Ultra-long-haul digital coherent PSK Y-00
quantum stream cipher transmission system:
supplement

KEN TANIZAWA* and FUMIO FUTAMI

Quantum ICT Research Institute, Tamagawa University, Tamagawagakuen 6-1-1, Machida, Tokyo 194-8610, Japan
*tanizawa@lab.tamagawa.ac.jp

This supplement published with The Optical Society on 18 March 2021 by The Authors under the terms of the Creative Commons Attribution 4.0 License in the format provided by the authors and unedited. Further distribution of this work must maintain attribution to the author(s) and the published article’s title, journal citation, and DOI.

Supplement DOI: https://doi.org/10.6084/m9.figshare.14179652

Parent Article DOI: https://doi.org/10.1364/OE.418302
Ultra-long-haul digital coherent PSK Y-00 quantum stream cipher transmission system: supplemental document

KEN TANIZAWA,1,* AND FUMIO FUTAMI1

1Quantum ICT Research Institute, Tamagawa University, Tamagawagakuen 6-1-1, Machida, Tokyo, 194-8610, Japan
*tanizawa@lab.tamagawa.ac.jp

This document provides supplementary information to “Ultra-long-haul digital coherent PSK Y-00 quantum stream cipher transmission system.”

1. Quantum-noise masking number in PSK Y-00 cipher

The quantum-noise masking number $\Gamma_Q$ in a PSK Y-00 cipher system was derived using semi-classical theory. An ideal heterodyne detection is assumed here. The variance of shot noise $\sigma_{\text{shot}}^2$ at ideal heterodyne detection with a local oscillator (LO) is calculated as

$$\sigma_{\text{shot}}^2 = 2e_i b, \tag{S1}$$

where $e$, $i_b$, and $B$ are the electric charge, bias current of a PD, and electrical signal bandwidth, respectively. The bias direct current is obtained as follows:

$$i_b = S(P_S + P_L), \tag{S2}$$

where $S$, $P_S$, and $P_L$ are the PD responsivity, optical power of the signal, and LO. The optical powers are defined for a single polarization. The signal current of the heterodyne detection $i_{\text{sig}}$ is expressed as

$$i_{\text{sig}} = 2S\sqrt{P_S \cdot P_L} \cos[(\omega_S - \omega_L) t + \varphi(t)], \tag{S3}$$

where $\omega_S$, $\omega_L$, and $\varphi(t)$ are the angular frequencies of the signal, LO, and modulated phase, respectively. The initial phase difference between the signal and LO is omitted for simplicity. The angle of uncertainty imposed by $\Delta \phi_{\text{shot}}$, as shown in Fig. S1, is calculated from Eqs. (S1)–(S3).

$$\tan\left(\frac{\Delta \phi_{\text{shot}}}{2}\right) \sim \frac{\Delta \phi_{\text{shot}}}{2} = \frac{\sigma_{\text{shot}}}{2S\sqrt{P_S \cdot P_L}} \tag{S4}$$

$$\Delta \phi_{\text{shot}} = \frac{2eB}{S\sqrt{P_S}} \tag{S5}$$

As the optical power of the LO is much larger than the signal power, $P_S + P_L = P_L$ is assumed. Meanwhile, the angle of adjacent signals of the cipher $\Delta \theta_{\text{basis}}$ is obtained from the order of data modulation $M$ and bit resolution of phase randomization $m$.

Fig. S1. Magnified image of signals masked by shot noise in PSK Y-00 cipher.
\[ \Delta \theta_{\text{basis}} = \frac{2\pi}{M \cdot 2^m} \] #(S6)

The PD responsivity \( S \) is calculated as
\[ S = \frac{\eta_q e}{h \nu_0}, \] #(S7)

where \( h, \nu_0, \) and \( \eta_q \) are the Planck constant, signal frequency, and quantum efficiency of the PD, respectively. Subsequently, using Eqs. (S5)–(S7), the quantum-noise masking number is defined as the ratio of \( \Delta \phi_{\text{shot}} \) and \( \Delta \theta_{\text{basis}} \):
\[ \Gamma_Q = \frac{\Delta \phi_{\text{shot}}}{\Delta \theta_{\text{basis}}} = \frac{M \cdot 2^m}{2\pi} \sqrt{\frac{2h \nu_0 B}{\eta_q^2 P_S}} \] #(S8)

2. Symbol error ratio (SER) of detecting PSK Y-00 cipher without a seed key

One can estimate the SER when an eavesdropper performs an ideal heterodyne measurement of the cipher. Only the signal masking by shot noise is considered. Figure S2 shows the model of multilevel phase detection. \( A_i \), \( \Delta_{\text{basis}} \), and \( \sigma_{\text{shot}} \) represent the phase level of the \( i \)th signal, distance between adjacent signals, and standard deviation of shot noise, respectively. The SER of the detection \( P_{\text{SER, eve}} \) is calculated as follows:
\[ P_{\text{SER, eve}} = 1 - \int_{A_i - \Delta_{\text{basis}} / 2}^{A_i + \Delta_{\text{basis}} / 2} \frac{1}{\sqrt{2\pi}\sigma_{\text{shot}}^2} e^{\left( -\frac{(x - A_i)^2}{2\sigma_{\text{shot}}^2} \right)} dx = \text{erfc} \left( \frac{\Delta_{\text{basis}}}{\sqrt{2}\sigma_{\text{shot}}} \right) \] #(S9)

In the model, the quantum-noise masking number \( \Gamma_Q = 2\sigma_{\text{shot}} / \Delta_{\text{basis}} \). Subsequently, Eq. (S9) is expressed as a function of the masking number \( \Gamma_Q \):
\[ P_{\text{SER, eve}} = \text{erfc} \left( \frac{1}{\sqrt{2}\Gamma_Q} \right) \] #(S10)

![Fig. S2. Model of multilevel phase detection limited by shot noise.](image)

3. Relation between bit error ratio (BER) \( P_{\text{BER}} \) and signal-to-noise ratio per bit \( E_b/N_0 \)

When data modulation is quadrature phase shift keying \((M = 4)\), a BER \( P_{\text{BER}} \) is obtained from a signal-to-noise ratio per bit \( E_b/N_0 \) as follows:
\[ P_{\text{BER}} = \frac{1}{2} \text{erfc} \left( \frac{E_b}{\sqrt{N_0}} \right) \] #(S11)
Using this equation, $E_b/N_0$ is calculated as 2.2 (3.42 dB) for a BER of $1.8 \times 10^{-2}$ which is a typical threshold of soft decision forward error correction (SD-FEC) with an overhead of 20%.