dB
Amplifier gain: G	18.0 dB
Noise figure of amplifier: $2n_{sp}$	5.5 dB
Target BER (HD-FEC threshold)	3.8×10^{-3}

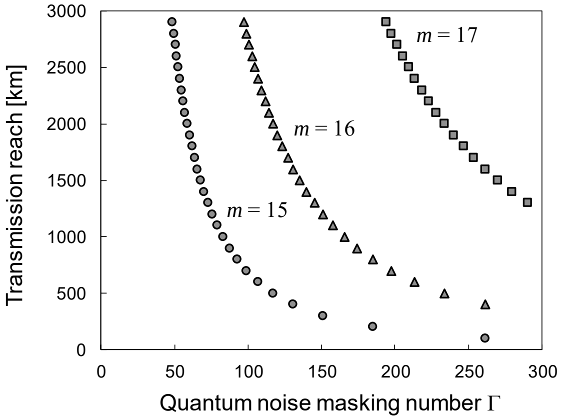

Fig. 5. Tradeoffs between quantum noise masking number and reach in long-haul transmission when m = 15, 16, and 17.

IV. Conclusion

We have reported theoretical analysis of the tradeoffs between the quantum noise masking number and transmission reach in PSK Y-00 cipher based on binary data modulation, provided that a fiber link consists of regularly repeated loss and gain. An analytic formula of the tradeoffs was derived. The tradeoffs were independent of a baud rate of Y-00 cipher. Two scenarios of ultra-long-haul (< 12,000 km) and long-haul (< 3,000 km) transmission systems were discussed using the formula. In both scenarios, the number of bases required to achieve the masking number of over 100 was 2^{16}.

ACKNOWLEDGMENT

The authors thank K. Kato for fruitful discussions.

REFERENCES

[1] G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, "Secure communication using mesoscopic coherent states," Phys. Rev. Lett., vol.22, 227901, 2003.

[2] F. Futami and O. Hirota, "40 Gb/s (4 × 10 Gb/s) Y-00 protocol for secure optical communication and its transmission over 120 km," in Proc. OFC, OTu1H.6, 2012.

[3] F. Futami and O. Hirota, " 100 Gbit/s (10 × 10 Gbit/s) Y-00 Cipher Transmission over 120 km for Secure Optical Fiber Communication between Data Centers," in Proc. OECC, MO1A2, 2014.

[4] 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," Optics Express, vol. 25, no. 26, pp. 33338-33349, 2017.

[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), 062326, 2005.

[6] C. Liang, G. S. Kanter, E. Corndorf, and P. Kumar, "Quantum Noise Protected Data Encryption in a WDM Network," IEEE Photon. Technol. Lett, vol. 17, no. 7, pp. 1573-1575, 2005.

[7] 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, 022335, 2005.

[8] F. Futami and O. Hirota, "Masking of 4096-level intensity modulation signals by noises for secure communication employing Y-00 cipher protocol," in Proc. ECOC, Tu.6.C.4, 2011.

[9] K. Kato and O. Hirota, "Quantum quadrature amplitude modulation system and its applicability to coherent state quantum cryptography," SPIE conference on quantum communication and imaging III. SPIE Proc. vol-5893, 2005.

[10] M. Nakazawa, M. Yoshida, T. Hirooka, and K. Kasai., "QAM quantum stream cipher using digital coherent optical transmission," Opt. Express 22, pp.4098-4107, 2014.

[11] K. Tanizawa, F. Futami, and O. Hirota, " Digital feedforward carrier phase estimation for PSK Y-00 quantum-noise randomized stream cipher," IEICE Communications Express, vol. 7, no. 1, pp. 1-6, 2018.

[12] K. Tanizawa and F. Futami, "Digital Coherent Detection with Decryption in PSK Y-00 Quantum Stream Cipher," in Proc. OECC, 5D1-1, 2018.

[13] K. Tanizawa and F. Futami, "PSK Y-00 Quantum Stream Cipher with 217 Levels Enabled by Coarse-to-Fine Modulation Using Cascaded Phase Modulators," in Proc. ECOC, We2.36, 2018.

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