Received: 30 March 2023 | Revised: 21 June 2023 | Accepted: 24 June 2023

IET Quantum Communication

DOI: 10.1049/qtc2.12064

ORIGINAL RESEARCH

Y00 quantum noise randomised cipher; theoretical and experimental background

Talehisa Iwakoshi

Department of Mechanical Engineering, Hosei University, Koganei, Tokyo, Japan

Correspondence

Talehisa Iwakoshi, Department of Mechanical Engineering, Hosei University, 3-7-2, Kajino-Cho, Koganei, Tokyo, Japan.
Email: takehisa.iwakoshi.33@hosei.ac.jp and t.iwakoshi.ac@gmail.com

Abstract

As past works have shown, information-theoretically secure implementations transmitters of Y00 quantum noise randomised cypher are possible. An advance to the provably secure Y00 protocol by bridging gaps between experimental results and theoretical analyses under so-called quantum collective measurement attacks with known plaintexts is aimed. It would be the strongest attack on the Y00 protocol in the context of quantum key distribution protocols. However, recently proposed security evaluations under the attacks were too abstract to apply to experiments. Therefore, security analyses directly evaluable with the equipped Y00 transmitters under attack are offered. Thus, new security indices are proposed instead of ordinary security measures, such as the bit-error-rate guarantee between optical signals or a masking size. Contrarily, unsolved problems are also listed.

KEYWORDS

cryptography, error statistics, information theory, optical fibre networks, protocols, public key cryptography, quantum communication, quantum information, quantum noise, quantum optics

1 | INTRODUCTION

Since 1984, the first invention of quantum key distribution (QKDs), the so-called BB84 [1, 2], B92 [3], or BBM92 [4], many researchers have been challenging to realise information-theoretically secure (ITS) cryptography using quantum properties.

Around 2000, H. P. Yuen invented a new scheme of the quantum communication protocol [5–11] to satisfy DARPA's requirements using the quantum property of optical communication laser as R. J. Glauber and E. C. G. Sudarshan formulated [12, 13]. Several names nowadays call the protocol: Alpha-Eta, Y00 protocol, Keyed Communication in Quantum noise (KCQ), Quantum Noise Randomized Cipher, and Quantum Noise Stream Cipher. This paper calls it the Y00 protocol to respect the inventor, H. P. Yuen. The protocol enables faster communications and compatibility with the ordinal optical network [6–8, 10], unlike the BB84 and other QKDs.

It looked attractive; however, quantum communication researchers, including QKDs researchers, have yet to be convinced about its security [14–17]. Then, fast-correlation attack (FCA) was proposed to breach the Y00 protocol [18], although the reference offered a countermeasure to turn off this attack. The technique is the so-called 'Irregular Mapping' [19].

Even though the Y00 protocol could be immune to FCAs, notice that FCAs are specific attacks, not general attacks. For example, despite spectacular recent results on the Y00 protocol [20–27], there have still been security analyses [28–34]. Contrarily, some new countermeasures and security indices have been proposed [35]. The situation means that the security of the Y00 protocol has yet to be established. If the Y00 protocol cannot establish ITS, quantum-resistant cryptography is much easier and will widespread because of the ease of use.

Therefore, past works investigated the more general attacks that combine Collective Attacks and Known-Plaintexts attacks to launch key-recovery attacks [36–38] to pave a road to the security proof of the Y00 protocol. Collective attacks are the most general attacks in the context of QKDs [39].

This work aims to bridge the gap between experimental results and the theoretical framework of Collective Attacks

with Known-Plaintext (CKP Attacks) so that experiments can firmly tie up theories.

In this work, Section 2 explains the security of the Y00 protocol as an abstract. Section 3 offers an overview of the security analyses of the Y00 protocol. Section 4 supplies some details of the security analyses. Then, the section describes unsolved problems to step forward to the ITS security proof of the Y00 protocol. Section 5 concludes this work and summarises the contents.

2 | BASICS OF Y00 PROTOCOL AND REQUIREMENTS

Before the paper explains the bridge between the experimental evaluations and theoretical formulations, this section describes the principle of the Y00 protocol, as depicted in Figure 1. Concrete implementations and past works are in [40, 41].

1. The two legitimate transmitters prepare a shared secret key, $\boldsymbol{k}(m)$.
2. They expand the key into pseudo-random stream numbers (PRSNs) $\boldsymbol{s}_{t,n}$.
3. Based on the PRSNs, they modulate laser symbols $\boldsymbol{p}(m(t))$ and thresholds $Th(m(t))$.
4. The thresholds allow the receiver to discriminate the symbols by the thresholds.
5. The transmitters can exchange the plaintext $\boldsymbol{x}(t)$ the symbol represents at time t.
6. The attacker lacking the key cannot set the threshold, facing bit errors by noise.

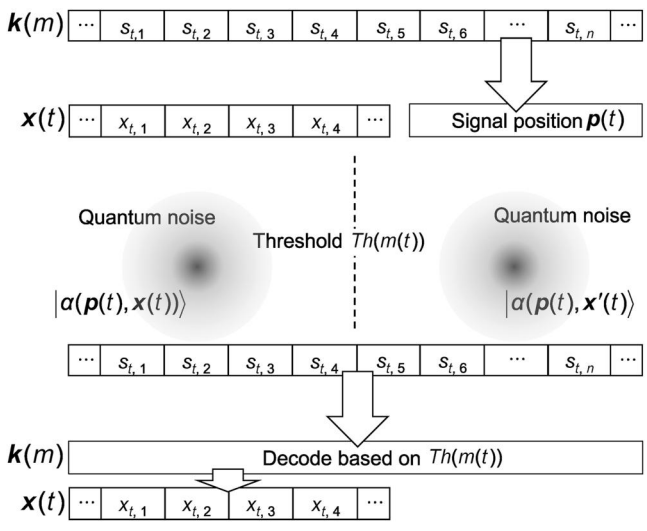

FIGURE 1 Overview of the Y00 protocol. The legitimate sender positions $p(m(t))$ of optical positions based on pseudo-random stream numbers (PRSNs), whilst plaintext $\boldsymbol{x}(t)$ corresponds to one of them. The legitimate receiver can decode $\boldsymbol{x}(t)$ by setting the discrimination threshold $Th(m(t))$ based on the shared PRSNs.

As previously stated, R. J. Glauber and E. C. G. Sudarshan formulated that the laser is in a quantum state [12, 13]. The property is given as follows [42].

$$\langle\alpha|\alpha'\rangle = \exp\left(\frac{1}{2}\left[\alpha\alpha'^{\dagger} - \alpha'\alpha^{\dagger}\right] - \frac{1}{2}|\alpha - \alpha'|^2\right) \quad (1)$$

Therefore, a product of any two quantum states constructs a Gaussian distribution of the quantum noise.

To implement a Y00 transmitter, any optical modulations are available if the six conditions above are satisfied: amplitude modulation, intensity modulation, phase modulation, quadrature amplitude modulation (QAM), or if any others exist. This study chooses QAM keying Y00 protocol as a concrete example without loss of generality.

2.1 | Security triad for information communications

Even though the quantum noise hides the signals corresponding to the messages from the attackers, the original Y00 protocol allows the attacker to alternate the messages by relocating the optical signals corresponding to the message bits [43, 44].

The above attack is possible when the attacker knows the messages previously. For example, legitimate users may access broadcasted data such as operating system images to update or high-quality multimedia, say 10^9–10^{11} bytes or even more. Hence, the attackers, as they are legitimate network users, would know the original data before the legitimate users access it. Therefore, the following security triad must be ensured [45, 46].

C. Confidentiality: Only legitimate users can read their plaintexts.
I. Integrity: The attackers cannot alter plaintexts.
A. Accessibility: Legitimate users can communicate whenever they want without disturbance by attackers.

In short, the original Y00 protocol could satisfy confidentiality and availability but lacked integrity.

Of course, cryptography must satisfy more requirements. For instance, deniability and authenticity are provided by digital signatures. However, this study focuses only on the above triads.

Past studies discussed how a new modulation could meet integrity [47, 48]. Without knowing the secondary key, the attackers' optical modulation generates pseudo-random optical location-plaintext correspondence. Hence, a hush value of the message data notifies the legitimate users of the alternation. Figure 2 illustrates the overview. Figure 3a illustrates the signal positioning four to carrier 2-bit information. Figure 3b shows an extension of the procedure of Figure 3a to M-ary information.

For simplification, a pair of the primary key $\boldsymbol{k}(m)$ and the secondary key $\boldsymbol{k}(m')$ is denoted as (m, m').

2.2 | Importance of CKP

The importance of the CKP attacks is that the attackers have the most advantages in obtaining the initial keys of the Y00 transmitters. The reason is as follows.

When the attacker is only allowed to decrypt the ciphertext, it is far easier for the attacker to find the correct initial keys rather than the correct ciphertext from the enormous possible ciphertext because of the quantum noise. For example, consider the following situation [38].

Suppose the two pseudo-random number generators are Linear Feedback Shift Registers (LFSRs) with a key length of 127 bits. Then the number of possible two keys $|\{\boldsymbol{k}(m, m')\}|$ is as follows.

$$|\{\boldsymbol{k}(m,m')\}| = \left(2^{127}-1\right)^2 \sim 2^{254} \tag{2}$$

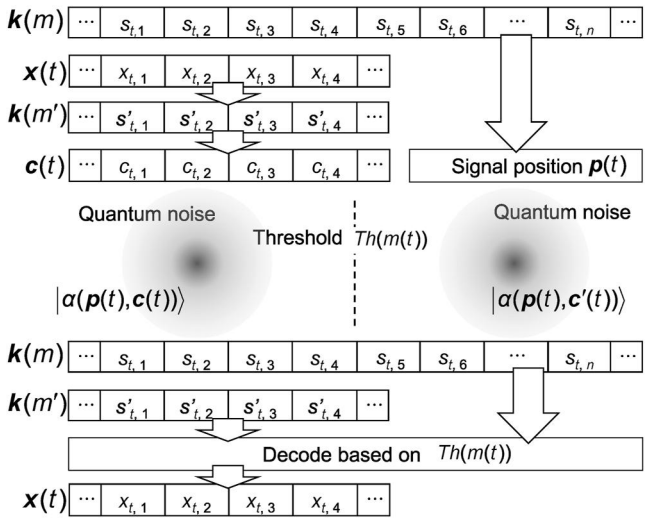

FIGURE 2 Y00 protocol with integrity. A secondary key $\boldsymbol{k}(m')$ encodes the plaintext $\boldsymbol{x}(t)$ to randomise signal position $\boldsymbol{p}(t)$ and $\boldsymbol{x}(t)$ correspondence.

Contrarily, suppose the cycle of LFSRs T of the key length 127 bits is $2^{127}-1$, the signal level L is 4096, and the masking size γ is 10. Then, the number of possible ciphertexts $|\{\boldsymbol{c}(m, m')\}|$ is as follows.

$$|\{\boldsymbol{c}(m,m')\}| = \gamma^{T/\log_2 L} = 10^{(2^{127}-1)/\log_2 4096} \sim 2^{8.0\times 10^{75}} \tag{3}$$

The rough estimations show that finding the initial keys are far easier [38]. Then, the attackers perform measurements to obtain the most likely keys to decrypt the ciphertexts, neither the correct ciphertexts nor the plaintexts. Therefore, the Y00 transmitters must protect the initial keys or the key streams, as FCA or Generalised Fast Correlation attacks (GFC attacks [37]) have shown. As explained in Ref. [38], the masking size that hides the correct ciphertexts is not a problem. The key space's size hidden in quantum noise is the problem. The exact reasons for the insufficiency of the widely used masking size, symbol-error rate (SER), or bit error-rate (BER) are described in Section 3.5. The above indices do not consider the Law of Large Numbers.

3 | OVERVIEW OF SECURITY ANALYSIS

This section provides an overview of security analysis. Especially the importance of CKP attacks and the corresponding security guarantee is discussed.

3.1 | Attack scheme

This subsection describes the scheme of the attacks. The situation is depicted in Figure 4. First, the attacker splits optical signals with a split ratio η nearly equal to one on the attacker's side. Then, the attackers store the signals to the quantum

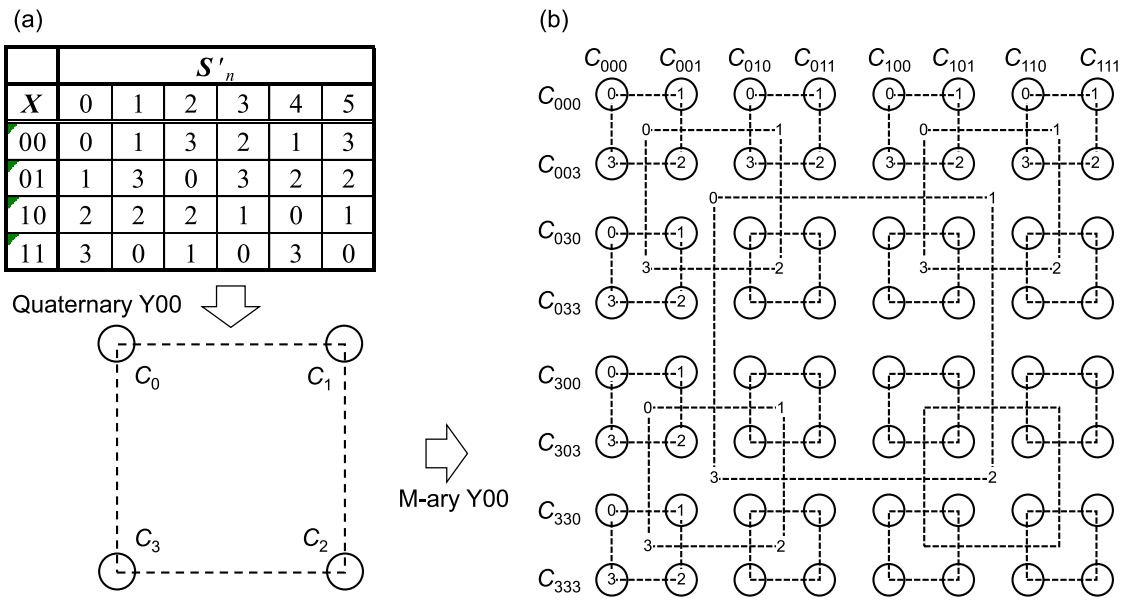

FIGURE 3 (a) Quaternary Y00 to realise integrity. (b) M-ary extended Y00 realise integrity. Using the encoding table multiple times easily extends quaternary Y00 to M-ary Y00. It applies to even 256-ary Y00 that encodes 1 byte at once.

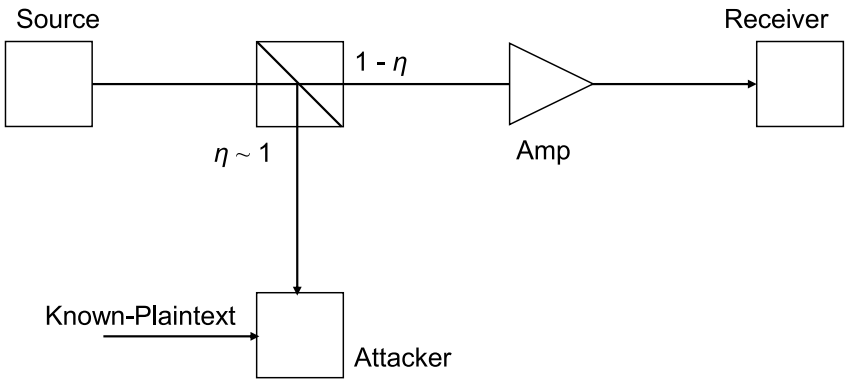

FIGURE 4 The attacker uses a beam splitter to rob the optical signal with the splitting ratio of $\eta \sim 1$. The attacker also places an optical amplifier between the splitter and the receiver to compensate. This study does not concern Man-In-The-Middle attacks.

memories to perform the optimal measurements on the memories to find the initial keys. At the same time, the attacker places an optical amplifier between the beam splitter and the legitimate receiver to compensate for the optical losses caused by beam splitting.

The legitimate receiver can be omitted since the splitting ratio $\eta \sim 1$.

3.2 | Requirements for information-theoretically secure Y00

To realise ITS Y00 transmitters, the attackers are assumed to have maximum knowledge according to Kerckhoffs' principle or Shannon's maxim, 'the enemy knows the system'.

The following items are what the attackers are supposed to know, which means the attacker knows anything except the secret keys.

1. The prior distribution of the secret key appearance.
2. Encoding along the manners of the Y00 protocol.
3. Full plaintext.
4. All side channels or back doors.

This study excludes the fourth point for simplification; however, the fourth point should be remembered for real-world security.

3.3 | Reduction from collective known-plaintext attacks to GFC attacks

The detailed descriptions are in Section 4.1. However, this section briefly describes why CKP attacks are equivalent to GFC attacks.

A sequence of Y00 signals is the tensor product of quantum states.

$$\rho(m, m', \boldsymbol{x}) := \otimes_{t=1}^{T} \rho(m, m', \boldsymbol{x}; t) \tag{4}$$

The notation $(m, m', \boldsymbol{x}; t)$ is an abbreviation of a set of generated running key pairs from the initial key pair (m, m') and a plaintext $\boldsymbol{x}$ at a timeslot t, $(m(t), m'(t), \boldsymbol{x}(t))$.

Suppose that a set of measurement operators at timeslot t $\{M(m, m'; t|\boldsymbol{x})\}$ is provided that satisfies the optimality corresponding to $\{\rho(m, m', \boldsymbol{x}; t)\}$ [36–38, 49, 50]. Then the tensor product $\{M(m, m'|\boldsymbol{x})\}$ is a set of optimal measurements corresponding to $\{\rho(m, m', \boldsymbol{x})\}$.

$$M(m, m'|\boldsymbol{x}) := \otimes_{t=1}^{T} M(m, m'; t|\boldsymbol{x}) \tag{5}$$

Here, the notation $(m, m'; t|\boldsymbol{x})$ is an index at timeslot t of a sequence generated from (m, m') conditioned on the known plaintext $\boldsymbol{x}$.

Therefore, a collective measurement on a series of the Y00 signals using quantum memories is no longer required; GFC attacks without the memories are sufficient.

3.4 | Upper-bound of successful attack probability

From this subsection, T_{LCM} denotes a least common multiple of the time cycle of the running key generated from $\boldsymbol{k}(m)$ and $\boldsymbol{k}(m')$, and N is the number of rounds of T_{LCM} [36]. Through time duration $N{\cdot}T_{\mathrm{LCM}}$, the attackers' success probability in obtaining the initial keys is given by the following inequality. The details are in Section 4.2.

$$\begin{aligned} &\Pr(m, m'|m, m', \boldsymbol{x}) \le 1 \\ &\quad - [1 - \Pr(m, m'; 0|m, m', \boldsymbol{x})]\exp[-N/N_{\mathrm{Breach}}] \end{aligned} \tag{6}$$

$$1/N_{\mathrm{Breach}} = T_{\mathrm{LCM}} \ln(\min_t[1 - \Pr(m, m'; t|m, m', \boldsymbol{x})])^{-1} \tag{7}$$

The term $[1 - \Pr(m, m'; t \mid m, m', \boldsymbol{x})]$ denotes the discrimination error probability of a signal at time slot t from a similar symbol trajectory with different initial keys. The situation is depicted in Figures 5a,b and 6a,b with thresholds to discriminate the symbol.

However, it is difficult to derive the thresholds for arbitral timeslot t for any plaintexts, as illustrated in Figure 6a [38]. Thus, the following approximation is possible, as illustrated in Figure 6b.

The ordinary thresholds to determine the correct symbol at timeslot t are in a square when QAM Y00s are equipped [38].

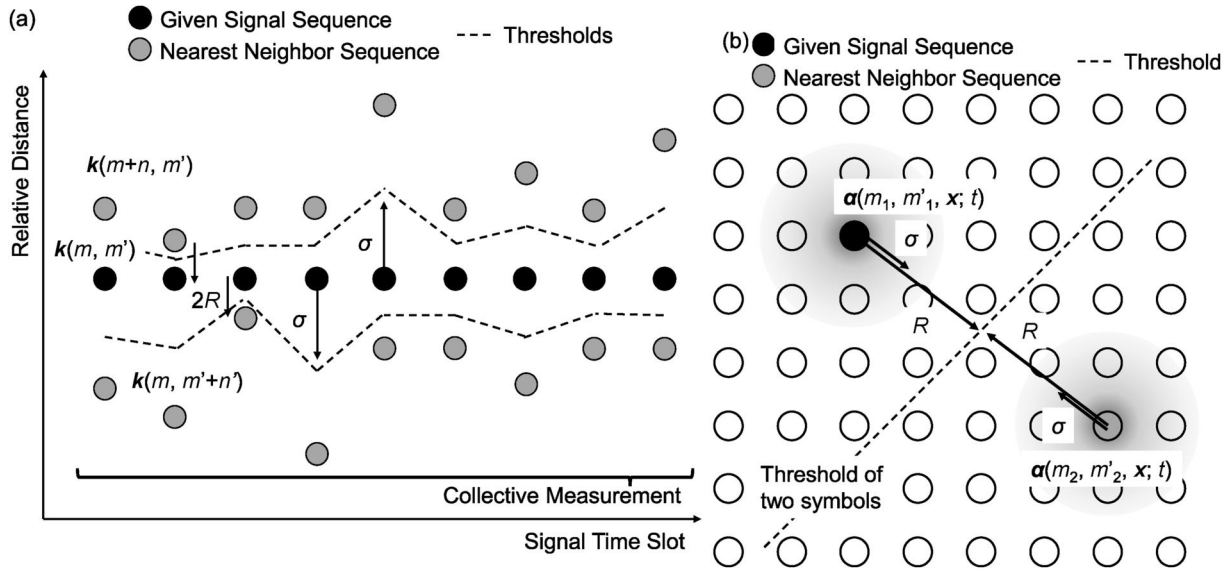

FIGURE 5 Quantum noise distribution σ and thresholds related to R under general cases. (a) Timeslot sequences. (b) A time slice of signal constellation geometry.

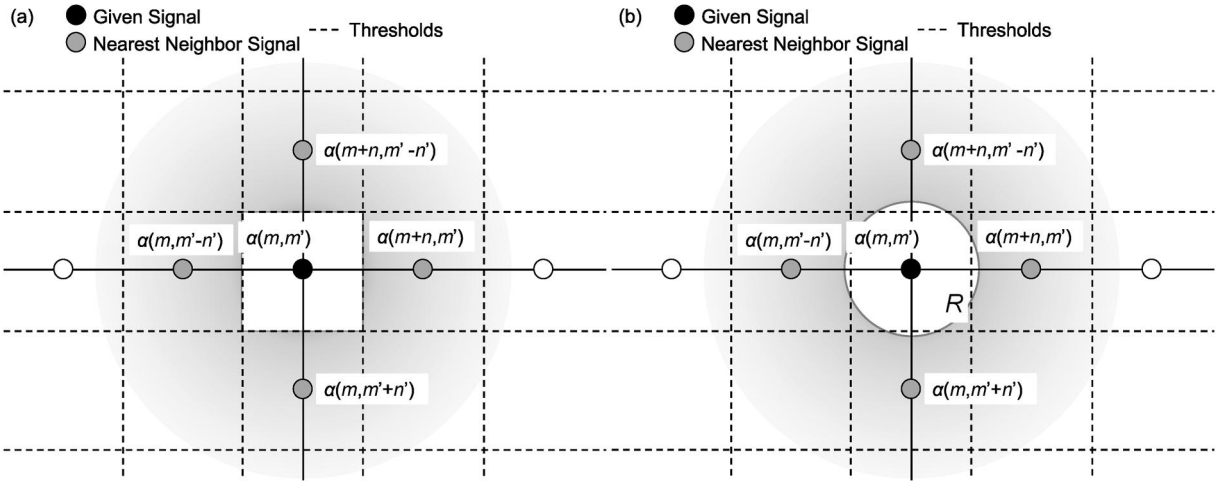

FIGURE 6 Quantum noise covering nearest neighbour states to hide initial keys. (a) The exact situation. (b) An approximate situation.

Under the approximation in Figure 6, the term $\min_t [1 - \Pr(m, m'; t|m, m', \boldsymbol{x})]$ is easily derived when the nearest signal is depicted in Figure 5b as follows.

$$\begin{aligned} &1 - \Pr(m, m'; t|m, m', \boldsymbol{x}) \\ &= \int_{R(t)}^{+\infty} \left[2\pi\sigma^2\right]^{-1} \exp\left[-\frac{1}{2}r^2/\sigma^2\right] r dr d\theta \\ &= \int_{R(t)}^{+\infty} \frac{1}{2}\sigma^{-2} \exp\left[-\frac{1}{2}r^2/\sigma^2\right] dr^2 = \exp\left[-\frac{1}{2}R(t)^2/\sigma^2\right] \end{aligned} \tag{8}$$

$$1/N_{\text{Breach}} = \min_t \frac{1}{2} T_{\text{LCM}} R(t)^2/\sigma^2 \tag{9}$$

The radius $R(t)$ is determined as follows [51]. For the nearest symbol of two different initial keys, determine S_{Th} that satisfies the following equality.

$$\begin{aligned} &\frac{\Pr(m_1, m_1')}{2\pi\sigma^2} \exp\left[-\frac{\left(S(m_1, m_1'; t|\boldsymbol{x}) - S_{\text{Th}}\right)^2}{2\sigma^2}\right] \\ &= \frac{\Pr(m_2, m_2')}{2\pi\sigma^2} \exp\left[-\frac{\left(S(m_2, m_2'; t|\boldsymbol{x}) - S_{\text{Th}}\right)^2}{2\sigma^2}\right] \end{aligned} \tag{10}$$

Here, $S(m_n, m'_n; t|\boldsymbol{x})$ are the geometrical points of signals in QAM modulation. A set of S_{Th} constructs the threshold around the correct symbol $S(m_1, m'_1; t|\boldsymbol{x})$, as illustrated in Figure 6a. However, the threshold to separate the symbol from other symbols is complex to analyse. Hence, an approximated

threshold is introduced, as illustrated in Figure 6b. The closest point is taken to construct R as follows.

$$\min_t R(t) = \min_{m,m',\boldsymbol{x};t|} |S(m,m';t|\boldsymbol{x}) - S_{\mathrm{Th}}| \tag{11}$$

Of course, the above may not directly apply to experimental results because the above is an approximation. Some arbitrarily to fit the experimental results is allowed.

3.5 | Contrast between GFC attacks and individual attacks

CKP or GFC attacks concern the repeated measurements of the same symbols or bits under known plaintext. This point differs greatly from ordinary security indices such as Bit-Error Rate (BER) or SER.

When the attacks perform measurements such as CKP or GFC attacks, the effective valiance of the noise reduces as follows, from Equations (6)–(9). The concept was already given in Refs [36–38].

$$\sigma(N)^2 \propto \sigma^2/N \to 0 \tag{12}$$

The above means that the attackers obtain more correct symbol sequences by repeating the measurements as time passes. Rewriting Equation (9) concludes the following.

$$\begin{aligned} N/N_{\mathrm{Breach}} &= \min_t \frac{1}{2} T_{\mathrm{LCM}} R(t)^2 \left[N/\sigma^2\right] \\ &= \min_t \frac{1}{2} T_{\mathrm{LCM}} R(t)^2/\sigma(N)^2 \end{aligned} \tag{13}$$

Contrarily, measurements without repetition, such as ordinary BER, SER, and FCAs, give the following result. These are simple results of statistics.

$$\sigma(N)^2 \propto \sigma^2 \tag{14}$$

Therefore, the attackers are supposed to repeatedly measure the cycle of signal sequences to perform GFC attacks regardless of the running key mapping [19].

3.6 | Key refreshment timing

As Equation (6) shows, and the attackers' probability of obtaining the correct keys asymptotically approaches unity. Before the Y00 transmitters are breached, the shared keys must be refreshed.

Let a breach probability threshold that the legitimate users maintain be P_{Th}. Then the following inequality must be satisfied.

$$\begin{aligned} &\Pr(m,m'|m,m',\boldsymbol{x}) \le 1 \\ &-[1-\Pr(m,m';0|\boldsymbol{x})]\exp[-N/N_{\mathrm{Breach}}] \le P_{\mathrm{Th}} \end{aligned} \tag{15}$$

Hence, the time slot that the key refreshment must be done is as follows.

$$NT_{\mathrm{LCM}} \le \frac{2\sigma^2}{R^2} \ln\left(\frac{1-\Pr(m,m';0|\boldsymbol{x})}{1-P_{\mathrm{Th}}}\right) \tag{16}$$

The procedure of fresh keys exchanges is as follows.

1. The legitimate users exchange random bits.
2. The part of the random bits is used to choose a universal hash function.
3. A chosen function hashes the other part of the random bits.
4. The generated hashed bits are the fresh keys.

However, it should be avoided to exchange fresh keys when the attackers' confidence in the correct key reaches P_{Th}. The following are the reasons.

1. The attacker uses the most likely current keys to estimate the fresh keys.
2. In this case, the fresh key may be insecure. The attacker may have some hints about the generated keys.
3. The above means application of Leftover-Hash Lemma (LHL) should be carefully done [37, 52, 53].

Hence, preparing fresh keys for the next round at the beginning of the current round would be recommended to avoid letting the attacker gain the advantage. Even in this case, the generated random bits may not be completely Independent and identically Distributed for the attackers. LHL may not be strictly applied. Section 4.4 explains.

4 | THEORY IN DETAILS AND OPEN QUESTIONS

This section supplies the details to derive formulae. The section also sorts unsolved problems for researchers following the study.

4.1 | Reduction from quantum to classical measurement

As described, R. J. Glauber and E. C. G. Sudarshan formulated [12, 13] that coherent light (laser) is in a quantum state. Similarly, optical receivers also have quantum properties [54]. However, the contributions of optical detections have a long history in the manner of classical measurements [51]. Therefore, a reduction from quantum to classical measurement should be easy.

The individual attacks on QKDs are to let the attackers measure an individual quantum memory after performing a unitary operation between a photon and a quantum memory the attacker possesses in QKDs. The collective attacks are to let the attackers perform unitary operations between the

sequence of photons and quantum memories, then store the intercepted signals in the quantum memories until an optimal measurement is performed to obtain the final key.

By the described situations, individual attacks are far weaker than collective attacks in the case of QKDs. However, collective attacks are too difficult to experiment with because quantum memories are required, making security verification difficult.

Instead, GFC attacks on the Y00 protocol are equivalent to CKP attacks for the following reasons. Equations (17)–(24) describe the necessary-and-sufficient condition of an optimal M-ary quantum measurement. For one Y00 signal, consider a set of optimal measurements for the attacker $\{M(m, m'|\boldsymbol{x})\}$ and a set of sequential quantum states $\{\rho(m, m'|\boldsymbol{x})\}$, where $\boldsymbol{x}$ is the known plaintext.

$$\rho(m,m',\boldsymbol{x}) := \otimes_{t=1}^{T}\ \rho(m,m',\boldsymbol{x};t) \tag{17}$$

$$M(m,m'|\boldsymbol{x}) := \otimes_{t=1}^{T} M(m,m';t|\boldsymbol{x}) \tag{18}$$

$$\sum\nolimits_{(m,m')} M(m,m'|\boldsymbol{x}) = I \tag{19}$$

$$W(m,m'|\boldsymbol{x}) := -\Pr(m,m'|\boldsymbol{x})\rho(m,m'|\boldsymbol{x}) \tag{20}$$

$$\begin{aligned}\Gamma :=& \sum\nolimits_{(m,m')} M(m,m'|\boldsymbol{x})W(m,m'|\boldsymbol{x})\\ =& \sum\nolimits_{(m,m')} W(m,m'|\boldsymbol{x})M(m,m'|\boldsymbol{x})\end{aligned} \tag{21}$$

$$\begin{aligned}&[W(m,m'|\boldsymbol{x})-\Gamma]M(m,m'|\boldsymbol{x})\\ &= M(m,m'|\boldsymbol{x})[W(m,m'|\boldsymbol{x})-\Gamma] = \mathbf{0}\end{aligned} \tag{22}$$

$$\begin{aligned}&M(m_1,m_1'|\boldsymbol{x})\left[W(m_1,m_1'|\boldsymbol{x})\right.\\ &\left.-W(m_2,m_2'|\boldsymbol{x})\right]M(m_2,m_2'|\boldsymbol{x}) = \mathbf{0}\end{aligned} \tag{23}$$

$$W(m,m'|\boldsymbol{x}) - \Gamma \geq 0 \tag{24}$$

Here, $-$ tr Γ is an average success probability.

When the set of optimal measurements $\{M(m, m'; t|\boldsymbol{x})\}$ corresponding to $\{\rho(m, m'; t|\boldsymbol{x})\}$, Equations (17)−(24) are satisfied. Hence, the CKP attacks with quantum memory [38] reduce GFC attacks [37]. However, an open question is how to derive $\{M(\mathrm{m}, \mathrm{m}'; t|\boldsymbol{x})\}$ and experimentally equip.

4.2 | Upper-bound of successful attack probability

From this subsection, T_{LCM} denotes a coprime of the time cycle of the primary key $\boldsymbol{k}(m)$ and secondary key $\boldsymbol{k}(m')$ [37, 38], and N is the number of rounds of T_{LCM} [37, 38]. Through time duration $N{\cdot}T_{\mathrm{LCM}}$, the attackers' success probability in obtaining the initial keys is given by the following inequality.

$$\begin{aligned}&\Pr(m,m'|m,m',\boldsymbol{x}) \leq 1\\ &\quad -[1-\Pr(m,m';0|\boldsymbol{x})]\exp[-N/N_{\mathrm{Breach}}]\end{aligned} \tag{25}$$

$$1/N_{\mathrm{Breach}} = T_{\mathrm{LCM}}\ln(\min_t[1-\Pr(m,m';t|m,m',\boldsymbol{x})])^{-1} \tag{26}$$

The following is the derivation that is similar to the procedure in Ref. [37]. The success probability in obtaining the correct keys is as follows.

$$\begin{aligned}&\Pr(m,m'|m,m',\boldsymbol{x}) = 1-[1-\Pr(m,m';\ 0|\boldsymbol{x})]\\ &\bullet \prod\nolimits_{t=1}^{NT_{\mathrm{LCM}}}[1-\Pr(m,m';t|m,m',\boldsymbol{x})]\end{aligned} \tag{27}$$

$$\begin{aligned}&\prod\nolimits_{t=1}^{NT_{\mathrm{LCM}}}[1-\Pr(m,m';t|m,m',\boldsymbol{x})]\\ &\quad \geq (\min_t[1-\Pr(m,m';t|m,m',\boldsymbol{x})])^{NT_{\mathrm{LCM}}}\end{aligned} \tag{28}$$

$$\begin{aligned}&\ln(\min_t[1-\Pr(m,m';t|m,m',\boldsymbol{x})])^{NT_{\mathrm{LCM}}}\\ &= -NT_{\mathrm{LCM}}\ln(\min_t[1-\Pr(m,m';t|m,m',\boldsymbol{x})])^{-1}\end{aligned} \tag{29}$$

From Equations (25)–(29), Equation (6) and are derived.

4.3 | Running key mapping

Before describing unsolved problems, this section describes what experiments and theories should do with the security guarantee of the Y00 protocol.

An explicit example is that theories alone cannot determine $\min_t R(t)$ in Equation (9). Some upper bounds to the limit should be derived. Contrarily, statistics by experiments or numerical simulations may be easier to evaluate, although numerical simulations cannot include all physical processes.

Another problem is how many key pairs must be hidden under quantum or classical noises. To equip more secure Y00 transmitters, almost all symbols' trajectories generated all possible key pairs must be hidden under the noise, as illustrated in Figure 7. Nearly equal to unit Fidelity means the series of quantum states are hard to discriminate. Contrarily, if Fidelity is small enough, two trajectories are easy to discriminate, resulting in a security breach. Fidelity drastically decreases even with one pair of discriminable states at the same timeslot. The following equation is an example.

$$\begin{aligned}&\mathrm{tr}\left[\otimes_{t=1}^{T_{\mathrm{LCM}}}\left|\alpha(m_1,m_1',\boldsymbol{x};t)\right\rangle\left\langle\alpha(m_1,m_1',\boldsymbol{x};t)\right|\right]\left[\otimes_{t=1}^{T_{\mathrm{LCM}}}\left|\alpha(m_2,m_2',\boldsymbol{x};t)\right\rangle\left\langle\alpha(m_2,m_2',\boldsymbol{x};t)\right|\right]\\ &= \prod\nolimits_{t=1}^{T_{\mathrm{LCM}}}\left|\left\langle\alpha(m_1,m_1',\boldsymbol{x};t)\middle|\alpha(m_2,m_2',\boldsymbol{x};t)\right\rangle\right|^2 = F(\rho(m_1,m_1',\boldsymbol{x}),\rho(m_2,m_2',\boldsymbol{x}))^2\end{aligned} \tag{30}$$

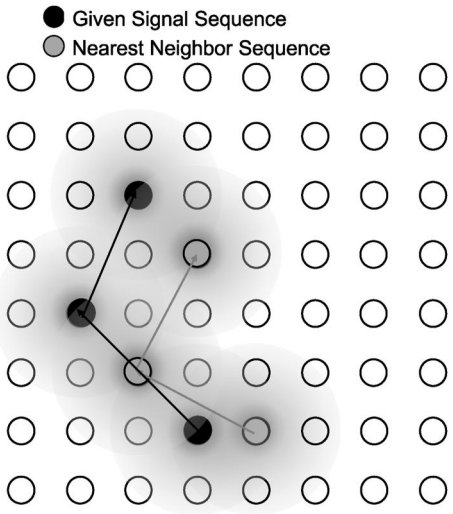

FIGURE 7 Close trajectory suitable for the security of the Y00 protocol.

Figure 7 asks, 'In what degree should the trajectories be similar by mapping to symbol positions in what way?' It is easy to make all trajectories similar by enlarging the noise variance σ^2 generated from classical or quantum randomness. However, it affects the communication properties between legitimate users.

Moreover, is it a 'quantum' stream cypher if such additional noises are applied? Making all trajectories similar under the same plaintexts is also possible by assists of the classical noise or the classical noise generated from quantum random number generators. It would not be 'quantum' stream encryptions but rather one of the physical-layer encryptions. Therefore, the mapping method to determine the symbol positions from running keys is important. This problem must be the theoretical work.

Furthermore, the Y00 protocol cannot exchange and authenticate the initial keys alone, whilst the Y00 is symmetric-key encryption, at least at this phase. Some opinions say that ordinary public-key cryptography can distribute the initial keys for the Y00 protocol. It is wrong because it never is ITS, even if it once introduced computationally secure cryptography. After all, the attackers with infinite-computational power would target the computationally complex cryptography. It is why ITS cryptographies, including the Y00 protocol, are expected. This problem is shared with QKDs.

To claim ITS is very severe to justify yet. Before summarising, this study addresses these problems for the future of the Y00 protocol because software quantum-resistant cryptography is far more convenient if the Y00 protocol does not meet these requirements.

4.4 | Security of fresh key generation in quantum noise

There should be various methods of key refreshment. For example, one study [55] used SHA3-512 for privacy amplification. However, the attackers' probability of obtaining the fresh keys must be estimated. The attackers' observations before the fresh-key distillation would gain an advantage in estimating the fresh-keys. Therefore, the LHL must be carefully applied [37, 56, 57].

LHL restricts the upper bound of the attackers' probability of obtaining the correct fresh key.

$$\sum_{h,c}\Pr(h,c)\left|\Pr(\boldsymbol{k}_{\mathrm{F}}|h,c)-2^{-|\boldsymbol{k}_{\mathrm{F}}|}\right|\le 2\sqrt{2^{|\boldsymbol{k}_{\mathrm{F}}|-\kappa}} \tag{31}$$

$$-\log_2\left[\sum_h \Pr(h)\max_c \Pr(c|h)\right]\ge\kappa \tag{32}$$

Here, $\boldsymbol{k}_{\mathrm{F}}=h(c)$ is a fresh key generated from a hash function h and a random unknown plaintext c transmitted by the Y00 protocol.

Furthermore, applying the following inequalities,

$$\sum_{h,c\left|\Pr(\boldsymbol{k}_{\mathrm{F}}|h,c)-2^{-|\boldsymbol{k}_{\mathrm{F}}|}\right|\ge 0}\Pr(h,c)\left[\Pr(\boldsymbol{k}_{\mathrm{F}}|h,c)-2^{-|\boldsymbol{k}_{\mathrm{F}}|}\right] \le 2\sqrt{2^{|\boldsymbol{k}_{\mathrm{F}}|-\kappa}} \tag{33}$$

$$\sum_{h,c\left|\Pr(\boldsymbol{k}_{\mathrm{F}}|h,c)-2^{-|\boldsymbol{k}_{\mathrm{F}}|}\right|\le 0}\Pr(h,c)\left[\Pr(\boldsymbol{k}_{\mathrm{F}}|h,c)-2^{-|\boldsymbol{k}_{\mathrm{F}}|}\right]\le 0 \tag{34}$$

Therefore, the following inequality is derived.

$$\sum_{h,c}\Pr(h,c)\Pr(\boldsymbol{k}_{\mathrm{F}}|h,c)\le 2^{-|\boldsymbol{k}_{\mathrm{F}}|}+2\sqrt{2^{|\boldsymbol{k}_{\mathrm{F}}|-\kappa}} \tag{35}$$

We must generate the key before $t=1$. Therefore,

$$\Pr(h,c)=\sum_{(m,m';0)}\Pr(h,c|m,m',\boldsymbol{x};0)\Pr(m,m',\boldsymbol{x};0) \tag{36}$$

If the probability distribution satisfies Equations (37)–(39) in the sense of LHL, then LHL is applicable.

$$\Pr(h,c|m,m',\boldsymbol{x};0)=\Pr(h)\Pr(c|h,m,m',\boldsymbol{x};0) \tag{37}$$

$$\Pr(h)=2^{-|\{h\}|} \tag{38}$$

$$-\log_2\max_c\Pr(c)\ge\kappa \tag{39}$$

However, notice that any (c, h) depends on the conditions (m, m', $\boldsymbol{x}$) as shown in Equation (36) whilst it is unknown how h is chosen independently from any other parameters as LHL requests. Otherwise, theorists may need to modify LHL so that it meets experiments or to find equipping Equation (38).

4.5 | List of unsolved problems

As this study described, many problems still need to be addressed.

1. Estimating the threshold radius R, or exact derivations illustrated in Figure 6a (Section 3.4).
2. Derivation of a set of optimal measurements for the attackers (Section 4.1) and experimental implementations.
3. Mapping signal positions to protect the initial keys from CKP attacks (Section 4.3).
4. Secure key agreements like Information-Theoretic Security (Section 4.3).
5. Security guarantee for fresh key generations (Section 4.4).

The experimental progress of the Y00 protocol has been spectacular. However, if these results were not theoretically guaranteed, the Y00 protocol cannot be evaluated. More theoretical works which tie up experiments are required.

5 | CONCLUSIONS

This study addressed several problems with the Y00 protocol. Solved problems are key-refreshment timing and determining the upper bound of the security-breach probability under the assumption that experiments estimate the security threshold parameter. Various problems are unsolved, mostly addressed in Section 4. They are specially listed in Section 4.5. The study concludes that theories must solve the following problem so that the Y00 protocol is useful—especially the security of refreshed key, procedures of initial key agreements, and key mapping to the Y00 constellation that experimental confirmations are required. Unless these problems are addressed, quantum-resistant cryptography would take advantage because of its easier use.

AUTHOR CONTRIBUTIONS

The author has done the whole study to write the whole manuscript.

CONFLICT OF INTEREST STATEMENT

No conflict of interest.

DATA AVAILABILITY STATEMENT

No data nor programs.

PERMISSION TO REPRODUCE MATERIALS FROM OTHER SOURCES

None.

ORCID

Talehisa Iwakoshi https://orcid.org/0000-0001-7236-1591

REFERENCES

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. Proc. IEEE Int. Conf. Comput. Syst. Signal Process. 175(0) (1984)
2. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. Theor. Comput. Sci. 560, 7–11 (2014). https://doi.org/10.1016/j.tcs.2014.05.025
3. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. 68(21), 3121–3124 (1992). https://doi.org/10.1103/PhysRevLett.68.3121
4. Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bell's theorem. Phys. Rev. Lett. 68(5), 557–559 (1992). https://doi.org/10.1103/PhysRevLett.68.557
5. Barbosa, G.A., et al.: Secure communication using mesoscopic coherent states. Phys. Rev. Lett. 90(22), Art. no. 227901 (2003). https://doi.org/10.1103/PhysRevLett.90.227901
6. Yuen, H.P., et al.: Security of Y-00 and similar quantum cryptographic protocols. https://apps.dtic.mil/dtic/tr/fulltext/u2/a442128.pdf (2004)
7. Kanter, G.S., et al.: Exploiting quantum and classical noise for securing high-speed optical communication networks. In: Fluctuations and Noise in Photonics and Quantum Optics III, vol. 5842, pp. 74–86. SPIE (2005)
8. Corndorf, E., et al.: Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks. Phys. Rev. A 71(6), 062326 (2005). https://doi.org/10.1103/PhysRevA.71.062326
9. Nair, R., et al.: Quantum-noise randomized ciphers. Phys. Rev. A 74(5), 052309 (2006). https://doi.org/10.1103/PhysRevA.74.052309
10. Yuen, H.P.: Physical cryptography: a new approach to key generation and direct encryption. In: Performing Organization Report Number; AFRL-SR-AR-TR-10-0001. https://apps.dtic.mil/sti/pdfs/ADA512847.pdf (2009)
11. Yuen, H.P.: Key generation: foundations and a new quantum approach. IEEE J. Sel. Top. Quant. Electron. 15(6), 1630–1645 (2009). https://doi.org/10.1109/JSTQE.2009.2025698
12. Glauber, R.J.: Coherent and incoherent states of the radiation field. Phys. Rev. 131(6), 2766–2788 (1963). https://doi.org/10.1103/PhysRev.131.2766
13. Sudarshan, E.C.G.: Equivalence of semiclassical and quantum mechanical descriptions of statistical light beams. Phys. Rev. Lett. 10(7), 277–1963 (1963). https://doi.org/10.1103/PhysRevLett.10.277
14. Nishioka, T., et al.: How much security does Y-00 protocol provide us? Phys. Lett. A 327(1), 28–32 (2004). https://doi.org/10.1016/j.physleta.2004.04.083
15. Nishioka, T., et al.: Reply to: "Comment on: 'How much security does Y-00 protocol provide us?'". Phys. Lett. A 346(1-3), 7–16 (2005). https://doi.org/10.1016/j.physleta.2005.08.023
16. Donnet, S., et al.: Cryptanalysis of Y-00 under heterodyne measurement and fast correlation attack. In: 2006 European Conference on Optical Communications, pp. 1–2. IEEE. https://doi.org/10.1109/ECOC.2006.4801097
17. Donnet, S., et al.: Security of Y-00 under heterodyne measurement and fast correlation attack. Phys. Lett. A 356(6), 406–410 (2006). https://doi.org/10.1016/j.physleta.2006.04.002
18. Mihaljević, M.J.: Generic framework for the secure Yuen 2000 quantum-encryption protocol employing the wire-tap channel approach. Phys. Rev. A 75(5), 052334 (2007). https://doi.org/10.1103/PhysRevA.75.052334
19. Shimizu, T., Hirota, O., Nagasako, Y.: Running key mapping in a quantum stream cipher by the Yuen 2000 protocol. Phys. Rev. A 77(3), 034305 (2008). https://doi.org/10.1103/PhysRevA.77.034305
20. Jiao, H., et al.: Physical-layer security analysis of a quantum-noise randomized cipher based on the wire-tap channel model. Opt. Express 25(10), 10947–10960 (2017). https://doi.org/10.1364/OE.25.010947
21. Li, Z., et al.: Performance analysis of noise channel model for quantum noise stream cipher. In: 2020 IEEE 20th International Conference on Communication Technology (ICCT), pp. 1217–1220. IEEE (2020). https://doi.org/10.1109/ICCT50939.2020.9295812
22. Chen, Y., et al.: Security analysis of QAM quantum-noise randomized cipher system. IEEE Photon. J. 12(4), 1–14 (2020). https://doi.org/10.1109/JPHOT.2020.3009252
23. Tan, Y., et al.: Performance analysis of physical-layer security in ISK quantum-noise randomized cipher based on wiretap channel. Opt. Commun. 461, 125151 (2020). https://doi.org/10.1016/j.optcom.2019.125151
24. Wang, Y., et al.: Experimental demonstration of secure 100 Gb/s IMDD transmission over a 50 km SSMF using a quantum noise stream cipher and optical coarse-to-fine modulation. Opt. Express 29(4), 5475–5486 (2021). https://doi.org/10.1364/OE.418589
25. Li, Y., et al.: Blind nonlinearity equalization by machine-learning-based clustering for QAM-based quantum noise stream cipher transmission.

China Commun. 19(8), 127–137 (2022). https://doi.org/10.23919/JCC.2022.08.010
26. Sun, J., et al.: Experimental demonstration of 201.6-Gbit/s coherent probabilistic shaping QAM transmission with quantum noise stream cipher over a 1200-km standard single mode fiber. Opt. Express 31(7), 11344–11353 (2023). https://doi.org/10.1364/OE.484431
27. Deng, Q., et al.: Quantum noise secured terahertz communications. In: Optical Fiber Communication Conference, pp. W2A-33. Optica Publishing Group (2023). https://doi.org/10.1364/OFC.2023.W2A.33
28. Jiao, H., et al.: Physical-layer security analysis of PSK quantum-noise randomized cipher in optically amplified links. Quant. Inf. Process. 16(8), 1–16 (2017). https://doi.org/10.1007/s11128-017-1637-4
29. Jiao, H., et al.: Physical-layer security analysis of a quantum-noise randomized cipher based on the wire-tap channel model. Opt. Express 25(10), 10947–10960 (2017). https://doi.org/10.1364/OE.25.010947
30. Li, Z., et al.: Analysis of statistical characteristics for quantum noise stream cipher. In: 24th National Laser Conference & Fifteenth National Conference on Laser Technology and Optoelectronics, vol. 11717, pp. 251–255. SPIE (2020). https://doi.org/10.1117/12.2585615
31. Chen, Y., et al.: Security analysis of QAM quantum-noise randomized cipher system. IEEE Photon. J. 12(4), 1–14 (2020). https://doi.org/10.1109/JPHOT.2020.3009252
32. Zhang, M., et al.: Security analysis of quantum noise stream cipher under fast correlation attack. In: Optical Fiber Communication Conference, pp. Th1A-5. Optical Society of America (2021). https://doi.org/10.1364/OFC.2021.Th1A.5
33. Zhang, M., et al.: Security analysis of a QAM modulated quantum noise stream cipher under a correlation attack. Opt. Express 30(22), 40645–40656 (2022). https://doi.org/10.1364/OE.472581
34. Li, Y., et al.: Analysis of the encryption penalty in a QAM-based quantum noise stream dcipher. Opt. Express 31(12), 19006–19020 (2023). https://doi.org/10.1364/OE.489043
35. Feng, G., et al.: Security enhancement based on input-output correlation protection of nonlinear combinatorial function in quantum noise stream cipher. In: 2022 Asia Communications and Photonics Conference (ACP), pp. 722–724. IEEE (2022). https://doi.org/10.1109/ACP55869.2022.10088962
36. Iwakoshi, T.: 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). https://doi.org/10.1117/1.OE.57.12.126103
37. Iwakoshi, T.: Analysis of Y00 protocol under quantum generalization of a fast correlation attack: toward information-theoretic security. IEEE Access 8, 23417–23426 (2020). https://doi.org/10.1109/ACCESS.2020.2969455
38. Iwakoshi, T.: Security evaluation of Y00 protocol based on time-translational symmetry under quantum collective known-plaintext attacks. IEEE Access 9, 31608–31617 (2021). https://doi.org/10.1109/ACCESS.2021.3056494
39. Renner, R.: Security of quantum key distribution. Int. J. Quant. Inf. 6(01), 1–127 (2008). https://doi.org/10.1142/S0219749908003256
40. Verma, P.K., El Rifai, M., Chan, K.W.C.: Secure communication based on quantum noise. In: Multi-Photon Quantum Secure Communication, pp. 85–95. Springer, Singapore (2019). https://doi.org/10.1007/978-981-10-8618-2_4
41. Mariamichael, J., Raj, A., Selvaraj, R.: Survey on quantum noise stream cipher implemented optical communication systems. J. Opt. Commun. 2023(0) (2023). https://doi.org/10.1515/joc-2022-0057
42. Walls, D.F., Milburn, G.J.: Quantum Optics. Springer Science & Business Media (2007). ISBN: 9783540285731, 3540285733
43. Iwakoshi, T.: Study of tolerability against defacing of Y 00 quantum stream cipher. In: Tamagawa University Quantum ICT Research Institute Bulletin 1.1 (2011)
44. Iwakoshi, T.: Bit-Inversion attack prevention using quadruple-signal-based Y-00 systems. In: Tamagawa University Quantum ICT Research Institute Bulletin 2.1 (2012)
45. Hughes, J., Cybenko, G.: Quantitative metrics and risk assessment: the three tenets model of cybersecurity. Technol. Innovat. Manag. Rev. 3, 8–24 (2013). https://doi.org/10.22215/timreview/712
46. Jason, A.: The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Syngress (2014)
47. Iwakoshi, T., Hirota, O.: Polarity inversion attack prevention by physical properties of Y00 quantum stream cipher. In: Proceedings Volume 8899, Emerging Technologies in Security and Defence; and Quantum Security II; and Unmanned Sensor Systems X (2013). https://doi.org/10.1117/12.2029029.88990M
48. Iwakoshi, T.: Message-falsification prevention with small quantum mask in quaternary Y00 protocol. IEEE Access 7, 74482–74489 (2019). https://doi.org/10.1109/ACCESS.2019.2921023
49. Yuen, H.P., Kennedy, R., Lax, M.: Optimum testing of multiple hypotheses in quantum detection theory. IEEE Trans. Inf. Theor. 21(2), 125–134 (1975). https://doi.org/10.1109/TIT.1975.1055351
50. Helstrom, C.W.: Quantum detection and estimation theory. In: Volume 123, Mathematics in Science and Engineering. Academic Press (1976). ISBN: 9780080956329, 0080956327
51. Van Trees, H.L., Bell, K.L., Tian, Z.: Detection, Estimation, and Modulation Theory, Part I: Detection, Estimation, and Linear Modulation Theory: 2nd Edition. John Wiley & Sons (2004)
52. Håstad, J., et al.: A pseudorandom generator from any one-way function. SIAM J. Comput. 28(4), 1364–1396 (1999). https://doi.org/10.1137/S0097539793244708
53. Barak, B., et al.: Leftover hash lemma, revisited. In: Advances in Cryptology–CRYPTO 2011: 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings 31. Springer, Berlin (2011). https://doi.org/10.1007/978-3-642-22792-9_1
54. Personick, S.: Application of quantum estimation theory to analog communication over quantum channels. IEEE Trans. Inf. Theor. 17(3), 240–246 (1971). https://doi.org/10.1109/TIT.1971.1054643
55. Lei, C., et al.: Integration of self-adaptive physical-layer key distribution and encryption in optical coherent communication. J. Lightwave Technol., 1–8 (2023). https://doi.org/10.1109/JLT.2023.3257963
56. Yuen, H.P.: Security of quantum key distribution. IEEE Access 4, 724–749 (2016). https://doi.org/10.1109/ACCESS.2016.2528227
57. Iwakoshi, T.: Bit-error-rate guarantee for quantum key distribution and its characteristics compared to leftover hash lemma. In: Quantum Information Science and Technology IV, vol. 10803. SPIE (2018). https://doi.org/10.1117/12.2500457

How to cite this article: Iwakoshi, T.: Y00 quantum noise randomised cipher; theoretical and experimental background. IET Quant. Comm. 4(4), 181–190 (2023). https://doi.org/10.1049/qtc2.12064