Analysis of Y00 Protocol Under Quantum Generalization of a Fast Correlation Attack: Toward Information-Theoretic Security

TAKEHISA IWAKOSHI, (Member, IEEE)

Department of Information Engineering, Mie University, Tsu 514-8507, Japan

e-mail: iwakoshi@cs.info.mie-u.ac.jp

ABSTRACT In our previous work, it was demonstrated that the attacker could not pin-down the correct keys to start the Y00 protocol with a probability of one under the assistance of unlimitedly long known-plaintext attacks and optimal quantum measurements on the attacker's quantum memory. However, there were several assumptions that the Y00 system utilized linear-feedback shift registers as pseudo-random-number generators, and a fast correlation attack was disabled by irregular mapping on the Y00 systems. This study generalizes such an attack to remove the assumptions of the previous work. The framework of the security analyses of this study reiterates two well-known results from the past: (1) Y00 systems would be cryptanalyzed when the system is not designed well; (2) the system is possibly information-theoretically secure when the system is designed well, although the attacker's confidence in the correct key increases over time but the success probability of key recovery does not reach unity in finite time; (3) the breach probability of the shared keys increases with time. Hence, a key-refreshment procedure for the Y00 protocol is provided herein. Such security analyses are important not only in key refreshment but also in initial key agreement.

INDEX TERMS Information-theoretic security, optical network, quantum cryptography, quantum detection theory, secure communications.

I. INTRODUCTION

Since the first concept of quantum key distribution (QKD) was invented [1], [2], whether information-theoretically secure (ITS) communication is realizable using the laws of quantum physics is a topic that has garnered immense attention.

Around the year 2000, the Y00 protocol (its original name was $\alpha\eta$) was proposed by Yuen [3]–[6] for compatibility to existing high-speed and long-distance optical communication infrastructure [3]–[15]. However, the Y00 protocol had been believed to be non-ITS since the fast correlation attack (FCA) on the Y00 protocol was found [16], [17], even after "irregular mapping" was equipped as a countermeasure to the FCA [17], [18]. Hence, the Y00 protocol is believed to be computational secure, while QKDs are said to be ITS.

In our previous work [19], it was shown that the attacker "Eve" could not guess the correct secret keys shared by

legitimate users "Alice" and "Bob" with a probability of one even under an unlimitedly long known-plaintext attack (KPA) with the assistance of quantum memory to utilize the quantum and classical multiple-hypotheses testing theory [20]–[22]. The key aspect of the unlimitedly long KPA is to simplify the security analysis of the Y00 protocol because the signals cyclically appear when the effect of the plaintext is subtracted. However, our previous work still assumed that the Y00 system was designed as is; therefore, no security guarantee existed as to how ITS would be realizable against unknown computational attacks.

The purpose of this study is to show that well-designed Y00 systems are immune to the quantum generalization of FCA with the assistance of the unlimitedly long KPA and quantum memories that Eve possesses without any computational assumptions. The analyses in this study demonstrate two results: the central claim of the FCA was recovered against a specific class of Y00 systems not well-designed, while the others would be ITS under the unlimitedly long KPA with the generalized framework of FCA. The framework of the

quantum generalization of FCA corresponds to "collective attacks" or "coherent attacks" in the context of QKDs [23], while the existing security analyses of the Y00 protocol were "individual attacks" in the context of QKDs [7]–[18].

The security analyses in this study provide clear security parameters: the security breach time of the Y00 systems, and the minimum error pattern probability that determines the breach time.

This paper is structured as follows. Section II will describe the differences between the conventional stream ciphers and the Y00 protocol in terms of probabilities and information theory to show how the Y00 would be ITS along with the principle of the Y00 protocol. Section III describes the quantum detection theory that Eve performs on her quantum memory storing wire-tapped quantum states. Section IV describes the known concepts of FCA and how it will be generalized in this study. The section also describes the conditions for designing non-ITS Y00 systems and ITS Y00 systems, reiterating known results [16]–[19] in terms of the security breach time. Even if the Y00 system is implemented to be ITS, Eve's success probability increases in the end; hence, Section V describes how the Y00 system securely exchanges fresh keys. Section VI describes the remaining problem, while Section VII states the conclusions.

II. BRIEF DESCRIPTION OF PRINCIPLES OF Y00 PROTOCOL
This section describes the differences between the conventional stream ciphers and quantum-noise-randomized stream ciphers, such as the Y00 protocol.

A. BRIEF DESCRIPTION OF CONVENTIONAL MATHEMATICAL STREAM CIPHERS
Let Set(V) denote the set of possible variables V, let |Set(V)| denote the number of elements in Set(V). Conventional stream ciphers expand an initial short key $k \in$ Set(K) into a longer keystream $s \in$ Set(S) by a pseudo-random-number generator (PRNG). If the KPA is longer than the period of s, it completely reveals s. Alice sends her message $x \in$ Set(X) encoded into her ciphertext $c \in$ Set(C) by

$$C := X + S \bmod 2. \tag{1}$$

Then, Eve can recover k, irrespective of the complexity of the key expansion algorithm because the key expansion is deterministic, and Eve knows the PRNG, according to Shannon's maxim. In terms of conditional probabilities,

$$\Pr(S|C, X) = \Pr(K|C, X) = 1. \tag{2}$$

In terms of Shannon entropy,

$$H(S|C, X) = H(K|C, X) = 0. \tag{3}$$

B. PRINCIPLE OF THE Y00 PROTOCOL
To start the Y00 protocol, Alice and Bob must share secret keys, k and Δk. Then, they expand $(k, \Delta k) \in$ Set($K, \Delta K$) into key streams $(s, \Delta x) \in$ Set($S, \Delta X$) using the common PRNGs

equipped in the transmitter and receiver. Subsequently, s is chopped to every $\log_2 M$ bit to form an M-ary string $s(t)$ at time slot t. A message bit $x(t)$ is encoded into a coherent state $|\alpha[m(t)]\rangle$ as follows:

$$m(t) := \text{Map}[s(t)] + M(\text{Map}[s(t)] + x(t) + \Delta x(t) \bmod 2). \tag{4}$$

Map[$s(t)$] is a projection from $s(t)$ to Map[$s(t)$] $\in \{0, 1, 2, 3, \ldots, M-1\}$. For the detailed characteristics and concrete Map[·], the references [11]–[13] are helpful to understand. Therefore, $x(t) \in \{0, 1\}$ corresponds to a set of quantum states $\{|\alpha[m(t)]\rangle, |\alpha[m(t) + M]\rangle\}$ when Map[$s(t)$] $+\Delta x(t)$ is an even number; otherwise, $\{|\alpha[m(t) + M]\rangle, |\alpha[m(t)]\rangle\}$. In contrast, Bob's receiver sets an optimal threshold to discriminate the set of quantum states based on the shared $(s, \Delta x)$. Therefore, he decodes $x(t)$ because he knows the value of Map[$s(t)$] $+\Delta x(t)$. Meanwhile, Eve must discriminate the $2M$-ary signals hidden under the overlapping quantum and classical noise because she does not know whether Map[$s(t)$] $+\Delta x(t)$ is even or odd and also does not know $x(t)$.

When Eve can launch KPA longer than T_{LCM}, which is the least common multiple (LCM) of PRNGs' periods in a Y00 system, she will launch an optimal measurement to guess the most probable shared keys. Accordingly, in such a case, the quantum detection theory for multiple-hypothesis testing is required to evaluate the security of the Y00 protocol. Eve obtains the coherent states separated from a beam-splitter as $\rho_E[m(t)]$ and stores the time sequence in her quantum memory. The quantum sequence $\rho_E(s, \Delta x, x)$ with the splitting ratio η is denoted as follows:

$$\rho_E(s, \Delta x, x) := |\eta\alpha(s, \Delta x, x)\rangle\langle\eta\alpha(s, \Delta x, x)|$$
$$= \bigotimes_{t=1}^{T} |\eta\alpha[m(t)]\rangle\langle\eta\alpha[m(t)]| \tag{5}$$

Note that a set of $(s, \Delta x)$ is generated from $(k, \Delta k)$. Therefore, Eve needs to solve a |Set($K, \Delta K$)|-ary discrimination problem based on the unlimitedly long KPA like in the case of the conventional stream cipher, although the number of possible signal sequences is $(2M)^T$, which is considerably larger than |Set($K, \Delta K$)|.

C. SECURITY FRAMEWORK OF THE Y00 PROTOCOL
Shannon proved the necessary condition of perfect secrecy in his Theorem 6 [24] as

$$\Pr(X|C) = \Pr(X). \tag{6}$$

After Shannon's perfect secrecy, Wyner showed that almost perfect secrecy could be maintained if the channel to Eve is noisy enough [25]. Such a degradation for Eve is realized only on the physical layer [26]. However, the property of noise on the wire-tap channel is unknown in general situations, especially in the case that Eve has no restrictions on her performance except the laws of physics.

In the case of a Y00 system, the property of noise depends on the implementation of the system. Eve cannot avoid

quantum noise in eavesdropping ideal Y00 systems because of overlapping quantum noise caused by the Born rule, as described in Section IV. Consider the following simplified situation. Alice and Bob communicate by a stream cipher

$$C := X + S \bmod 2. \tag{7}$$

In contrast, Eve receives a ciphertext C_E with an error pattern E caused by the noise as

$$C_E := X + S + E \bmod 2. \tag{8}$$

From (8), Eve would be able to recover S if she had known E and X and had observed C_E. Hence,

$$\Pr(S|E, C_E, X) = 1. \tag{9}$$

However, because Eve never knows E,

$$H(S|C_E, X) \geq H(S, C_E, X) - H(C_E, X, E) = 0. \tag{10}$$

The equality in (10) holds only when E is a deterministic function of C_E and X, which never happens until (8) is satisfied except when Eve can estimate S by algebraic attacks such as FCA, corresponding to the security analysis by equations (6)–(8) in a previous study [6]. The derivation of (10) as well as the reason why the FCA succeeded are given in Appendix A.

Hence, the ideal Y00 protocol never allows Eve to obtain S as well as K deterministically, which is significantly different from conventional stream ciphers in Section II.A. Therefore, (10) suggests that an ideal Y00 system is ITS.

Accurately, von Neumann entropy is more suitable than Shannon entropy because Eve is supposed to store wire-tapped quantum states in her quantum memory. However, Eve must measure her memory to obtain the most likely results. Therefore, Shannon entropy is sufficient because the measured results are classical. The above point will be discussed in Section IV.E.

D. 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 can access the decryption system, then injects ciphertext 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 systems. Therefore, there is no significant difference between unlimitedly long KPA in this study and other cryptologic attack classes.

III. BRIEF DESCRIPTION OF QUANTUM DETECTION THEORY

This section describes how Eve utilizes her quantum memory and performs the optimal measurement. The description shows that Eve's success probability in obtaining the correct keys never reaches unity.

A. BRIEF DESCRIPTION OF THE QUANTUM DETECTION THEORY

From this section onward, $(s, \Delta x) \in \mathrm{Set}(S, \Delta X)$ is abbreviated as $r \in \mathrm{Set}(R)$ for simplicity. In the quantum detection theory, $W(r, x)$ is a Hermitian risk operator, and $\{M_E(r|x)\}$ is a set of Eve's optimal measurement operators to minimize her average error rate conditioned on the known x [20], [21]. The necessary-and-sufficient conditions of Eve's optimum $\{M_E(r|x)\}$ in (11) are described by (12)–(17).

$$M_E(r|x) := |(r|x)\rangle\langle(r|x)|. \tag{11}$$

$$\sum_{r \in \mathrm{Set}(R)} M_E(r|x) = I. \tag{12}$$

$$W(r, x) := -\sum_{r' \in \mathrm{Set}(R)} \delta_{r,r'} \Pr(r') \rho_E(r', x)$$
$$= -\Pr(r) |\eta\alpha(r, x)\rangle\langle\eta\alpha(r, x)| \tag{13}$$

$$\Gamma(x) := \sum_{r \in \mathrm{Set}(R)} M_E(r|x) W(r, x)$$
$$= \sum_{r \in \mathrm{Set}(R)} W(r, x) M_E(r|x) \tag{14}$$

$$[W(r, x) - \Gamma(x)] M_E(r|x)$$
$$= M_E(r|x) [W(r, x) - \Gamma(x)] = 0 \tag{15}$$

$$M_E(r|x) [W(r', x) - W(r, x)] M_E(r'|x) = 0. \tag{16}$$

$$W(r, x) - \Gamma(x) \geq 0. \tag{17}$$

Once $\{M_E(r|x)\}$ is determined, from the Cauchy–Schwarz inequality, Eve's average success probability with known x denoted by $-\mathrm{tr}\,\Gamma(x)$ is maximized as follows [19].

$$[-\mathrm{tr}\Gamma(x)]^2$$
$$= \left[\sum_{r \in \mathrm{Set}(R)} \Pr(r) |\langle\eta\alpha(r, x)|(r|x)\rangle|^2\right]^2$$
$$\leq \left[\sum_{r \in \mathrm{Set}(R)} \Pr(r)^2\right] \left[\sum_{r \in \mathrm{Set}(R)} |\langle\eta\alpha(r, x)|(r|x)\rangle|^4\right]. \tag{18}$$

The equality is satisfied when Eve can choose $\{M_E(r|x)\}$ so that it satisfies (19).

$$\Pr(r) = \frac{|\langle\eta\alpha(r, x)|(r|x)\rangle|^2}{\sum_{r \in \mathrm{Set}(R)} |\langle\eta\alpha(r, x)|(r|x)\rangle|^2}. \tag{19}$$

Hence, Eve's average success probability (20) is satisfied if and only if (21) is satisfied.

$$\max[-\mathrm{tr}\Gamma(x)] = \frac{\sum_{r \in \mathrm{Set}(R)} |\langle\eta\alpha(r, x)|(r|x)\rangle|^4}{\sum_{r \in \mathrm{Set}(R)} |\langle\eta\alpha(r, x)|(r|x)\rangle|^2} < 1. \tag{20}$$

$$|\langle\eta\alpha(r, x)|(r|x)\rangle|^2 < 1. \tag{21}$$

B. QUANTUM DETECTION FOR SEQUENTIAL COHERENT SIGNALS

To provide detailed analyses for the sequential Y00 signals, the over-completeness property of coherent states in (22) is required with $D(\text{All})$ covering the entire complex plains. In (23), $D(r \mid x)$ is an integration domain for signals originated from (r, x), satisfying (24)–(26).

$$\bigotimes_{t=1}^{T} \int_{\alpha(t) \in D(\text{All})} \pi^{-1} |\alpha(t)\rangle \langle\alpha(t)| \, d\alpha(t) = I. \qquad (22)$$

$$M_{\text{E}}(r+e|x) := \bigotimes_{t=1}^{T} \int_{\alpha(t) \in D(r+e|x)} \pi^{-1} |\alpha(t)\rangle \langle\alpha(t)| \, d\alpha(t). \qquad (23)$$

$$\bigcup_{e \in \text{Set}[E(r|x)]} D(r+e|x) = D(r|x). \qquad (24)$$

$$\bigcup_{r \in \text{Set}(R)} D(r|x) = D(\text{All}). \qquad (25)$$

$$D(r+e|x) \cap D(r'+e' \neq r+e|x) = \emptyset. \qquad (26)$$

$$M_{\text{E}}(r|x) := \sum_{e \in \text{Set}[E(r|x)]} M_{\text{E}}(r+e|x). \qquad (27)$$

Here, e is an error pattern from the correct r as a result of Eve's measurement operator $M_{\text{E}}(r+e|x)$ for the convenience in security analyses discussed in Section IV. $\text{Set}[E(r|x)]$ is a set of error patterns e originated from r conditioned on x.

IV. QUANTUM GENERALIZATION OF FCA AND SECURITY REQUIREMENTS

Our previous study [19] showed that the Y00 protocol would be secure against an unlimitedly long KPA under several assumptions. This section removes the assumptions to generalize FCA to evaluate the security of the Y00 protocol. Thus, the disadvantage of the Y00 protocol compared with that of the QKD + One-Time Pad (OTP) described in Section IV-A. of [27] would be removed.

A. BASIC CONCEPT OF FCA AND GENERALIZATION

The fundamental concept of the original FCA is as follows [16], [17].

1. Unless Map [·] is designed well, some bits in $r(t)$ are not sufficiently hidden in quantum noise.
2. Hence, it reveals some bits in the keystream from the linear feedback shift register (LFSR) to Eve.
3. Eve calculates the most likely seed key from the revealed bits in the keystream; some erroneous bits are even corrected by applying error-correction code.

Fig. 3 of the literature [16] showed the above situation. Then, the literature [17] formulated the attack scheme. However, if Map [·] is well-designed, quantum noise hides all bits in $r(t)$ almost equally, as proposed by the literature [17] and [18]. A numerical simulation is performed in the literature [18]. However, note that the above countermeasure is for a specific attack against a particular Y00 implementation. There should be more general attacks.

To construct a more general attack, the above assumptions listed in the literature [19] must be removed as follows.

1. A Y00 system employs arbitrary PRNGs to expand the shared secret keys into r.
2. Map [·] is not specified; however, some of the bits in $r(t)$ may not be covered by quantum noise.
3. Eve guesses the most likely r by a collective measurement on her quantum memory, including known plaintext, which is different from an individual measurement on each signal in the original FCA.

All analyses are performed similarly to the discussions in Section II.

B. DETAILED DESCRIPTION OF GENERALIZED ATTACK

Let us denote the duration of KPA as $T = N \cdot T_{\text{LCM}}$ and the number of error patterns e as $n(e| x, r)$ during T. Then,

$$\sum_{e \in \{0,1\}^{|e|}} n(e|r, x) = N. \qquad (28)$$

Here, $|e| = T_{\text{LCM}} \log_2 (2M)$ is the length of the error patterns e. Then, Eve's success probability $\Pr(r|r, x)$ is given as

$$\begin{aligned} 1 \geq{}& \Pr(r|r, x) \\ ={}& \sum_{\substack{\{n(e|r,x)\} \\ \in \Omega(r|x)}} [N!] \prod_{e \in \{0,1\}^{|e|}} [n(e|r, x)!]^{-1} \Pr(e|r, x)^{n(e|r,x)}. \end{aligned} \qquad (29)$$

Here, $\Omega(r|x)$ is a set of $\{n(e|r, x)\}$ whereby the detected state originates from r under known x, and its complemental set is $\Omega(r|x)^{\text{C}} := \Omega(\text{All}) - \Omega(r|x)$. The upper bound of $\Pr(r|r, x)$ is

$$\Pr(r|r, x) \leq 1 - [1 - \Pr(r)] \exp\left[-\left(N / N_{\text{Breach}}\right) \ln 2\right]. \qquad (30)$$

Here, N_{Breach} is defined as follows:

$$1/N_{\text{Breach}} := -\log_2[(2M)^{T_{\text{LCM}}} \min_{e \in \{0,1\}^{|e|}} \Pr(e|r, x)]. \qquad (31)$$

$$\min_{e \in \{0,1\}^{|e|}} \Pr(e|r, x) \leq (2M)^{-T_{\text{LCM}}}. \qquad (32)$$

The derivations for (29)–(31) are described in Appendix B. The relation between $\Pr(r|r, x)$ and $-\text{tr}\Gamma(x)$ is given by

$$-\text{tr}\Gamma(x) = \sum_{r \in \text{Set}(R)} \Pr(r) \Pr(r|r, x). \qquad (33)$$

C. NON-ITS Y00 SYSTEMS

If $1 > N_{\text{Breach}} \to 0$, then the Y00 system reaches $\Pr(r|r, x) \to 1$ immediately after the protocol begins. Such a condition is satisfied when

$$1/2 > (2M)^{T_{\text{LCM}}} \min_{e \in \{0,1\}^{|e|}} \Pr(e|r, x) \to 0. \qquad (34)$$

Therefore, in the generalized framework of FCA in this study, the known results [16], [17] are obtained under the condition (34). Such Y00 systems cannot be ITS irrespective of the complexity of PRNGs' algorithms, as discussed in Section II.

As a conclusion of this section, the generalization of FCA on Y00 systems is given in terms of the information theory and probabilities under Eve's optimal quantum measurement without any computational assumptions. It was shown that there exist some non-ITS Y00 systems if their implementations are invalid.

D. REQUIREMENTS ON ITS Y00 SYSTEMS

To implement an ITS Y00 system, the requirement is $\infty > N_{\text{Breach}} \geq 1$. Therefore,

$$1 > (2M)^{T_{\text{LCM}}} \min_{e \in \{0,1\}^{|e|}} \Pr(e|r,x) \geq 1/2. \qquad (35)$$

If (35) is satisfied, then the right-hand side of (30) never reaches unity while $\infty > N \geq 0$, which is unlike the conventional stream ciphers described in Section II-A, although Eve's success probability asymptotically increases as time T increases. Therefore, the generalization framework of FCA in this study again recovers the known result [19].

Moreover, the following simple case satisfies the condition.

$$\Pr(r|r,x) = \Pr(r). \qquad (36)$$

when

$$(2M)^{T_{\text{LCM}}} \min_{e \in \{0,1\}^{|e|}} \Pr(e|r,x) = 1. \qquad (37)$$

The above result means that irrespective of how long Eve launches KPA, her guessing probability remains the same as her pure guessing probability because of the infinitely long N_{Breach}, although the condition may not be satisfied.

The above conclusions are an analogy of OTP with a non-IID key string. If the key string is far from IID, its statistical property may give Eve a hint on the plaintext corresponding to r in this work because of the absence of (6) (more details are described in Appendix C).

E. EFFECT OF EVE'S LOCAL OPERATIONS

This section discusses whether Eve can obtain any advantage by her local quantum operations, including any trace-preserving completely positive (TPCP) maps in her quantum memory. Such quantum operations include classical operations, as well. Hence, her optical amplifications on the stolen signals are theoretically included.

Without her local operations, her optimal measurement is given by (18), which is given here again.

$$-\text{tr}\Gamma(x) = \sum_{r \in \text{Set}(R)} \Pr(r) |\langle \eta\alpha(x,r)|(r|x)\rangle|^2$$
$$= \sum_{r \in \text{Set}(R)} \Pr(r)\text{tr}\left[M_{\text{E}}(r|x)\rho_{\text{E}}(r,x)\right]. \qquad (38)$$

When she performs a TPCP operation Λ_{E} on her system, her optimal measurement operator is denoted as $\{M'_{\text{E}}(r|x)\}$; hence, her success probability is $-\text{tr}\Gamma'(x)$.

$$-\text{tr}\Gamma'(x) = \sum_{r \in \text{Set}(R)} \Pr(r)\text{tr}\left[M'_{\text{E}}(r|x)\Lambda_{\text{E}}(\rho_{\text{E}}(r,x))\right]. \qquad (39)$$

Therefore, the problem is whether $-\text{tr}\Gamma'(x) > -\text{tr}\Gamma(x)$ or not.

Such a Λ_{E} is rewritten by a unitary operator U_{EQ} by adding a virtual ancilla Q to Eve's system.

$$\Lambda_{\text{E}}(\rho_{\text{E}}(r,x)) := \text{tr}_{\text{Q}}\left[U_{\text{EQ}}\left(\rho_{\text{E}}(r,x) \otimes |0\rangle\langle 0|_{\text{Q}}\right)U^{\dagger}_{\text{EQ}}\right]. \qquad (40)$$
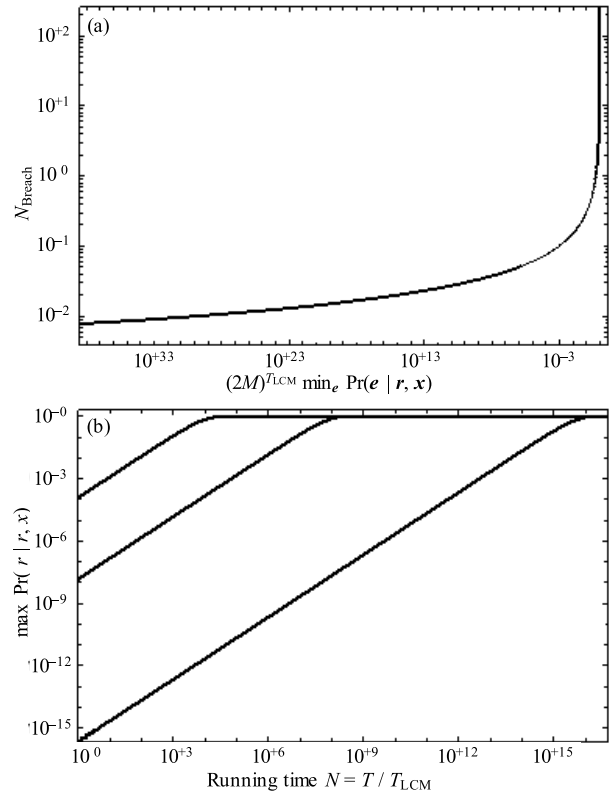

FIGURE 1. (a) N_{Breach} vs. $\min_e$ P(e |r, x) in (31), (b) Eve's success probability with parameters in (30) of $\Pr(r) = |\text{Set}(R)|^{-1} = (2^{256} - 1)^{-2}$, $1/N_{\text{Breach}} = 1 - 2^{-13}, 1 - 2^{-26}, 1 - 2^{-52}$ from the top curve.

Then,

$$-\text{tr}\Gamma'(x) = \sum_{r \in \text{Set}(R)} \Pr(r)\text{tr}\left[M''_{\text{EQ}}(r|x)\rho_{\text{EQ}}(r,x)\right]. \qquad (41)$$

$$M''_{\text{EQ}}(r|x) := U^{\dagger}_{\text{EQ}}M'_{\text{EQ}}(r|x)U_{\text{EQ}}. \qquad (42)$$

$$\rho_{\text{EQ}}(r,x) := \rho_{\text{E}}(r,x) \otimes |0\rangle\langle 0|_{\text{Q}}. \qquad (43)$$

If (44) is satisfied $\{M''_{\text{E}}(r|x)\}$ is an optimal measurement satisfying (12)–(17),

$$\text{tr}_{\text{E}}\left[M''_{\text{EQ}}(r|x)\rho_{\text{EQ}}(r,x)\right] = M_{\text{E}}(r|x)\rho_{\text{E}}(r,x). \qquad (44)$$

Otherwise, $-\text{tr}\Gamma'(x) < -\text{tr}\Gamma(x)$. Therefore, her local TPCP operations never give her any advantages.

The above conclusion sounds natural since the Holevo quantity bounds the accessible information, while the quantum data processing inequality tells degradation of the accessible information by TPCP maps (more details in Appendix D).

F. NUMERICAL EXAMPLE

FIGURE 1(a) shows characteristics of (31) while 1(b) shows examples of (30) with parameters in its caption.

With regard to the time scale of N_{Breach}, her success probability reaches almost unity. Because her success probability must be sufficiently suppressed, the legitimate users must set a security threshold P_{Th} to a certain level, and then, they must estimate the actual breach time of the shared key. However,

N_{Breach} is very sensitive to $\min_e \Pr(e \mid r, x)$ when the users need sufficiently long N_{Breach}. Hence, in the actual situation, parameters must be carefully estimated from the designs of the corresponding Y00 systems.

G. POSSIBLY BETTER IMPLEMENTATIONS
To realize a condition close to the ideal situation (36), the simple implementation described in Section II-B. may not be sufficient.

A possible solution is to add a classical randomization technique named deliberate signal randomization (DSR). Security enhancement by the technique originated was obtained from a previous study [3]. Then, implementation using an additional PRNG was proposed [8], [11], called the "keyed DSR." The concept of DSR is a modification of (4).

$$m(t) := \text{Map}\left[s(t) + d(t) \bmod 2\right]$$
$$+ M\left(\text{Map}\left[s(t)\right] + x(t) + \Delta x(t) \bmod 2\right). \quad (45)$$

Here, $d(t)$ is a random string of length $|d(t)| = |s(t)|$. If $d(t)$ has a probability distribution of independent and identically distributed (IID), arbitral error patterns e will occur with the same probability. However, the keyed DSR will not satisfy the IID condition because $d(t)$ is deterministic. It would enlarge the key-space of Y00 systems and give a longer T_{LCM}; however, it will never be an essential solution because the output of PRNG is periodic. A true-random DSR is recommended. Another possible solution is to scramble $\text{Map}[\cdot]$ by an additional PRNG as $\text{Map}(t)[\cdot]$.

PRNGs in Y00 systems must be chosen carefully. Recall that the Y00 systems described in this study consist of at least two PRNGs; one is for s to select the signal level, and the other is for Δx to scramble the plaintext x. It is well-known that LFSRs do not even have a statistically good property. A combination of several LFSRs shows correlations between them. At least statistically better PRNGs must be chosen, such as Mersenne Twister [28] or TinyMT [29].

H. EFFECT OF TRUE-RANDOM DSR
By a true-random DSR, pure states being sent from Alice become mixed states for Eve, as follows:

$$\rho_{\text{E}}(r, x) := \sum_{d \in \{0,1\}^{|d|}} \Pr(d) \left|\eta\alpha(r, x, d)\right\rangle \left\langle\eta\alpha(r, x, d)\right|. \quad (46)$$

If $\Pr(d)$ is uniform, $\Pr(d) = M^{-T}$. Thus, Eve's success probability $-\text{tr}\Gamma'(x)$ is given by her corresponding optimal measurement $\{M'_{\text{E}}(r|x)\}$ as follows:

$$-\text{tr}\Gamma'(x) = \sum_{r \in Set(R)} \Pr(r)\text{tr}\left[M'_{\text{E}}(r|x)\rho_{\text{E}}(r, x)\right]. \quad (47)$$

The above situation is similar to the situation in Section IV.E, in which Eve performs her local TPCP operations, resulting in her local quantum system becoming a mixed state. Hence, by a similar procedure,

$$-\text{tr}\Gamma'(x) = \sum_{r \in Set(R)} \Pr(r)\text{tr}\left[M''_{\text{EQ}}(r|x)\rho_{\text{EQ}}(r, x)\right]. \quad (48)$$

$$M''_{\text{EQ}}(r|x) := U^{\dagger}_{\text{EQ}} M'_{\text{EQ}}(r|x) U_{\text{EQ}}. \quad (49)$$

$$\rho_{\text{EQ}}(r, x) := \rho_{\text{E}}(r, x) \otimes |0\rangle \langle 0|_{\text{Q}}. \quad (50)$$

Because Section IV.E concluded that Eve's local TPCP operations never give her any advantages by the same discussion, the conclusion is $-\text{tr}\Gamma'(x) \leq -\text{tr}\Gamma(x)$, as well.

V. KEY-REFRESHMENT BY LEFTOVER HASHING IN QUANTUM NOISE
Section IV.D showed that Y00 systems would be ITS if their implementations are appropriate. However, Eve becomes confident regarding the correct keys over time. Therefore, this section provides a method to refresh the shared keys between Alice and Bob before the Y00 systems are threatened.

A. LEFTOVER HASH LEMMA
To share a set of fresh keys, Alice or Bob sends a random string $x \in \text{Set}(X)$ instead of their messages, where x is an error correction code containing a hash function $h \in \text{Set}(H)$, and a seed key $k_{\text{R}} \in \text{Set}(K_{\text{R}})$ to generate $(k_{\text{new}}, \Delta k_{\text{new}})$ as follows.

$$(k_{\text{New}}, \Delta k_{\text{New}}) = h(k_{\text{R}}). \quad (51)$$

Because Eve never knows X, her attack is now limited to ciphertext only attacks (COA).

According to the ordinary leftover hash lemma (LHL) [30], [31] there exists a strong $(\tau, \kappa, \varepsilon)$-randomness extractor to obtain the final key of its length τ with Eve's min-entropy $H_{\infty}(X|R, C_{\text{E}})$,

$$H_{\infty}(X|R, C_{\text{E}})$$
$$= -\log_2 \sum_{(r, c_{\text{E}}) \in \text{Set}(R, C_{\text{E}})} \Pr(r, c_{\text{E}}) \max_x \Pr(x|r, c_{\text{E}}). \quad (52)$$

Note that C_{E} is the ciphertext observed by Eve under the effect of quantum noise and DSR, which corresponds to X for legitimate users.

$$H_{\infty}(X|R, C_{\text{E}}) \geq \kappa. \quad (53)$$

$$\sum_{(r, c_{\text{E}}) \in \text{Set}(R, C_{\text{E}})} \Pr(r, c_{\text{E}}) \left|\Pr(H(K_{\text{R}})|r, c_{\text{E}}) - 2^{-\tau}\right| \leq 2\varepsilon. \quad (54)$$

$$\varepsilon = \exp\left(\frac{1}{2}\left[\tau - H_{\infty}(X|R, C_{\text{E}})\right] \ln 2\right). \quad (55)$$

B. OPTIMUM LEFTOVER HASHING
From (53)–(55), the upper-bound of Eve's average guessing probability on $H(K_{\text{R}})$ is

$$\sum_{(r, c_{\text{E}}) \text{Set} \in (R, C_{\text{E}})} \Pr(r, c_{\text{E}}) \Pr(H(K_{\text{R}})|r, c_{\text{E}}) \leq 2\varepsilon + 2^{-\tau}. \quad (56)$$

The derivation of (56) is shown in Appendix E.

As discussed previously [32], [33], there is an optimum sacrifice amount in LHL as follows.

$$\partial(2\varepsilon + 2^{-\tau})/\partial\tau = 0 \Rightarrow \tau = \frac{1}{3}H_{\infty}(X|R, C_{\text{E}}). \quad (57)$$

If the final key is shorter than the above amount, it is considered "over-sacrificing," whereas if the final key is longer than the optimal final key, it is considered "under-sacrificing." Hence,

$$\sum_{(r, c_E) \in \text{Set}(R, C_E)} \Pr(r, c_E) \Pr(H(K_R)|r, c_E)$$
$$\leq 3 \exp\left[-\frac{1}{3} H_\infty(X|R, C_E) \ln 2\right] = 3 \times 2^{-\tau} \ll P_{\text{Th}}. \quad (58)$$

The parameter P_{Th} is the threshold discussed in Section IV.F.

In the case of the Y00 protocol, there is no classical channel to exchange h contrarily to QKDs, in which h is openly known to Eve. However, she would also try to guess the most likely X based on her most confident keys denoted by r_E. Then, the following inequality is derived.

$$H_\infty(X|R_E, C_E)$$
$$\geq -\log_2 \sum_{c_E \in \text{Set}(C_E)} \Pr(c_E) \max_{r_E, x} \Pr(x|r_E, c_E)$$
$$:= \min_{r_E} H_\infty(X|R_E, C_E). \quad (59)$$

Then, instead of (57), the following is the optimal key length.

$$\tau = \frac{1}{3} \min_{r_E} H_\infty(X|R_E, C_E). \quad (60)$$

Eve's corresponding guessing probability on $H(K_R)$ is

$$\sum_{c_E \in \text{Set}(C_E)} \Pr(c_E) \Pr(H(K_R)|r_E, c_E)$$
$$\leq 3 \exp\left[-\frac{1}{3} \min_{r_E} H_\infty(X|R_E, C_E) \ln 2\right] = 3 \times 2^{-\tau} \ll P_{\text{Th}}. \quad (61)$$

Therefore, to obtain the valid lengths of the fresh keys for the Y00 protocol, typically $|k_{\text{new}}| + |\Delta k_{\text{new}}| = |h(k_R)| = 256$ or 512 bit, $\min_r H_\infty(X|R, C_E)/3$ must be requested for the final key lengths, while Eve's guessing probability on $H(K_R)$ must be suppressed, as suggested previously by (61).

VI. FUTURE REMARKS

In the key-refreshment process discussed in Section V, Eve may launch so-called "entangling probe attacks" to steal fresh keys as well as the initial keys discussed in Section VI.D of our previous study [27] by preparing her quantum system and then performing joint unitary operations on her system with the signal states between Alice and Bob. Further generalization may be possible that Eve would keep eavesdropping by entangling probe attack during the key-refreshment/initial-key-agreement as well as KPA during the message exchanges after the key-refreshment, which corresponds to coherent attack in QKDs.

The effect of such an attack on the Y00 protocol may be limited; however, evaluation of the strength of such classes of attacks is required. At least, in the key refreshment process, quantum minimax problem in [13], [34], [35] may be helpful; Alice and Bob exchange the keys with a prior probability

to minimize Eve's success probability, while Eve derives her optimal measurement operators to maximize her success probability.

In contrast, in the message transmission processes, Eve would not require such a class of attacks because the plaintext is already available to her, while the purpose of the entangling probe attack is to steal the exchanged information in the context of QKDs.

Rather, a problem in this study is that the analyses would not give any concrete designs of the Y00 systems because all analyses have done abstractly. This is because to explore whether Y00 systems can be designed to be ITS, and what is the necessary conditions. Hence it would neither guarantee whether existing Y00 systems are ITS. As it was explained in the introduction, the prototype Y00 system was breached by FCA as it was. Hence, there may be some Y00 systems which would not satisfy the requirement given in this study, while some may satisfy the requirement. The importance of this study is that the possibility of ITS Y00 systems was clarified, and the essential parameters to design ITS Y00 systems were given. Some more studies would be required to develop simpler indices to evaluate the security of designed Y00 systems compared to the security indices given in this study hard to estimate.

VII. CONCLUSION

This study showed the essential security parameters to request the Y00 systems to be ITS and what parameter determines whether the designed Y00 systems are non-ITS or ITS against an attacker who has unlimited computational power with the assistance of quantum memory and unlimitedly long known-plaintext attacks. The analyzed condition is called "collective attacks" or "coherent attacks" in the context of QKD protocols. The conclusions are that Y00 systems remain ITS under certain conditions explicitly provided in this study. Furthermore, this study showed that the attacker's confidence in the shared correct key set increases as time passes. Therefore, a method to refresh the sets of shared keys is proposed using LHL. It had been believed that Y00 protocols are computationally secure. However, this study showed ITS Y00 systems are possible by pointing out what parameters are essential to design ITS Y00 systems. To find the above requirement, security analyses were done abstractly. Hence, a problem in this study is that the analyses would not give any concrete designs of ITS Y00 systems. Thus, it would not guarantee whether existing Y00 systems are ITS. As it was explained in the introduction, the prototype Y00 system was breached by the fast correlation attack. There should be non-ITS Y00 systems while others are ITS which satisfy the security requirements given in this study. The importance of this study is that it showed the possibility and the destination to design ITS Y00 systems. Some more studies would be required to find a more straightforward method to evaluate the security of the designed systems compared to using the security parameters given in this study, which is hard to estimate.

APPENDIX

A. DERIVATION OF (10)

From the equality between conditional and joint entropies,

$$H(S|C_E, X) = H(S, C_E, X) - H(C_E, X). \quad (62)$$

An inequality between a conditional entropy and entropy with additional information gives

$$H(C_E, X) \leq H(C_E, X, E). \quad (63)$$

The equality is satisfied only when E is a deterministic function of C_E and X irrespective of what S is. Such a situation occur when a sufficient number of bits in S are not hidden under quantum noise enough; then Eve can correct errors by simulation of the system and estimate the error patterns to correct errors using error-correcting code with LFSR, leading to successful FCAs [16], [17].

Eve would obtain S if she could know E. Hence,

$$H(S, C_E, X, E) - H(C_E, X, E) = H(S|C_E, X, E) = 0. \quad (64)$$

Therefore, (10) is derived from (62)–(64).

B. DERIVATION OF (29)–(31)

Consider the following summation with $\Omega(\text{All})$ as a set of all patterns of $\{n(e|r, x)\}$ with the total being N. Denote a set of possible signal sequences originating from the shared key stream r as $\Omega(r|x)$, and its complemental set $\Omega(r|x)^C := \Omega(\text{All}) - \Omega(r|x)$.

$$1 = [\Pr(e_0|r, x) + \Pr(e \neq e_0|r, x)]^T$$
$$= \sum_{\substack{\{n(e|r,x)\} \\ \in \Omega(\text{All})}} \binom{N}{n(e_0|r, x)} \binom{\Pr(e_0|r, x)^{n(e_0|r,x)} \times [\Pr(e_1|r, x)}{+\Pr(e \neq e_0, e_1|r, x)]^{T-n(e_0|r,x)}}$$
$$= \sum_{\substack{\{n(e|r,x)\} \\ \in \Omega(\text{All})}} [N!] \prod_{e \in \{0,1\}^{|e|}} [n(e|r, x)!]^{-1} \Pr(e|r, x)^{n(e|r,x)}. \quad (65)$$

The last equation is derived from

$$\binom{N}{n_1} \binom{N-n_1}{n_2} \binom{N-n_1-n_2}{n_3} \cdots \binom{N-\ldots-n_{|e|}}{n_{|e|}}$$
$$= [N!] \prod_{k=1}^{|e|} [n_k!]^{-1}. \quad (66)$$

Furthermore, note that

$$1 = \sum_{\substack{\{n(e|r,x)\} \\ \in \Omega(\text{All})}} [N!] \prod_{e \in \{0,1\}^{|e|}} [n(e|r, x)!]^{-1} \Pr(e|r, x)^{n(e|r,x)}$$
$$\geq \sum_{\substack{\{n(e|r,x)\} \\ \in \Omega(r|x)}} [N!] \prod_{e \in \{0,1\}^{|e|}} [n(e|r, x)!]^{-1} \Pr(e|r, x)^{n(e|r,x)}$$
$$:= \Pr(r|r, x). \quad (67)$$

Hence, $\Pr(r \mid x, r)$ is strictly less than unity unless $|\Omega(r|x)| = |\Omega(\text{All})|$. Then, using $\Omega(r|x)^C$,

$$1 - \Pr(r|r, x)$$
$$= \sum_{\substack{\{n(e|r,x)\} \\ \in \Omega(r|x)^C}} [N!] \prod_{e \in \{0,1\}^{|e|}} [n(e|r, x)!]^{-1} \Pr(e|r, x)^{n(e|r,x)}. \quad (68)$$

Now, using the following inequality,

$$\sum_{\substack{\{n(e|r,x)\} \\ \in \Omega(r|x)^C}} [N!] \prod_{e \in \{0,1\}^{|e|}} [n(e|r, x)!]^{-1} \Pr(e|r, x)^{n(e|r,x)}$$
$$\geq \min_{\{n(e|r,x)\} \in \Omega(r|x)^C} \prod_{e \in \{0,1\}^{|e|}} \Pr(e|r, x)^{n(e|r,x)}$$
$$\times \sum_{\{n(e|r,x)\} \in \Omega(r|x)^C} [N!] \prod_{e \in \{0,1\}^{|e|}} [n(e|r, x)!]^{-1}. \quad (69)$$

In contrast, the size of $|\Omega(r|x)|$ must be $\Pr(r)(2M)^T$ because there are $(2M)^T$ patterns of possible detected signal patterns, which suggest $|\Omega(\text{All})| = (2M)^T$. Hence,

$$|\Omega(r|x)^C| := \sum_{\{n(e|r,x)\} \in \Omega(r|x)^C} [N!] \prod_{e \in \{0,1\}^{|e|}} [n(e|r, x)!]^{-1}$$
$$= [1 - \Pr(r)](2M)^T. \quad (70)$$

Therefore, (29)–(31) are derived by letting $n(e|r, x) = N$ for the $\min_e \Pr(e|r, x)$ as follows.

$$\left(\min_{\{n(e|r,x)\} \in \Omega(r|x)^C} \prod_{e \in \{0,1\}^{|e|}} \Pr(e|r, x)^{n(e|r,x)} \right)$$
$$\times \left(\sum_{\{n(e|r,x)\} \in \Omega(r|x)^C} [N!] \prod_{e \in \{0,1\}^{|e|}} [n(e|r, x)!]^{-1} \right)$$
$$= [1 - \Pr(r)] \left[\min_{e \in \{0,1\}^{|e|}} (2M)^{T_{\text{LCM}}} \Pr(e|r, x) \right]^N. \quad (71)$$

C. IMPERFECT ONE-TIME PAD ANALOGY IN SECTION IV-D

Although the discussion and schematic view were given in the reference [19], the explanation on the security of the Y00 protocol explained by the analogy of imperfect OTP is given here. Suppose that Eve measures her quantum memory every T_{LCM} of the PRNGs. Eve's failure probability in obtaining the correct r in $N = T/T_{\text{LCM}}$ measurements is

$$\Pr(\text{Fail.}; N) = \sum_{n=0}^{Ceil[N/2]} \binom{N}{n} \Pr(\text{Fail.})^n [1 - \Pr(\text{Fail.})]^{N-n}. \quad (72)$$

Here, $\Pr(\text{Fail})$ is Eve's failure probability in a single measurement. By a similar discussion in Appendix B,

$$\Pr(\text{Fail.}; N) = 1 - \Pr(\text{Suc.}; N)$$
$$\geq \min_n \Pr(\text{Fail.})^n [1 - \Pr(\text{Fail.})]^{N-n}$$
$$\sum_{n=0}^{Ceil[N/2]} \binom{N}{n}$$
$$\geq [1 - \Pr(\text{Fail.})]^N (2N)^{-1/2} \exp(NH_2(1/2) \ln 2)$$
$$= (2N)^{-1/2} \exp(N \ln[2 - 2\Pr(\text{Fail.})]) \quad (73)$$

The term $\ln[2 - 2\Pr\Pr(\text{Fail.})] < 0$ when $\Pr(\text{Fail}) > 1/2$. Thus, the right-hand side of the following formula asymptotically raises to one.

$$\Pr(\text{Suc.}; N) \leq 1 - (2N)^{-1/2} \exp(N \ln[2 - 2\Pr(\text{Fail.})]). \quad (74)$$

The above result qualitatively explains the result of Eve's successful measurement formulated by (30), as well as a result in the reference [19].

D. ROLES OF VON NEUMAN ENTROPY IN SECTION *IV-E*

The quantum data processing inequality [36] is described as

$$S\left(\rho_E(x)\right) \geq S\left(\Lambda_E\left(\rho_E(x)\right)\right) - S_e. \tag{75}$$

$$S_e : = S\left(\Lambda_E\left(\rho_E(x)\right) \otimes |0\rangle\langle 0|_Q\right)$$

$$\leq S\left(\Lambda_E\left(\rho_E(x)\right)\right) + S\left(|0\rangle\langle 0|_Q\right). \tag{76}$$

$$\rho_E(x) : = \sum_{r \in \mathrm{Set}(R)} \Pr(r)\rho_E(r, x). \tag{77}$$

Hence,

$$S\left(\rho_E(x)\right) \geq S\left(\Lambda_E\left(\rho_E(x)\right)\right) - S_e \geq 0. \tag{78}$$

The above conclusion is because the von Neuman entropy for the pure state is zero. The Holevo quantity is

$$S\left(\rho_E(x)\right) - \sum_{r \in \mathrm{Set}(R)} \Pr(r)S\left(\rho_E(r, x)\right) = S\left(\rho_E(x)\right). \tag{79}$$

Because $\rho_E(r, x)$ defined by (5) is a pure state, hence the second term at the left-hand side of (79) is zero.

E. DERIVATION OF (56)

From LHL (53)–(55), the following decomposition is derived.

$$2\varepsilon \geq \sum_{(r, c_E) \in \mathrm{Set}(R, C_E)} \Pr(r, x_E)\left|\Pr(H(K_R)|r, c_E) - 2^{-\tau}\right|$$

$$= \sum_{\Pr(H(K_R)|r, c_E) \geq 2^{-\tau}} \Pr(r, x_E)\left[\Pr(H(K_R)|r, c_E) - 2^{-\tau}\right]$$

$$+ \sum_{\Pr(H(K_R)|r, c_E) \leq 2^{-\tau}} \Pr(r, c_E)\left[2^{-\tau} - \Pr(H(K_R)|r, c_E)\right]. \tag{80}$$

The first term on the last side of (80) shows,

$$2\varepsilon \geq \sum_{\substack{\Pr(H(K_R)|r, c_E) \\ \geq 2^{-\tau}}} \Pr(r, c_E)\left[\Pr(H(K_R)|r, c_E) - 2^{-\tau}\right]. \tag{81}$$

The second term in the last side of (80) shows

$$\sum_{\Pr(H(K_R)|r, c_E) \leq 2^{-\tau}} \Pr(r, c_E)\left[2^{-\tau} - \Pr(H(K_R)|r, c_E)\right] \geq 0. \tag{82}$$

Combining (81) and (82), (56) can be derived.

ACKNOWLEDGMENT

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.*, Bengaluru, India, vol. 175, Dec. 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.

[3] H. P. Yuen, "KCQ: A new approach to quantum cryptography I. General principles and key generation," 2003, *arXiv:quant-ph/0311061*. [Online]. Available: https://arxiv.org/abs/quant-ph/0311061

[4] G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, "Secure communication using mesoscopic coherent states," *Phys. Rev. Lett.*, vol. 90, no. 22, 2003, Art. no. 227901, doi: 10.1103/PhysRevLett.90.227901.

[5] C. Liang, G. Kanter, E. Corndorf, and P. Kumar, "Quantum noise protected data encryption in a WDM network," *IEEE Photon. Technol. Lett.*, vol. 17, no. 7, pp. 1573–1575, Jul. 2005, doi: 10.1109/lpt.2005.848264.

[6] H. 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] O. Hirota, M. Sohma, M. Fuse, and K. Kato, "Quantum stream cipher by the Yuen 2000 protocol: Design and experiment by an intensity-modulation scheme," *Phys. Rev. A, Gen. Phys.*, vol. 72, no. 2, 2005, Art. no. 022335, doi: 10.1103/PhysRevA.72.022335.

[8] O. Hirota, T. Shimizu, T. Katayama, and K. Harasawa, "10 Gbps quantum stream cipher by Y-00 for super HDTV transmission with provable security," *Proc. SPIE*, vol. 6710, Sep. 2007, Art. no. 67100K, doi: 10.1117/12.731378.

[9] Y. Doi, S. Akutsu, M. Honda, K. Harasawa, O. Hirota, S. Kawanishi, K. Ohhata, and K. Yamashita, "360 km field transmission of 10 Gbit/s stream cipher by quantum noise for optical network," in *Proc. Opt. Fiber Commun. Conf. (OFC)*, Mar. 2010, pp. 1–3, doi: 10.1364/OFC.2010.OWC4.

[10] K. Harasawa, O. Hirota, K. Yamashita, M. Honda, K. Ohhata, S. Akutsu, T. Hosoi, and Y. Doi, "Quantum encryption communication over a 192-km 2.5-Gbit/s line with optical transceivers employing Yuen-2000 protocol based on intensity modulation," *J. Lightw. Technol.*, vol. 29, no. 3, pp. 316–323, Feb. 2011, doi: 10.1109/jlt.2010.2099207.

[11] 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.

[12] 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, doi: 10.1117/12.2237852.

[13] K. Kato, "Quantum enigma cipher as a generalization of the quantum stream cipher," *Proc. SPIE*, vol. 9980, Sep. 2016, Art. no. 998005, doi: 10.117/12.2237570.

[14] F. Futami, K. Guan, J. Gripp, K. Kato, K. Tanizawa, S. Chandrasekhar, and P. J. Winzer, "Y-00 quantum stream cipher overlay in a coherent 256-Gbit/s polarization multiplexed 16-QAM WDM system," *Opt. Express*, vol. 25, no. 26, pp. 33338–33349, 2017, doi: 10.1364/OE.25.033338.

[15] 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. OFC Conf. Opt. Soc. Amer.*, 2018, Art. no. Tu2G-5, doi: 10.1364/OFC.2018.Tu2G.5.

[16] 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.

[17] M. J. Mihaljević, "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, 2017, Art. no. 052334, doi: 10.1103/PhysRevA.75.052334.

[18] 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, 2008, Art. no. 034305, doi: 10.1103/PhysRevA.77.034305.

[19] T. Iwakoshi, "Guessing probability under unlimited known-plaintext attack on secret keys for Y00 quantum stream cipher by quantum multiple hypotheses testing," *Opt. Eng.*, vol. 57, no. 12, p. 1, Dec. 2018, doi: 10.1117/1.oe.57.12.126103.

[20] C. W. Helstrom, "Quantum detection and estimation theory," *J. Stat. Phys.*, vol. 1, no. 2, pp. 231–252, 1969.

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

[22] 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.

[23] R. Renner, "Security of quantum key distribution," *Int. J. Quantum Inf.*, vol. 6, no. 1, pp. 1–127, Feb. 2008, doi: 10.1142/s0219749908003256.

[24] 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.

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

[26] L. Chen and G. Gong, *Communication System Security*. London, U.K.: Chapman & Hall, 2012.

[27] 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.

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

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

[30] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby, "A pseudorandom generator from any one-way function," *SIAM J. Comput.*, vol. 28, no. 4, pp. 1364–1396, Jan. 1999.

[31] B. Barak, Y. Dodis, H. Krawczyk, O. Pereira, K. Pietrzak, F. X. Standaert, and Y. Yu, "Leftover hash lemma, revisited," in *Proc. Annu. Cryptol. Conf.* Berlin, Germany: Springer, 2011, pp. 1–20, doi: 10.1007/978-3-642-22792-9_1.

[32] T. Iwakoshi, "Bit-error-rate guarantee for quantum key distribution and its characteristics compared to leftover hash lemma," *Proc. SPIE*, vol. 10803, Oct. 2018, Art. no. 1080309, doi: 10.1117/12.2500457.

[33] T. Iwakoshi, "Fundamental limit and trade-off between security and secure key generation rate in quantum key distribution," *Metrol. Meas. Syst.*, vol. 26, no. 1, pp. 125–137, 2019, doi: 10.24425/mms.2019.126333.

[34] O. Hirota and S. Ikehara, "Minimax strategy in the quantum detection theory and its application to optical communications," *IEICE Trans.*, vol. 65, no. 11, pp. 627–633, 1982.

[35] O. Hirota, K. Kato, M. Shoma, and T. S. Usuda, "Quantum key disribution with unconditional security for all-optical fiber network," *Proc. SPIE*, vol. 5161, pp. 320–331, Feb. 2004, doi: 10.1117/12.504978.

[36] B. Schumacher and M. A. Nielsen, "Quantum data processing and error correction," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 4, p. 2629, 1996, doi: 10.1103/PhysRevA.54.2629.

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 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. He joined Mie University, in July 2019 to continue his studies.

●●●