Optical Engineering

OpticalEngineering.SPIEDigitalLibrary.org

Guessing probability under unlimited known-plaintext attack on secret keys for Y00 quantum stream cipher by quantum multiple hypotheses testing

Takehisa Iwakoshi

SPIE.

Takehisa Iwakoshi, "Guessing probability under unlimited known-plaintext attack on secret keys for Y00 quantum stream cipher by quantum multiple hypotheses testing," *Opt. Eng.* **57**(12), 126103 (2018), doi: 10.1117/1.OE.57.12.126103.

Guessing probability under unlimited known-plaintext attack on secret keys for Y00 quantum stream cipher by quantum multiple hypotheses testing

Takehisa Iwakoshi*
Tamagawa University, Quantum ICT Research Institute, Machida, Tokyo, Japan

Abstract. Although quantum key distribution is regarded as promising secure communication, security of Y00 protocol proposed by Yuen in 2000 for the affinity to conventional optical communication is not well-understood yet; its security has been evaluated only by the eavesdropper's error probabilities of detecting individual signals or masking size, the number of hidden signal levels under quantum and classical noise. Our study is the first challenge of evaluating the guessing probabilities on shared secret keys for pseudorandom number generators in a simplified Y00 communication system based on quantum multiple hypotheses testing theory. The result is that even unlimitedly long known-plaintext attack only lets the eavesdropper guess the shared secret keys of limited lengths with a probability strictly <1. This study will give some insights for detailed future works on this quantum communication protocol. [DOI: 10.1117/1.OE.57.12.126103]

Keywords: quantum cryptography; secure communications; quantum optics; quantum detection theory.

Paper 181279 received Sep. 4, 2018; accepted for publication Nov. 14, 2018; published online Dec. 10, 2018.

1 Introduction

Recent heating-up in the development race of quantum computers brings attention to secure communications that are resistant to quantum computers. Quantum key distribution (QKD) has been said to be the most promising technology to protect communications from cryptanalysis even with quantum computers.

On the other hand, Y00 protocol proposed by Yuen (its original name is $\alpha\eta$) in 2000[1–3] is compatible to conventional high-speed and long-distance optical communication technologies while it sends messages directly and hides them under quantum noise, enhancing the security of conventional cryptographies.[4–14] However, its security has not been well-understood except some evaluations by unicity distance,[15,16] numerical analyses by masking sizes that are the numbers of signal levels hidden under quantum noise,[17,18] or error probability in eavesdropping on individual signals.[19] Therefore, since fast correlation attack on Y00 protocol was found,[20,21] Y00 protocol has been believed to be computationally secure while QKDs are information-theoretically secure, although "irregular mapping" was equipped on Y00 systems as a countermeasure to fast correlation attack.[22]

This study gives the first example of security analysis on Y00 protocol with an unlimitedly long known-plaintext attack (KPA) by quantum multiple hypotheses testing theory. It shows that Y00 protocol is secure with guessing probabilities on the two shared secret keys of 128 bits strictly <1 even under unlimitedly long KPA. However, as time passes the attack increases the guessing probability, hence fresh keys have to be sent instead of messages before Y00 communication systems are breached. In this case, if the probability distribution of the provided fresh key is uniform, the guessing probability on the key has to be evaluated by ciphertext-only attack (COA). There are still some assumptions in this study, therefore, this study is not rigorous yet. However, it will give a better understanding of the security of Y00 protocol and some insights for detailed future works.

One of the major methods to evaluate information-theoretic security has been calculation of the guessing probability on secret keys since Shannon[23] and in the literature following.[24,25] Therefore, this study follows these concepts as well to evaluate the security of Y00 protocol.

2 Known Works on Security Evaluations on Information-Theoretic Secure Cryptography

The founder of the information theory, Shannon proved that the "perfect secrecy" is satisfied only when the length of the encryption key $\boldsymbol{k}$ with its probability distribution independent and identically distributed has to be longer than the plaintext $\boldsymbol{x}$, which is one-time pad.[23] Then the ciphertext string $\boldsymbol{c}$ is given by the modulo-2 addition of $\boldsymbol{x}$ and $\boldsymbol{k}$:

$$\boldsymbol{x}+\boldsymbol{k}=\boldsymbol{c}(\mathrm{mod}\,2). \tag{1}$$

Therefore,

$$\Pr(\boldsymbol{x}|\boldsymbol{c})=\Pr(\boldsymbol{x}). \tag{2}$$

Alimomeni and Safavi-Naini[24] proposed "guessing secrecy," generalizing Shannon's concept; the encryption is not perfectly secure, but the key is obtained only probabilistically by Eve's guess as

$$\sum_{\boldsymbol{c}\in\boldsymbol{C}}\Pr(\boldsymbol{c})\max_{\boldsymbol{x}\in\boldsymbol{X}}\Pr(\boldsymbol{x}|\boldsymbol{c})=\max_{\boldsymbol{x}\in\boldsymbol{X}}\Pr(\boldsymbol{x}). \tag{3}$$

Iwamoto and Shikata[25] proposed "worst-case guessing secrecy," considering the worst scenario such as

$$\max_{(\boldsymbol{x},\boldsymbol{c})\in(\boldsymbol{X},\boldsymbol{C})}\Pr(\boldsymbol{x}|\boldsymbol{c})=\max_{\boldsymbol{x}\in\boldsymbol{X}}\Pr(\boldsymbol{x}). \tag{4}$$

*Address all correspondence to Takehisa Iwakoshi, E-mail: t.iwakoshi@lab.tamagawa.ac.jp

Therefore, this study follows the above concepts "guessing probability on the key" to evaluate the security of Y00 protocol.

3 Security of Conventional Stream Ciphers Under Long Known-Plaintext Attack

This section treats the security of conventional stream ciphers with KPA; those are not randomized by quantum noise to give a better understanding on the security of Y00 protocol, which is a stream cipher randomized by quantum noise. In conventional stream ciphers, a shared secret key $\boldsymbol{k}$ is fed into the pseudorandom number generator (PRNG) to generate a key stream $\boldsymbol{s}$. A plaintext string $\boldsymbol{x}$ from a sender, Alice, is converted into a ciphertext string $\boldsymbol{c} = \boldsymbol{x} + \boldsymbol{s} \bmod 2$. To decode $\boldsymbol{c}$, the receiver, Bob, feeds the shared $\boldsymbol{k}$ into his common PRNG, then recovers $\boldsymbol{x} = \boldsymbol{c} + \boldsymbol{s} \bmod 2$. If Eve has the same PRNG and knows $\boldsymbol{x}$ during a period of $\boldsymbol{s}$, she obtains $\boldsymbol{s}$ completely, hence her correspondence table of $\boldsymbol{k} \leftrightarrow \boldsymbol{s}$ recovers the original key $\boldsymbol{k}$ no matter how much computationally complex the key expansion process is. Then Eve can read all messages from the next period. In terms of conditional probability, this means

$$\Pr(\boldsymbol{s}|\boldsymbol{c},\boldsymbol{x}) = \Pr(\boldsymbol{k}|\boldsymbol{c},\boldsymbol{x}) = 1. \tag{5}$$

4 Security of Y00 protocol Under KPA During Least Common Multiple of PRNGs' Periods

This section describes the security of Y00 protocol with KPA during the least common multiple (LCM) of the two PRNGs' periods using quantum multiple hypotheses testing theory.[26,27]

4.1 *Principles of Binary Y00 Quantum Stream Cipher*

To start Y00 protocol, the legitimate users Alice and Bob have to share a secret key $\boldsymbol{k}$. Then they expand $\boldsymbol{k}$ into a key stream $\boldsymbol{s}$ using a common PRNG equipped in each transmitter/receiver. Then $\boldsymbol{s}$ is chopped every $\log_2 M$ bits to form M-ary string $\boldsymbol{s}(t)$ of times lot t while a message bit $x(t)$ is encoded into a coherent state $|\alpha[m(t)]\rangle$ using $\boldsymbol{s}(t)$ as

$$m(t) \coloneqq \mathrm{Map}[\boldsymbol{s}(t)] + M\{\mathrm{Map}[\boldsymbol{s}(t)] + x(t) \bmod 2\}. \tag{6}$$

$\mathrm{Map}[\boldsymbol{s}(t)]$ is a projection from $\boldsymbol{s}(t)$ to $\mathrm{Map}[\boldsymbol{s}(t)] \in \{0,1,2,3,\ldots,M-1\}$. Therefore, the message bit $x(t) \in \{0,1\}$ corresponds to a set of quantum states $\{|\alpha[m(t)]\rangle, |\alpha[m(t)+M]\rangle\}$ for even number $\mathrm{Map}[\boldsymbol{s}(t)]$, otherwise $\{|\alpha[m(t)+M]\rangle, |\alpha[m(t)]\rangle\}$. On the other hand, Bob's receiver sets an optimal threshold(s) to discriminate the set of quantum states. Therefore, he decodes $x(t)$ since he knows $\mathrm{Map}[\boldsymbol{s}(t)]$ thanks to the common PRNG and the shared $\boldsymbol{k}$. On the other hand, the eavesdropper, Eve, has to discriminate $2M$-ary signals hidden under overlapping quantum and classical noise since she does not know whether $\mathrm{Map}[\boldsymbol{s}(t)]$ is even or odd, hence $x(t)$ neither.

When Eve launches KPA, a number of the hidden signal level under noise effectively halves, hence it might help Eve to guess $\boldsymbol{k}$.

To avoid the situation, overlap-selection-keying was proposed.[28] An additional pair of PRNGs with another shared key $\Delta\boldsymbol{k}$ are equipped in both a transmitter and a receiver to randomize the plaintext $\boldsymbol{x}$ with pseudorandom number $\Delta\boldsymbol{x}$ as

$$m(t) \coloneqq \mathrm{Map}[\boldsymbol{s}(t)] + M\{\mathrm{Map}[\boldsymbol{s}(t)] + x(t) + \Delta x(t) \bmod 2\}. \tag{7}$$

Then the transmitter Alice sends a coherent state $\rho[m(t)]$ with classical randomizations named DSR and DER[19] although these are omitted in this study for simplicity.

Eve obtains coherent states separated from a beam-splitter $\rho'[m(t)]$ and stores its time sequence in her quantum memory. Denote the quantum sequence $\rho'(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x})$ with the splitting ratio η as

$$\begin{aligned}\rho'(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x}) &\coloneqq |\eta\alpha(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x})\rangle\langle\eta\alpha(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x})| \\ &= \otimes_{t=0}^{T-1} |\eta\alpha[m(t)]\rangle\langle\eta\alpha[m(t)]|.\end{aligned} \tag{8}$$

Note that a set of $(\boldsymbol{s},\Delta\boldsymbol{x}) \in (\boldsymbol{S},\Delta\boldsymbol{X})$ is generated from $(\boldsymbol{k},\Delta\boldsymbol{k}) \in (\boldsymbol{K},\Delta\boldsymbol{K})$. Therefore, there are only $2^{|\boldsymbol{K}|+|\Delta\boldsymbol{K}|}$ patterns of signal sequences, although the number of signal levels is $2M$ and the period of KPA is T. Hence, what Eve needs is not $2M \cdot T$-ary quantum decision theory but $2^{|\boldsymbol{K}|+|\Delta\boldsymbol{K}|}$-ary one, no matter how long the key-stream lengths of $\boldsymbol{s}$ and $\Delta\boldsymbol{x}$ are. Therefore, the main problem is whether Eve can determine the correct $(\boldsymbol{s},\Delta\boldsymbol{x})$ in the LCM of the periods of $(\boldsymbol{s},\Delta\boldsymbol{x})$ denoted as T_{LCM}, like in case of the conventional stream cipher explained in Sec. 3 or she needs longer than T_{LCM}.

4.2 *Brief Description of M-ary Quantum Detection Theory*

Before this section starts, here are some assumptions to be satisfied.

- The projection $\mathrm{Map}[\cdot]$ stays unchanged during the running of Y00 protocol.
- $\mathrm{Map}[\cdot]$ is known to Eve according to the Kerckhoffs' principle, as known as Shannon's maxim.
- $\mathrm{Map}[\cdot]$ is well-designed irregular mapping so that quantum noise covers all bits in $\boldsymbol{s}(t)$ equally.

The set of Eve's measurement operators $\{E(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x})\}$ satisfies

$$\sum_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})} E(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}) = I. \tag{9}$$

By the Born rule, the measurement operator $E(\boldsymbol{s}',\Delta\boldsymbol{x}'|\boldsymbol{x})$ gives Eve a measurement result $(\boldsymbol{s}',\Delta\boldsymbol{x}') \in (\boldsymbol{S},\Delta\boldsymbol{X})$ from a quantum state $\rho'(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x})$ with a probability of

$$\mathrm{tr}[E(\boldsymbol{s}',\Delta\boldsymbol{x}'|\boldsymbol{x})\rho'(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x})] = \Pr(\boldsymbol{s}',\Delta\boldsymbol{x}'|\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x}). \tag{10}$$

Quantum multiple hypotheses testing theory based on the Bayes criterion is applicable to decide which $(\boldsymbol{s}',\Delta\boldsymbol{x}')$ is the most possible. Let the Bayes cost in the theory be as described in

$$C(\boldsymbol{s},\Delta\boldsymbol{x},\boldsymbol{s}',\Delta\boldsymbol{x}'|\boldsymbol{x}) \coloneqq -\delta_{\boldsymbol{s},\boldsymbol{s}'}\delta_{\Delta\boldsymbol{x},\Delta\boldsymbol{x}'}. \tag{11}$$

When the prior probability is $\Pr(\boldsymbol{s}, \Delta\boldsymbol{x})$, the average Bayes cost is

$$\mathrm{Ex}[C] = -\sum_{(\boldsymbol{s},\Delta\boldsymbol{x}),(\boldsymbol{s}',\Delta\boldsymbol{x}')\in(\boldsymbol{S},\Delta\boldsymbol{X})} \Pr(\boldsymbol{s}, \Delta\boldsymbol{x})\delta_{\boldsymbol{s},\boldsymbol{s}'}\delta_{\Delta\boldsymbol{x},\Delta\boldsymbol{x}'} \times \mathrm{tr}[\rho'(\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x})E(\boldsymbol{s}', \Delta\boldsymbol{x}'|\boldsymbol{x})]. \tag{12}$$

The Hermitian risk operators are

$$\begin{aligned} W(\boldsymbol{x},\boldsymbol{s}',\Delta\boldsymbol{x}') &:= \sum_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})} \Pr(\boldsymbol{s},\Delta\boldsymbol{x})(-\delta_{\boldsymbol{s},\boldsymbol{s}'}\delta_{\Delta\boldsymbol{x},\Delta\boldsymbol{x}'})\rho'(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x}). \\ &= -\Pr(\boldsymbol{s}',\Delta\boldsymbol{x}')\rho'(\boldsymbol{x},\boldsymbol{s}',\Delta\boldsymbol{x}') \\ &= -\Pr(\boldsymbol{s}',\Delta\boldsymbol{x}')|\eta\alpha(\boldsymbol{x},\boldsymbol{s}',\Delta\boldsymbol{x}')\rangle\langle\eta\alpha(\boldsymbol{x},\boldsymbol{s}',\Delta\boldsymbol{x}')|. \end{aligned} \tag{13}$$

To minimize Eve's error probability, the necessary and sufficient conditions are[26]

$$[W(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x}) - \Gamma]E(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}) = E(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x})[W(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x}) - \Gamma] = 0, \tag{14}$$

$$E(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})[W(\boldsymbol{x}, \boldsymbol{s}', \Delta\boldsymbol{x}') - W(\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x})]E(\boldsymbol{s}', \Delta\boldsymbol{x}'|\boldsymbol{x}) = \mathbf{0}, \tag{15}$$

$$W(\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x}) - \Gamma \geq 0, \tag{16}$$

$$\begin{aligned} \Gamma &:= \sum_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})} E(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})W(\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x}) \\ &= \sum_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})} W(\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x})E(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x}). \end{aligned} \tag{17}$$

Then Eve's maximum success probability of obtaining the correct $(\boldsymbol{s}, \Delta\boldsymbol{x})$ is

$$\begin{aligned} \Pr(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x}) &= 1 - (1 + \mathrm{tr}\,\Gamma) = -\mathrm{tr}\,\Gamma \\ &= \sum_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})} \Pr(\boldsymbol{s}, \Delta\boldsymbol{x})\langle\eta\alpha(\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x})| \\ &\quad \cdot\ E(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})|\eta\alpha(\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x})\rangle. \end{aligned} \tag{18}$$

Now, denote $E(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})$ as

$$E(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x}) := |(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})\rangle\langle(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})|. \tag{19}$$

From Eq. (15),

$$\begin{aligned} &\Pr(\boldsymbol{s},\Delta\boldsymbol{x})\langle(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x})|\eta\alpha(\boldsymbol{x},\boldsymbol{s}',\Delta\boldsymbol{x}')\rangle\langle\eta\alpha(\boldsymbol{x},\boldsymbol{s}',\Delta\boldsymbol{x}')|(\boldsymbol{s}',\Delta\boldsymbol{x}'|\boldsymbol{x})\rangle \\ &= \Pr(\boldsymbol{s}',\Delta\boldsymbol{x}')\langle(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x})|\eta\alpha(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x})\rangle\langle\eta\alpha(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x})|(\boldsymbol{s}',\Delta\boldsymbol{x}'|\boldsymbol{x})\rangle. \end{aligned} \tag{20}$$

For pure states, from Eq. (8),

$$\begin{aligned} \langle\eta\alpha(\boldsymbol{x}, \boldsymbol{s}', \Delta\boldsymbol{x}')|\eta\alpha(\boldsymbol{x}, \boldsymbol{s}', \Delta\boldsymbol{x}')\rangle &= 1 \\ &= \sum_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})} |\langle\eta\alpha(\boldsymbol{x}, \boldsymbol{s}', \Delta\boldsymbol{x}')|(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})\rangle|^2. \end{aligned} \tag{21}$$

Therefore, Eq. (20) gives $2^{2|\boldsymbol{K}|+2|\Delta\boldsymbol{K}|} - 2^{|\boldsymbol{K}|+|\Delta\boldsymbol{K}|}$ equalities and Eq. (21) gives $2^{|\boldsymbol{K}|+|\Delta\boldsymbol{K}|}$ equalities. Thus there are $2^{2|\boldsymbol{K}|+2|\Delta\boldsymbol{K}|}$ equations in total, and there are $2^{3|\boldsymbol{K}|+3|\Delta\boldsymbol{K}|}$ variables including $\{\Pr(\boldsymbol{s}, \Delta\boldsymbol{x})\}$.

To remove remained variables $\{\Pr(\boldsymbol{s}, \Delta\boldsymbol{x})\}$, apply Cauchy–Schwarz inequality to Eq. (18):

$$\begin{aligned} -\mathrm{tr}\,\Gamma &= \sum_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})} \Pr(\boldsymbol{s}, \Delta\boldsymbol{x})|\langle\eta\alpha(\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x})|(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})\rangle|^2 \\ &\leq \left[\sum_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})} \Pr\,(\boldsymbol{s}, \Delta\boldsymbol{x})^2\right]^{1/2} \\ &\quad \times \left[\sum_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})} |\langle\eta\alpha(\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x})|(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})\rangle|^4\right]^{1/2}. \end{aligned} \tag{22}$$

Let Eve know the prior probability $\Pr(\boldsymbol{s}, \Delta\boldsymbol{x})$ under Shannon's maxim. Then Eve can choose her $\{E(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})\}$ so that the equality of Eq. (23) is satisfied

$$\Pr(\boldsymbol{s}, \Delta\boldsymbol{x}) = \frac{|\langle\eta\alpha(\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x})|(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})\rangle|^2}{\sum_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})} |\langle\eta\alpha(\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x})|(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})\rangle|^2}. \tag{23}$$

Therefore, the prior probability distribution $\{\Pr(\boldsymbol{s}, \Delta\boldsymbol{x})\}$ vanishes as follows:

$$\max[-\mathrm{tr}\,\Gamma] = \frac{\sum_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})} |\langle\eta\alpha(\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x})|(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})\rangle|^4}{\sum\limits_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})} |\langle\eta\alpha(\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x})|(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})\rangle|^2}. \tag{24}$$

The condition Eq. (23) satisfies Eq. (14) trivially, and Eqs. (15) and (16) are converted as follows:

$$\begin{aligned} &|\langle\eta\alpha(\boldsymbol{x}, \boldsymbol{s}', \Delta\boldsymbol{x}')|(\boldsymbol{s}', \Delta\boldsymbol{x}'|\boldsymbol{x})\rangle|^2\langle(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})|\eta\alpha(\boldsymbol{x}, \boldsymbol{s}', \Delta\boldsymbol{x}')\rangle \\ &\quad \times \langle\eta\alpha(\boldsymbol{x}, \boldsymbol{s}', \Delta\boldsymbol{x}')|(\boldsymbol{s}', \Delta\boldsymbol{x}'|\boldsymbol{x})\rangle \\ &= |\langle\eta\alpha(\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x})|(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})\rangle|^2\langle(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})|\eta\alpha(\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x})\rangle \\ &\quad \times \langle\eta\alpha(\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x})|(\boldsymbol{s}', \Delta\boldsymbol{x}'|\boldsymbol{x})\rangle. \end{aligned} \tag{25}$$

$$\begin{aligned} &\langle(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})|[W(\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x}) - \Gamma]|(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})\rangle \\ &\quad \times \sum_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})} |\langle\eta\alpha(\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x})|(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})\rangle|^2 \\ &\quad = -|\langle\eta\alpha(\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x})|(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})\rangle|^4 \\ &\quad + \sum_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})} |\langle\eta\alpha(\boldsymbol{x}, \boldsymbol{s}, \Delta\boldsymbol{x})|(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x})\rangle|^4 \geq 0. \end{aligned} \tag{26}$$

Therefore, Eq. (26) originated from Eq. (16) is also satisfied while a new condition is Eq. (25). The absolute value of Eq. (25) is

$$\begin{aligned}&|\langle\eta\alpha(\boldsymbol{x},\boldsymbol{s}',\Delta\boldsymbol{x}')|(\boldsymbol{s}',\Delta\boldsymbol{x}'|\boldsymbol{x})\rangle|^4|\langle(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x})|\eta\alpha(\boldsymbol{x},\boldsymbol{s}',\Delta\boldsymbol{x}')\rangle|^2\\&\quad=|\langle\eta\alpha(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x})|(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x})\rangle|^4|\langle(\boldsymbol{s}',\Delta\boldsymbol{x}'|\boldsymbol{x})|\eta\alpha(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x})\rangle|^2.\end{aligned}\tag{27}$$

4.3 *Security of Y00 under KPA on Secret Key: In Case of Exact Signal Detections for Eve*

Although it is impossible for Eve to obtain the correct signal sequence without any errors because of quantum noise in Y00 protocol, it is worth considering an imaginary case where Eve could detect signals without any errors to compare Y00 protocol with conventional stream ciphers in Sec. 3.

The situation where Eve could detect signals without any errors is that, from the Born rule,

$$|\langle(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x})|\eta\alpha(\boldsymbol{x},\boldsymbol{s}'\neq\boldsymbol{s},\Delta\boldsymbol{x}'\neq\Delta\boldsymbol{x})\rangle|^2=0.\tag{28}$$

Equation (28) also implies from Eq. (21) that

$$\begin{aligned}&\langle\eta\alpha(\boldsymbol{x},\boldsymbol{s}',\Delta\boldsymbol{x}')|\eta\alpha(\boldsymbol{x},\boldsymbol{s}',\Delta\boldsymbol{x}')\rangle=1\\&\quad=|\langle\eta\alpha(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x})|(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x})\rangle|^2.\end{aligned}\tag{29}$$

Then from the left-hand side of Eq. (22),

$$-\mathrm{tr}\,\Gamma=\sum_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})}\Pr(\boldsymbol{s},\Delta\boldsymbol{x})|\langle\eta\alpha(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x})|(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x})\rangle|^2=1.\tag{30}$$

Therefore, through one period of $(\boldsymbol{s},\Delta\boldsymbol{x})$, that is T_{LCM}, Eve would obtain the correct $(\boldsymbol{s},\Delta\boldsymbol{x})$ with a probability of 1. Then the situation is the same as conventional stream ciphers. Therefore, the effect of unavoidable quantum noise in Eq. (28) as a nonzero factor should play an important role in Y00 protocol.

4.4 *Security of Y00 under KPA on Secret Key: In Case of Erroneous Signal Detections for Eve*

Unless Eve's detections are error-free expressed by Eq. (28), from Eq. (21),

$$|\langle\eta\alpha(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x})|(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x})\rangle|^2<1.\tag{31}$$

Therefore, Eq. (24) satisfies the following inequality as well:

$$\max[-\mathrm{tr}\,\Gamma]=\frac{\sum_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})}|\langle\eta\alpha(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x})|(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x})\rangle|^4}{\sum\limits_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})}|\langle\eta\alpha(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x})|(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x})\rangle|^2}<1.\tag{32}$$

Even if $\Pr(\boldsymbol{s},\Delta\boldsymbol{x})$ is uniform, that is $\Pr(\boldsymbol{s},\Delta\boldsymbol{x})=2^{-|\boldsymbol{K}|-|\Delta\boldsymbol{K}|}$, since Eve has to make the success probability in measurement larger than the failure probability,

$$|\langle\eta\alpha(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x})|(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x})\rangle|^2\geq|\langle\eta\alpha(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x})|(\boldsymbol{s}',\Delta\boldsymbol{x}'|\boldsymbol{x})\rangle|^2.\tag{33}$$

Then from Eqs. (21) and (22),

$$\begin{aligned}-\mathrm{tr}\,\Gamma&=\sum_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})}\Pr(\boldsymbol{s},\Delta\boldsymbol{x})|\langle\eta\alpha(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x})|(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x})\rangle|^2\\&=2^{-|\boldsymbol{K}|-|\Delta\boldsymbol{K}|}\sum_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})}|\langle\eta\alpha(\boldsymbol{x},\boldsymbol{s},\Delta\boldsymbol{x})|(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x})\rangle|^2\\&\geq2^{-|\boldsymbol{K}|-|\Delta\boldsymbol{K}|}.\end{aligned}\tag{34}$$

Therefore, Eve has an advantage in obtaining the correct $(\boldsymbol{s},\Delta\boldsymbol{x})$ compared to pure-guessing. Thus even Eve launches KPA using quantum multiple hypotheses testing theory during an LCM of the periods of two PRNGs; she cannot pin down the keys deterministically, far different from conventional stream ciphers. The problem is how long Y00 protocol stays secure.

5 Security of Y00 Protocol under Unlimitedly Long KPA

This section describes the security of Y00 protocol under unlimitedly long KPA so that Eve guesses the most likely by the Bayes criterion.[29]

5.1 *Y00 Protocol Under Unlimitedly Long KPA*

Since $(\boldsymbol{s},\Delta\boldsymbol{x})$ is pseudorandom of a period of T_{LCM} while the plaintext $\boldsymbol{x}$ is supposed not to repeat, Eve can statistically confirm the most likely $(\boldsymbol{s},\Delta\boldsymbol{x})$ during $N\cdot T_{\mathrm{LCM}}$ periods as shown in Table 1.

At the n'th period of $n\in\{1,2,3,\dots,N\}$, Eve measures coherent states $|\eta\alpha(\boldsymbol{x}_n,\boldsymbol{s},\Delta\boldsymbol{x})\rangle$ with a set of operators denoted as $\{E(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_n)\}$ based on known plaintext $\boldsymbol{x}_n$:

$$\begin{aligned}&[W(\boldsymbol{x}_n,\boldsymbol{s},\Delta\boldsymbol{x})-\Gamma]E(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_n)\\&\quad=E(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_n)[W(\boldsymbol{x}_n,\boldsymbol{s},\Delta\boldsymbol{x})-\Gamma]=0,\end{aligned}\tag{35}$$

Table 1 A timetable of a set of variables (m, s, Δx, and x).

t	0	1	…	$T_{\mathrm{LCM}}-1$	T_{LCM}	…	$2T_{\mathrm{LCM}}-1$	$2T_{\mathrm{LCM}}$	…	$3T_{\mathrm{LCM}}-1$	$3T_{\mathrm{LCM}}$	…
$\boldsymbol{m}$	$m(0)$	$m(1)$	…	$m(T_{\mathrm{LCM}}-1)$	$m(T_{\mathrm{LCM}})$	…	$m(2T_{\mathrm{LCM}}-1)$	$m(2T_{\mathrm{LCM}})$	…	$m(3T_{\mathrm{LCM}}-1)$	$m(3T_{\mathrm{LCM}})$	…
$\boldsymbol{s}$	$\boldsymbol{s}(0)$	$\boldsymbol{s}(1)$	…	$\boldsymbol{s}(T_{\mathrm{LCM}}-1)$	$\boldsymbol{s}(0)$	…	$\boldsymbol{s}(T_{\mathrm{LCM}}-1)$	$\boldsymbol{s}(0)$	…	$\boldsymbol{s}(T_{\mathrm{LCM}}-1)$	$\boldsymbol{s}(0)$	…
$\Delta\boldsymbol{x}$	$\Delta x(0)$	$\Delta x(1)$	…	$\Delta x(T_{\mathrm{LCM}}-1)$	$\Delta x(0)$	…	$\Delta x(T_{\mathrm{LCM}}-1)$	$\Delta x(0)$	…	$\Delta x(T_{\mathrm{LCM}}-1)$	$\Delta x(0)$	…
$\boldsymbol{x}$	$x(0)$	$x(1)$	…	$x(T_{\mathrm{LCM}}-1)$	$x(T_{\mathrm{LCM}})$	…	$x(2T_{\mathrm{LCM}}-1)$	$x(2T_{\mathrm{LCM}})$	…	$x(3T_{\mathrm{LCM}}-1)$	$x(3T_{\mathrm{LCM}})$	…

$$E(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_n)[W(\boldsymbol{x}_n,\boldsymbol{s}',\Delta\boldsymbol{x}')-W(\boldsymbol{x}_n,\boldsymbol{s},\Delta\boldsymbol{x})]E(\boldsymbol{s}',\Delta\boldsymbol{x}'|\boldsymbol{x}_n)=\boldsymbol{0}, \tag{36}$$

$$W(\boldsymbol{x}_n,\boldsymbol{s},\Delta\boldsymbol{x})-\Gamma_n\geq 0, \tag{37}$$

$$\begin{aligned}\Gamma_n &:= \sum_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})} E(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_n)W(\boldsymbol{x}_n,\boldsymbol{s},\Delta\boldsymbol{x}) \\ &= \sum_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})} W(\boldsymbol{x}_n,\boldsymbol{s},\Delta\boldsymbol{x})E(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_n).\end{aligned} \tag{38}$$

Since Eve just performs $2^{|\boldsymbol{K}|+|\Delta\boldsymbol{K}|}$-ary quantum hypotheses testing to obtain $(\boldsymbol{s},\Delta\boldsymbol{x})$ based on known $\boldsymbol{x}_n$, the results are independent of n. Therefore, from the Born rule, define as follows:

$$|\langle(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_n)|\eta\alpha(\boldsymbol{x}_n,\boldsymbol{s}',\Delta\boldsymbol{x}')\rangle|^2 := \Pr(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_0,\boldsymbol{s}',\Delta\boldsymbol{x}'), \tag{39}$$

$$\Gamma_0 := \Gamma_n. \tag{40}$$

Suppose that Eve has obtained $n(\boldsymbol{s},\Delta\boldsymbol{x})$ times of her measurement result $(\boldsymbol{s},\Delta\boldsymbol{x})$ during $N\cdot T_{\mathrm{LCM}}$ periods, then such a probability is

$$\begin{aligned}\Pr(n(\boldsymbol{s},\Delta\boldsymbol{x})|\boldsymbol{x}_0,\boldsymbol{s},\Delta\boldsymbol{x}) &:= {}_N C_{n(\boldsymbol{s},\Delta\boldsymbol{x})} \Pr(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_0,\boldsymbol{s},\Delta\boldsymbol{x})^{n(\boldsymbol{s},\Delta\boldsymbol{x})} \\ &\times[1-\Pr(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_0,\boldsymbol{s},\Delta\boldsymbol{x})]^{N-n(\boldsymbol{s},\Delta\boldsymbol{x})}.\end{aligned} \tag{41}$$

At the boundary where Eve makes a wrong decision, the Bayes criterion requests,

$$\Pr(\boldsymbol{s},\Delta\boldsymbol{x})\Pr(n_{\mathrm{Th}}|\boldsymbol{x}_0,\boldsymbol{s},\Delta\boldsymbol{x}) = \Pr(\boldsymbol{s}',\Delta\boldsymbol{x}')\Pr(n_{\mathrm{Th}}|\boldsymbol{x}_0,\boldsymbol{s}',\Delta\boldsymbol{x}'). \tag{42}$$

Two nearest probability distributions give the following boundary conditions:

$$\begin{aligned}\Pr(n_{\mathrm{Th}}|\boldsymbol{x}_0,\boldsymbol{s},\Delta\boldsymbol{x}) &= {}_N C_{n_{\mathrm{Th}}} \Pr(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_0,\boldsymbol{s},\Delta\boldsymbol{x})^{n_{\mathrm{Th}}} \\ &\times[1-\Pr(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_0,\boldsymbol{s},\Delta\boldsymbol{x})]^{N-n_{\mathrm{Th}}},\end{aligned} \tag{43}$$

$$\begin{aligned}\Pr(n_{\mathrm{Th}}|\boldsymbol{x}_0,\boldsymbol{s}',\Delta\boldsymbol{x}') &= {}_N C_{n_{\mathrm{Th}}} \Pr(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_0,\boldsymbol{s}',\Delta\boldsymbol{x}')^{n_{\mathrm{Th}}} \\ &\times[1-\Pr(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_0,\boldsymbol{s}',\Delta\boldsymbol{x}')]^{N-n_{\mathrm{Th}}}.\end{aligned} \tag{44}$$

Substituting Eqs. (43) and (44) into Eq. (42), n_{Th} is given in

$$\begin{aligned}&\log_2\frac{\Pr(\boldsymbol{s},\Delta\boldsymbol{x})\Pr(n_{\mathrm{Th}}|\boldsymbol{x}_0,\boldsymbol{s},\Delta\boldsymbol{x})}{\Pr(\boldsymbol{s}',\Delta\boldsymbol{x}')\Pr(n_{\mathrm{Th}}|\boldsymbol{x}_0,\boldsymbol{s}',\Delta\boldsymbol{x}')}=0 \\ &\quad=\log_2\frac{\Pr(\boldsymbol{s},\Delta\boldsymbol{x})}{\Pr(\boldsymbol{s}',\Delta\boldsymbol{x}')}+n_{\mathrm{Th}}\log_2\frac{\Pr(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_0,\boldsymbol{s},\Delta\boldsymbol{x})}{\Pr(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_0,\boldsymbol{s}',\Delta\boldsymbol{x}')} \\ &\qquad+(N-n_{\mathrm{Th}})\log_2\frac{1-\Pr(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_0,\boldsymbol{s},\Delta\boldsymbol{x})}{1-\Pr(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_0,\boldsymbol{s}',\Delta\boldsymbol{x}')},\end{aligned} \tag{45}$$

$$n_{\mathrm{Th}}=\frac{N\log_2\frac{1-\Pr(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_0,\boldsymbol{s}',\Delta\boldsymbol{x}')}{1-\Pr(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_0,\boldsymbol{s},\Delta\boldsymbol{x})}+\log_2\frac{\Pr(\boldsymbol{s}',\Delta\boldsymbol{x}')}{\Pr(\boldsymbol{s},\Delta\boldsymbol{x})}}{\log_2\frac{\Pr(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_0,\boldsymbol{s},\Delta\boldsymbol{x})[1-\Pr(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_0,\boldsymbol{s}',\Delta\boldsymbol{x}')]}{\Pr(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_0,\boldsymbol{s}',\Delta\boldsymbol{x}')[1-\Pr(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_0,\boldsymbol{s},\Delta\boldsymbol{x})]}}. \tag{46}$$

This situation is depicted in Fig. 1.

There are $2^{|\boldsymbol{K}|+|\Delta\boldsymbol{K}|}$ patterns of possible probability distributions, and only one is for the correct $(\boldsymbol{s},\Delta\boldsymbol{x})$. Therefore, maximizing n_{Th} by all wrong sets of $(\boldsymbol{s}',\Delta\boldsymbol{x}')$ and defining it as max n_{Th},

$$\begin{aligned}\Pr(\mathrm{fail}) &= \sum_{n(\boldsymbol{s},\Delta\boldsymbol{x})=0}^{\max n_{\mathrm{Th}}} {}_N C_{n(\boldsymbol{s},\Delta\boldsymbol{x})} \Pr(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_0,\boldsymbol{s},\Delta\boldsymbol{x})^{n(\boldsymbol{s},\Delta\boldsymbol{x})} \\ &\times[1-\Pr(\boldsymbol{s},\Delta\boldsymbol{x}|\boldsymbol{x}_0,\boldsymbol{s},\Delta\boldsymbol{x})]^{N-n(\boldsymbol{s},\Delta\boldsymbol{x})}.\end{aligned} \tag{47}$$

Thus Eve's success probability in obtaining the correct $(\boldsymbol{s},\Delta\boldsymbol{x})$ corresponding to the shared secret keys $(\boldsymbol{k},\Delta\boldsymbol{k})$ in the Y00 system is Pr(success) = 1–Pr(fail).

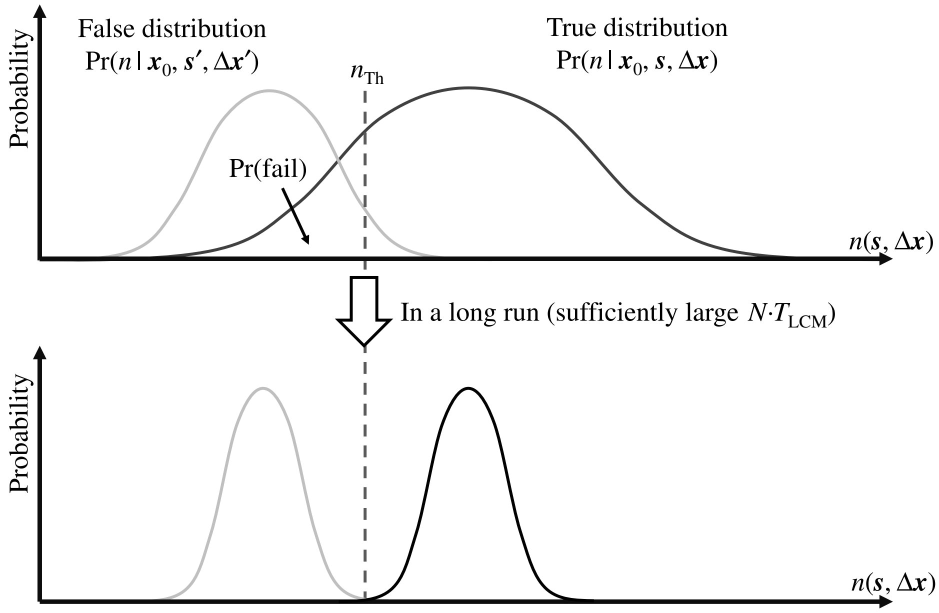
False distribution
$\Pr(n\,|\,\boldsymbol{x}_0,\boldsymbol{s}',\Delta\boldsymbol{x}')$
True distribution
$\Pr(n\,|\,\boldsymbol{x}_0,\boldsymbol{s},\Delta\boldsymbol{x})$
n_{Th}
Probability
Pr(fail)
$n(\boldsymbol{s},\Delta\boldsymbol{x})$
In a long run (sufficiently large $N{\cdot}T_{\mathrm{LCM}}$)
Probability
$n(\boldsymbol{s},\Delta\boldsymbol{x})$

Fig. 1 Schematic view of how the security of Y00 system is evaluated by Eve's failure probability.

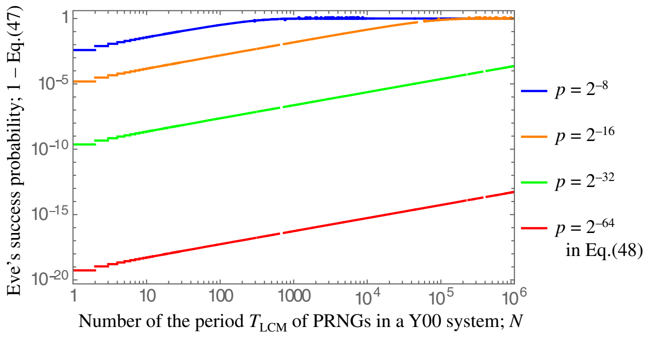

Fig. 2 Eve's success probability in guessing the correct keys in the long run. From the top, $p = 2^{-8}$, $p = 2^{-16}$, $p = 2^{-32}$, and $p = 2^{-64}$ in Eqs. (48)–(50).

To perform numerical simulation, all conditional probabilities $\{\Pr(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x}_0, \boldsymbol{s}', \Delta\boldsymbol{x}')\}$ defined in Eq. (39) have to be determined. However, those parameters are dependent on implementations of Y00 systems including key-expansion algorithms. Therefore, this study gives numerical examples as follows. Assume initial key lengths are $|\boldsymbol{K}| = |\Delta\boldsymbol{K}| = 128$ bits and

$$\Pr(\boldsymbol{s}, \Delta\boldsymbol{x}|\boldsymbol{x}_0, \boldsymbol{s}, \Delta\boldsymbol{x}) = \Pr(\boldsymbol{x}', \Delta\boldsymbol{x}'|\boldsymbol{x}_0, \boldsymbol{x}', \Delta\boldsymbol{x}') \coloneqq p, \tag{48}$$

$$\begin{aligned}&\Pr({}^{\forall}\boldsymbol{s}' \neq \boldsymbol{s}, {}^{\forall}\Delta\boldsymbol{x}' \neq \Delta\boldsymbol{x}|\boldsymbol{x}_0, \boldsymbol{s}, \Delta\boldsymbol{x})\\ &\quad = \Pr({}^{\forall}\boldsymbol{s} \neq \boldsymbol{s}', {}^{\forall}\Delta\boldsymbol{x} \neq \Delta\boldsymbol{x}'|\boldsymbol{x}_0, \boldsymbol{s}', \Delta\boldsymbol{x}')\\ &\quad = (1 - p)/(2^{2\times128} - 1),\end{aligned} \tag{49}$$

$$\Pr({}^{\forall}\boldsymbol{s}, {}^{\forall}\Delta) = 2^{-2\times128}. \tag{50}$$

The numerical simulation result with the above situation is shown in Fig. 2.

As Eve's success probability of obtaining the correct $(\boldsymbol{s}, \Delta\boldsymbol{x})$ in one T_{LCM} smaller, Eve needs a larger number of N, which is a repetition number of the period T_{LCM} of the two PRNGs. However, note that even with $p = 2^{-16}$, Eve needs $N = 10^4$ periods to pin-down the correct $(\boldsymbol{k}, \Delta\boldsymbol{k})$ with a probability of almost 1. When $p = 2^{-64}$, even $N = 10^6$ periods are not enough for Eve, only allowing her to guess the correct $(\boldsymbol{k}, \Delta\boldsymbol{k})$ with a probability of about 10^{-13}. Therefore, it was shown that Y00 protocol can go beyond the Shannon Limit of cryptography.[30]

While Eve's success probability is small enough, Alice has to send fresh keys to Bob to continue secure quantum communications. In this case, Eve's probability of obtaining the fresh keys has to be evaluated by COA with probabilistically known $(\boldsymbol{k}, \Delta\boldsymbol{k})$, that is,

$$\Pr(\boldsymbol{k}_{\mathrm{new}}, \Delta\boldsymbol{k}_{\mathrm{new}}) = \sum_{(\boldsymbol{s},\Delta\boldsymbol{x})\in(\boldsymbol{S},\Delta\boldsymbol{X})} \Pr(\boldsymbol{s}, \Delta\boldsymbol{x}) \Pr(\boldsymbol{k}_{\mathrm{new}}, \Delta\boldsymbol{k}_{\mathrm{new}}|\boldsymbol{s}, \Delta\boldsymbol{x}). \tag{51}$$

6 Results and Discussions: Assumptions Used in Security Analysis and Future Works

In this work, it was shown that even a Y00 system with a few-hundred bits of shared keys can be secure far longer than the period of its PRNGs, such as 10^6 periods if its implementations are well-designed. The security analyses in this study applied the following assumptions.

1. Irregular mapping[3] makes quantum noise cover all bits in the chopped key stream equally.
2. Irregular mapping is fixed and known to Eve during her eavesdropping.

Hence, there are still necessities of further studies to give mathematically more rigorous analyses when the above assumptions are not satisfied. Also, the security of fresh keys is not given in this study yet. Hence, it has to be analyzed in the next work.

7 Appendix A: Simulation Code for Fig. 2 on Mathematica 11.3

Simulation code for Fig. 2 on Mathematica 11.3

```
ps[p_]: = p;
pf[p_]: = (1 - ps[p])/(2^(128*2)-1);
nth[n_, p_]: = n*Log[2, (1 - pf[p])/(1 - ps[p])]/Log[2, ps[p]
              *(1 - pf[p]) / pf[p] / (1 - ps[p])];
prob[n_,p_]: = 1 - CDF[BinomialDistribution[n, ps[p]],
              Floor[nth[n, p]]];
Show [Table [LogLogPlot [prob [Floor[m], 2^(-b)],
     {m, 1,10^6},
  PlotRange -> {{1, 10^6}, {5*10^(-21), 4}}, Frame ->
    True,
  PlotLegends -> {Switch[b, 8, "p=2-8", 16, "p=2-16", 32,
    "p=2-32", 64, "p=2-64"]},
  PlotStyle->{Switch[b, 8, Blue, 16, Orange, 32, Green,
    64, Red]}], {b, {8, 16, 32, 64}}]]
```

References

1. H. P. Yuen, "KCQ: a new approach to quantum cryptography I. General principles and key generation," arXiv:quant-ph/0311061 (2003).
2. G. A. Barbosa et al., "Secure communication using mesoscopic coherent states," *Phys. Rev. Lett.* **90**(22), 227901 (2003).
3. H. P. Yuen, "Key generation: foundations and a new quantum approach," *IEEE J. Sel. Top. Quantum Electron.* **15**, 1630–1645 (2009).
4. E. Corndorf et al., "Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks," *Phys. Rev. A* **71**, 062326 (2005).
5. C. Liang et al., "Quantum noise protected data encryption in a WDM network," *IEEE Photonic Technol. Lett.* **17**, 1573–1575 (2005).
6. O. Hirota et al., "Quantum stream cipher by the Yuen 2000 protocol: design and experiment by an intensity-modulation scheme," *Phys. Rev. A* **72**, 022335 (2005).
7. Y. Doi et al., "360 km field transmission of 10 Gbit/s stream cipher by quantum noise for optical network," in *Proc. Optical Fiber Communication Conf. (OFC)*, p. OWC4 (2010).
8. K. Harasawa et al., "Quantum encryption communication over a 192-km 2.5-Gbit/s line with optical transceivers employing Yuen-2000 protocol based on intensity modulation," *J. Lightwave Technol.* **29**(3), 316–323 (2011).
9. F. Futami, "Experimental demonstrations of Y-00 cipher for high capacity and secure optical fiber communications," *Quantum Inf. Process.* **13**, 2277–2291 (2014).
10. M. Nakazawa et al., "QAM quantum stream cipher using digital coherent optical transmission," *Opt. Express* **22**, 4098–4107 (2014).
11. M. Yoshida et al., "Single-channel 40 Gbit/s digital coherent QAM quantum noise stream cipher transmission over 480 km," *Opt. Express* **24**, 652–661 (2016).
12. F. Futami et al., "Experimental investigation of security parameters of Y-00 quantum stream cipher transceiver with randomization technique, part I," *Proc. SPIE* **10409**, 104090I (2017).
13. F. Futami et al., "Dynamic routing of Y00 quantum stream cipher in field-deployed dynamic optical path network," in *Optical Fiber Communication Conf.*, Optical Society of America, p. Tu2G-5 (2018).
14. F. Futami et al., "Y-00 quantum stream cipher overlay in a coherent 256-Gbit/s polarization multiplexed 16-QAM WDM system," *Opt. Express* **25**(26), 33338–33349 (2017).

15. R. Nair et al., "Quantum-noise randomized ciphers," *Phys. Rev. A* **74**, 052309 (2006).
16. R. Nair and H. P. Yuen, "Comment on: 'Exposed-key weakness of $\alpha\eta$' [Phys. Lett. A 370 (2007) 131]," *Phys. Lett. A* **372**, 7091–7096 (2008).
17. O. Hirota, "Practical security analysis of a quantum stream cipher by the Yuen 2000 protocol," *Phys. Rev. A* **76**, 032307 (2007).
18. T. Iwakoshi, F. Futami, and O. Hirota, "Quantitative analysis of quantum noise masking in quantum stream cipher by intensity modulation operating at G-bit/sec data rate," *Proc. SPIE* **8189**, 818915 (2011).
19. K. Kato, "Enhancement of quantum noise effect by classical error control codes in the intensity shift keying Y00 quantum stream cipher," *Proc. SPIE* **9225**, 922508 (2014).
20. S. Donnet et al., "Security of Y-00 under heterodyne measurement and fast correlation attack," *Phys. Lett. A* **356**, 406–410 (2006).
21. M. J. Mihaljevic, "Generic framework for the secure Yuen 2000 quantum-encryption protocol employing the wire-tap channel approach," *Phys. Rev. A* **75**, 052334 (2007).
22. T. Shimizu, O. Hirota, and Y. Nagasako, "Running key mapping in a quantum stream cipher by the Yuen 2000 protocol," *Phys. Rev. A* **77**, 034305 (2008).
23. C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.* **28**(4), 656–715 (1949).
24. M. Alimomeni and R. Safavi-Naini, "Guessing secrecy," *Lect. Notes Comput. Sci.* **7412**, 1–13 (2012).
25. M. Iwamoto and J. Shikata, "Information theoretic security for encryption based on conditional Rényi entropies," *Lect. Notes Comput. Sci.* **8317**, 103–121 (2013).
26. C. W. Helstrom, "Quantum detection and estimation theory," *J. Stat. Phys.* **1**(2), 231–252 (1969).
27. H. P. Yuen, R. Kennedy, and M. Lax, "Optimum testing of multiple hypotheses in quantum detection theory," *IEEE Trans. Inf. Theory* **21**(2), 125–134 (1975).
28. O. Hirota et al., "Quantum key distribution with unconditional security for all-optical fiber network," *Proc. SPIE* **5161**, 320–332 (2004).
29. H. L. Van Trees, K. L. Bell, and Z. Tian, *Detection, Estimation, and Modulation Theory, Part I: Detection, Estimation, and Linear Modulation Theory*, 2nd edn., Kindle, John Wiley & Sons, New York (2004).
30. O. Hirota et al., "Getting around the Shannon limit of cryptography," *SPIE Newsroom* (1 September 2010).

Biography of the author is not available.