Communications in Physics, Vol. 32, No. 3 (2022), pp. 223-232
DOI: https://doi.org/10.15625/0868-3166/17064

SECURE INFORMATION EXCHANGE WITHOUT PRIOR KEY DISTRIBUTION VIA SINGLE-PHOTON HYPERSTATES

NGUYEN BA AN[1,2,†]

[1] *Thang Long Institute of Mathematics and Applied Sciences,*
Thang Long University, Nghiem Xuan Yem, Hoang Mai, Hanoi, Vietnam

[2] *Center for Theoretical Physics, Institute of Physics,*
Vietnam Academy of Science and Technology, 18 Hoang Quoc Viet, Hanoi, Vietnam

E-mail: [†]nban@iop.vast.vn

Received 12 April 2022; *Accepted for publication 29 April 2022*; *Published 30 May 2022*

Abstract. *Methods for two distant parties to exchange their secret messages using single photons are considered. There existed several such methods but they are either insecure or face with information leakage problem. Recently, Ye et al. [Quantum Inf. Process.* ***20*** *(2021) 209] have reported a method using single photons in both polarization and spatial degrees of freedom that is both efficient and resistant from information leakage. However, this method is not so feasible as it has specific limitations, namely, it requires availability of quantum memory and high classical communication cost. In this paper a new method to overcome the above-said limitations is proposed. The proposed method is also efficient because it also uses single photons in two degrees of freedom. However, the encoding operation in the proposed method is modified so that no quantum memory is demanded at all and the execution of the method is simpler compared to that of Ye et al.. Moreover, the cost of classical communication in our method is 50% cheaper than that in the method of Ye et al. Therefore, the proposed method proves to be feasible, simple and economical that could be realized by means of current technologies.*

Keywords: secure information exchange; information leakage; single-photon hyperstates.

Classification numbers: 03.67.Ac.

I. INTRODUCTION

Quantum entanglement (see, e.g., [1]) is irreplaceable resource for many quantum tasks such as superdense coding [2], teleportation [3], remote state preparation [4], joint remote state preparation [5], quantum computation [6], quantum error correction [7], and so on. However, there are tasks that can be accomplished either with or without entanglement. For example, quantum key distribution can be done by using entangled photon pairs [8] or unentangled photons [9]. Quantum secret sharing can also be realized either with the aid of entanglement [10] or simply with the use of single photons which are unentangled with each other [11].

Intriguing is a kind of protocols called quantum dialogue [12, 13] or more general bidirectional secure quantum direct communication [14] that aim at simultaneous exchange of secret information between two distant parties (Alice and Bob) without the need of quantum key distribution in advance.

In this paper we are concerned with methods for secure information exchange without prior key distribution using single photons, i.e., quantum entanglement is not exploited at all. At the early stage, each of the photons to be used for the task is prepared impromptu in one of the four states $|h\rangle$, $|v\rangle$, $|+\rangle = (|h\rangle + |v\rangle)/\sqrt{2}$ and $|-\rangle = (|h\rangle - |v\rangle)/\sqrt{2}$, with $|h\rangle$ ($|v\rangle$) denoting state of horizontally (vertically) polarized photon. That is, the photon is encoded in one degree of freedom (DOF), the polarization DOF, and each photon is worth one qubit. However, like other elementary particles, a photon possesses several inherent properties so that it can be characterized in multiple DOFs at the same time. State of such a photon is here referred to as hyperstate. Quite clearly, use of photon hyperstates boosts the efficiency of quantum tasks because a single photon in this case stores more than one qubit (precisely, N qubits if N DOFs are simultaneously exploited to characterize the photon).

In the next section, Sec. II, we first briefly review the existing methods for bidirectional secure quantum direct communication using single photons in hyperstates associated with both polarization degree of freedom (P-DOF) and spatial degree of freedom (S-DOF) and then propose our improved method. Finally, we make conclusion in Sec. III.

II. EXISTING METHODS AND OUR METHOD

Suppose Alice has a secret message in form of a sequence of bits $A = \{i_n, j_n \in \{0,1\}; n = 1,2,...,N\}$ while Bob has another secret message in form of another sequence of bits $B = \{k_n, l_n \in \{0,1\}; n = 1,2,...,N\}$ and they wish to exchange their messages in a secure fashion.

Conventionally, Alice and Bob can do that if they share beforehand two secret keys $K^{(1)} = \{x_n^{(1)}, y_n^{(1)} \in \{0,1\}; n = 1,2,...,N\}$ and $K^{(2)} = \{x_n^{(2)}, y_n^{(2)} \in \{0,1\}; n = 1,2,...,N\}$ with $x_n^{(1,2)}, y_n^{(1,2)}$ being random bits known only to the two communicators Alice and Bob. The keys can be created either classically when Alice and Bob meet in person or quantumly when they are at remote locations by performing quantum key distribution protocols [8,9]. Anyway, the keys $K^{(1,2)}$ should be shared prior to exchanging the messages. Alice encrypts her message to be $A' = A \oplus K^{(1)} = \{p_n^{(1)}, q_n^{(1)} \in \{0,1\}; n = 1,2,...,N\}$, where $p_n^{(1)} = i_n \oplus x_n^{(1)}$, $q_n^{(1)} = j_n \oplus y^{(1)}$ with $\oplus$ implying the XOR operation, then publicly publishes A' for Bob to decrypt $A = A' \oplus K^{(1)}$. After that, Bob uses the second key to encrypt his message to be $B' = B \oplus K^{(2)} = \{p_n^{(2)}, q_n^{(2)} \in \{0,1\}; n = 1,2,...,N\}$, where $p_n^{(2)} = k_n \oplus x_n^{(2)}$, $q_n^{(2)} = l_n \oplus y^{(2)}$, then publicly announces B' allowing Alice to decrypt $B = B' \oplus K^{(2)}$. A point worth noting is that for the messages' exchange two different keys are necessary, i.e., Bob cannot reuse $K^{(1)}$ to encrypt his message. If he did so, from the published encrypted messages A' and B' any eavesdropper Eve can learn the classical correlation $A \oplus B$ between the communicators' messages. Such a security loophole is referred to as information leakage which will be discussed in more detail later.

We now consider a possible urgent situation when Alice and Bob have no chance to share any secret keys in advance. It turns out that using single photons would allow Alice and Bob directly (i.e., without a prior key sharing) exchange their messages. Aiming to achieve that purpose there exists a number of methods some of which will be mentioned in what follows. Let $A =$

$\{i,j \in \{0,1\}\}$ and $B=\{k,l \in \{0,1\}\}$ for simplicity. The authors of [15] suggested a method, called Method 1, whereby they exploit hyperstates of travelling single photons. In certain bases associated with the P-DOF and S-DOF Bob prepares a photon in a hyperstate characterized by his secret bits k,l and sends the photon to Alice. Alice encodes her secret bits i,j by applying relevant operators on the hyperstate, changing it to that characterized by $k\oplus i, l\oplus j$ and sends the photon back to Bob. Because Bob prepared the photon he is able to measure it in the right bases to identify its characteristics determined by the measurement outcomes denoted by $\alpha = k\oplus i$, $\beta = l\oplus j$. From α,β Bob infers Alice's bits as $i=k\oplus\alpha$ and $j=l\oplus\beta$. Thus, Method 1 transfers two bits i,j from Alice to Bob. It is as good as that by means of superdense coding [2]. Note that differently from the superdense coding where two entangled photons are needed (one is travelling and the other always staying with Bob), in Method 1 there is only one photon in double DOFs. Moreover, the superdense coding requires difficult two-photon joint measurement while Method 1 demands only simple one-photon measurement. Method 1 is thus more feasible. For Bob to transfer his bits to Alice, it seems that Bob reveals his measurement outcomes α,β from which Alice could obtain Bob's bits as $k=i\oplus\alpha$ and $l=j\oplus\beta$ as she knows i,j. However, bad thing is that the bits α,β themselves reflect classical correlations between Alice's and Bob's bits, which Eve can learn for free by just listening to the public announcement. From the information theory point of view, this implies occurrence of an information leakage [16, 17]. Hence, Method 1 does not work for fully secure direct information exchanging. The authors of [18] developed another method, called Method 2, which consists of three steps. In step 1 Alice prepares an original photon state $|r\rangle_{origin}$ with a random $r\in\{0,1\}$ where $|0\rangle = |h\rangle$ and $|1\rangle = |v\rangle$. She then transforms the original state to $|r\oplus i\rangle_{origin}$ with i being her secret bit and sends the photon to Bob. In step 2 Bob encodes his bit k by further transforming $|r\oplus i\rangle_{origin}$ to $|r\oplus i\oplus k\rangle_{origin}$. Next, he takes an ancillary photon in state $|0\rangle_{ancilla}$ and performs a controlled-NOT (CNOT) on the two photons with the original photon as the control and the ancillary photon as the target, resulting in the two-photon separable state $|r\oplus i\oplus k\rangle_{origin}|r\oplus i\oplus k\rangle_{ancilla} = CNOT\,|r\oplus i\oplus k\rangle_{origin}|0\rangle_{ancilla}$. Bob returns the original photon to Alice while measures the ancillary photon in the basis $\{|0\rangle,|1\rangle\}$ to determine $r\oplus i\oplus k = p$. In step 3 Alice measures the original photon also in the basis $\{|0\rangle,|1\rangle\}$ to obtain the same value p. Since r is known to Alice, she infers Bob's bit as $k=r\oplus i\oplus p$. After that, Alice broadcasts r in order for Bob to decode Alice's bit as $i=r\oplus k\oplus p$. Method 2 is bidirectional but faces the following serious problem. The problem is that all the photon states in Method 2 are in a known basis $\{|0\rangle,|1\rangle\}$. So, in step 1, when the original photon travels from Alice to Bob, Eve measures it in the basis $\{|0\rangle,|1\rangle\}$ to learn $r\oplus i = q$ without any traces left behind. Later, in stage 2, when Bob sends Alice the original photon, Eve again measures it in the right basis to also learn $p=r\oplus i\oplus k$. Finally, in stage 3, when Alice reveals r Eve uses it together with q and p to deduce both Alice's bit $i=r\oplus q$ and Bob's bit $k=q\oplus p$. Thus, despite the randomness of r, Method 2 is totally insecure as opposed to the claim of the authors. The insecurity of Method 2 was attempted to overcome by Method 3 [19] employing photon hyperstates in both P-DOF and S-DOF. Alice and Bob apply different local encoding operation chosen separately from the Pauli operators in Eqs. (7) - (8) and Hadamard operators in Eqs. (9) - (10). As one photon in a hyperstate carries two bits of information, the capacity of Method 3 is high. The authors said that their method is information-leakage free but that is not so because the bits they announce are in fact the XOR values of their secret bits. Later, a possible method, Method 4, was proposed in Refs. [20, 21] to countermeasure against information leakage by modifying the way of encoding. Namely, a secret bit of Alice is encoded by one of two random options, say, options A1 and A2, with the aid of Hadamard operators. Bob also has to options B1 or B2 with the aid of Pauli operators to encode his bit. By doing so, depending on her encoding choice (A1 or A2), Alice can decode Bob's bit independent of his encoding option. Likewise, depending on his encoding choice (B1 or B2), Bob can decode Alice's bit independent of her encoding option. Eve is unable to obtain neither Alice's bit nor Bob's bit nor their classical correlation because she is ignorant of the applied encoding options of Alice and Bob. Method 4 thus escapes the risk of information leakage. The limitation is its inefficacy: only two bits can be exchanged (one from Alice to Bob and one the other way around), not talking about the quite confused encoding options. Recently, a new method, Method 5, has appeared [22] which gets rid of information leakage but still suffers from a technical drawback. We shall present Method 5 in detail to see how it works and then find way to cope with its drawback. For convenience, we shall introduce our mathematical notations.

The hyperstate of a photon in both P-DOF and S-DOF has the most general form

$$|\Psi\rangle_{PS} = x\,|h\rangle_P\,|a_0\rangle_S + y\,|h\rangle_P\,|a_1\rangle_S + z\,|v\rangle_P\,|a_0\rangle_S + t\,|v\rangle_P\,|a_1\rangle_S\,, \tag{1}$$

with $|h\rangle_P$ ($|v\rangle_P$) state in P-DOF of a photon which is horizontally (vertically) polarized, $|a_0\rangle_S$ ($|a_1\rangle_S$) state in S-DOF of a photon which propagates along spatial path a_0 (a_1) and x, y, z, t complex coefficients satisfying the normalization constraint $|x|^2+|y|^2+|z|^2+|t|^2=1$. Of our concern are the following sixteen specific hyperstates which we mathematically formulate as

$$|\psi_{b_P,m,b_S,n}\rangle_{PS} = |b_P,m\rangle_P\,|b_S,n\rangle_S\,, \tag{2}$$

with $b_P, b_S, m, n \in \{0,1\}$. In Eq. (2) b_P identifies the basis in P-DOF: $b_P = 0$ (1) implies the basis $\{|h\rangle_P\,,\,|v\rangle_P\}$ $(\{|+\rangle_P = (|h\rangle_P + |v\rangle_P)/\sqrt{2}$, $|-\rangle_P = (|h\rangle_P - |v\rangle_P)/\sqrt{2}\})$ and $m = 0$ (1) indicates $|h\rangle_P$ or $|+\rangle_P$ ($|v\rangle_P$ or $|-\rangle_P$). That is,

$$|0,0\rangle_P = |h\rangle_P\,, |0,1\rangle_P = |v\rangle_P\,, \tag{3}$$

$$|1,0\rangle_P = |+\rangle_P\,, |1,1\rangle_P = |-\rangle_P\,. \tag{4}$$

As for S-DOF, $b_S = 0$ (1) implies the basis $\{|a_0\rangle_S\,,\,|a_1\rangle_S\}$ $(\{|s\rangle_S = (|a_0\rangle_S + |a_1\rangle_S)/\sqrt{2}$, $|a\rangle_S = (|a_0\rangle_S - |a_1\rangle_S)/\sqrt{2})$ and $n = 0$ (1) indicates $|a_0\rangle_S$ or $|s\rangle_S$ ($|a_1\rangle_S$ or $|a\rangle_S$). That is,

$$|0,0\rangle_S = |a_0\rangle_S\,, |0,1\rangle_S = |a_1\rangle_S\,, \tag{5}$$

$$|1,0\rangle_S = |s\rangle_S\,, |1,1\rangle_S = |a\rangle_S\,. \tag{6}$$

Clearly, the hyperstates (2) are particular cases of (1), i.e., $|\psi_{o,o,o,o}\rangle_{PS} = |\Psi\rangle_{PS}|_{x=1}\,,\ |\psi_{o,o,o,1}\rangle_{PS} = |\Psi\rangle_{PS}|_{y=1}\,,\ |\psi_{o,o,1,o}\rangle_{PS} = |\Psi\rangle_{PS}|_{x=y=1/\sqrt{2}}\,,\ |\psi_{o,o,1,1}\rangle_{PS} = |\Psi\rangle_{PS}|_{x=-y=1/\sqrt{2}}$ and so on. Any of the sixteen hyperstates (2) is easy to produce from the hyperstate $|0,0\rangle_P\,|0,0\rangle_S$ by means of linear-optics toolkits such as beam-splitter, polarization beam-splitter, half-wave/quarter-wave plates, etc.. Secret bits can be hidden in photon hyperstates by application of unitary operators

$$Y_P = |h\rangle_P\,\langle v| - |v\rangle_P\,\langle h|\,, \tag{7}$$

$$Y_S = |a_0\rangle_S\,\langle a_1| - |a_1\rangle_S\,\langle a_0|\,, \tag{8}$$

$$H_P = |+\rangle_P\,\langle h| + |-\rangle_P\,\langle v|\,, \tag{9}$$

$$H_S = |s\rangle_S\,\langle a_0| + |a\rangle_S\,\langle a_1|\,. \tag{10}$$

It is straightforward to verify that, for any $x, y \in \{0,1\}$,

$$Y_P^x \otimes Y_S^y \left|b_P, m\right\rangle_P \left|b_S, n\right\rangle_S = (-1)^{x(b_P+m+x)+y(b_S+n+y)} \left|b_P, m\oplus x\right\rangle_P \left|b_S, n\oplus y\right\rangle_S, \quad (11)$$

$$H_P^x \otimes H_S^y \left|b_P, m\right\rangle_P \left|b_S, n\right\rangle_S = \left|b_P \oplus x, m\right\rangle_P \left|b_S \oplus y, n\right\rangle_S. \quad (12)$$

From Eqs. (11) and (12), the operators Y_P, Y_S change the basis state but not the type of basis, whereas the operators H_P, H_S change the basis type but keep the basis state unchanged. In what follows the global phase factor $(-1)^{x(b_P+m+x)+y(b_S+n+y)}$ in Eq.(11) will be omitted because it causes no physical effects in the tasks under consideration.

In Method 5 [22] at the beginning Bob chooses random b_P, m, b_S, n to prepare two photons in the hyperstate $|\phi\rangle_{PS}^{(1)} |\phi\rangle_{PS}^{(2)}$ with $|\phi\rangle_{PS}^{(1)} = |\phi\rangle_{PS}^{(2)} = |b_P, m\rangle_P |b_S, n\rangle_S$ and sends both photons to Alice. Alice hides her secret bits i, j in $|\phi\rangle_{PS}^{(1)}$ by applying $Y_P^i Y_S^j$ on it, i.e.,

$$|\phi\rangle_{PS}^{(1)} \to \left|\phi_{ij}\right\rangle_{PS}^{(1)} = |b_P, m\oplus i\rangle_P |b_S, n\oplus j\rangle_S, \quad (13)$$

and returns $\left|\phi_{ij}\right\rangle_{PS}^{(1)}$ to Bob, while stores $|\phi\rangle_{PS}^{(2)}$ intact in a quantum memory. Upon receiving $\left|\phi_{ij}\right\rangle_{PS}^{(1)}$ Bob applies $Y_P^k Y_S^l$ on it to encode his secret bits k, l. The hyperstate $\left|\phi_{ij}\right\rangle_{PS}^{(1)}$ becomes

$$\left|\phi_{ij,kl}\right\rangle_{PS}^{(1)} = |b_P, m\oplus i\oplus k\rangle_P |b_S, n\oplus j\oplus l\rangle_S. \quad (14)$$

Bob then measures $\left|\phi_{ij,kl}\right\rangle_{PS}^{(1)}$ in the bases in which he prepared the photons. Because the measurement bases are right (i.e., b_P for P-DOF and b_S for S-DOF), measurement outcomes should be

$$p = m\oplus i\oplus k, \quad (15)$$

$$q = n\oplus j\oplus l, \quad (16)$$

i.e., the measured photon should be found in the hyperstate $|b_P, p\rangle_P |b_S, q\rangle_S$. Since Bob knows m, n, k, l he can immediately decode Alice's bits from his measurement outcomes p, q as

$$i = m\oplus p\oplus k, \quad (17)$$

$$j = n\oplus q\oplus l. \quad (18)$$

As for the photon kept in Alice's quantum memory, it is still in the hyperstate $|\phi\rangle_{PS}^{(2)} = |b_P, m\rangle_P |b_S, n\rangle_S$ unknown to her, so it does not help Alice in any decoding. To enable Alice's decoding, Bob needs to announce the bases b_P, b_S together with the outcomes p, q. Only after hearing b_P, b_S from Bob's announcement Alice starts measuring $|\phi\rangle_{PS}^{(2)}$ in the right bases to determine m, n. Then, combining m, n with p, q she is able to decode Bob's secret bits as

$$k = m\oplus p\oplus i, \quad (19)$$

$$l = n\oplus q\oplus j. \quad (20)$$

As the announced bits p and q (see Eqs. (15) and (16)) contain random m, n unknown to the outsider, Method 5 circumvents the information leakage. However, a quantum memory is required to store photon in hyperstate $|\phi\rangle_{PS}^{(2)}$ for a time duration long enough: Alice can measure $|\phi\rangle_{PS}^{(2)}$ only after Bob finishes his encoding process, measurement and announcement. The requirement of such a quantum memory makes Method 5 infeasible technically.

To avoid use of quantum memory we shall construct an improved method as follows. At the initial time $t = 0$ Bob chooses a pair of random bits b_P, b_S serving as the bases for preparing two identical photons, each in the same hyperstate $|b_P,0\rangle_P\,|b_S,0\rangle_S$. The initial two-photon hyperstate can be written in the form

$$|\Psi_0\rangle_{PS} = |\phi_0\rangle_{PS}^{(1)}\,|\psi_0\rangle_{PS}^{(2)} \tag{21}$$

where

$$|\phi_0\rangle_{PS}^{(1)} = |\psi_0\rangle_{PS}^{(2)} = |b_P,0\rangle_P\,|b_S,0\rangle_S\,, \tag{22}$$

with the super-indices (1) and (2) labeling the photon 1 and photon 2, respectively. Then, at time $t = 1$, he chooses another pair of random bits α, β and applies $Y_P^{\alpha} \otimes Y_S^{k}$ on photon 1 and $Y_P^{\beta} \otimes Y_S^{l}$ on photon 2 to transform $|\Psi_0\rangle_{PS}$ to

$$|\Psi_1\rangle_{PS} = |\phi_1\rangle_{PS}^{(1)}\,|\psi_1\rangle_{PS}^{(2)}\,, \tag{23}$$

where

$$|\phi_1\rangle_{PS}^{(1)} = |b_P,\alpha\rangle_P\,|b_S,k\rangle_S \tag{24}$$

and

$$|\psi_1\rangle_{PS}^{(2)} = |b_P,\beta\rangle_P\,|b_S,l\rangle_S\,, \tag{25}$$

with k, l Bob's two secret bits. Bob continues by sending the two photons of $|\Psi_1\rangle_{PS}$ to Alice.

At a later time $t = 2$, when Alice receives the hyperstate $|\Psi_1\rangle_{PS}$, she encodes her secret bits i, j by applying $Y_P^{i} \otimes Y_S^{\mu}$ on photon 1 and $Y_P^{j} \otimes Y_S^{\nu}$ on photon 2, with μ, ν new randomly chosen bits. These actions transform the hyperstate $|\Psi_1\rangle_{PS}$ to

$$|\Psi_2\rangle_{PS} = |\phi_2\rangle_{PS}^{(1)}\,|\psi_2\rangle_{PS}^{(2)}\,, \tag{26}$$

where

$$|\phi_2\rangle_{PS}^{(1)} = |b_P,\alpha \oplus i\rangle_P\,|b_S,k \oplus \mu\rangle_S \tag{27}$$

and

$$|\psi_2\rangle_{PS}^{(2)} = |b_P,\beta \oplus j\rangle_P\,|b_S,l+\nu\rangle_S\,, \tag{28}$$

which is sent back to Bob. Next, at time $t = 3$, right after arrival of $|\Psi_2\rangle_{PS}$, Bob measures each of the two photons in the bases b_P, b_S. As b_P, b_S are the bases in which Bob had prepared the photons, the hyperstate he will find by the measurement must be of the form

$$|\Psi_3\rangle_{PS} = |\phi_3\rangle_{PS}^{(1)}\,|\psi_3\rangle_{PS}^{(2)}\,, \tag{29}$$

where

$$|\phi_3\rangle_{PS}^{(1)} = |b_P,d\rangle_P\,|b_S,f\rangle_S\,, \tag{30}$$

with

$$d = \alpha \oplus i, f = k \oplus \mu, \tag{31}$$

and

$$|\psi_3\rangle_{PS}^{(2)} = |b_P,g\rangle_P\,|b_S,h\rangle_S\,, \tag{32}$$

with

$$g = \beta \oplus j, h = l+\nu. \tag{33}$$

The bits d, f, g and h are regarded as Bob's measurement outcomes. After the measurement Bob keeps d and g with him for later use but publicly announces f and h by means of an open reliable classical communication channel.

Finally, at time $t = 4$, with the known α, β, d and g Bob can straightforwardly decode Alice's secret bits as

$$i = \alpha \oplus d, j = \beta \oplus g, \tag{34}$$

while Alice can also straightforwardly decode Bob's secret bits as

$$k = f \oplus \mu, l = h + \nu, \tag{35}$$

because she knows f and h from Bob's announcement and μ, ν are previously chosen by her.

In our method only two bits f and h are to be announced. Notably, $f = k \oplus \mu$ and $h = l + \nu$ are themselves random and their XOR value $f \oplus h = k \oplus \mu \oplus l \oplus \nu$ is random too, thanks to the fact that μ and ν have been on purpose chosen randomly by Alice at time $t = 2$. Therefore, any third party listening to the broadcasted bits f and h does not gain any meaningful information. That means that our method is information leakage free as was Method 5. Interestingly, our method is superior to Method 5. A detailed comparison with Method 5 shows that method 5 and our method are equally efficient: both methods allow to exchange four secret bits (two from Alice to Bob and two from Bob to Alice). Nevertheless, from a practical point of view, our method is more feasible, simpler and more economical than Method 5 that is justified by the following three specific features. Firstly, as described above, Method 5 requires a long-effective quantum memory device for Alice to keep one photon (photon 2) until she hears Bob's announcement of the bases b_P, b_S of the photon preparation. Only after having known b_P, b_S Alice will be in the position to make her measurement on photon 2 to decode Bob's secret bits. In contrast, our method does not require such quantum memory, so our method is more feasible. Secondly, in Method 5 both Alice and Bob should do their measurements, while in our method only Bob must measure the photons at time $t = 3$ immediately after he obtains them, so our method is simpler in execution. Thirdly, in Method 5 four bits of classical communication, namely, b_P, b_S (which are the two bases in which the photons were prepared) and p, q (which are the two outcomes of Bob's measurement on photon 1), must be publicly revealed, while in our method the number of to-be-disclosed bits is only two, namely, f and h (which are two out of the four measurement outcomes of Bob), so in our method the classical communication cost is just 50% of that consumed in Method 5, implying that our method is more economical. Fig. 1 visually displays the processing steps of our method.

To securely exchange the whole long messages $A = \{i_n, j_n \in \{0,1\}; n = 1,2,...,N\}$ and $B = \{k_n, l_n \in \{0,1\}; n = 1,2,...,N\}$ Alice and Bob must obey certain procedures to detect possible eavesdropping attacks. Since the photons travel forth and back in open space between Alice and Bob and eavesdroppers always ambush on the quantum channels as spies, detecting various kinds of eavesdropping attacks is compulsory to ensure the security. The most well-known and effective detection strategy makes use of so-called decoy photons. The decoy-photon-based technique is familiar in the literature so we just outline it briefly here. Instead of preparing two photons in the hyperstate $|\Psi_1\rangle_{PS}$ of Eq. (23), Bob prepares a batch $\mathscr{B}_1$ of ordered photon pairs as

$$\mathscr{B}_1 = \{|\Psi_{1,n}\rangle_{PS}; n = 1,2,...,N\}, \tag{36}$$

where

$$|\Psi_{1,n}\rangle_{PS} = |\phi_{1,n}\rangle_{PS}^{(1)} |\psi_{1,n}\rangle_{PS}^{(2)}, \tag{37}$$

with

$$|\phi_{1,n}\rangle_{PS}^{(1)} = |b_P, \alpha_n\rangle_P |b_S, k_n\rangle_S \tag{38}$$

and

$$|\psi_{1,n}\rangle_{PS}^{(2)} = |b_P, \beta_n\rangle_P |b_S, l_n\rangle_S. \tag{39}$$

In the above formulae $\{\alpha_n, \beta_n\}$ are random bits and $\{k_n, l_n\}$ Bob's secret bits. It is crucial to emphasize that though $\{\alpha_n, \beta_n\}$ are random they are chosen by Bob so nobody except Bob knows

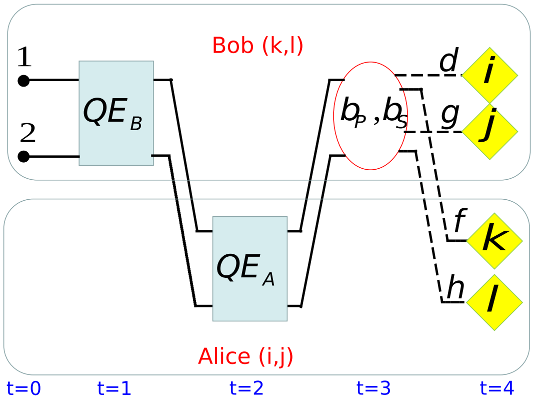

Fig. 1. Schematic illustration of chronological steps in our method. The secret bits to be exchanged are i, j possessed by Alice and k, l possessed by Bob. Bob kicks off with two photons in the same hyperstate $|b_P,0\rangle_P\,|b_S,0\rangle_S$ (see Eq. (2)). The rectangular with QE_B (QE_A) represents Bob's (Alice's) quantum operation in which P-DOF Pauli operators in Eq. (7) and S-DOF ones in Eq. (8) are used to encode his (her) secret bits k, l (i, j) as well as to introduce necessary random bits α, β (μ, ν). The oval with b_P, b_S represents the photon measurement in the bases b_P, b_S. Photon is displayed by a solid line, while dashed lines are classical communication channels used for announcement of the measurement outcomes h, g, f and h. The diamond is the classical decoding calculation based on the measurement outcomes. Time flies from left to right. See text for more details.

them. After successful preparation of the photon batch $\mathscr{B}_1$, Bob takes a large enough number of decoy photon pairs and inserts them into batch $\mathscr{B}_1$ with the positions of the decoy photons recorded. Each photon of a decoy photon pair is randomly put in one of the four states $|h\rangle$, $|v\rangle$, $|+\rangle$ or $|-\rangle$. Then, by the block transmission technique [23], Bob transmits Alice the photon block consisting of both the photons in batch $\mathscr{B}_1$ and the inserted decoy photons. After Alice receives the photon block, Bob guides Alice to figure out the decoy photons and they together carry out the security check as described explicitly in [9]. If the security level is acceptable (i.e., it is higher than a prefixed threshold), Alice remove all the decoy photons and encodes her secret bits i_n, j_n on the photons in batch $\mathscr{B}_1$ to form a new batch $\mathscr{B}_2$,

$$\mathscr{B}_2 = \{|\Psi_{2,n}\rangle_{PS}; n = 1, 2, ..., N\}, \tag{40}$$

where

$$|\Psi_{2,n}\rangle_{PS} = |\phi_{2,n}\rangle^{(1)}_{PS}\,|\psi_{2,n}\rangle^{(2)}_{PS}, \tag{41}$$

where

$$|\phi_{2,n}\rangle^{(1)}_{PS} = |b_P, \alpha_n \oplus i_n\rangle_P\,|b_S, k_n \oplus \mu_n\rangle_S \tag{42}$$

and

$$|\psi_{2,n}\rangle^{(2)}_{PS} = |b_P, \beta_n \oplus j_n\rangle_P\,|b_S, l_n + \nu_n\rangle_S, \tag{43}$$

with randomly chosen bits μ_n and ν_n known solely by Alice. Alice also makes use of the same decoy photon technique and transmits to Bob the new block consisting of both the photons in batch $\mathscr{B}_2$ and the new decoy photons which she prepared and inserted into batch $\mathscr{B}_2$. After Bob confirms receipt of the photon block, Alice tells Bob the positions of the decoy photons and they together check the security level. If the error rate is lower than a prefixed threshold, Bob disregards all the decoy photons and measures each photon pair in batch $\mathscr{B}_2$ in the bases b_P, b_S. What he should find are a sequence of hyperstates

$$\{|\Psi_{3,n}\rangle_{PS} = |\phi_{3,n}\rangle_{PS}^{(1)} |\psi_{3,n}\rangle_{PS}^{(2)}\}, \tag{44}$$

where

$$|\phi_{3,n}\rangle_{PS}^{(1)} = |b_P, d_n\rangle_P |b_S, f_n\rangle_S, \tag{45}$$

with

$$d_n = \alpha_n \oplus i_n, f_n = k_n \oplus \mu_n \tag{46}$$

and

$$|\psi_{3,n}\rangle_{PS}^{(2)} = |b_P, g_n\rangle_P |b_S, h_n\rangle_S, \tag{47}$$

with

$$g_n = \beta_n \oplus j_n, h_n = l_n + \nu_n. \tag{48}$$

Next, Bob lets Alice know the measurement outcomes f_n and h_n so that Alice's decoding reads

$$k_n = f_n \oplus \mu_n, l_n = h_n + \nu_n. \tag{49}$$

Bob himself decodes Alice's bits as

$$i_n = \alpha_n \oplus d_n, j_n = \beta_n \oplus g_n. \tag{50}$$

The above decoding rules are valid for every n, meaning that Alice's secret message $A = \{i_n, j_n; n = 1, 2, ..., N\}$ and Bob's secret message $B = \{k_n, l_n; n = 1, 2, ..., N\}$ are absolutely securely exchanged.

III. CONCLUSION

We have briefly reviewed existing quantum methods for exchanging secret messages between two distant parties employing single photons as information shuttles. Some methods are shown insecure, others appear not fully secure in the sense that, though the exchanged secret bits themselves cannot be cracked, their classical correlations leak out to an outsider who needs no efforts other than listening to the public announcement of the authorized communicator. From an information theory point of view, such a security loophole has the name 'information leakage'. Recently, in 2021, there is an efficient method [22] which is resistant of information leakage by utilizing single-photon hyperstates (i.e., states of single photons in both polarization and spatial degrees of freedom). Yet, this method suffers from a technical difficulty that it necessitates long-working quantum memory. Although single photons are quite easy to prepare and operate even in multiple degrees of freedom, quantum memory devices working for a long enough time are still challenging at present. So the method in [22] is regarded as of little feasibility in practice. Our method in this paper also uses single-photon hyperstates but the way the secret bits are encoded is modified by judiciously introducing relevant random bits by the two communicators so that the photons can be measured right away as they arrive without the need of keeping them intact for some time till their actual measurement. That is, no quantum memory is required for our method. Furthermore, in our method only Bob (not both Bob and Alice) needs to carry out measurement and the classical communication cost in our method is just half of that in the method of [22]. With the just-mentioned features our improved method is more feasible, simpler and cheaper than that in [22] and is thus within the reach of available modern quantum technologies.

ACKNOWLEDGMENTS

The author is grateful to Thang Long Institute of Mathematics and Applied Sciences and Thang Long University for supporting the author's research direction on the field of quantum information and quantum computation.

REFERENCES

[1] E. Schrödinger, Discussion of probability relations between separated systems, *Mathematical Proceedings of the Cambridge Philosophical Society* **31** (1935) 555.

[2] C. Bennett and S. Wiesner, *Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states*, *Phys. Rev. Lett.* **69** (1992) 2881.

[3] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and K. W. Wootters, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, *Phys. Rev. Lett.* **70** (1993) 1895.

[4] C. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal and W. K. Wootters, *Remote state preparation*, *Phys. Rev. Lett.* **87** (2001) 077902.

[5] B. A. Nguyen and J. Kim, *Joint remote state preparation*, *J. Phys. B: At. Mol. Opt. Phys.* **41** (2008) 095501.

[6] P. W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, *Proceedings 35th Annual Symposium on Foundations of Computer Science* (1994) 124.

[7] A. R. Calderbank, E.M. Rains, P. W. Shor and N.J. A. Sloane, *Quantum error correction via codes over GF(4)*, *IEEE Trans. Inf. Theory* **44** (1998) 1369.

[8] A. Ekert, *Quantum cryptography based on Bell's theorem*, *Phys. Rev. Lett.* **67** (1991) 661.

[9] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* **175** (1984) 8.

[10] M. Hillery, V. Bužek, and A. Berthiaume, *Quantum secret sharing*, *Phys. Rev. A* **59** (1999) 1829.

[11] G. P. Guo and G. C. Guo, *Quantum secret sharing without entanglement*, *Phys. Lett. A* **310** (203) 247.

[12] B. A. Nguyen, *Quantum dialogue*, *Phys. Lett. A* **328** (2004) 6.

[13] B. A. Nguyen, *Secure dialogue without a prior key distribution*, *J. Kor. Phys. Soc.* **47** (2005) 562.

[14] Y. Chen, Z. X. Man and Y.J. Xia, *Quantum bidirectional secure direct communication via entanglement swapping*, *Chinese Phys. Lett.* **24** (2007) 19.

[15] D. Liu, J. L. Chen and W.Jiang, *Quantum secure communication protocol with signature*, *Int. J. Theor. Phys.* **51** (2012) 2923.

[16] F. Gao, F. Z. Guo, Q. Y. Wen and F. C. Zhu, *Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication*, *Sci. China Ser. G: Phys, Mech. and Astr.* **51** (2008) 559.

[17] Y. G. Tan and Q. Y. Cai, *Classical correlation in quantum dialogue*, *Int. J. Quant. Inf.* **6** (2008) 325.

[18] N. R. Zhou, T. X. Hua, G. T. Wu, C. S. He and Y. Zhang, Single-photon secure quantum dialogue protocol without information leakage, *Int. J. Theor. Phys.* **53** (2014) 3829.

[19] L. L. Wang, W. P. Ma. D. S. Shen and M. L.Wang, *Efficient bidirectional quantum secure direct communication with single photons in both polarization and spatial-mode degrees of freedom*, *Int. J. Theor. Phys.* **54** (2015) 3443.

[20] Z. H. Liu, H. W. Chen and W. J. Liu, *Information leakage problem in efficient bidirectional quantum secure direct communication with single photons in both polarization and spatial-mode degrees of freedom*, *Int. J. Theor. Phys.* **55** (2016) 4681.

[21] C. Zhang and H. Situ, *Information leakage in efficient bidirectional quantum secure direct communication with single photons in both polarization and spatial-mode degrees of freedom*, *Int. J. Theor. Phys.* **55** (2016) 4702.

[22] T. Y. Ye, H. K. Li and J. L. Hu, *Information leakage resistant quantum dialogue with single photons in both polarization and spatial-mode degrees of freedom*, *Quantum Inf. Process.* **20** (2021) 209.

[23] G. L. Long and X. S. Liu, *Theoretically efficient high-capacity quantum-key-distribution scheme*, *Phys. Rev. A* **65** (2002) 032302.