IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 17, 2021, accepted January 25, 2021, date of publication February 2, 2021, date of current version March 1, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3056494

Security Evaluation of Y00 Protocol Based on Time-Translational Symmetry Under Quantum Collective Known-Plaintext Attacks

TAKEHISA IWAKOSHI, (Member, IEEE)
Department of Information Engineering, Mie University, Mie 514-8507, Japan
e-mail: iwakoshi@cs.info.mie-u.ac.jp

ABSTRACT In this paper, we concretely formulate to derive the attacker's success probability of obtaining the shared secret keys for the Y00 protocol under a combination of a quantum collective attack with infinitely-long known-plaintext, naming it "collective known-plaintext attack" in this work. In contrast, our previous work showed only the necessary condition to design Y00 transmitters to be information-theoretic secure. The keystone of the security evaluations in this work is the time-translational symmetry of the Y00 signals modulated by pseudo-random number generators, such as linear-feedback shift registers or Mersenne twisters. With the assist of a true-random deliberate-signal-randomization, information-theoretic security would be realized. By numerical simulations, we can determine whether the designed Y00 transmitters are information-theoretic secure. However, this work's security evaluation may not apply to the transmitters with cryptographically-secure pseudo-random number generators because they might not have time-translational symmetry, even though such Y00 transmitters may be securer. We also describe future challenges for theorists to accelerate designing securer Y00 transmitters.

INDEX TERMS Beyond Shannon-limit of cryptography, information-theoretic security, physical-layer encryption, quantum multi-hypotheses testing theory, secure communications.

I. INTRODUCTION

Since the invention of the first concept of quantum key distribution (QKD) [1], [2], it has been the center of attention how information-theoretically secure (ITS) communications are realizable using the laws of quantum physics.

Around 2000, H. P. Yuen proposed a protocol with a code-name "$\alpha\eta$" to DARPA [3]–[6] to realize quantum encryption compatible with the current optical network. Today, the protocol is called "Quantum-Noise Stream Cipher," or some researchers call it "Y00" to show respect to the inventor, although Yuen named it "keyed-communication in Quantum-noise" (KCQ) [6]. A well-described review on works before 2017 is [7].

The prototype Y00 transmitter was cryptanalyzed by a fast correlation attack [8], [9]. Even after a countermeasure [9], [10] was equipped, it was thought to be for the specific attack, not for general attacks. Hence, almost for 20 years, the protocol had been thought to be non-ITS. Some researchers in quantum cryptography have commented, "the Y00 security is folklore." The comment motivated us to formulate ITS Y00 security since 2019 [11].

Thus, the main reason for the unpopularity of the Y00 protocol may be that its security is not well-understood yet, although its significant affinity to the current broadband optical communication infrastructure has been experimentally confirmed with the current technologies [12], [13].

In this work, we give concrete evaluation procedures applicable to implemented Y00 transmitters to evaluate their security based on the probability of successful attacks, as H. P. Yuen has emphasized in [6], [18], [19] and some other literature stated [20], [21]. Past security evaluations of Y00 transmitters under KPAs have been done under individual quantum measurements to evaluate the attacker's error rate (individual KPAs). However, individual KPAs might have over-estimated the security level of the Y00 protocol.

Our previous work [11] showed that the Y00 protocol possibly realizes ITS when it is well-designed even under known-plaintext attack (KPA) with the assists of quantum collective measurements [22] (collective KPA), in which the attacker performs an optimal quantum measurement on her quantum memory storing the series of Y00 signals to obtains

The associate editor coordinating the review of this manuscript and approving it for publication was Tianhua Xu.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

the shared secret keys. It is analogous to collective attacks in the context of QKD's adding infinitely-long known-plaintext attacks in the security evaluation of the Y00 protocol.

However, no concrete designs of transmitters were given in our previous work [11]; it showed only the possibility of ITS Y00 transmitters. Hence, we need security evaluation procedures under collective KPAs to give concrete designs of ITS Y00 transmitters.

The collective KPAs are realistically possible when all users, including the attacker, can access public datasets such as operating system (OS) upgrading, the original image for a clean installation, broadcasting, or high-quality multimedia. The data size of multimedia in a Blu-ray disc can store about 100 gigabytes. These data sizes increase as we have more network capacities. Thus, sufficiently long collective KPAs are realistically possible.

In this work, we give a concrete formulation to realize ITS Y00 transmitters by paying attention to pseudo-random number generators' characteristics (PRNGs). By the characteristics of PRNGs, the Y00 signals have time-translate symmetry. Hence, such symmetry makes the security analysis easier. Here, we notify that the security evaluations based on the time-translational symmetry cannot be applied to any cryptographic-secure PRNGs because they might not be symmetrical. To evaluate Y00 transmitters with cryptographic-secure PRNGs, a further generalization of this work is required.

Our study is constructed as follows. Section II provides fundamental knowledge on the Y00 protocol. Section III describes the overview of our security evaluation strategy based on the time-translational symmetry of the Y00 signals. Section IV evaluates the confidentiality of the shared secret keys of the Y00 transmitters and the message integrity. Section V discusses the connection between our results in this study and our previous study. Section VI describes future perspectives. Then Section VII states conclusions.

II. BASICS OF PROTOCOL AND PREVIOUS RESULTS

This section describes the principles of Y00 protocol with Message Integrity. Before we start the discussions, we denote $\{V\}$ as a set of possible variables V while $|\{V\}|$ denotes the number of elements in $\{V\}$.

A. BASIC BACKGROUNDS

C. E. Shannon proved that One-Time Pad (OTP) is unconditionally secure as follows [23].

$$\Pr(\boldsymbol{X}|\boldsymbol{C}) = \Pr(\boldsymbol{X}) \tag{1}$$

$\boldsymbol{C}$ is a ciphertext string where $\boldsymbol{C} = \boldsymbol{X} + \boldsymbol{S} \bmod 2$, where $\boldsymbol{X}$ is a plaintext string, and $\boldsymbol{S}$ is the true-random keystream. To satisfy (1), the probability distribution of $\boldsymbol{S}$ must be independent and identically distributed (IID), denoted as

$$\Pr(\boldsymbol{S}) = 1\big/|\{\boldsymbol{S}\}|. \tag{2}$$

After Shannon's work, A. D. Wyner showed that (2) is not necessary only when the attacker, Eve, observes inevitable noise $\boldsymbol{Q}$ on her wire-tap channel [24], [25]. The legitimate users', Alice and Bob, encrypt and decrypt the messages as

$$\boldsymbol{C} = \boldsymbol{X} + \boldsymbol{S} \bmod 2. \tag{3}$$

Here, $\boldsymbol{S}$ is generated from a PRNG with a shared secret key $\boldsymbol{K}$ as a PRNG seed; hence, $\boldsymbol{S}$ is not IID.

Eve observes a degraded ciphertext $\boldsymbol{C}_{\mathrm{E.}}$ instead of $\boldsymbol{C}$ by noise $\boldsymbol{Q}$ as follows.

$$\boldsymbol{C}_{\mathrm{E}} = \boldsymbol{C} + \boldsymbol{Q} \bmod 2. \tag{4}$$

Hence, $\boldsymbol{S}$ and its seed $\boldsymbol{K}$ cannot be uniquely determined unless $\boldsymbol{Q} = \boldsymbol{Q}(\boldsymbol{X}, \boldsymbol{C}_{\mathrm{E}})$ under KPA [11],

$$H(\boldsymbol{S}|\boldsymbol{C}_{\mathrm{E}}, \boldsymbol{X}) > 0. \tag{5}$$

Contrarily, OTP under KPA necessarily reveals the secret key $\boldsymbol{S}$ as follows.

$$H(\boldsymbol{S}|\boldsymbol{C}, \boldsymbol{X}) = 0. \tag{6}$$

Equivalently, even though $\boldsymbol{S}$ is discarded once it was used,

$$\Pr(\boldsymbol{S}|\boldsymbol{C}, \boldsymbol{X}) = 1. \tag{7}$$

However, if Eve is almighty excepting physics laws' restrictions as QKDs assume, Wyner's assumption faces difficulties. The Y00 protocol is one of the solutions to add inevitable physical noise on the wire-tap channel.

B. OTHER CLASSES OF ATTACKS

The readers may wonder why this study treats only KPA while there are several classes of attacks as follows.

1) Ciphertext only attacks (COA); The attacker utilizes the only ciphertext to obtain the plaintext or the key.
2) Known plaintext attacks (KPA); The attacker knows the plaintext then tries to find the encryption key.
3) Chosen plaintext attacks (CPA); The attacker can access the encryption system to obtain the pair of a known plaintext and the corresponding ciphertext.
4) Chosen ciphertext attacks (CCA); The attacker injects ciphertext into decryption systems to obtain the corresponding plaintext.

In any classes except COA, the attacker can obtain the pair of the plaintext and the corresponding ciphertext to perform key-recovery attacks in the Y00 transmitters. Therefore, there is no significant difference between infinitely-long KPAs in this study and other cryptologic attack classes.

Moreover, our previous work [11] showed that Eve's any local operations, no matter classical or quantum, never give her any advantages in cryptanalyses in the context of optimal quantum measurement and quantum data-processing inequality.

Readers may still doubt whether PRNGs achieve ITS with the assist of quantum noise. However, we described precise explanations in Appendix.C of our previous work [11] by analogous imperfect OTP; ITS would still be maintained, although Eve would gradually be aware of the encoded contents.

C. COMMENT ON "IMPOSSIBILITY OF UNCONDITIONAL SECURITY" BY Y00 PROTOCOL

Another collective security analysis on the Y00 protocol by P. A. Tregubov and A. S. Trushechkin [14] is precisely explained and invalidated in this section.

They stated their security analysis assumes that the Y00 protocol transfers "qubits" in finite-dimensional Hilbert spaces, which have orthonormal states, as we see in their Definition 2, Section 4, 5, and 6.

The quantum states in the Y00 protocol never are orthonormal in infinite-dimensional Hilbert spaces; it is well-known that coherent states never be orthogonal as firstly formulated by R. J. Glauber [15] and E. C. G. Sudarshan [16], also in several textbooks on quantum optics [17]. Hence, their security analysis has a fatal error from the beginning to apply it to the Y00 protocol, although their discussion may apply to finite-dimensional quantum stream ciphers.

D. PRINCIPLE OF Y00 PROTOCOL

The Y00 protocol's principle is to create the inevitable noise on the wire-tap channel by its design even under Eve's collective KPAs, as we explained in the previous work [11].

To start the Y00 protocol, Alice and Bob must share secret keys $(\boldsymbol{k}_m, \boldsymbol{\Delta k}_{m'}) \in \{(\boldsymbol{K}, \boldsymbol{\Delta K})\}$. Then, they expand $(\boldsymbol{k}_m, \boldsymbol{\Delta k}_{m'})$ into key streams $(\boldsymbol{s}_m, \boldsymbol{\Delta x}_{m'}) \in \{(\boldsymbol{S}, \boldsymbol{\Delta X})\}$ using the common PRNGs equipped in the transmitter and receiver, such as linear feedback shift register (LFSR) or Mersenne twister [26], [27]. Subsequently, $\boldsymbol{s}_m$ is chopped to every $(\log_2 L)$ bit to form an L-ary string $\boldsymbol{s}_m(t)$ at time slot t. A message bit $x(t)$ is encoded into a coherent state $\left|\alpha[l_{(m,m')}(t)]\right\rangle$ as follows:

$$l_{(m,m')}(t) := \mathrm{Map}\left[s_m(t)\right] + L\left(\mathrm{Map}\left[s_m(t)\right] + x(t) + \Delta x_{m'}(t) \bmod 2\right). \tag{8}$$

Map$[\boldsymbol{s}_m(t)]$ is a projection from $\boldsymbol{s}_m(t)$ to Map$[\boldsymbol{s}_m(t)]$ $\{0, 1, 2, 3, \ldots, L-1\}$. For the detailed characteristics and concrete Map$[\cdot]$, the references [7], [28]–[30] help understand. Therefore, $x(t)\{0, 1\}$ corresponds to a set of quantum states $\{\left|\alpha[l_{(m,m')}(t)]\right\rangle, \left|\alpha[l_{(m,m')}(t) + L]\right\rangle\}$ when Map$[\boldsymbol{s}_m(t)] + \Delta x_{m'}(t)$ is an even number; otherwise, $\{\left|\alpha[l_{(m,m')}(t) + L]\right\rangle, \left|\alpha[l_{(m,m')}(t)]\right\rangle\}$. In contrast, Bob's receiver sets an optimal threshold to discriminate against the set of quantum states based on the shared $(\boldsymbol{s}_m, \Delta\boldsymbol{x}_{m'})$. Therefore, he decodes $x(t)$ because he knows the value of Map$[\boldsymbol{s}_m(t)] + \Delta x_{m'}(t)$. Meanwhile, Eve must discriminate against the $2L$-ary signals to obtain $x(t)$ under COAs, which is hidden under the overlapping quantum and classical noise because she does not know whether Map$[\boldsymbol{s}_m(t)] + \Delta x_{m'}(t)$ is even or odd.

When Eve can launch KPA longer than the least common multiple (LCM) of PRNGs' periods for $(\boldsymbol{S}, \boldsymbol{\Delta X})$ denoted as T_{LCM}, she launches an optimal measurement to obtain the most probable corresponding shared keys $(\boldsymbol{K}, \boldsymbol{\Delta K})$. In such a case, the quantum detection theory for multi-hypotheses [31]–[33] is required to evaluate the security of the Y00 protocol. Eve obtains the coherent states separated from a beam-splitter of splitting ratio η_{E} to store the signal sequence.

$$\begin{aligned}|\eta_{\mathrm{E}}\boldsymbol{\alpha}(\boldsymbol{k}_m, \boldsymbol{\Delta k}_{m'}, \boldsymbol{x})\rangle &:= |\boldsymbol{\alpha}_{\mathrm{E}}(\boldsymbol{k}_m, \boldsymbol{\Delta k}_{m'}, \boldsymbol{x})\rangle \\ &= \otimes_{t=1}^{N\cdot T_{\mathrm{LCM}}} |\alpha_{\mathrm{E}}[l_m(t-1)]\rangle\,. \end{aligned}\tag{9}$$

Here, η_{E} may be almost one; Eve may insert an optical amplifier to Bob's side to compensate for the optical loss by η_{E}. Hence, η_{E} being almost one is possible.

Since $(\boldsymbol{s}_m, \Delta x_{m'})$ is generated from $(\boldsymbol{k}_m, \boldsymbol{\Delta k}_{m'})$, Eve needs to perform a $|\{\boldsymbol{K}, \boldsymbol{\Delta K}\}|$ -ary discrimination based on the collective KPA [34].

E. MESSAGE INTEGRITY IMPLEMENTATION IN Y00

Confidentiality, Integrity, and Availability are the triad of information security, as we have discussed in our past work [34], referring to the original definitions described in the literature [35], [36], which are often overlooked in QKDs except [37].

In our past work [34], quaternary (more generally, p-ary with $p \geq 3$) Y00 protocols with scrambling the signal positions corresponding message bits can prevent Eve from forging messages even by KPAs. Hence, the message integrity is also realized by adding conventional hash-values of the message, such as SHA or even MD5. The message integrity cannot be equipped on malleable stream ciphers, including OTP and even ordinary Y00 protocols.

An example of the Y00 protocol with message integrity is as follows. Instead of a binary signal described in the previous section, Quaternary Y00 protocols use four signals $\{\left|\alpha[l_{(m,m')}(t) + z\cdot L]\right\rangle | z = 0, 1, 2, 3\}$, where the $4L$ signal level is determined as follows, instead of (8).

$$l_{(m,m')}(t) := \mathrm{Map}\left[s_m(t)\right] + L\cdot \mathrm{LT}(X, \Delta X)\,. \tag{10}$$

$$X := x(t) + \mathrm{Map}\left[s_m(t)\right] \bmod 4. \tag{11}$$

$$\Delta X := \Delta x_{m'}(t) \in \{0, 1, 2, 3, 4, 5\}. \tag{12}$$

Instead of the previous descriptions, $x(t)$ is a 2-bit plaintext, while $\Delta x_{m'}(t)$ is a 6-level additional pseudo-random number. LT$(X, \Delta X)$ is a look-up table shown in TABLE 1.

In this study, we use the above notations instead of the binary Y00 notations in Section II.D.

The previous work showed that Eve's success probability in obtaining the correct secret keys would rise as time passes [34]. However, Eve's success probability in breaching message integrity remains around 1/3 per signal on average because the legitimate users refresh the secret keys before Eve's success probability in obtaining the correct keys reaches $P_{\mathrm{Th}} \ll 1$ [11].

The above property is crucial to prevent impersonation using identifications and certification forging known by all users in a network, including Eve. Hence, the Y00 protocol with message integrity may be useful for key-refreshments [11] as well as ITS initial-key distribution [34] with ITS digital signature [38].

TABLE 1. Example of LT(X, ΔX) in (10) with (11) and (12).

LT	ΔX					
X	0	1	2	3	4	5
00	0	1	3	2	1	3
01	1	3	0	3	2	2
10	2	2	2	1	0	1
11	3	0	1	0	3	0

F. IMPORTANCE OF COLLECTIVE KPAS

Individual KPAs assume that Eve would discriminate γ^T -ary signals to find the correct keystream during an attack duration T with a masking size γ [7], that the number of signal levels under the quantum noise. However, what Eve requires based on KPAs is to search the correct secret keys in the key-space $|\{\boldsymbol{K}, \boldsymbol{\Delta K}\}|$, far less than γ^T searches, under Shannon's maxim as known as Kerckhoffs' principle. The assumption implies that Eve knows the transmitters' implementations; hence, Eve would find most likely signal sequences from noisy observations [11]. For example, under the assumptions that

$$\gamma := \left[(2\sigma_Q)/(\Delta A)\right]^d \sim 10. \tag{13}$$

$$T \sim (2^{|\{\boldsymbol{K},\boldsymbol{\Delta K}\}|} - 1)(\log_2 L)^{-1}. \tag{14}$$

$$L \sim 2048. \tag{15}$$

$$|\{\boldsymbol{K}, \boldsymbol{\Delta K}\}| \sim 2^{512}. \tag{16}$$

Here, σ_Q is the standard deviation of the Y00 noise, $\boldsymbol{\Delta} A$ is the signal distance. The parameter $d = 1$ for intensity-shift keying (ISK), amplitude-shift keying (ASK), and phase-shift keying (PSK), while $d = 2$ for quadrature-amplitude modulations (QAM).

Then, Eve's success probabilities in obtaining the correct keys based on her error rate are, by order-of-magnitudes,

$$\gamma^{-T} \sim 2^{-4.0\times 10^{153}} \ll |\{\boldsymbol{K}, \boldsymbol{\Delta K}\}|^{-1} \sim 2^{-512}. \tag{17}$$

Hence, individual KPAs over-estimate the security level of Y00 transmitters. Another reason is given in Section V.B.

The importance of collective KPAs is as follows. Suppose that almost all network users, including Eve, can access the same data set, such as OS upgrades, an original image of the OS, broadcasting, or highly qualified multimedia. For example, today's data transmissions of OS upgrading or multimedia in a Blu-ray disc are of the order of $10^9 \sim 10^{11}$ bytes. These data sizes increase as we have more network capacities. Thus, sufficiently long collective KPAs are realistically possible. Another importance of collective KPAs is that it would make the security evaluations easier because the Y00 signal sequence becomes periodic thanks to the transmitters' PRNGs [33].

III. THEORETICAL FRAMEWORKS

This section describes the Y00 security evaluation with concrete formulations based on time-translational symmetry, originating from the M-sequences' property. Section III.A. overview of our security evaluation strategy. Then, Section III.B and Section III.C formulate the time-translational properties of the Y00 signals.

A. OVERVIEW OF ANALYSES STRATEGY

In the following sections, we omit the plaintext $\boldsymbol{x}$ because we consider only the case of KPA unless it must be written.

Suppose that $\boldsymbol{k}_m$ is variable while $\boldsymbol{\Delta k}_{m'}$ is fixed for the simplicity of the discussions. Because most Y00 systems utilize PRNGs with M-sequence [25], the Y00 signal sequences have a time-translational symmetry as in FIGURE 1; at the specific periods, the inner state of the PRNGs reproduce the same states given by other initial keys $(\boldsymbol{k}_m, \boldsymbol{\Delta k}_{m'})$. We write the initial keys $(\boldsymbol{k}_m, \boldsymbol{\Delta k}_{m'})$ as (m, m').

FIGURE 2 illustrates how quantum signals evolve as time passes. Assume that the correct signal sequence is $\left|\boldsymbol{\alpha}(m, m')\right\rangle$ and the nearest-neighbor states $\left|\boldsymbol{\alpha}(m \pm n, m' \pm n')\right\rangle$ under $m \pm n \bmod |\{\boldsymbol{\Delta K}\}|$ and $m' \pm n' \bmod |\{\boldsymbol{K}\}|$, which is discussed in Section III.C. Then, Eve must discriminate the signal sequence $\left|\boldsymbol{\alpha}(m, m')\right\rangle$ from others by setting two boundaries $\boldsymbol{\alpha}_{\,\mathrm{B}\pm,\pm}(m, m')$ between $\left|\boldsymbol{\alpha}(m, m')\right\rangle$ and $\left|\boldsymbol{\alpha}(m \pm n, m' \pm n')\right\rangle$, and two boundaries $\boldsymbol{\alpha}_{\,\mathrm{B}\pm,\mp}(m, m')$ between $\left|\boldsymbol{\alpha}(m, m')\right\rangle$ and $\left|\boldsymbol{\alpha}(m \pm n, m' \mp n')\right\rangle$, respectively. Eve's detection domain $D(m, m')$ described in Section IV.B must be within these four boundaries.

B. TIME-TRANSLATIONAL SYMMETRY OF Y00 SIGNALS

This section investigates the property of a time-translational operator U and V under modulo $|\{\boldsymbol{K}\}|$ and $|\{\boldsymbol{\Delta K}\}|$, respectively.

For a fixed $\boldsymbol{\Delta k}_{m'}$, the operator U works as follows.

$$U \left|\boldsymbol{\alpha}(m, m')\right\rangle = \left|\boldsymbol{\alpha}(m+1, m')\right\rangle. \tag{18}$$

Furthermore, the properties of the conjugate operator $U^\dagger$ are,

$$\left\langle\boldsymbol{\alpha}(m, m')\right| U^\dagger = \left\langle\boldsymbol{\alpha}(m+1, m')\right|. \tag{19}$$

Hence,

$$\begin{aligned}\left\langle\boldsymbol{\alpha}(m, m')\right| U^\dagger U \left|\boldsymbol{\alpha}(m, m')\right\rangle &= \left\langle\boldsymbol{\alpha}(m+1, m')\right| \boldsymbol{\alpha}(m+1, m')\big\rangle \\ &= \left\langle\boldsymbol{\alpha}(m, m')\right| \boldsymbol{\alpha}(m, m')\big\rangle. \end{aligned}\tag{20}$$

$$\therefore U^\dagger U = I. \tag{21}$$

The property (21) indicates that U is a unitary operator. Therefore,

$$\left|\boldsymbol{\alpha}(m, m')\right\rangle = U^m \left|\boldsymbol{\alpha}(0, m')\right\rangle. \tag{22}$$

Furthermore, (22) means U must be cyclic as follows.

$$U^{|\{\boldsymbol{K}\}|} = I. \tag{23}$$

Hence,

$$U^{|\{\boldsymbol{K}\}|-1} = U^\dagger U U^{|\{\boldsymbol{K}\}|-1} = U^\dagger I. \tag{24}$$

The result (24) means that the $U^\dagger$ is a reversal time-translational operator as follows.

$$U^\dagger \left|\boldsymbol{\alpha}(m, m')\right\rangle = \left|\boldsymbol{\alpha}(m-1, m')\right\rangle. \tag{25}$$

In a similar manner to (18)–(25), the operator V works as follows.

$$V \left|\boldsymbol{\alpha}(m, m')\right\rangle = \left|\boldsymbol{\alpha}(m, m'+1)\right\rangle. \tag{26}$$

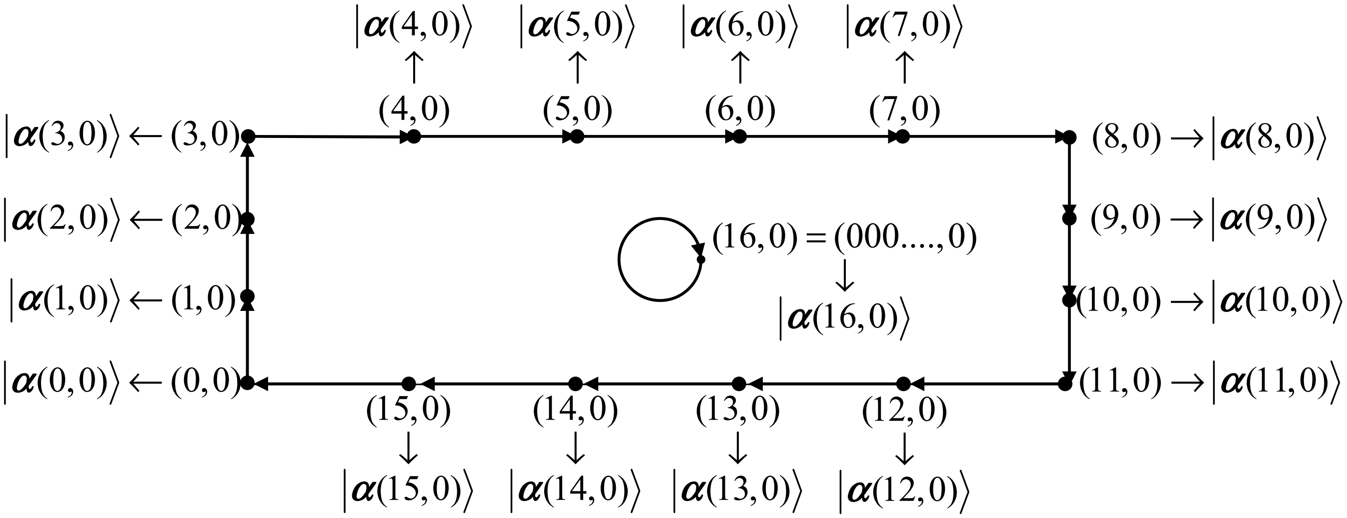

FIGURE 1. A schematic picture of correspondence between a PRNG's internal state in Y00 transmitters and the generated quantum states. In this figure, $|\{K\}| = 16$ and Δk are fixed to Δk_0. However, typically $|\{K\}| = |\{\Delta K\}| = 2^{128} - 1$ or $2^{256} - 1$.

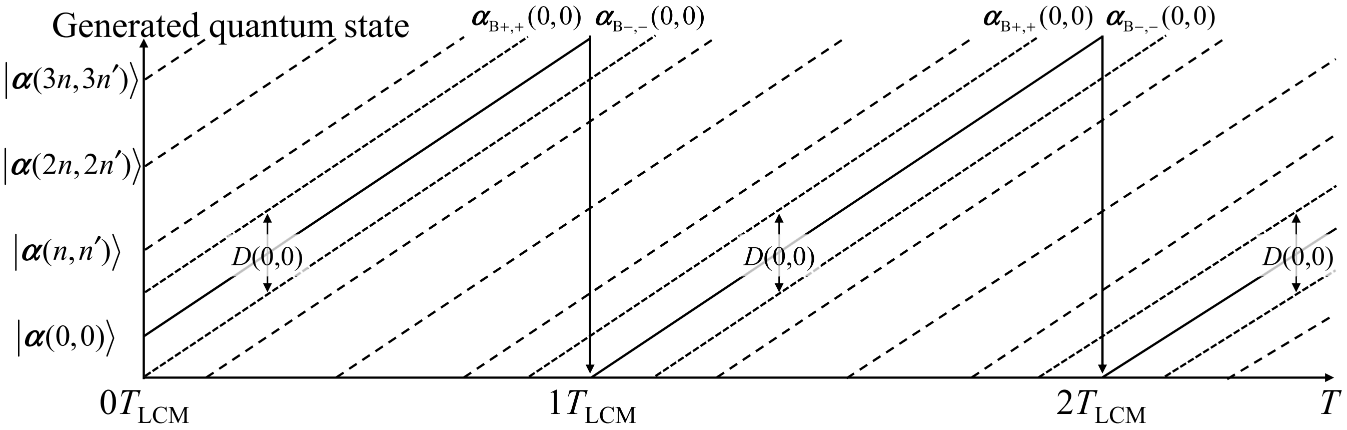

FIGURE 2. A schematic view of the boundaries to discriminate the quantum states and the integration domain for Eve.

$$V^{|\{\Delta K\}|} = I. \tag{27}$$

Therefore, V is also a unitary operator with similar properties U has. Note that U and V commute.

From the properties of U and V, there exists $\left|\alpha'\right\rangle$ corresponding to arbitral $|\alpha\rangle$ such that

$$\left|\alpha'\right\rangle := U^n V^{n'} |\alpha\rangle . \tag{28}$$

It is merely because U and V are the time-translational unitary operators. For instance, the following equation is satisfied by merely exchanging the series of the components of $|\alpha\rangle$.

$$\left|\langle\alpha|\, V^{\dagger n'} U^{\dagger n} U^n V^{n'} \,|\alpha\rangle\right| = \left|\left\langle\alpha' \mid \alpha'\right\rangle\right| = |\langle\alpha \mid \alpha\rangle| . \tag{29}$$

C. NEAREST-NEIGHBOR STATES

To determine the thresholds between signals in FIGURE 2, we must define "nearest-neighbor states" to an arbitral $\left|\alpha(m, m')\right\rangle$ by fidelity. Suppose that $\left|\alpha(n, n')\right\rangle$ is the nearest-neighbor state to $|\alpha(0, 0)\rangle$. Then,

$$\left|\left\langle\alpha(n, n') \mid \alpha(0, 0)\right\rangle\right| := \max_{(m,m')\neq(0,0)} \left|\left\langle\alpha(m, m') \mid \alpha(0, 0)\right\rangle\right| . \tag{30}$$

Thanks to the time-translational symmetry in Section III.B, we obtain another nearest-neighbor state.

$$\begin{aligned}\left|\left\langle\alpha(n, n') \mid \alpha(0, 0)\right\rangle\right| &= \left|\left\langle\alpha(n, n')\right| U^n V^{n'} V^{\dagger n'} U^{\dagger n} \left|\alpha(0, 0)\right\rangle\right| \\ &= \left|\left\langle\alpha(0, 0) \mid \alpha(-n, -n')\right\rangle\right| .\end{aligned} \tag{31}$$

Hence, we are ready to derive $D(n, n')$ boundaries in Section IV, precisely formulated in Section IV.B.

The above result is generalized as follows.

$$\begin{aligned}&\left|\left\langle\alpha(n, n') \mid \alpha(0, 0)\right\rangle\right| \\ &\quad = \left|\left\langle\alpha(n, n')\right| V^{\dagger\pm m} U^{\dagger\pm m'} U^{\pm m} V^{\pm m'} \left|\alpha(0, 0)\right\rangle\right| \\ &\quad = \left|\left\langle\alpha(n \pm m, n' \pm m') \mid \alpha(m, m')\right\rangle\right| . \\ &\left|\left\langle\alpha(n, n') \mid \alpha(0, 0)\right\rangle\right|\end{aligned} \tag{32}$$

$$
\begin{aligned}
&= \left| \left\langle \boldsymbol{\alpha}(n,n') \right| V^{\dagger\mp m} U^{\dagger\pm m'} U^{\pm m} V^{\mp m'} \left| \boldsymbol{\alpha}(0,0) \right\rangle \right| \\
&= \left| \left\langle \boldsymbol{\alpha}(n \pm m, n' \mp m') \right. \left| \boldsymbol{\alpha}(m,m') \right\rangle \right| . \qquad (33)\\
&\quad \text{For } \left(n \pm m \bmod |\{\boldsymbol{K}\}| \,, n' \pm m' \bmod |\{\boldsymbol{\Delta K}\}|\right) \\
&\quad \text{and } \left(n \pm m \bmod |\{\boldsymbol{K}\}| \,, n' \mp m' \bmod |\{\boldsymbol{\Delta K}\}|\right) . \qquad (34)
\end{aligned}
$$

Therefore, $\left|\boldsymbol{\alpha}(m,m')\right\rangle$ has four nearest-neighbor states; $\left|\boldsymbol{\alpha}(m \pm n, m' \pm n')\right\rangle$ and $\left|\boldsymbol{\alpha}(m \pm n, m' \mp n')\right\rangle$. Here, (n, n') depends on the implementation parameters in (10).

However, note that all states cyclically appear as nearest-neighbor states under U and V if $|\{\boldsymbol{K}\}|$ is coprime of n while $|\{\boldsymbol{\Delta K}\}|$ is also coprime of n'. Especially if both of $|\{\boldsymbol{K}\}|$ and $|\{\boldsymbol{\Delta K}\}|$ are prime numbers, all states appear under time-translational operations no matter what (n, n') is.

IV. THEORETICAL SECURITY EVALUATIONS

This section describes the principles of the Y00 protocol with and without true-random deliberate signal randomization (TR-DSR), using the quantum detection theory [31]–[33].

A. OPTIMAL MEASUREMENT UNDER BAYES' CRITERION

As the previous work derived [11], we suppose that Eve launches KPA of unlimited duration. Hence, she stores the signals into her quantum memory from the beam splitter in Section II.D.

The necessary-and-sufficient conditions to optimize Eve's average success probability with her measurement operators $\{M_{\mathrm{E}}(m,m')\}$ are [31]–[33] (refer equation (50) in [32], and set the cost coefficients as $C_{ij} = -\delta_{ij}$)

$$
\begin{aligned}
&\sum\nolimits_{(m,m') \in \{\boldsymbol{K}, \boldsymbol{\Delta K}\}} M_{\mathrm{E}}(m,m') \\
&\quad = I. \qquad (35)\\
W(m,m') &:= -\sum\nolimits_{(n,n') \in \{\boldsymbol{K}, \boldsymbol{\Delta K}\}} \delta_{n,m}\delta_{n',m'} \Pr(m,m')\rho_{\mathrm{E}}(n,n') \\
&\quad = -\Pr(m,m')\rho_{\mathrm{E}}(m,m') \qquad (36)\\
&M_{\mathrm{E}}(n,n')\left[W(m,m') - W(n,n')\right] M_{\mathrm{E}}(m,m') \\
&\quad = \mathbf{0}. \qquad (37)\\
&W(m,m') - \Gamma \\
&\quad \geqslant \mathbf{0}. \qquad (38)\\
&\Gamma := \sum\nolimits_{(m,m') \in \{\boldsymbol{K}, \boldsymbol{\Delta K}\}} M_{\mathrm{E}}(m,m') W(m,m') \\
&\quad = \sum\nolimits_{(m,m') \in \{\boldsymbol{K}, \boldsymbol{\Delta K}\}} W(m,m') M_{\mathrm{E}}(m,m'). \qquad (39)
\end{aligned}
$$

The following value is Eve's expected success probability of obtaining the correct (m, m').

$$
\mathrm{Ex}[\Pr(\mathrm{Success})] = -\operatorname{tr}\Gamma. \qquad (40)
$$

B. CONFIDENTIALITY OF SHARED KEYS WITHOUT TR-DSR

From the discussions in Section III.A, $\{M_{\mathrm{E}}(m,m')\}$ must satisfy

$$
\begin{aligned}
\rho_{\mathrm{E}}(m,m') &:= \left|\boldsymbol{\alpha}_{\mathrm{E}}(m,m')\right\rangle\left\langle\boldsymbol{\alpha}_{\mathrm{E}}(m,m')\right| . \qquad (41)\\
&V^{\dagger m'} U^{\dagger m} M_{\mathrm{E}}(n,n') U^{m} V^{m'} \\
&\quad \cdot \left[W(0,0) - W(n-m, n'-m')\right] \\
&\quad \cdot V^{\dagger m'} U^{\dagger m} M_{\mathrm{E}}(m,m') U^{m} V^{m'} = 0. \qquad (42)
\end{aligned}
$$

If $\{M_{\mathrm{E}}(m,m')\}$ is time-translational symmetric, (42) is automatically satisfied. The following formulation of $\{M_{\mathrm{E}}(m,m')\}$ satisfies the requirement with an over-completeness factor [17],

$$
M_{\mathrm{E}}(m,m') := \int_{\boldsymbol{\alpha} \in D(m,m')} (\boldsymbol{d} \cdot \boldsymbol{\alpha})\, \pi^{-N \cdot T_{\mathrm{LCM}}} \left|\boldsymbol{\alpha}\right\rangle \left\langle\boldsymbol{\alpha}\right| . \qquad (43)
$$

$$
(\boldsymbol{d} \cdot \boldsymbol{\alpha}) := \prod\nolimits_{t=1}^{N \cdot T_{\mathrm{LCM}}} d\alpha(t). \qquad (44)
$$

Here, (44) is a shorthand notation to perform the integral (43).

At the boundaries between $D(m, m')$ and $D(m \pm n, m' \pm n')$, the following equality must be satisfied.

$$
\boldsymbol{\alpha} = \boldsymbol{\alpha}' = \boldsymbol{\alpha}_{\mathrm{B}\pm,\pm}(m,m'). \qquad (45)
$$

Hence,

$$
\begin{aligned}
&\Pr(m \pm n, m' \pm n') \left\langle \boldsymbol{\alpha}_{\mathrm{E}}(m,m') + \boldsymbol{\alpha} \right| \left. \boldsymbol{\alpha}_{\mathrm{E}}(m \pm n, m' \pm n') \right\rangle \\
&\quad \cdot \left\langle \boldsymbol{\alpha}_{\mathrm{E}}(m \pm n, m' \pm n') \right. \left| \boldsymbol{\alpha}_{\mathrm{E}}(m \pm n, m' \pm n') + \boldsymbol{\alpha} \right\rangle \\
&= \Pr(m,m') \left\langle \boldsymbol{\alpha}_{\mathrm{E}}(m,m') + \boldsymbol{\alpha} \right| \left. \boldsymbol{\alpha}_{\mathrm{E}}(m,m') \right\rangle \\
&\quad \cdot \left\langle \boldsymbol{\alpha}_{\mathrm{E}}(m,m') \right. \left| \boldsymbol{\alpha}_{\mathrm{E}}(m \pm n, m' \pm n') + \boldsymbol{\alpha} \right\rangle . \qquad (46)
\end{aligned}
$$

From the properties of coherent states, (47)–(49) are satisfied.

$$
\begin{aligned}
\left\langle \boldsymbol{\alpha} \right| \left. \boldsymbol{\alpha}' \right\rangle &= \exp\left[\boldsymbol{\alpha}'\boldsymbol{\alpha}^{\dagger} - \frac{1}{2}|\boldsymbol{\alpha}|^2 - \frac{1}{2}\left|\boldsymbol{\alpha}'\right|^2\right] \\
&= \exp\left[\frac{1}{2}\boldsymbol{\alpha}'\boldsymbol{\alpha}^{\dagger} - \frac{1}{2}\boldsymbol{\alpha}\boldsymbol{\alpha}'^{\dagger} - \frac{1}{2}\left|\boldsymbol{\alpha} - \boldsymbol{\alpha}'\right|^2\right]. \qquad (47)\\
\left|\left\langle \boldsymbol{\alpha} \right| \left. \boldsymbol{\alpha}' \right\rangle\right| &= \exp\left[-\frac{1}{2}\left|\boldsymbol{\alpha} - \boldsymbol{\alpha}'\right|^2\right]. \qquad (48)\\
\boldsymbol{\alpha} &:= (\boldsymbol{\alpha}(1), \boldsymbol{\alpha}(2), \boldsymbol{\alpha}(3), \ldots, \boldsymbol{\alpha}(N \cdot T_{\mathrm{LCM}})) . \qquad (49)
\end{aligned}
$$

Substituting (47)–(49) into (46), then, calculate the $\log_e$ of the result. Thus, (50) is derived.

$$
\begin{aligned}
&\ln\left[\Pr(m \pm n, m' \pm n')/\Pr(m,m')\right] \\
&= \boldsymbol{\alpha}_{\mathrm{E}}(m,m')\boldsymbol{\alpha}_{\mathrm{B}\pm,\pm}(m,m')^{\dagger} + \boldsymbol{\alpha}_{\mathrm{B}\pm,\pm}(m,m')\boldsymbol{\alpha}_{\mathrm{E}}(m,m')^{\dagger} \\
&- \frac{1}{2}\left|\boldsymbol{\alpha}_{\mathrm{E}}(m,m')\right|^2 - \frac{1}{2}\left|\boldsymbol{\alpha}_{\mathrm{B}\pm,\pm}(m,m')\right|^2 \\
&- \boldsymbol{\alpha}_{\mathrm{E}}(m \pm n, m' \pm n')\boldsymbol{\alpha}_{\mathrm{B}\pm,\pm}(m,m')^{\dagger} \\
&- \boldsymbol{\alpha}_{\mathrm{B}\pm,\pm}(m,m')\boldsymbol{\alpha}_{\mathrm{E}}(m \pm n, m' \pm n')^{\dagger} \\
&+ \frac{1}{2}\left|\boldsymbol{\alpha}_{\mathrm{E}}(m \pm n, m' \pm n')\right|^2 + \frac{1}{2}\left|\boldsymbol{\alpha}_{\mathrm{B}\pm,\pm}(m,m')\right|^2. \qquad (50)
\end{aligned}
$$

The time-translational operations and (49) implies,

$$
\left|\boldsymbol{\alpha}_{\mathrm{E}}(m,m')\right|^2 = \left|\boldsymbol{\alpha}_{\mathrm{E}}(m \pm n, m' \pm n')\right|^2. \qquad (51)
$$

Hence, we obtain,

$$
\begin{aligned}
&\ln\left[\Pr(m \pm n, m' \pm n')/\Pr(m,m')\right] \\
&= \left[\boldsymbol{\alpha}_{\mathrm{E}}(m,m') - \boldsymbol{\alpha}_{\mathrm{E}}(m \pm n, m' \pm n')\right]\boldsymbol{\alpha}_{\mathrm{B}\pm,\pm}(m,m')^{\dagger} \\
&+ \boldsymbol{\alpha}_{\mathrm{B}\pm,\pm}(m,m')\left[\boldsymbol{\alpha}_{\mathrm{E}}(m,m') - \boldsymbol{\alpha}_{\mathrm{E}}(m \pm n, m' \pm n')\right]^{\dagger}.
\end{aligned}
\qquad (52)
$$

Therefore, the boundary conditions are as follows, with an arbitral real number b.

$$\boldsymbol{\alpha}_{\mathrm{B}\pm,\pm}(m, m') = \frac{\ln\left[\Pr(m \pm n, m' \pm n')/\Pr(m, m')\right]}{2[\boldsymbol{\alpha}_{\mathrm{E}}(m \pm n, m' \pm n') - \boldsymbol{\alpha}_{\mathrm{E}}(m, m')]^{\dagger}} + \frac{b}{2}\left[\boldsymbol{\alpha}_{\mathrm{E}}(m \pm n, m' \pm n') + \boldsymbol{\alpha}_{\mathrm{E}}(m, m')\right]. \tag{53}$$

$$\boldsymbol{\alpha}_{\mathrm{B}\pm,\mp}(m, m') = \frac{\ln\left[\Pr(m \pm n, m' \mp n')/\Pr(m, m')\right]}{2[\boldsymbol{\alpha}_{\mathrm{E}}(m \pm n, m' \mp n') - \boldsymbol{\alpha}_{\mathrm{E}}(m, m')]^{\dagger}} + \frac{b}{2}\left[\boldsymbol{\alpha}_{\mathrm{E}}(m \pm n, m' \mp n') + \boldsymbol{\alpha}_{\mathrm{E}}(m, m')\right]. \tag{54}$$

When all the prior probabilities are equal, the boundaries (53) and (54) fit our intuition; see [40].

Thus, we obtained the boundaries $\boldsymbol{\alpha}_{\mathrm{B}\pm,\pm}(m, m')$ and $\boldsymbol{\alpha}_{\mathrm{B}\pm,\mp}(m, m')$ in which $D(m, m')$ in (43) exists. Therefore, Eve's optimal measurement operators $\{M_{\mathrm{E}}(m, m')\}$ satisfies (55) as follows.

$$\begin{aligned}&\sum\nolimits_{(m,m')\in\{\boldsymbol{K},\boldsymbol{\Delta K}\}} M_{\mathrm{E}}(m, m')\\ &= \sum\nolimits_{(m,m')\in\{\boldsymbol{K},\boldsymbol{\Delta K}\}} \int_{\boldsymbol{\alpha}\in D(m,m')} (\boldsymbol{d}\cdot\boldsymbol{\alpha})\, \pi^{-N\cdot T_{\mathrm{LCM}}} \left|\boldsymbol{\alpha}\right\rangle \left\langle\boldsymbol{\alpha}\right|\\ &= I.\end{aligned} \tag{55}$$

Eve's success probability for an individual (m, m') case is

$$\begin{aligned}&\Pr\left(m, m'|m, m', x\right)\\ &= \int_{\boldsymbol{\alpha}\in D(m,m')} (\boldsymbol{d}\cdot\boldsymbol{\alpha})\, \pi^{-N\cdot T_{\mathrm{LCM}}} \exp\left[-\left|\boldsymbol{\alpha}-\boldsymbol{\alpha}_{\mathrm{E}}(m, m')\right|^{2}\right]\\ &< 1.\end{aligned} \tag{56}$$

Eve's expected success probability (40) is rewritten as

$$-\operatorname{tr}\Gamma = \sum\nolimits_{(m,m')\in\{\boldsymbol{K},\boldsymbol{\Delta K}\}} \Pr(m, m') \Pr\left(m, m'|m, m', \boldsymbol{x}\right) < 1. \tag{57}$$

Therefore, we can conclude that Eve's success probability of her attacks strongly depends on the area of $D(m, m')$; as the area becomes narrower, securer the Y00 transmitters would be.

Note that $D(m, m')$ still depends on the transmitters' implementations because of (10)–(12); however, now we have a solution to derive Eve's success probabilities once the Y00 transmitters are designed.

Moreover, if we rewrite (56) by decomposing the vector notations of the signal series every T_{LCM} round as follows,

$$\begin{aligned}\Pr\left(m, m'|m, m', x\right) &= \pi^{-N\cdot T_{\mathrm{LCM}}}\\ &\times \int_{\substack{\boldsymbol{\alpha}_{T_{\mathrm{LCM}}}\\ \in D(m,m')}} \left(\boldsymbol{d}\cdot\boldsymbol{\alpha}_{T_{\mathrm{LCM}}}\right) \exp\left[-N\left|\boldsymbol{\alpha}_{T_{\mathrm{LCM}}}\right.\right.\\ &\left.\left. - \boldsymbol{\alpha}_{\mathrm{E}}(m, m')_{T_{\mathrm{LCM}}}\right|^{2}\right].\end{aligned} \tag{58}$$

The above result immediately indicates that a two-dimensional Gaussian distribution in the integral has a variance of $(2N)^{-1}$. Hence, the variance decreases as N increases, as illustrated in our past work [39].

C. CONFIDENTIALITY OF SHARED KEYS WITH TR-DSR

When we apply TR-DSR, the Y00 signals are described by mixed states. (59) represents a discrete TR-DSR modulation while (60) describes the continuous modulation.

$$\begin{aligned}\rho_{\mathrm{E}}(m, m') &:= \sum\nolimits_{\boldsymbol{\alpha}'_{\mathrm{E}}\in\{\eta_{\mathrm{E}}\boldsymbol{\alpha}_{\mathrm{DSR}}\}} \Pr(\boldsymbol{\alpha}'_{\mathrm{E}}) \left|\boldsymbol{\alpha}_{\mathrm{E}}(m, m')\right.\\ &\left. + \boldsymbol{\alpha}'_{\mathrm{E}}\right\rangle \left\langle \boldsymbol{\alpha}_{\mathrm{E}}(m, m') + \boldsymbol{\alpha}'_{\mathrm{E}}\right|.\end{aligned} \tag{59}$$

$$\begin{aligned}\rho_{\mathrm{E}}(m, m') &:= \int_{\boldsymbol{\alpha}'_{\mathrm{E}}\in\{\eta_{\mathrm{E}}\boldsymbol{\alpha}_{\mathrm{DSR}}\}} \left(\boldsymbol{d}\cdot\boldsymbol{\alpha}'_{\mathrm{E}}\right) \Pr(\boldsymbol{\alpha}'_{\mathrm{E}}) \left|\boldsymbol{\alpha}_{\mathrm{E}}(m, m')\right.\\ &\left. + \boldsymbol{\alpha}'_{\mathrm{E}}\right\rangle \left\langle \boldsymbol{\alpha}_{\mathrm{E}}(m, m') + \boldsymbol{\alpha}'_{\mathrm{E}}\right|.\end{aligned} \tag{60}$$

For high-rate true-random number generation, laser chaos is proposed; they achieved 650 Gbps [41]. To derive the boundaries for the mixed states above, we must solve (37) similarly in Section IV.B. However, there are no analytical solutions to derive the boundaries. Hence, we continue our discussions, assuming we have obtained the boundaries by numerical analyses.

Once we obtain the boundaries $\boldsymbol{\alpha}_{\mathrm{B}\pm,\pm}(m, m')$ and $\boldsymbol{\alpha}_{\mathrm{B}\pm,\mp}(m, m')$ to determine $D(m, m')$ with (60), by similar calculations to (56) and (57),

$$\begin{aligned}&\Pr\left(m, m'|m, m', \boldsymbol{x}\right)\\ &= \pi^{-N\cdot T_{\mathrm{LCM}}}\\ &\times \iint_{\substack{\boldsymbol{\alpha}\in D(m,m')\\ \boldsymbol{\alpha}'_{\mathrm{E}}\in\{\eta_{\mathrm{E}}\boldsymbol{\alpha}_{\mathrm{DSR}}\}}} \Pr(\boldsymbol{\alpha}'_{\mathrm{E}}) \exp\left[-\left|\boldsymbol{\alpha}\right.\right.\\ &\left.\left. - \boldsymbol{\alpha}_{\mathrm{E}}(m, m') - \boldsymbol{\alpha}'_{\mathrm{E}}\right|^{2}\right] (\boldsymbol{d}\cdot\boldsymbol{\alpha}) \left(\boldsymbol{d}\cdot\boldsymbol{\alpha}'_{\mathrm{E}}\right).\end{aligned} \tag{61}$$

$$-\operatorname{tr}\Gamma = \sum\nolimits_{(m,m')\in\{\boldsymbol{K},\boldsymbol{\Delta K}\}} \Pr(m, m') \Pr\left(m, m'|m, m', \boldsymbol{x}\right). \tag{62}$$

D. MESSAGE INTEGRITY

The confidentiality threshold P_{Th} must upper-bound Eve's success probability of obtaining the correct shared keys to refresh the shared keys described in our previous work [11]. In the key-refreshment process and the initial key-agreement process [34], the message integrity must be guaranteed.

Suppose that Eve launches a man-in-the-middle (MITM) attack between Alice and Bob based on a fully (or partly) known-plaintext attack. When she successfully captures the correct key with a probability of $\Pr\left(m, m'|m, m', \boldsymbol{x}\right) < P_{\mathrm{Th}}$, she can forge a message perfectly; otherwise, she fails in forging with a probability of 1/3 per signal on average [34].

In the above situation, Eve's success probability in alternating $\boldsymbol{x}$ into $\boldsymbol{x}_{\mathrm{E}}$ is when Eve could obtain the correct keys. Otherwise, she fails in alternating. Hence,

$$\begin{aligned}&\Pr\left(x_{\mathrm{E}}|m, m'\right)\\ &= \sum\nolimits_{(m_{\mathrm{E}},m'_{\mathrm{E}})} \Pr\left(x_{\mathrm{E}}, m_{\mathrm{E}}, m'_{\mathrm{E}}|m, m'\right)\end{aligned}$$

$$
\begin{aligned}
&= 1 \times \Pr\left(m, m'|m, m'\right) \\
&\quad + \sum\nolimits_{\substack{l(m_{\mathrm{E}}, m'_{\mathrm{E}}) \\ \neq (m,m')}} \Pr\left(x_{\mathrm{E}}|m_{\mathrm{E}}, m'_{\mathrm{E}}, m, m'\right) \\
&\quad \times \Pr\left(m_{\mathrm{E}}, m'_{\mathrm{E}}|m, m'\right). \qquad (63)
\end{aligned}
$$

Denote the numbers of non-zero parts in $(\boldsymbol{x} - \boldsymbol{x}_{\mathrm{E}})$ mod 4 as $d(\boldsymbol{x}_{\mathrm{E}}, \boldsymbol{x})$, including the hash value of $\boldsymbol{x}$. Hence, when the hash value length is $h(\boldsymbol{x})$,

$$
d(\boldsymbol{x}_{\mathrm{E}}, \boldsymbol{x}) \geqslant h(\boldsymbol{x}) + 1. \qquad (64)
$$

By a similar application of Markov inequality in Section V.C of [19], Eve's success probability in alternating $\boldsymbol{x}$ into $\boldsymbol{x}_{\mathrm{E}}$ is upper-bounded as follows.

$$
\begin{aligned}
&\Pr\left(\boldsymbol{x}_{\mathrm{E}}|m_{\mathrm{E}}, m'_{\mathrm{E}}, m, m'\right) \\
&\quad = \Pr\left[\left(\boldsymbol{x}_{\mathrm{E}}|m_{\mathrm{E}}, m'_{\mathrm{E}}, m, m'\right)\right| \\
&\qquad\quad \left.\Pr\left(\boldsymbol{x}_{\mathrm{E}}|m_{\mathrm{E}}, m'_{\mathrm{E}}, m, m'\right) \geqslant P_{\mathrm{In}}\right] \\
&\qquad \times \Pr\left[\Pr\left(\boldsymbol{x}_{\mathrm{E}}|m_{\mathrm{E}}, m'_{\mathrm{E}}, m, m'\right) \geqslant P_{\mathrm{In}}\right] \\
&\qquad + \Pr\left[\left(\boldsymbol{x}_{\mathrm{E}}|m_{\mathrm{E}}, m'_{\mathrm{E}}, m, m'\right)\right| \\
&\qquad\quad \left.\Pr\left(\boldsymbol{x}_{\mathrm{E}}|m_{\mathrm{E}}, m'_{\mathrm{E}}, m, m'\right) < P_{\mathrm{In}}\right] \\
&\qquad \times \Pr\left[\Pr\left(\boldsymbol{x}_{\mathrm{E}}|m_{\mathrm{E}}, m'_{\mathrm{E}}, m, m'\right) < P_{\mathrm{In}}\right]. \qquad (65)
\end{aligned}
$$

Hence,

$$
\begin{aligned}
&\Pr\left(\boldsymbol{x}_{\mathrm{E}}|m_{\mathrm{E}}, m'_{\mathrm{E}}, m, m'\right)_{(m_{\mathrm{E}}, m'_{\mathrm{E}}) \neq (m,m')} \\
&\quad < 1 \times \exp\left[-\left(h(\boldsymbol{x}) + 1\right) \ln 3\right] {P_{\mathrm{In}}}^{-1} + P_{\mathrm{In}} \times 1. \qquad (66)
\end{aligned}
$$

Thus, substituting $\Pr\left(m, m'|m, m', \boldsymbol{x}\right) < P_{\mathrm{Th}}$ and (65) into (66), the upper-bound is

$$
\Pr\left(\boldsymbol{x}_{\mathrm{E}}|m, m'\right) < P_{\mathrm{Th}} + \exp\left[-\left(h(\boldsymbol{x}) + 1\right) \ln 3\right] {P_{\mathrm{In}}}^{-1} + P_{\mathrm{In}}. \qquad (67)
$$

More precisely, this is because Eve's success probability in alternating is

$$
\begin{aligned}
&\Pr\left[\Pr\left(\boldsymbol{x}_{\mathrm{E}}|m_{\mathrm{E}}, m'_{\mathrm{E}}, m, m'\right)_{(m_{\mathrm{E}}, m'_{\mathrm{E}}) \neq (m,m')} \geqslant P_{\mathrm{In}}\right] \\
&\quad \times \Pr\left[\left(\boldsymbol{x}_{\mathrm{E}}|m_{\mathrm{E}}, m'_{\mathrm{E}}, m, m'\right)\right| \\
&\qquad \left.\Pr\left(\boldsymbol{x}_{\mathrm{E}}|m_{\mathrm{E}}, m'_{\mathrm{E}}, m, m'\right)_{(m_{\mathrm{E}}, m'_{\mathrm{E}}) \neq (m,m')} \geqslant P_{\mathrm{In}}\right] \\
&< {P_{\mathrm{In}}}^{-1} \operatorname{Ex}\left[\Pr\left(\boldsymbol{x}_{\mathrm{E}}|m_{\mathrm{E}}, m'_{\mathrm{E}}, m, m'\right)\right]_{(m_{\mathrm{E}}, m'_{\mathrm{E}}) \neq (m,m')} \times 1. \qquad (68)
\end{aligned}
$$

$$
\begin{aligned}
&\Pr\left[\Pr\left(\boldsymbol{x}_{\mathrm{E}}|m_{\mathrm{E}}, m'_{\mathrm{E}}, m, m'\right)_{(m_{\mathrm{E}}, m'_{\mathrm{E}}) \neq (m,m')} < P_{\mathrm{In}}\right] \\
&\quad \times \Pr\left[\left(\boldsymbol{x}_{\mathrm{E}}|m_{\mathrm{E}}, m'_{\mathrm{E}}, m, m'\right)\right| \\
&\qquad \left.\Pr\left(x_{\mathrm{E}}|m_{\mathrm{E}}, m'_{\mathrm{E}}, m, m'\right)_{(m_{\mathrm{E}}, m'_{\mathrm{E}}) \neq (m,m')} < P_{\mathrm{In}}\right] \\
&< 1 \times P_{\mathrm{In}}. \qquad (69)
\end{aligned}
$$

To minimize the upper-bound,

$$
{P_{\mathrm{In}}}^{2} = \exp\left[-\left(h(\boldsymbol{x}) + 1\right) \ln 3\right]. \qquad (70)
$$

Hence, Eve's success probability in alternating the message is

$$
\Pr\left(\boldsymbol{x}_{\mathrm{E}}|m, m'\right) < P_{\mathrm{Th}} + 2 \exp\left[-\frac{1}{2}\left(h(\boldsymbol{x}) + 1\right) \ln 3\right]. \qquad (71)
$$

Therefore, the shared key's refreshment process must be performed while (71) is satisfied to guarantee the fresh keys' integrity [34].

V. CONNECTION BETWEEN PAST AND THIS WORK

Hence, the problem is how large Eve's average success probability and Eve's maximum success probability are and how long the breaching time is. This section describes how our previous result [11] is connected to the result of this work.

A. ESTIMATION OF BREACHING ROUND

We already have a result in the precious work as follows.

$$
\begin{aligned}
&\Pr\left(m, m'|m, m'\right) \\
&\quad \leqslant 1 - \left[1 - \Pr\left(m, m'\right)\right] \exp\left[-\left(N / N_{\mathrm{Breach}}\right) \ln 2\right]. \qquad (72)
\end{aligned}
$$

On the other hand, this study concluded (57). Hence, we obtain an inequality related to the breaching round N_{Breach}.

$$
1 / N_{\mathrm{Breach}} \geqslant N^{-1} \log_2 \left[\frac{1 - \Pr\left(m, m'\right)}{1 - \Pr\left(m, m'|m, m'\right)}\right]. \qquad (73)
$$

We also concluded in our previous work that the Y00 transmitters are non-ITS if $1/N_{\mathrm{Breach}} \geq 1$. Hence, we are now ready to confirm whether the given Y00 transmitter is ITS or not by substituting parameters in (73), which are given by numerical simulations based on (57) or (61).

B. ESTIMATION OF BREACHING ROUND BY INDIVIDUAL KPAS

Contrarily to the case of collective KPAs, individual KPAs estimate the breaching-round far longer. In this sense, we cannot say individual KPAs correctly evaluate the security level of Y00 transmitters.

The reason is as follows. In a similar manner in our previous work [11],

$$
\begin{aligned}
&1 - \Pr\left(m, m'|m, m'\right) \\
&\quad \leqslant \max\nolimits_{\{n(e|m,m')\} \in \Omega(m,m')^{\mathrm{C}}} \prod\nolimits_{e \in \{0,1\}^{|e|}} \Pr\left(e|m, m'\right)^{n(e|m,m')} \\
&\qquad \times \sum\nolimits_{\{n(e|m,m')\} \in \Omega(m,m')^{\mathrm{C}}} [N!] \prod\nolimits_{e \in \{0,1\}^{|e|}} \left[n(e|m, m')!\right]^{-1}. \qquad (74)
\end{aligned}
$$

Hence,

$$
\begin{aligned}
&\Pr\left(m, m'|m, m'\right) \\
&\quad \geqslant 1 - \left[1 - \Pr(m, m')\right] \exp\left[-\left(N / N_{\mathrm{Individual}}\right) \ln 2\right]. \qquad (75)
\end{aligned}
$$

$$
\begin{aligned}
&\left[1 - \Pr(m, m')\right] (2M)^{T} \\
&\quad = \sum\nolimits_{\{n(e|m,m')\} \in \Omega(m,m')^{\mathrm{C}}} [N!] \prod\nolimits_{e \in \{0,1\}^{|e|}} \left[n(e|m, m')!\right]^{-1}. \qquad (76)
\end{aligned}
$$

$$
\begin{aligned}
&1 / N_{\mathrm{Individual}} \\
&\quad := -\log_2 \left[(2M)^{T_{\mathrm{LCM}}} \max\nolimits_{e \in \{0,1\}^{|e|}} \Pr(e|m, m')\right] \\
&\quad > -\log_2 \left[(2M)^{T_{\mathrm{LCM}}} \Pr(\mathbf{0}|m, m')\right]. \qquad (77)
\end{aligned}
$$

Note that $\Pr(\mathbf{0}|m, m')$ is Eve's probability in obtaining error-free keystreams. Hence, the probability corresponds to Eve's success probability in obtaining the correct (m, m') by individual KPAs. The above result concludes that $N_{\text{Individual}} \geq N_{\text{Breach}}$ as follows.

$$\begin{aligned} 1/N_{\text{Breach}} &\geqslant N^{-1}\log_2\left[\frac{1-\Pr\left(m, m'\right)}{1-\Pr\left(m, m'|m, m'\right)}\right] \\ &> 1/N_{\text{Individual}}. \end{aligned} \tag{78}$$

Therefore, we recommend evaluating the security of Y00 transmitters under collective KPAs in the described procedure through Section III to Section V.

VI. FUTURE PERSPECTIVES

From the previous discussion, we showed the importance of evaluating the security of the Y00 transmitters under collective KPAs. This section discusses some future perspectives as challenging tasks for theorists in this field to accelerate the designing of securer Y00 transmitters.

A. ON EXPERIMENTAL EVALUATIONS

In the above discussions, we have shown how we evaluate the security of Y00 transmitters. This section briefly describes how we evaluate Y00 transmitters by experiments.

Thanks to the notation (49), we can decompose $D(m, m')$ boundaries (53) and (54) deriving boundaries in each timeslot. Hence, we can experimentally confirm how much noise is Y00 transmitters have outside of $D(m, m')$. However, the detectors' noise must be carefully subtracted because Eve's detector is supposed to be noiseless.

One possible problem is that deriving the boundaries of the $D(m, m')$ relies on numerical simulations, although it is not impossible. Therefore, more straightforward methods to derive them are expected.

B. THEORETICAL DIRECTIONS FOR BETTER TRANSMITTERS

This study showed how to evaluate given Y00 transmitters; however, it is still a severe problem to derive designs of better Y00 transmitters from the theory. If there could be theoretical formulations to give designs of the transmitters, the development would be accelerated.

It would also be better to equip cryptographically secure pseudo-random number generators in the Y00 transmitters to secure them. However, we cannot apply our theory in this study to such pseudo-random number generators that have no time-translational symmetry.

VII. CONCLUSION

In this work, we analytically described the security of the Y00 protocol, while we lacked in details of the measurement operators in our past works. By operating numerical simulations, we can now evaluate the security of designed Y00 transmitters thanks to the given measurement operators. However, an inverse problem is still a challenging task: how we design securer transmitters by theories. We hope more theorists would be interested in this field since the significant affinity of the Y00 protocol to the current broadband optical communication infrastructure has already been studied well.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, vol. 175, pp. 175–179, 1984.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, Dec. 2014, doi: 10.1016/j.tcs.2014.05.025.

[3] G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, "Secure communication using mesoscopic coherent states," *Phys. Rev. Lett.*, vol. 90, no. 22, Jun. 2003, Art. no. 227901. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a446503.pdf, doi: 10.1103/PhysRevLett.90.227901.

[4] H. P. Yuen, P. Kumar, E. Corndorf, and R. Nair, "Security of Y-00 and similar quantum cryptographic protocols," 2004, *arXiv:quant-ph/0407067*. [Online]. Available: https://arxiv.org/abs/quant-ph/0407067

[5] H. P. Yuen, "Physical cryptography: A new approach to key generation and direct encryption," Dept. Elect. Eng. Comput. Sci., Northwestern Univ., Evanston, IL, USA, Tech. Rep. AFRL-SR-AR-TR-10-0001, 2009. [Online]. Available: https://apps.dtic.mil/sti/pdfs/ADA512847.pdf

[6] H. P. Yuen, "Key generation: Foundations and a new quantum approach," *IEEE J. Sel. Topics Quantum Electron.*, vol. 15, no. 6, pp. 1630–1645, Nov./Dec. 2009, doi: 10.1109/JSTQE.2009.2025698.

[7] P. K. Verma, M. El Rifai, and K. W. C. Chan, "Secure communication based on quantum noise," in *Multi-Photon Quantum Secure Communication*. Singapore: Springer, 2019, pp. 85–95, doi: 10.1007/978-981-10-8618-2_4.

[8] S. Donnet, A. Thangaraj, M. Bloch, J. Cussey, J.-M. Merolla, and L. Larger, "Security of Y-00 under heterodyne measurement and fast correlation attack," *Phys. Lett. A*, vol. 356, no. 6, pp. 406–410, Aug. 2006, doi: 10.1016/j.physleta.2006.04.002.

[9] M. J. Mihaljevic, "Generic framework for the secure Yuen 2000 quantum-encryption protocol employing the wire-tap channel approach," *Phys. Rev. A, Gen. Phys.*, vol. 75, no. 5, May 2007, Art. no. 052334, doi: 10.1103/PhysRevA.75.052334.

[10] T. Shimizu, O. Hirota, and Y. Nagasako, "Running key mapping in a quantum stream cipher by the Yuen 2000 protocol," *Phys. Rev. A, Gen. Phys.*, vol. 77, no. 3, Mar. 2008, Art. no. 034305, doi: 10.1103/PhysRevA.77.034305.

[11] T. Iwakoshi, "Analysis of Y00 protocol under quantum generalization of a fast correlation attack: Toward information-theoretic security," *IEEE Access*, vol. 8, pp. 23417–23426, 2020, doi: 10.1109/ACCESS.2020.2969455.

[12] F. Futami, T. Kurosu, K. Tanizawa, K. Kato, S. Suda, and S. Namiki, "Dynamic routing of Y-00 quantum stream cipher in field-deployed dynamic optical path network," in *Proc. Opt. Fiber Commun. Conf.* Washington, DC, USA: Optical Society America, 2018, pp. Tu2G-5, doi: 10.1364/OFC.2018.Tu2G.5.

[13] K. Tanizawa and F. Futami, "Photonic generation of quantum noise assisted cipher at microwave frequencies for secure wireless links," in *Proc. Opt. Fiber Commun. Conf. (OFC)*. Washington, DC, USA: Optical Society America, 2020, pp. M4A-3, doi: 10.1364/OFC.2020.M4A.3.

[14] P. A. Tregubov and A. S. Trushechkin, "Quantum stream ciphers: Impossibility of unconditionally strong algorithms," *J. Math. Sci.*, vol. 252, no. 1, pp. 90–103, Jan. 2021, doi: 10.1007/s10958-020-05144-x.

[15] R. J. Glauber, "The quantum theory of optical coherence," *Phys. Rev.*, vol. 130, no. 6, p. 2529, 1963, doi: 10.1103/PhysRev.130.2529.

[16] E. C. G. Sudarshan, "Equivalence of semiclassical and quantum mechanical descriptions of statistical light beams," *Phys. Rev. Lett.*, vol. 10, no. 7, p. 277, 1963, doi: 10.1103/PhysRevLett.10.277.

[17] D. F. Walls and G. J. Milburn, *Quantum Optics*. Springer, 2007.

[18] H. P. Yuen, "Fundamental quantitative security in quantum key generation," *Phys. Rev. A, Gen. Phys.*, vol. 82, no. 6, Dec. 2010, Art. no. 062304, doi: 10.1103/PhysRevA.82.062304.

[19] H. P. Yuen, "Security of quantum key distribution," *IEEE Access*, vol. 4, pp. 724–749, 2016, doi: 10.1109/ACCESS.2016.2528227.

[20] M. Alimomeni and R. Safavi-Naini, "Guessing secrecy," in *Proc. Int. Conf. Inf. Theoretic Secur.* Berlin, Germany: Springer, 2012, pp. 1–13.

[21] I. Mitsugu and J. Shikata, "Information-theoretic security for encryption based on conditional Rényi entropies," in *Proc. Int. Conf. Inf. Theoretic Secur.* Cham, Switzerland: Springer, 2013, pp. 103–121.

[22] E. Biham, M. Boyer, G. Brassard, J. Van De Graaf, and T. Mor, "Security of quantum key distribution against all collective attacks," *Algorithmica*, vol. 34, no. 4, pp. 372–388, Nov. 2002, doi: 10.1007/s00453-002-0973-6.

[23] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x.

[24] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975, doi: 10.1002/j.1538-7305.1975.tb02040.x.

[25] L. Chen and G. Gong, *Communication System Security*. London, U.K.: Chapman & Hall/CRC, (2012).

[26] M. Matsumoto and T. Nishimura, "Mersenne twister: A 623-dimensionally equidistributed uniform pseudo-random number generator," *ACM Trans. Model. Comput. Simul.*, vol. 8, no. 1, pp. 3–30, Jan. 1998, doi: 10.1145/272991.272995.

[27] M. Saito and M. Matsumoto. *Tiny Mersenne Twister*. Accessed: Jun. 2011. [Online]. Available: http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/TINYMT/index.html

[28] K. Kato, "Enhancement of quantum noise effect by classical error control codes in the intensity shift keying Y-00 quantum stream cipher," *Proc. SPIE*, vol. 9225, Oct. 2014, Art. no. 922508, doi: 10.1117/12.2060631.

[29] F. Futami, K. Kato, and O. Hirota, "A novel transceiver of the Y-00 quantum stream cipher with the randomization technique for optical communication with higher security performance," *Proc. SPIE*, vol. 9980, Sep. 2016, Art. no. 99800O, doi: 10.1117/12.2237852.

[30] K. Kato, "Quantum enigma cipher as a generalization of the quantum stream cipher," *Proc. SPIE*, vol. 9980, Sep. 2016, Art. no. 998005, doi: 10.1117/12.2237570.

[31] H. Yuen, R. Kennedy, and M. Lax, "Optimum testing of multiple hypotheses in quantum detection theory," *IEEE Trans. Inf. Theory*, vol. IT-21, no. 2, pp. 125–134, Mar. 1975, doi: 10.1109/TIT.1975.1055351.

[32] C. W. Helstrom, "Quantum detection and estimation theory," *J. Stat. Phys.*, vol. 1, no. 2, pp. 231–252, 1969, doi: 10.1007/BF01007479.

[33] C. W. Helstrom, *Quantum Detection and Estimation Theory*, vol. 3, no. 1. New York, NY, USA: Academic, 1976, p. 1.

[34] T. Iwakoshi, "Message-falsification prevention with small quantum mask in quaternary Y00 protocol," *IEEE Access*, vol. 7, pp. 74482–74489, 2019, doi: 10.1109/ACCESS.2019.2921023.

[35] J. Hughes and G. Cybenko, "Quantitative metrics and risk assessment: The three tenets model of cybersecurity," *Technol. Innov. Manage. Rev.*, vol. 3, no. 8, pp. 15–24, Aug. 2013, doi: 10.22215/timreview/712.

[36] *Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary*, Standard ISO/IEC 27000:2018, Feb. 2018. [Online]. Available: https://www.iso.org/standard/73906.html

[37] T. Satoh, S. Nagayama, S. Suzuki, T. Matsuo, and R. Van Meter, "Attacking the quantum Internet," 2020, *arXiv:2005.04617*. [Online]. Available: http://arxiv.org/abs/2005.04617

[38] C. M. Swanson and D. R. Stinson, "Unconditionally secure signature schemes revisited," in *Proc. Int. Conf. Inf. Theoretic Secur.* Berlin, Germany: Springer, 2011, pp. 100–116, doi: 10.1007/978-3-642-20728-0_10.

[39] T. Iwakoshi, "Guessing probability under unlimited known-plaintext attack on secret keys for Y00 quantum stream cipher by quantum multiple hypotheses testing," *Proc. SPIE*, vol. 57, no. 12, 2018, Art. no. 126103, doi: 10.1117/1.OE.57.12.126103.

[40] H. L. Van Trees, K. L. Bell, and Z. Tian, *Detection, Estimation, and Modulation Theory, Part I: Detection, Estimation, And Linear Modulation Theory*, 2nd ed. Hoboken, NJ, USA: Wiley, 2004.

[41] L. Zhang, B. Pan, G. Chen, L. Guo, D. Lu, L. Zhao, and W. Wang, "640-Gbit/s fast physical random number generation using a broadband chaotic semiconductor laser," *Sci. Reports*, vol. 7, p. 45900, Apr. 2017, doi: 10.1038/srep45900.

TAKEHISA IWAKOSHI (Member, IEEE) received the B.S. degree in physics from Osaka University, Osaka, Japan, in 2001, and the M.S. degree in 2003. He joined the Hitachi Central Research Laboratory of Hitachi Inc., in April 2003. Then, he stayed in Semiconductor Leading Edge Technologies, Inc. from January 2007 to July 2008. He joined his current workplace, Quantum ICT Research Institute at Tamagawa University, in April 2011. Since July 2019, he joined Mie University to continue his studies.