

Practical quantum encryption protocol with varying encryption configurations

Junxu Li, Zixuan Hu, and Sabre Kais ^{*}

Department of Chemistry, Department of Physics and Astronomy, and Purdue Quantum Science and Engineering Institute, Purdue University, West Lafayette, Indiana 47907, USA



(Received 24 February 2021; accepted 4 June 2021; published 28 June 2021)

Quantum communication is an important application that derives from the burgeoning field of quantum information and quantum computation. Focusing on secure communication, quantum cryptography has two major directions of development, namely quantum key distribution and quantum encryption. In this work we propose a quantum encryption protocol that utilizes a quantum algorithm to create blocks of ciphertexts based on quantum states. The main feature of our quantum encryption protocol is that the encryption configuration of each block is determined by the previous blocks, such that additional security is provided. We then demonstrate our method by an example model encrypting the English alphabet, with numerical simulation results showing the large error rate of a mock attack by a potential adversary. The safety of the encryption method is further demonstrated against several possible attack models. With the improvements against noises, our quantum encryption protocol is a capable addition to the toolbox of quantum cryptography.

DOI: [10.1103/PhysRevResearch.3.023251](https://doi.org/10.1103/PhysRevResearch.3.023251)

I. INTRODUCTION

Utilizing quantum technologies for communication has been a major focus of the field of quantum computation and quantum information [1–4]. In particular, with emphasis on secure communication, quantum cryptography has seen enormous progress with both theoretical and experimental advances [5–7]. One major direction of quantum cryptography, quantum key distribution (QKD) [7–10], enables secure key generation and distribution by exploiting the nonlocality of quantum entanglement. The other major direction of quantum cryptography, quantum encryption [11–13], uses quantum computing techniques to create quantum states that carry the ciphertext.

The development of physical realizations of qubit systems and quantum circuits has led to a variety of breakthroughs including the success of ground-to-satellite communication [14,15], which enables reliable ultralong-distance quantum key distribution, and electron spin state teleportation with high fidelity, which proclaims the feasibility to achieve quantum teleportation in molecular systems [16]. There also arise pioneers of quantum teleportation in various systems such as atomic ensembles [17], electron spins in quantum dots [18], trapped ions [19], and superconducting circuits [20]. With these state-of-the-art advances in experimental techniques, one can envision the near-future realization of highly

complex and sophisticated quantum communication protocols protected by quantum encryption methods.

In this work, we propose a quantum communication protocol with quantum encryption. As a block cipher, the plaintexts and the corresponding ciphertexts are sent in sequential blocks encrypted by a fixed number of qubits. The main feature that makes our quantum encryption method different from others is that the encryption configuration of each block is determined by the previous blocks, such that adjacent blocks are more likely to use different encryption configurations. This makes the encryption more difficult to break for a potential adversary. In the first section, we present the basic communication process in detail, where an example setup for the encryption and decryption processes is discussed. In the second section we discuss the security of the quantum encryption protocol against a potential adversary. In particular, we demonstrate the encryption of the English alphabet with an example model, showing the large error rate of a mock attack in a numerical simulation. We then give potential improvements of the quantum encryption that aim to reduce noises and further increase security. In the last section, we will discuss the protection against other possible attacks, and the appropriate length of a single piece of message for the best performance of the method.

II. THEORETICAL FRAMEWORK

Consider a scenario shown in Fig. 1: Alice is nearly isolated from the outside environment, and the only connection with the outside environment is N qubits $\{q_1, q_2, \dots, q_N\}$. Alice attempts to communicate with her friend Bob via these qubits. Alice works periodically: (1) At $t = kT, k = 0, 1, 2, \dots$, she will prepare $\{q_1, q_2, \dots, q_N\}$ to be the state $|\Psi_k\rangle$, where k means the state is prepared at time kT . (2) During $t \in (kT, kT + t_1]$, Bob can perform arbitrary

^{*}kais@purdue.edu

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

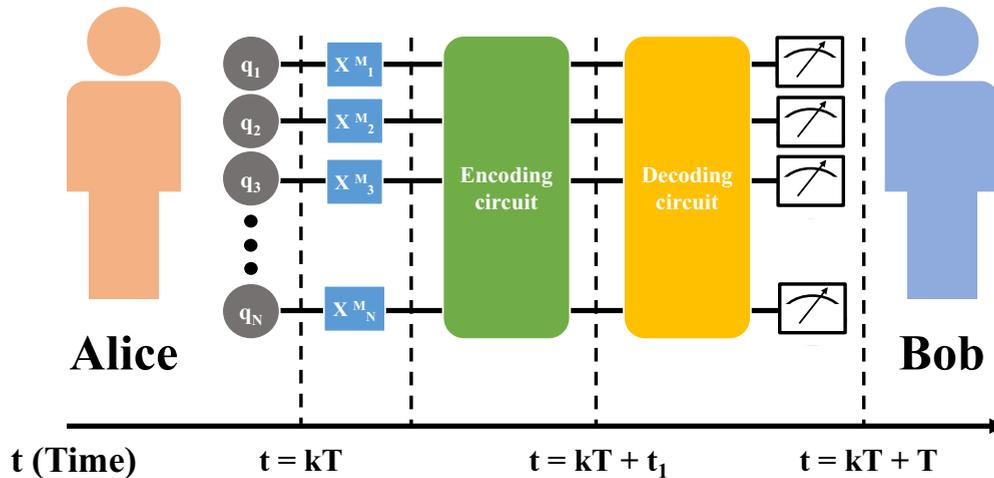


FIG. 1. Communication strategy between Alice and Bob. Alice is isolated from the outside environment. Alice’s friend Bob attempts to communicate with Alice. The only connection between Alice and Bob is some shared qubits. Both Alice and Bob can apply arbitrary operations on the qubits, and Bob can apply Z measurement on every single qubit. When $t = kT$, where $k = 0, 1, 2, 3, \dots$, all qubits q_1, q_2, \dots, q_N will be set at state $|0\rangle$. Alice will start preparing the qubits at state $|\Phi_k\rangle = |M_1 M_2 \dots M_N\rangle$, and X represents the Pauli- X operation. Later, these qubits will be encoded into state $|\Psi_k\rangle$ via the encoding circuit (the green box). Alice needs to finish these processes before $t = kT + t_1$, and $t_1 < T$. Then Bob will start to decode the qubits, and then apply Z measurements on each qubit. Measurements are required to be done before $t = kT + T$, after which all qubits will be reset at state $|0\rangle$.

operations and measurements on the qubits, while during $t \in (kT + t_1, kT + T]$, only Alice herself can operate on the qubits, where $0 < t_1 < T$, and both Alice and Bob have enough time to finish their operations. Noise is negligible. (3) They are still able to communicate even when Alice cannot measure these qubits. When the noises and gate errors are ignored, we assume that Alice cannot receive any information from outside.

Alice and Bob apply a special quantum encoding circuit for encryption in their communication. The plaintext is divided into blocks with the same length. The structure of the encoding circuit depends on the previous block plaintext. The k th block of the ciphertext $|\Psi_k\rangle$ can be described as a function of the initial plaintext $|\Phi_k\rangle$ and the encoding circuit U_k :

$$|\Psi_k\rangle = U_k |\Phi_k\rangle, \tag{1}$$

where $U_k = U_k(|\Phi_{k-1}\rangle)$ is determined by the previous plaintext $|\Phi_{k-1}\rangle$.

During each time interval T , Alice will transport N -bit information via the N qubits. Note that one complete set of orthogonal eigenstates of these N qubits can be described as $\{|0\rangle, |1\rangle, \dots, |2^N - 1\rangle\}$, and an integer n from 0 to $2^N - 1$ can also represent the N -bit information just by rewriting n into the binary digit form. At time $t = kT$, Alice attempts to transport message n to Bob with the plaintext of the k th block $n(t = kT)$, and we denote $n(t = kT)$ as $n(k)$. For simplicity, in the following discussion the plaintext $|\Phi_k\rangle$ in Eq. (1) will be written as $|n(k)\rangle$. Alice encodes information into the quantum state $|\Psi_k\rangle = U_k |n(k)\rangle$, where $U_k = U_k(n(k - 1))$ is determined by the former n instead of a constant operation. They make an agreement that the first block is encrypted by the encoding circuit $U_0 = U_0(|0\rangle)$.

Figure 2 is a sketch of the encryption process. When $k > 1$, the k th ciphertext $|\Psi_k\rangle$ is generated by encrypting the plaintext $|n(k)\rangle$ and the encoding circuit U_k , $|\Psi_k\rangle = U_k |n(k)\rangle$, where the

encoding operation $U_k = U_k(|n(k - 1)\rangle)$ is determined by the former plaintext $|n(k - 1)\rangle$ and $\Theta_{1,2}$. $\Theta_{1,2}$ are some parameters shared by all encoding operations, and will be discussed when we demonstrate the encoding operations.

Generally, it requires a number of repeating measurements to get a quite accurate estimation of a certain quantum state; as an example, the widely used quantum tomography [21] requires exponential measurements to pin a quantum state. In addition, Alice’s special communication strategy makes it extremely difficult to extract the information from the N qubits. As no copy is offered, Bob needs to ensure that $n(k)$ can be derived after only one single measurement (here we ignored the noises and errors; strategies against noises in the circuit are discussed later). Besides, the encoding operator U_k is determined by the former plaintext n , so that all following results can no longer be convincing if we make a wrong estimation for even one single n . However, next we show that knowing the first encoding operator and the way in which the following encoding operators depend on the previous plaintexts, consequently Bob can indeed obtain $n(k)$ with ease. The difficulty created by the communication strategy therefore falls to Eve, the potential adversary who does not know the encoding operators.

Here, we will demonstrate the whole process of encryption and decryption. For simplicity, we assume that 6 qubits $\{q_1, q_2, \dots, q_6\}$ are used by Alice to communicate with Bob. Generally, 10 numbers, 26 capital letters and 26 small ones, a mark to divide words (blank space), and a mark to divide sentence (like, or .) are required in communication, so that in total 64 states $|\Psi\rangle$ are needed. As $2^6 = 64$, 6 qubits are already enough to encode the English alphabet together with numbers and marks. Sometimes special characters might be required in the communication, and methods to design encoding circuits for more qubits are presented in the Appendix. In fact, various encryption operations can be applied based

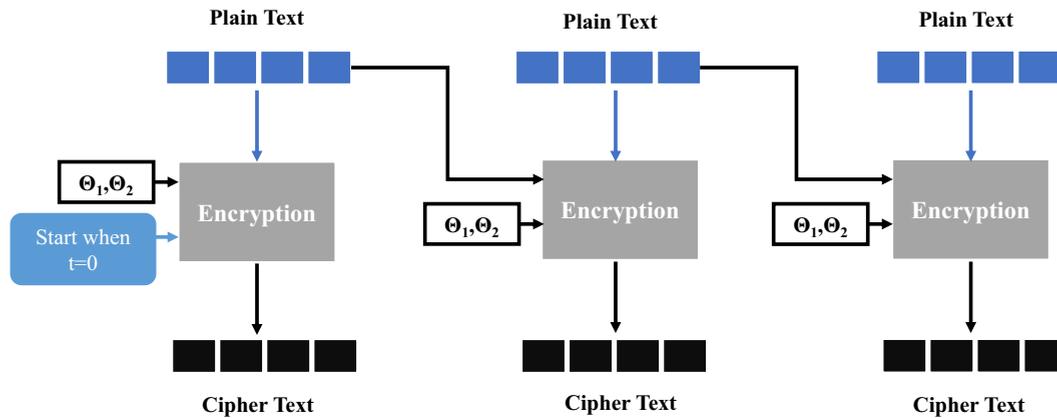


FIG. 2. Sketch of the encryption process. Binary message is divided into several blocks; each of them has the same length. Alice and Bob have set their clocks at the same time before being separated. They share the encoding operation encrypting the first block. When $k > 1$, the k th ciphertext $|\Psi_k\rangle$ is generated by encrypting the plaintext $|\Phi_k\rangle$ and the encoding circuit $U_k, |\Psi_k\rangle = U_k|\Phi_k\rangle$, where the encoding operation $U_k = U_k(|\Phi_{k-1}\rangle)$ is determined by the former plaintext $|\Phi_{k-1}\rangle$ and $\Theta_{1,2}$. $\Theta_{1,2}$ are some parameters shared by all encoding operations, and will be discussed when we demonstrate the encoding operations.

on the previous plaintext, and there is huge freedom choosing the configurations, which consequently makes it difficult for further studying. Hence, in the following model, we will consider a simple example where all U_k can be decomposed into 2-qubit control gates u_{ij} ,

$$u_{ij} = |0\rangle\langle 0|_i \otimes R_j(\Theta_1) + |1\rangle\langle 1|_i \otimes R_j(\Theta_2), \quad (2)$$

where $i, j \in \{1, 2, 3, 4, 5, 6\}, i \neq j$. q_j is controlled by q_i . $R(\Theta)$ is a single-qubit rotation gate, and $\Theta = (\theta_1, \theta_2, \theta_3, \theta_4)$ is a four-dimensional vector; $R(\Theta) = \exp(-i\theta_1 R_z(\theta_2) R_y(\theta_3) R_z(\theta_4))$. For example, in the simplest situation, U_k has only two possible choices, and these two encoding circuit are as follows:

Encoding circuit 1: 3-qubit loop. q_1, q_2, q_3 form one loop of control rotation gates and q_4, q_5, q_6 form another. Initially, q_1, q_2, \dots, q_6 are prepared at state $|n\rangle$, and $n = 0, 1, 2, \dots, 2^N - 1$, where there are N qubits used in their communication. Then Alice can use the circuit shown in Fig. 3(a) to encode information into $|\Psi_k^{in}\rangle$. We note this circuit as U_{tri} , and one can use U_{tri}^{-1} to extract information encoded by U_{tri} .

Encoding circuit 2: 2-qubit loop. As shown in Fig. 3(b), q_1, q_2 form one loop, and $q_3, q_4; q_5, q_6$ form two other loops, respectively. Initially, q_1, q_2, \dots, q_6 are prepared at state $|n\rangle$; then Alice can use this circuit to encode information into $|\Psi_k^{in}\rangle$. We would like to note this circuit as U_{bin} , and one can apply U_{bin}^{-1} as well to extract information encoded by U_{bin} .

If $n(k-1)$ is odd, then Alice will use circuit 1 to encode $n(k)$; otherwise, she will choose circuit 2 to encode $n(k)$. Obviously, the encoding strategy is determined by the bit stored in q_6 , as when q_6 represents 1 then Alice will use circuit 1 for encoding; otherwise circuit 2 will be chosen. Bob knows the parameters Θ_1, Θ_2 ; then as shown in Fig. 4, he can combine the inverse of circuit 1 and 2 together as the decoding circuit, where R_1 and R_2 represent $R^{-1}(\Theta_1)$ and $R^{-1}(\Theta_2)$, respectively. One auxiliary qubit q_{aux} is introduced to represent the previous measurement result to q_6 . In fact, such a circuit is not the only possible solution to decode information from Alice's

special communication strategy. If we prefer to make it more difficult to decode, it is also a choice to design more different encoding operations for every state $|n\rangle$, yet more auxiliary qubits will be required for such complicated strategies.

Note that even in the simplest examples displayed above, we still apply control rotation gates instead of stand-alone single-qubit gates. The existence of multiqubit gates in encryption ensures that the change of a single qubit in the cipher, which corresponds to the concept of diffusion in classical cryptography [22].

In summary, the secret key in the protocol contains three parts: the selection of configurations of the encryption operations, the parameters such as $\Theta_{1,2}$ that determine the encryption operations, and the ways that the encoding operations are determined by the previous plaintext blocks. All parts are essential for successful encryption and decryption.

III. APPLICATION IN QUANTUM COMMUNICATION

In this section, we will study a more complicated situation. Assume that Eve attempts to eavesdrop on the communication between Alice and Bob. As shown in Fig. 5, still we design a scenario where Alice is nearly isolated from the outside environment, and the only connection between Alice and people outside is some qubits. Alice attempts to communicate with Bob, her friend, via these qubits. However, to wiretap the communication, Eve has prepared her own group of qubits to impersonate Bob. Now there are two groups of qubits: q_1, q_2, \dots, q_N and q'_1, q'_2, \dots, q'_N . Bob has access to operate and measure q_1, q_2, \dots, q_N , while Eve has the access to apply operation or measurement on q'_1, q'_2, \dots, q'_N . However, Alice does not know which group is under Bob's control. Consequently, she has to prepare two identical groups of ciphertext states.

In Sec. I, we have used two encoding operations: $U_{tri} = (u_{31} \cdot u_{23} \cdot u_{12}) \otimes (u_{64} \cdot u_{56} \cdot u_{45})$ [the 3-qubit encoding operations, shown in Fig. 3(a)], and $U_{bi} = (u_{21} \cdot u_{12}) \otimes (u_{43} \cdot u_{34}) \otimes (u_{65} \cdot u_{56})$ [the 2-qubit encoding operations, shown in

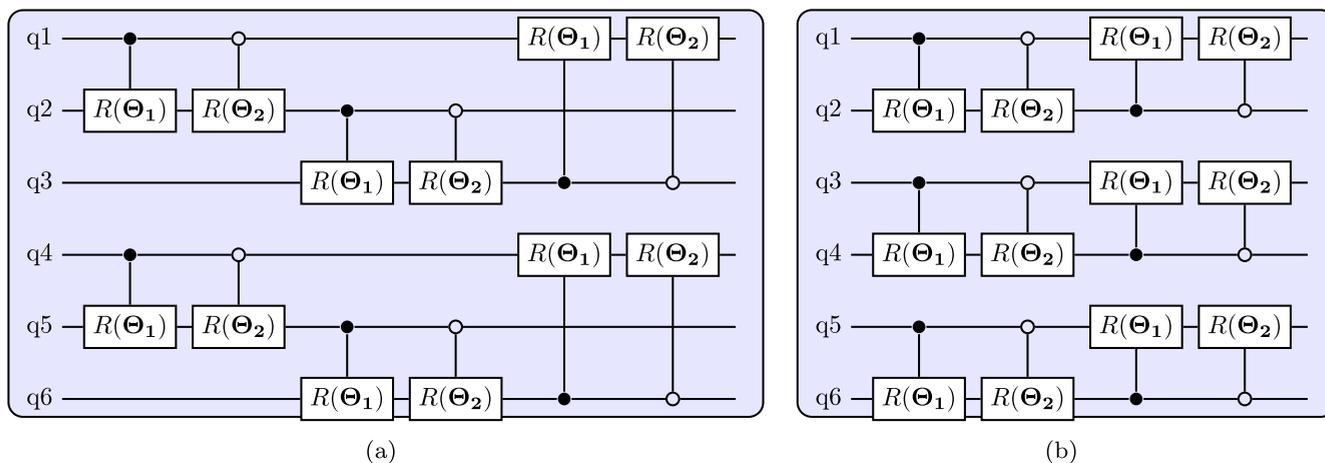


FIG. 3. Sketch of encoding circuit. Initially, q_1, q_2, \dots, q_6 are prepared at state $|n\rangle$; then Alice can use these circuits to encode information into $|\Psi_k\rangle$. (a) The encoding circuit based on 3-qubit control gate loop. q_1, q_2, q_3 form one loop and q_4, q_5, q_6 form another. We note this encoding circuit as U_{tri} , and one can use U_{tri}^{-1} to extract information encoded by U_{tri} . (b) The encoding circuit based on 2-qubit control gate loop. q_1, q_2 form one loop, and $q_3, q_4; q_5, q_6$ form two other loops, respectively. We would like to note this circuit as U_{bin} , and one can apply U_{bin}^{-1} as well to extract information encoded by U_{bin} . Here we only show two simple encryption operations as an example. There are in fact more choices, which will be discussed later.

Fig. 3(b)], where u_{ij} is described by Eq. (2). And we use U_{tri} to encode the new state $|n(k)\rangle$ if the previous $n(k-1)$ is odd, and use U_{bi} otherwise. Generally speaking, if Eve does not know the encoding strategy, or she cannot apply operations on the qubits, then it will be quite safe for Alice and Bob to communicate via this strategy (for more details see Appendix A1).

Review the information shared between Alice and Bob as follows:

S1. Alice will start to prepare qubits at certain states for communication since $t = 0$. Before $t = 0$ she will produce some random state. Alice and Bob have set their clock at the same time before they are separated.

S2. Six qubits are used in the communication. Note the eigenstates under Z measurements can be written as $|n\rangle$, where n is an integer from 0 to 63. State $|0\rangle$ represents the blank space, used as a word divider. $|1\rangle$ to $|26\rangle$ represent capital letters “A” to “Z”, $|27\rangle$ to $|52\rangle$ represent lowercase letters “a”

to “z”, and $|53\rangle$ to $|62\rangle$ represent numbers “0” to “9”. The last eigenstate $|63\rangle$ represents “,”, “.”, or other marks to divide sentences.

S3. Alice will prepare state $|\Psi(k)\rangle = U(n(k-1))|n\rangle$, where $U(n(k-1)) = U_{tri}$ if $n(k-1)$ is odd and $U(n(k-1)) = U_{bi}$ if $n(k-1)$ is even. Alice and Bob set that $U(t=0) = U_{bi}$.

Even if we assume that Eve knows the general strategy that the encoding operation of each block is determined by the plaintext of the previous block, without knowing the particular selection of encoding operations from the total set, and without knowing the plaintext of the previous block, the chance of her guessing the correct decoding operation and obtaining the plaintext is very low.

Then consider the worst situation where Eve also knows the selection of encryption operations and parameters $\Theta_{1,2}$. Besides, we assume that Eve has the authority to apply arbitrary operations on the qubits q'_1, q'_2, \dots, q'_N . In other words,

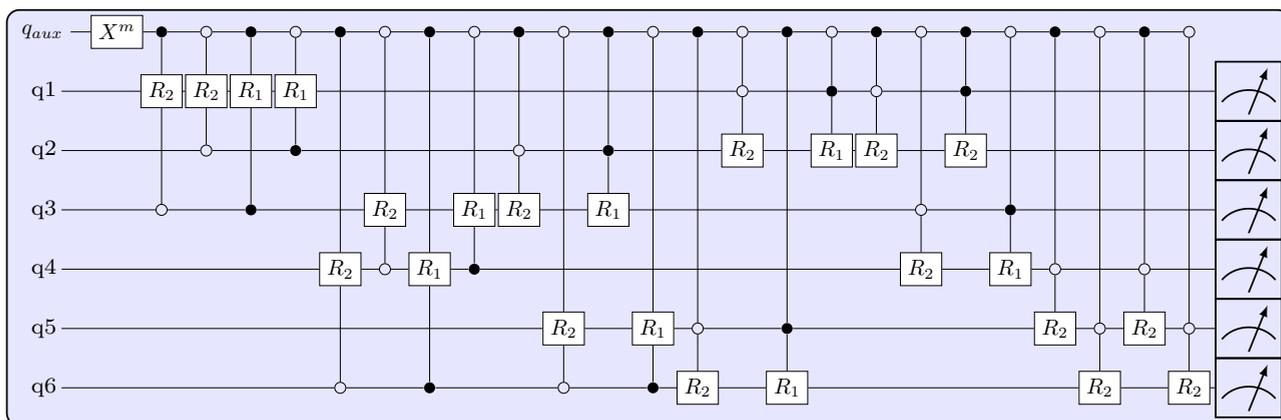


FIG. 4. A possible circuit to decode Alice’s information. q_{aux} is an auxiliary qubit, and in each period it is preset at state $|0\rangle$. m is the previous measurement results of q_6 . As Alice and Bob make an agreement that the first block is encrypted by $U_0 = U_0(|0\rangle)$, Bob will set $m = 0$ initially. Alice only performs operations on q_1 - q_6 . For simplicity, here we use R_1 and R_2 to represent $R^{-1}(\Theta_1)$ and $R^{-1}(\Theta_2)$, respectively.

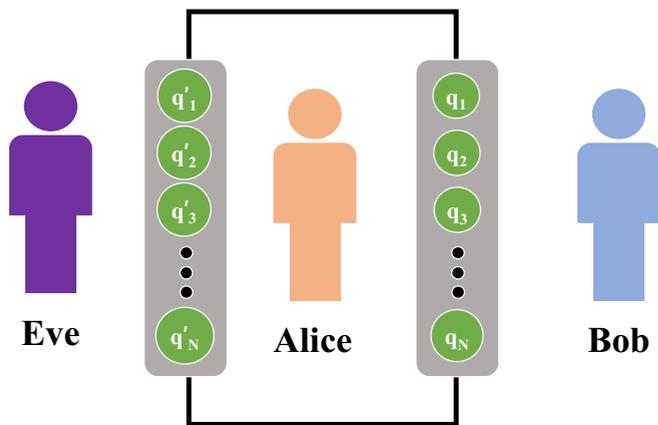


FIG. 5. Sketch of the relation among Alice, Bob, and Eve. Eve (left) attempts to wiretap the communication. Alice (middle) is locked in a “black room,” and the only connection between Alice and the outside environment is some qubits. Alice attempts to communicate with her friend Bob (right) via the qubits. However, there are two groups of qubits: q_1, q_2, \dots, q_N and q'_1, q'_2, \dots, q'_N . Bob has access to operate and measure q_1, q_2, \dots, q_N , while Eve has access to apply an operation or measurement on q'_1, q'_2, \dots, q'_N . However, Alice does not know which group is under Bob’s control. Consequently, Alice has to prepare two groups as the same state.

Eve knows almost all information that Alice and Bob share, with only one exception, the clock, which obstructs Eve from applying correct decryption operation on the first block. In order to miss the least information, by large chance Eve will start wiretapping as early as possible. According to the first communication strategy, before $t = 0$, Alice produces states randomly. On the other hand, Eve has no idea about the exact “ $t = 0$ ”. Consequently, at $t = 0$, Eve might apply the decoding operation U_{bi} , or U_{tri} . Once Eve applies U_{tri} , she can hardly decode the first state $|\Psi(t = 0)\rangle$ correctly; then she will get less information compared to Bob.

Though we have shown that there is a possibility to prevent Alice from getting all information, we need to note that

it is nearly impossible to prohibit Eve from getting “much information” under such communication strategies. [In this case, Eve can generally decode more than two-thirds of the message correctly, as shown in Fig. 6(a).] Even though Eve might decode state $|n\rangle$ as $|n'\rangle$ by mistake, once both n, n' are odd or even, the following states will all be decoded correctly.

Taking the above consideration into account, Alice and Bob can change the third strategy as follows:

S3. Alice will prepare state $|\Psi(k)\rangle = U(n(k - 1))|n\rangle$. Instead of having only two encoding options determined by the parity of the previous plaintext, Alice and Bob can pick up a total number of n different encoding options, determined by all n different possibilities of the previous block of plaintext. All $U(n)$ can be decomposed as a combination of $u_{ij} = u_{ij}(\Theta_1, \Theta_2)$ described by Eq. (2).

In the Appendix, we will provide one encoding operations set as an example for S3, which is also used in the following numerical simulations. For instance, Alice attempts to transport the famous quotation of Alexandre Dumas,

All human wisdom is contained in these words: Wait and hope.

The Count of Monte Cristo, Chap 117.

As in the encoding process, all marks such as “.” will be recognized as “,” and since there is no character representing “line break” or “new line”, the quotation will be converted into

All human wisdom is contained in these words. Wait and hope.
The Count of Monte Cristo. Chap 117.

Alice and Bob arrange that the $|\Psi(t = 0)\rangle$ is encoded by V_0 , and encoding operation V_m will be applied for the k th block t if $n(k - 1) = m$. For simplicity, definition of the encoding operations are presented in the Appendix. At $t = 0$ (according to Alice and Bob’s clock), Alice will start to prepare the 6 qubits at state

$$|\Psi(t = 0)\rangle = V_0|1\rangle, \tag{3}$$

where $|1\rangle$ is the plaintext, representing the first character “A” in the quotation. Before $t = t_1$, Alice should finish the

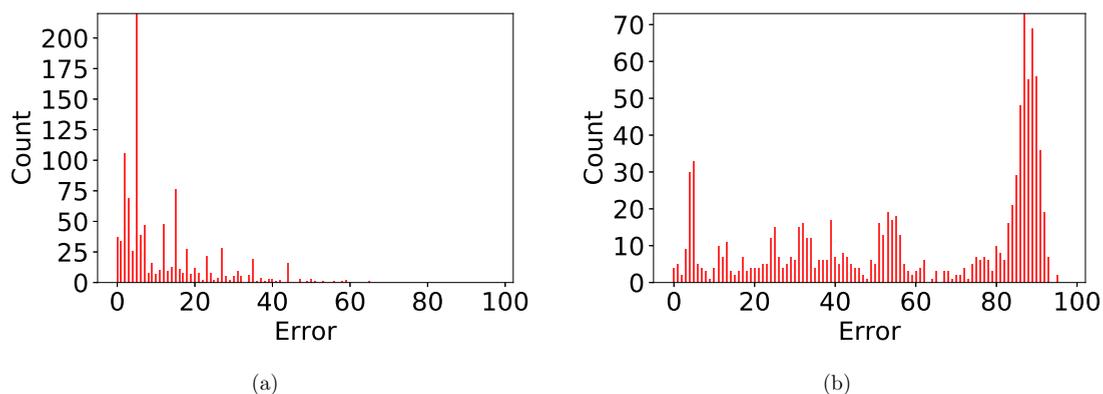


FIG. 6. Numerical simulation for Eve’s decoding process. Assume that Eve starts decoding before $t = 0$, and at $t = 0$ she has uniform probability to apply each decoding operation. “Error” represents the total errors that Eve makes when decoding the sentence. “Count” represents the frequency of certain total mistakes. A rectangle that locates at error = x with count = y infers that in the whole simulation, there are y times that Eve makes mistakes x times. Simulations are carried out 1000 times in total, $\Theta_1 = (0, 0.15\pi, 0.72\pi, 0.32\pi)$, $\Theta_2 = (0, 0.45\pi, 0.17\pi, 1.64\pi)$. (a) Only one previous state has a contribution to the encoding operation. (b) Two previous states are included to decide the next encoding operation.

preparation, and then Bob will start his decoding process. Bob will apply decoding operation V_0^{-1} , as he already knows that $|\Psi(t = 0)\rangle$ is encoded by V_0 . For simplicity, here we ignore the noise and errors in the whole process (new rules will be introduced into the communication strategy against noise, and we will give a brief discussion later). After Z measurement on each qubit, Bob will derive that $|\Phi(t = 0)\rangle = |1\rangle$. Bob finishes his measurement before $t = T$, and at $t = T$ all qubits are reset at state $|0\rangle$. The next character is “1”, corresponding to state $|38\rangle$ (or $|100110\rangle$ as binary). Now Alice should prepare state

$$|\Psi(t = T)\rangle = V_1|38\rangle = V_1|100110\rangle. \tag{4}$$

Alice and Bob can keep communicating in this way. Ignoring the errors and noise, Bob can always receive the correct information theoretically.

On the other hand, Eve finds it impossible to find $t = 0$ accurately for the absence of a shared clock. Additionally, Alice has already noticed her existence and will produce random states before $t = 0$. Here we can safely assume that Eve applies random decoding operations at $t = 0$. Assume that Alice has no bias when generating the random states before $t < 0$; Eve applies each decoding operation with the same possibility, $1/64$. Figure 6(a) shows the numerical simulation results of Eve’s decoding process when the encoding operation of each block is determined by only the previous plaintext. There are 97 characters in the sentence. From the histogram, one may notice that by a quite large chance, Eve will decode the whole sentence with fewer than 20 total mistakes. Obviously now the communication strategy is not safe enough, when the encoding operation of each block is determined by only one previous plaintext. In the following section, we will provide improvement to increase the security in communication.

To improve the security against wiretapping, consider the following encoding operation,

$$U(k) = V\{[n(k - 1) + n(k - 2)] \bmod 64\}, \tag{5}$$

where operation V are still the 64 encryption operations presented in the Appendix. Now the encoding operation at time t is decided by the two former blocks $n(t - T)$ and $n(t - 2T)$. In our example, at $t = 0$, Alice attempts to send the letter “A”, $n(t = 0) = 1$, and at $t = T$ Alice attempts to send “1”, $n(t = T) = 38$. $(1 + 38) \bmod 64 = 39$, so Alice will encode the third character (still “1”) as

$$|\Psi(t = 2T)\rangle = V_{39}|38\rangle. \tag{6}$$

Still, Alice and Bob make an agreement that the first block is encrypted by V_0 . Even though Alice will generate states randomly before $t = 0$, Bob does not need to measure them, and these random states will not effect their communication. In Fig. 6(b), we show the numerical simulation results of Eve’s decoding process under the improved communication strategy. Now Eve can find it extremely difficult to decode the communication. She might decode one character accidentally, yet that gives little help for the following block, unless she can decode two characters simultaneously. Comparing with Fig. 6(a), there are greater chances for Eve to make more mistakes, and the information transfer is safer than using only one block to determine the encoding operation.

Note that here we only introduced the former two states into the encoding operation. Theoretically, one can expand Eq. (5) into

$$U(t) = V\left\{\left[\sum_{\tau=t-t'}^{t-1} n(\tau)\right] \bmod 64\right\}. \tag{7}$$

Hence, one can include an arbitrary number of previous states into the determination of the encoding process.

Till now, the key in our design contains three parts. The first one is the selection of the encoding configurations from all possible configurations that can be applied on the plaintexts to create ciphertexts. These define the controls and targets of the control-unitary gates, and examples of the encoding configurations can be found in Fig. 3 and the Appendix. The second part of the key contains the parameters $\Theta_{1,2}$. These define the actual actions of the control-unitary gates and small differences of them will lead to extremely different encryption operations. In this paper only the simplest situation is discussed, where $\Theta_{1,2}$ are used multiple times in the encryption circuit. To introduce more potential choices for the key, one can replace the repeated $\Theta_{1,2}$ as independent parameters. Generally the more parameters there are in the encryption circuits, there will be more potential choices for the key and the communication will be more safe. The last part is the ways that the encoding configurations are selected by the plaintext of the previous blocks.

Numerical simulation shows that the communication is still reliable even when the second and third parts of the key are released. More theoretical discussions about quantum encryption can be found in our recent work [13].

Noise and errors are all ignored in the above discussion, while the noise might lead to some mistakes in real experiments. Here we provide a fourth strategy against noise and errors with error-detecting auxiliary characters:

S4. At time $t = klT$, where $k = 1, 2, \dots$, and l is a constant positive integer, Alice will prepare the qubits at some certain states, which depend on previous states. After decoding state $|\Psi(t = klT)\rangle$, Bob will make out whether he made any mistakes during $[(k - 1)lT, klT]$. To make up the mistake, they need one more wire that Bob is able to use to send messages back to Alice. Once Bob find the state $|\Psi(t = klT)\rangle$ out of expectation, he can send Alice a message, and then Alice will restart communication from the state $|\Psi(t = (k - 1)lT + T)\rangle$.

Strategy 4 works on the plaintexts, instead of the encoding process. Here we would provide one example to demonstrate how it works. To make it possible for Bob to self-check the encoding process, Alice rewrites the message by adding one auxiliary character every 9 characters (so that auxiliary characters will be the $10k$ th character). She sets the auxiliary character at position $10k$ to be the same value as the $[10(k - 1) - 1]$ th one. The message now will be

All human’ ’ wisdom i’n’s contain’ i’ed in the’n’s’e words.’e’
Wait and’.’ hope. Th’d’e Count o’h’f Monte C’o’risto.
Ch’C’ap 117.

Characters enclosed by apostrophes are auxiliary characters (please note that the apostrophes are included to mark the auxiliary characters, but they themselves are not part of the

message). Here Alice and Bob set the first auxiliary character as a blank space. The second auxiliary character is “n”, the same as the 9th character. The third auxiliary character is “i”, the same as the 19th character. Other auxiliary characters are generated similarly.

IV. FURTHER DISCUSSION

A. Other possible attacks

In addition to the situation discussed above, there are two other possible attacks as discussed in the following. One possible attack is that Eve could keep qubits in a quantum memory to apply decoding circuits to many blocks. Since one cannot perfectly clone an unknown quantum state, Eve cannot generate copies of the received qubits unless she knows the exact state. Thus, she cannot ensure that the first block can live long enough before she collects sufficient succeeding blocks. Meanwhile, difficulties arise when building a deeper circuit on a larger scale. The second possible attack is that Eve intercepts one qubit sent from Alice to Bob. According to S4, an auxiliary digit is included for correction. When Eve intercepts one qubit sent from Alice to Bob, Bob will find out that he can never get the result as expected when measuring the auxiliary digits. Alice and Bob can soon notice the existence of Eve, and stop their communication.

B. Appropriate length of message

Intuitively, if the message contains infinite words, no matter how many previous qubits are included in the encoding process as shown in Eq. (7), Eve will always be able to derive all following information, once she decodes enough characters continuously. Generally, the shorter the message is, the more difficult it will be for Eve to decode it. Therefore when designing the communication strategy, it will also be important to set an appropriate length. Here, we will show some numerical simulation results as an attempt to find the appropriate message length.

Figure 7 shows the trend of average error rate when the message becomes longer. The average error rate R is defined as

$$R = \frac{\sum_{j=1}^{j=M} e_j}{ML}, \tag{8}$$

where M is the total times of simulation, and L is length of the message, e_j is the errors that Eve makes in the j th time when decoding the message.

Further, we also compare the performance of $P(x)$ under various lengths of message, which is the probability that Eve makes more than xL mistakes when decoding a message with length L . Mathematically, $P(x)$ is defined as

$$P(x) = \frac{\sum_{j=1}^{j=M} \Gamma(e_j - xL)}{M}, \tag{9}$$

where Γ represents the threshold function, and $\Gamma(y) = 1$ if $y > 0$, otherwise $\Gamma(y) = 0$. Simulation results are shown in Fig. 8.

The same as the discussion before, here we still set $\Theta_1 = (0.45\pi, 4.04, 1.04, 0.92)$ and $\Theta_2 = (0, 0.35, 0.55\pi, 0.79)$ (just some random numbers, not the optimal ones). Based on

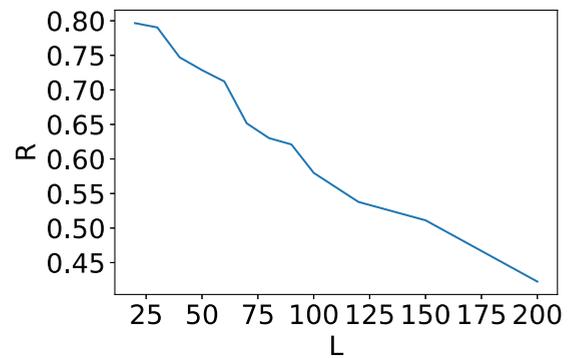


FIG. 7. Sketch of the trend of average error rate against the length of message. Here L represents the length of message and R represents the average error rate. In the simulation, Alice and Bob transport message encoded by the improved strategy (as we discussed in Sec. III, two previous states contribute to the next encoding method). Eve can apply arbitrary operations on the qubits, and knows all details except the exact time $t = 0$.

the simulation we suggest that when only two previous states contribute to the encoding process, it is better to transport a message of around 100 characters or less once; otherwise the risk of wiretapping can no longer be ignored. However, it can always be a solution to divide a long message into a branch of pieces.

V. CONCLUSION

In this work we have proposed a protocol of quantum encryption with varying encryption configurations. The plaintext is divided into blocks with the same length, and represented by the eigenstates under Z measurements. The operation encrypting each single block is determined by one or more previous blocks of the plaintexts. Thus, successful decryption of the former block is required when attempting to extract information from a new one. The key in the protocol contains several parts: the selection of configurations of the encryption

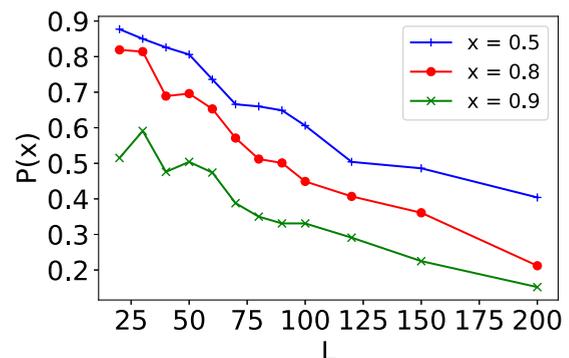


FIG. 8. Sketch of $P(x)$ against the length of message. Here L represents the length of message and $P(x)$ represents probability that Eve makes at least xL mistakes when decoding the message. In the simulation, Alice and Bob transport message encoded by the improved strategy (as we discussed in Sec. III, two previous states contribute to the next encoding method). Eve can apply arbitrary operations on the qubits, and knows all details except the exact time $t = 0$.

operations, the parameters that determine the encryption operations, and the ways the encoding operations are determined by the previous plaintext blocks. All parts are essential for successful encryption and decryption. Further, we studied the protection against wiretapping. Simulation results show that it is still difficult to decode the communication between Alice and Bob even when part of the key is released, and other possible attacks can hardly break the protection either. We also discussed an error-correction method against noises in the encryption and decryption circuits, and the appropriate length of the single piece of message for the best performance of the encryption method.

The data supporting the findings of this study are available within the paper and the Appendix. The data are also available from the authors upon reasonable request.

ACKNOWLEDGMENTS

We acknowledge financial support by Purdue Research Foundation and funding by the US Department of Energy (Office of Basic Energy Sciences) under Award No. de-sc0019215.

S.K. and J.L. designed the model and the computational framework. J.L. carried out the implementation and performed the calculations. All authors discussed the results and wrote the paper. S.K. was in charge of the overall direction and planning.

The authors declare that they have no competing interests.

APPENDIX

1. Optimization of parameters

In this section we will discuss one way to optimize the 6-qubit model for communication application by adjusting parameters Θ_1, Θ_2 .

$$\begin{aligned}
 |\psi_{1,2}(q_1, q_2)\rangle &= [\langle\phi_1^+|U(0)|q_1\rangle\langle 0|U(q_1)|q_2\rangle\langle\phi_2^+|0\rangle + \langle\phi_1^+|U(1)|q_1\rangle\langle 1|U(q_1)|q_2\rangle\langle\phi_2^+|1\rangle]|\phi_1^+\phi_2^+\rangle \\
 &+ [\langle\phi_1^-|U(0)|q_1\rangle\langle 0|U(q_1)|q_2\rangle\langle\phi_2^+|0\rangle + \langle\phi_1^-|U(1)|q_1\rangle\langle 1|U(q_1)|q_2\rangle\langle\phi_2^+|1\rangle]|\phi_1^-\phi_2^+\rangle \\
 &+ [\langle\phi_1^+|U(0)|q_1\rangle\langle 0|U(q_1)|q_2\rangle\langle\phi_2^-|0\rangle + \langle\phi_1^+|U(1)|q_1\rangle\langle 1|U(q_1)|q_2\rangle\langle\phi_2^-|1\rangle]|\phi_1^+\phi_2^-\rangle \\
 &+ [\langle\phi_1^-|U(0)|q_1\rangle\langle 0|U(q_1)|q_2\rangle\langle\phi_2^-|0\rangle + \langle\phi_1^-|U(1)|q_1\rangle\langle 1|U(q_1)|q_2\rangle\langle\phi_2^-|1\rangle]|\phi_1^-\phi_2^-\rangle.
 \end{aligned} \tag{A2}$$

Then we can define a new function $f(M_1, M_2|\Theta_1, \Theta_2)$ to describe how good the measurements M_1, M_2 are for Eve, and

$$f(M_1, M_2|\Theta_1, \Theta_2) = \sum_{q'_1, q'_2=0}^1 \left[|\langle\phi_1(q'_1)\phi_2(q'_2)|\psi_{1,2}(q'_1, q'_2)\rangle|^2 - \sum_{q''_1, q''_2 \neq q'_1, q'_2}^1 |\langle\phi_1(q''_1)\phi_2(q''_2)|\psi_{1,2}(q'_1, q'_2)\rangle|^2 \right], \tag{A3}$$

where we note $\phi_{1,2}(1) = \phi_{1,2}^+$ and $\phi_{1,2}(0) = \phi_{1,2}^-$. Theoretically, for given Θ_1, Θ_2 , the maximum of $f(M_1, M_2|\Theta_1, \Theta_2)$ only depends on M_1, M_2 , so that we can define function $g(\Theta_1, \Theta_2)$ as the maximum result. By adjusting Θ_1, Θ_2 , Alice and Bob can decide the optimal parameters that ensure the least possibility for Eve to derive the correct information.

In fact, if Eve can only measure each qubit instead of applying arbitrary operations on the qubits, then Al-

ice and Bob do not need to spend time optimizing the parameters. Here, we simulate the correct rate for different decoding strategies, as shown in Fig. 9. We assume that the document is transported via binary numbers, and every time Alice will transport 6-bit information via the 6 qubits. Qubits are encoded by circuit Fig. 3(b) if the former number is odd, or by circuit Fig. 3(a) if the former number is even. R represents

For simplicity, here Alice encodes the qubits only with operations shown in Figs. 3 and 4. On one hand, our circuit should be robust, as we need to make sure that Bob, who is to receive information via the qubits, can still make the correct decision when the quantum gates are imperfect or when there are environmental noises. In real experiments, the control gates cannot always be perfect as we designed. When one sets an $R_z(\theta)$ rotation gate, often an $R_z(\theta + \Delta\theta)$ gate is set, and generally we have $|\Delta\theta| \ll \theta$. On the other hand, we need to make sure that Eve, who attempts to wiretap the communication, cannot get too much information. Further, if we know that Eve has little chance to get any information after $t = N_A T$, then we can use the first N_A quantum states to transport some trivial information, so that Eve can get nothing useful. Here, we note $P_B(k|\Theta_1, \Theta_2)$ as the probability of Bob to get all information correctly before $t = kT$, and $P_E(k|\Theta_1, \Theta_2)$ for Eve. The aim of the optimization process is to find suitable parameters Θ_1, Θ_2 so that for a given constant $c > 1$, there exists an integer $N_T > 0$, such that $P_B(cN_T|\Theta_1, \Theta_2)$ is significantly larger than $P_A(N_T|\Theta_1, \Theta_2)$, after which we can ensure that the 6-qubit model can be used to transport $6(c - 1)N_T$ bits of information during time period $N_T T$.

At $t = 0$, the initial quantum state is $|0\rangle$, so that $|\Psi_1^m\rangle$ is certainly encoded by the 2-qubit loop shown in Fig. 3(b). Consider the minimum unit of a 2-qubit loop, qubits q_1 and q_2 . After the encoding process they will be prepared at state

$$\begin{aligned}
 |\psi_{1,2}\rangle &= U(0)|q_1\rangle \otimes \langle 0|U(q_1)|q_2\rangle|0\rangle + U(1)|q_1\rangle \\
 &\otimes \langle 1|U(q_1)|q_2\rangle|1\rangle.
 \end{aligned} \tag{A1}$$

For simplicity, here we defined the unitary operator $U(q)$, $q = 0, 1$ and $U(0) = R(\Theta_2)$ and $U(1) = R(\Theta_1)$. Assume Eve chooses measurement M_1 on q_1 and M_2 on q_2 , and their corresponding eigenstates are $|\phi_1^+\rangle, |\phi_1^-\rangle$ and $|\phi_2^+\rangle, |\phi_2^-\rangle$, where $|\phi^+\rangle = M|0\rangle$ and $|\phi^-\rangle = M|1\rangle$. For chosen measurements, we can rewrite Eq. (A1) as

ice and Bob do not need to spend time optimizing the parameters.

Here, we simulate the correct rate for different decoding strategies, as shown in Fig. 9. We assume that the document is transported via binary numbers, and every time Alice will transport 6-bit information via the 6 qubits. Qubits are encoded by circuit Fig. 3(b) if the former number is odd, or by circuit Fig. 3(a) if the former number is even. R represents

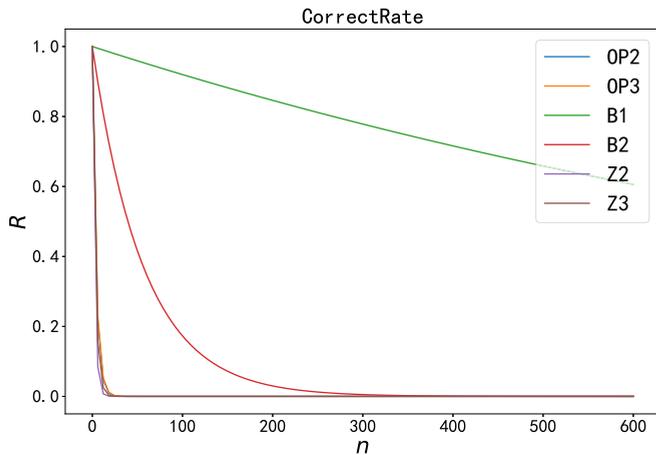


FIG. 9. Simulation result of correct rate for different decoding strategies. Here, we simulate the correct rate R for different decoding strategies when transporting n bits of information. Z2: Assume that all information is encoded by circuit Fig. 3(b), and one applies only Z measurement on every qubit. Z3: Assume that all information is encoded by circuit Fig. 3(a), and one applies only Z measurement on every qubit. OP2: Assume that all information is encoded by circuit Fig. 3(b), and one applies the optimal measurement on every single qubit. OP3: Assume that all information is encoded by circuit Fig. 3(a), and one applies the optimal measurement on every single qubit. B1: One can apply the decoding circuit Fig. 4. Due to the environment noise, fidelity of all operations is 0.995. B2: One can apply the decoding circuit Fig. 4. Due to the environment noise, fidelity of all operations is 0.9.

the correct rate, or the possibility to derive all information correctly when Alice transports totally n bits of information. Z2 (and Z3) represents that Eve directly applies Z measurements on every single qubit, and assume that the first state is encoded by the circuit Fig. 3(b) [Fig. 3(a)]. OP2 (and OP3) represents that Eve optimized her measurements on every single qubit, and assumes that the first state is encoded by the circuit Fig. 3(b) [Fig. 3(a)]. B1 (and B2) shows the performance of Bob's decoding process with different noise; the self-check strategy is not introduced. One can find that if only measurements on a single qubit are allowed, it is nearly impossible to wiretap the communication, even though there are only two encoding operations. In the simulation, we set $\Theta_1 = (0.45\pi, 4.04, 1.04, 0.92)$ and $\Theta_2 = [0, 0.35, 0.55\pi, 0.79]$ (just some random numbers, not the optimal ones).

2. Find the encoding operation from a single state

Here we will provide another method to find the encoding operation from one single state, and only consider the encoding operations shown in Figs. 3(a) and 3(b).

Assume that the first few states $|\Psi(t = 0, 1, 2, \dots, k)\rangle$ are encoded by one same encoding circuit, which is either circuit 1 or circuit 2. All details of these two circuits are already known; then it is also possible to find the encoding method from $|\Psi(t = 0, 1, 2, \dots, k)\rangle$. Here we will demonstrate the basic operations. For simplicity, note the 2 possible encoding methods as U_1 , U_2 , and one complete set of this system as

$\{|0\rangle, |1\rangle, |2\rangle, \dots, |2^N - 1\rangle\}$. Then we have

$$|\psi_{1,n}\rangle = U_1|n\rangle, \quad |\psi_{2,n}\rangle = U_2|n\rangle, \quad (\text{A4})$$

where $n = 0, 1, 2, \dots, 2^N - 1$. Though more than one quantum state are offered, they are not prepared at the same state. Still, we are provided with no copies, which is the main difficulty. For given quantum states encoded by the same circuit, the structure shown in Fig. 3(a) can be used to find the encoding circuit.

As one can notice from the figure, we need in total $3N$ qubits in the circuit. The first N qubits are prepared at the encoded states $|\psi(t)\rangle$, and the other $2N$ qubits are used as auxiliary qubits. Note that the rotation gates R_n satisfy $R_n|0\rangle = |n\rangle$. Initially, the system is prepared at $|\Psi_{in}\rangle = |\psi\rangle \otimes |0\rangle \otimes |0\rangle$, where every ket represents a state of N qubits. The very first step is to apply two control operations S_1 , S_2 , and

$$S_1 = \sum_{n=0}^{2^N-1} (|\psi_{1,n}\rangle\langle\psi_{1,n}| \otimes R_n) \otimes I, \quad (\text{A5})$$

$$S_2 = \sum_{n=0}^{2^N-1} (|\psi_{2,n}\rangle\langle\psi_{2,n}| \otimes I \otimes R_n). \quad (\text{A6})$$

As these two operations commute with each other, it does not matter if we change their order.

Assume that the given qubits are at state $|\psi_{1,m}\rangle$; after these operations the system will be converted to

$$|\Psi_1\rangle = \sum_{n=0}^{2^N-1} [c_{m,n}^1 |\psi_{2,n}\rangle \otimes |m\rangle \otimes |n\rangle], \quad (\text{A7})$$

where $c_{m,n}^1 = \langle\psi_{2,n}|\psi_{1,m}\rangle$. Now apply measurements on the auxiliary qubits so that the whole system will collapse. With possibility $P_{1,l} = |c_{m,l}^1|^2$ one will find the state at

$$|\Psi_{1,l}\rangle = |\psi_{2,l}\rangle \otimes |m\rangle \otimes |l\rangle. \quad (\text{A8})$$

Similarly, if the given qubits are prepared at state $|\psi_{2,m}\rangle$, then after these operations and measurements one will have possibility $P_{2,l} = |c_{m,l}^2|^2$ to find the system at state

$$|\Psi_{2,l}\rangle = |\psi_{1,l}\rangle \otimes |l\rangle \otimes |m\rangle \quad (\text{A9})$$

and $c_{m,n}^2 = \langle\psi_{1,n}|\psi_{2,m}\rangle$. To distinguish $|\psi_{1,l}\rangle$ and $|\psi_{2,l}\rangle$, one convenient solution is to apply operation U_1^\dagger , and measure the final state. If the result is $|l\rangle$, then we can conclude that given states are encoded by U_1 ; otherwise we believe that they are encoded by U_2 . Yet from one state the result might be not correct, as one might be led to the wrong decision under two situations. First, we could hardly move forward if $l = m$ after the first measurement. Besides, there is still the chance $|\langle\psi_{1,l}|l\rangle|^2$ will get the wrong result at the final step. As a conclusion, for a single given encoded state, the possibility to derive the correct encoding circuit is

$$P_{1,m} = 1 - |\langle\psi_{2,m}|\psi_{1,m}\rangle|^2 - \sum_{l=0, l \neq m}^{2^N-1} [|\langle\psi_{2,l}|\psi_{1,m}\rangle|^2 |\langle\psi_{2,l}|l\rangle|^2]. \quad (\text{A10})$$

Further, as

$$P_{1,m} \geq 1 - |\langle \psi_{2,m} | \psi_{1,m} \rangle|^2 - \left[\sum_{l=0, l \neq m}^{2^N-1} |\langle \psi_{2,l} | \psi_{1,m} \rangle|^2 \right] |\langle \psi_{2,l} | l \rangle|^2$$

$$= [1 - |\langle \psi_{2,m} | \psi_{1,m} \rangle|^2][1 - |\langle \psi_{2,l} | l \rangle|^2]. \quad (A11)$$

Once we can make sure that $[1 - |\langle \psi_{2,m} | \psi_{1,m} \rangle|^2][1 - |\langle \psi_{2,l} | l \rangle|^2] \geq \frac{1}{2}$, then it would be a choice of applying this method to find the encoding circuit. However, when more encoding operations are introduced, it would be much more difficult to find the encoding operation from one single state. In other words, decoding the former character by finding the encoding operation cannot help Eve to wiretap the communication.

3. Encoding circuits for more qubits

Here we will expand the encoding circuits to more qubits. Generally, 6 qubits are enough for common communications based on letters and numbers. However, sometimes special characters might be required, and then more qubits should be included in the communication. Still, the encoding operations will contain no more parameters except Θ_1, Θ_2 . Note that there are N qubits q_1, q_2, \dots, q_N used in communication.

Encoding operations design method I: A control gates loop that contains all qubits. Consider a permutation of the qubits; note the location of q_j as $p(j)$, where $0 \leq p(j) < N$, and $p(j) \neq p(k)$ when $j \neq k$. Then for every permutation p , there is a control gates loop as

$$U(p) = \left[\prod_{j=0}^{N-1} u_{p_j p_{j+1}} \right] \cdot u_{p_N p_0}. \quad (A12)$$

In the main article, we have defined that

$$u_{ij} = |0\rangle\langle 0|_i \otimes R_j(\Theta_1) + |1\rangle\langle 1|_i \otimes R_j(\Theta_2). \quad (A13)$$

Encoding operations design method II: Decompose the encoding operation as a combination of U_{bi} and U_{tri} . If N is even, we can always rewrite N as a sum of $N/2$ qubit pairs. Further if $N \geq 6$, we can rewrite N as a sum of some qubit triplets and some qubit pairs. For each qubit pair we can apply U_{bi} , and for each triplet we can apply U_{tri} . On the other hand, if $N \geq 3$ is odd, we can rewrite $N = 3 + (N - 3)$, where $N - 3$ is now an even number. Consider that the N qubits are divided into a pairs and b triplets; there exists a corresponding encoding operation,

$$U = \bigotimes_{j=0}^{j=a} u_{bi}^j \cdot \bigotimes_{k=0}^{k=b} u_{tri}^k, \quad (A14)$$

where the superscript represents the j th qubit pair or the k th triplet. Note here the u_{bi} is different from the U_{bi} in the main article. Instead, u_{bi} applies on qubit q_i and q_j is defined as

$$u_{bi} = u_{ij} \cdot u_{ji}. \quad (A15)$$

Similarly, u_{tri} applies on qubit triplet q_i, q_j, q_k and is defined as

$$u_{tri} = u_{ij} \cdot u_{jk} \cdot u_{ki}. \quad (A16)$$

Additionally, we will offer the 64 encoding operations corresponding to different former words. To reduce confusion, here we use V_n to represent the encoding operations. The subscript represents the former word, where each number represents a single letter, number, or notation. As discussed in the main article, 0 represents a blank space, used as a word divider. 1 to 26 represent characters capital letters ‘‘A’’ to ‘‘Z’’, 27 to 52 represent lowercase letters ‘‘a’’ to ‘‘z’’, and 53 to 62 represent numbers ‘‘0’’, ‘‘1’’ to ‘‘9’’. The last eigenstate 63 represents ‘‘;’’, ‘‘.’’, or other marks to divide sentences. As an example, V_1 will be used as the encoding operation at time t , if we find out that $n(t - 1) = 1$; in other words the former word is ‘‘A’’.

$$V_0 = (u_{12} \cdot u_{21}) \otimes (u_{34} \cdot u_{43}) \otimes (u_{56} \cdot u_{65}),$$

$$V_1 = (u_{12} \cdot u_{23} \cdot u_{31}) \otimes (u_{45} \cdot u_{56} \cdot u_{64}),$$

$$V_2 = (u_{12} \cdot u_{23} \cdot u_{31}) \otimes (u_{46} \cdot u_{65} \cdot u_{54}),$$

$$V_3 = (u_{12} \cdot u_{23} \cdot u_{31}) \otimes (u_{54} \cdot u_{46} \cdot u_{65}),$$

$$V_4 = (u_{12} \cdot u_{23} \cdot u_{31}) \otimes (u_{56} \cdot u_{64} \cdot u_{45}),$$

$$V_5 = (u_{12} \cdot u_{23} \cdot u_{31}) \otimes (u_{64} \cdot u_{45} \cdot u_{56}),$$

$$V_6 = (u_{12} \cdot u_{23} \cdot u_{31}) \otimes (u_{65} \cdot u_{54} \cdot u_{46}),$$

$$V_7 = (u_{13} \cdot u_{32} \cdot u_{21}) \otimes (u_{45} \cdot u_{56} \cdot u_{64}),$$

$$V_8 = (u_{13} \cdot u_{32} \cdot u_{21}) \otimes (u_{46} \cdot u_{65} \cdot u_{54}),$$

$$V_9 = (u_{13} \cdot u_{32} \cdot u_{21}) \otimes (u_{54} \cdot u_{46} \cdot u_{65}),$$

$$V_{10} = (u_{13} \cdot u_{32} \cdot u_{21}) \otimes (u_{56} \cdot u_{64} \cdot u_{45}),$$

$$V_{11} = (u_{13} \cdot u_{32} \cdot u_{21}) \otimes (u_{64} \cdot u_{45} \cdot u_{56}),$$

$$V_{12} = (u_{13} \cdot u_{32} \cdot u_{21}) \otimes (u_{65} \cdot u_{54} \cdot u_{46}),$$

$$V_{13} = (u_{21} \cdot u_{13} \cdot u_{32}) \otimes (u_{45} \cdot u_{56} \cdot u_{64}),$$

$$V_{14} = (u_{21} \cdot u_{13} \cdot u_{32}) \otimes (u_{46} \cdot u_{65} \cdot u_{54}),$$

$$V_{15} = (u_{21} \cdot u_{13} \cdot u_{32}) \otimes (u_{54} \cdot u_{46} \cdot u_{65}),$$

$$V_{16} = (u_{21} \cdot u_{13} \cdot u_{32}) \otimes (u_{56} \cdot u_{64} \cdot u_{45}),$$

$$V_{17} = (u_{21} \cdot u_{13} \cdot u_{32}) \otimes (u_{64} \cdot u_{45} \cdot u_{56}),$$

$$V_{18} = (u_{21} \cdot u_{13} \cdot u_{32}) \otimes (u_{65} \cdot u_{54} \cdot u_{46}),$$

$$V_{19} = (u_{23} \cdot u_{31} \cdot u_{12}) \otimes (u_{45} \cdot u_{56} \cdot u_{64}),$$

$$V_{20} = (u_{23} \cdot u_{31} \cdot u_{12}) \otimes (u_{46} \cdot u_{65} \cdot u_{54}),$$

$$V_{21} = (u_{23} \cdot u_{31} \cdot u_{12}) \otimes (u_{54} \cdot u_{46} \cdot u_{65}),$$

$$V_{22} = (u_{23} \cdot u_{31} \cdot u_{12}) \otimes (u_{56} \cdot u_{64} \cdot u_{45}),$$

$$V_{23} = (u_{23} \cdot u_{31} \cdot u_{12}) \otimes (u_{64} \cdot u_{45} \cdot u_{56}),$$

$$V_{24} = (u_{23} \cdot u_{31} \cdot u_{12}) \otimes (u_{65} \cdot u_{54} \cdot u_{46}),$$

$$V_{25} = (u_{31} \cdot u_{12} \cdot u_{23}) \otimes (u_{45} \cdot u_{56} \cdot u_{64}),$$

$$V_{26} = (u_{31} \cdot u_{12} \cdot u_{23}) \otimes (u_{46} \cdot u_{65} \cdot u_{54}),$$

$$V_{27} = (u_{13} \cdot u_{35} \cdot u_{51}) \otimes (u_{24} \cdot u_{46} \cdot u_{62}),$$

$$V_{28} = (u_{13} \cdot u_{35} \cdot u_{51}) \otimes (u_{26} \cdot u_{64} \cdot u_{42}),$$

$$V_{29} = (u_{13} \cdot u_{35} \cdot u_{51}) \otimes (u_{42} \cdot u_{26} \cdot u_{64}),$$

$$V_{30} = (u_{13} \cdot u_{35} \cdot u_{51}) \otimes (u_{46} \cdot u_{62} \cdot u_{24}),$$

$$V_{31} = (u_{13} \cdot u_{35} \cdot u_{51}) \otimes (u_{62} \cdot u_{24} \cdot u_{46}),$$

$$\begin{aligned}
V_{32} &= (u_{13} \cdot u_{35} \cdot u_{51}) \otimes (u_{64} \cdot u_{42} \cdot u_{26}), \\
V_{33} &= (u_{15} \cdot u_{53} \cdot u_{31}) \otimes (u_{24} \cdot u_{46} \cdot u_{62}), \\
V_{34} &= (u_{15} \cdot u_{53} \cdot u_{31}) \otimes (u_{26} \cdot u_{64} \cdot u_{42}), \\
V_{35} &= (u_{15} \cdot u_{53} \cdot u_{31}) \otimes (u_{42} \cdot u_{26} \cdot u_{64}), \\
V_{36} &= (u_{15} \cdot u_{53} \cdot u_{31}) \otimes (u_{46} \cdot u_{62} \cdot u_{24}), \\
V_{37} &= (u_{15} \cdot u_{53} \cdot u_{31}) \otimes (u_{62} \cdot u_{24} \cdot u_{46}), \\
V_{38} &= (u_{15} \cdot u_{53} \cdot u_{31}) \otimes (u_{64} \cdot u_{42} \cdot u_{26}), \\
V_{39} &= (u_{31} \cdot u_{15} \cdot u_{53}) \otimes (u_{24} \cdot u_{46} \cdot u_{62}), \\
V_{40} &= (u_{31} \cdot u_{15} \cdot u_{53}) \otimes (u_{26} \cdot u_{64} \cdot u_{42}), \\
V_{41} &= (u_{31} \cdot u_{15} \cdot u_{53}) \otimes (u_{42} \cdot u_{26} \cdot u_{64}), \\
V_{42} &= (u_{31} \cdot u_{15} \cdot u_{53}) \otimes (u_{46} \cdot u_{62} \cdot u_{24}), \\
V_{43} &= (u_{31} \cdot u_{15} \cdot u_{53}) \otimes (u_{62} \cdot u_{24} \cdot u_{46}), \\
V_{44} &= (u_{31} \cdot u_{15} \cdot u_{53}) \otimes (u_{64} \cdot u_{42} \cdot u_{26}), \\
V_{45} &= (u_{35} \cdot u_{51} \cdot u_{13}) \otimes (u_{24} \cdot u_{46} \cdot u_{62}), \\
V_{46} &= (u_{35} \cdot u_{51} \cdot u_{13}) \otimes (u_{26} \cdot u_{64} \cdot u_{42}), \\
V_{47} &= (u_{35} \cdot u_{51} \cdot u_{13}) \otimes (u_{42} \cdot u_{26} \cdot u_{64}), \\
V_{48} &= (u_{35} \cdot u_{51} \cdot u_{13}) \otimes (u_{46} \cdot u_{62} \cdot u_{24}),
\end{aligned}$$

$$\begin{aligned}
V_{49} &= (u_{35} \cdot u_{51} \cdot u_{13}) \otimes (u_{62} \cdot u_{24} \cdot u_{46}), \\
V_{50} &= (u_{35} \cdot u_{51} \cdot u_{13}) \otimes (u_{64} \cdot u_{42} \cdot u_{26}), \\
V_{51} &= (u_{51} \cdot u_{13} \cdot u_{35}) \otimes (u_{24} \cdot u_{46} \cdot u_{62}), \\
V_{52} &= (u_{51} \cdot u_{13} \cdot u_{35}) \otimes (u_{26} \cdot u_{64} \cdot u_{42}), \\
V_{53} &= (u_{51} \cdot u_{13} \cdot u_{35}) \otimes (u_{42} \cdot u_{26} \cdot u_{64}), \\
V_{54} &= (u_{51} \cdot u_{13} \cdot u_{35}) \otimes (u_{46} \cdot u_{62} \cdot u_{24}), \\
V_{55} &= (u_{51} \cdot u_{13} \cdot u_{35}) \otimes (u_{62} \cdot u_{24} \cdot u_{46}), \\
V_{56} &= (u_{51} \cdot u_{13} \cdot u_{35}) \otimes (u_{64} \cdot u_{42} \cdot u_{26}), \\
V_{57} &= (u_{53} \cdot u_{31} \cdot u_{15}) \otimes (u_{24} \cdot u_{46} \cdot u_{62}), \\
V_{58} &= (u_{53} \cdot u_{31} \cdot u_{15}) \otimes (u_{26} \cdot u_{64} \cdot u_{42}), \\
V_{59} &= (u_{53} \cdot u_{31} \cdot u_{15}) \otimes (u_{42} \cdot u_{26} \cdot u_{64}), \\
V_{60} &= (u_{53} \cdot u_{31} \cdot u_{15}) \otimes (u_{46} \cdot u_{62} \cdot u_{24}), \\
V_{61} &= (u_{53} \cdot u_{31} \cdot u_{15}) \otimes (u_{62} \cdot u_{24} \cdot u_{46}), \\
V_{62} &= (u_{53} \cdot u_{31} \cdot u_{15}) \otimes (u_{64} \cdot u_{42} \cdot u_{26}), \\
V_{63} &= (u_{21} \cdot u_{12}) \otimes (u_{43} \cdot u_{34}) \otimes (u_{65} \cdot u_{56}).
\end{aligned}$$

Please note that the above is just one design of the encoding operations. One can design arbitrary encoding sets for various demands.

-
- [1] D. P. DiVincenzo, Quantum computation, *Science* **270**, 255 (1995).
- [2] E. Knill and R. Laflamme, Power of One Bit of Quantum Information, *Phys. Rev. Lett.* **81**, 5672 (1998).
- [3] C. H. Bennett and D. P. DiVincenzo, Quantum information and computation, *Nature (London)* **404**, 247 (2000).
- [4] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Elementary gates for quantum computation, *Phys. Rev. A* **52**, 3457 (1995).
- [5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, *Rev. Mod. Phys.* **74**, 145 (2002).
- [6] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
- [7] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum Cryptography without Bell's Theorem, *Phys. Rev. Lett.* **68**, 557 (1992).
- [8] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, Quantum Cryptography with Entangled Photons, *Phys. Rev. Lett.* **84**, 4729 (2000).
- [9] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, *Rev. Mod. Phys.* **92**, 025002 (2020).
- [10] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li *et al.*, Entanglement-based secure quantum cryptography over 1,120 kilometres, *Nature (London)* **582**, 501 (2020).
- [11] P. O. Boykin and V. Roychowdhury, Optimal encryption of quantum bits, *Phys. Rev. A* **67**, 042317 (2003).
- [12] P. Hayden, D. Leung, P. W. Shor, and A. Winter, Randomizing quantum states: Constructions and applications, *Commun. Math. Phys.* **250**, 371 (2004).
- [13] Z. Hu and S. Kais, A quantum encryption scheme featuring confusion, diffusion, and mode of operation, [arXiv:2010.03062](https://arxiv.org/abs/2010.03062).
- [14] J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li *et al.*, Ground-to-satellite quantum teleportation, *Nature (London)* **549**, 70 (2017).
- [15] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, Satellite-to-ground quantum key distribution, *Nature (London)* **549**, 43 (2017).
- [16] B. K. Rugg, M. D. Krzyaniak, B. T. Phelan, M. A. Ratner, R. M. Young, and M. R. Wasielewski, Photodriven quantum teleportation of an electron spin state in a covalent donor-acceptor-radical system, *Nat. Chem.* **11**, 981 (2019).
- [17] J. F. Sherson, H. Krauter, R. K. Olsson, B. Julsgaard, K. Hammerer, I. Cirac, and E. S. Polzik, Quantum teleportation between light and matter, *Nature (London)* **443**, 557 (2006).
- [18] W. B. Gao, P. Fallahi, E. Togan, A. Delteil, Y. S. Chin, J. Miguel-Sanchez, and A. Imamoglu, Quantum teleportation from a propagating photon to a solid-state spin qubit, *Nat. Commun.* **4**, 2744 (2013).
- [19] M. D. Barrett, J. Chiaverini, T. Schaetz, J. Britton, W. M. Itano, J. D. Jost, E. Knill, C. Langer, D. Leibfried, R. Ozeri *et al.*, Deterministic quantum teleportation of atomic qubits, *Nature (London)* **429**, 737 (2004).
- [20] L. Steffen, Y. Salathe, M. Oppliger, P. Kurpiers, M. Baur, C. Lang, C. Eichler, G. Puebla-Hellmann, A. Fedorov, and A. Wallraff, Deterministic quantum teleportation with feed-

- forward in a solid state system, [Nature \(London\) 500](#), 319 (2013).
- [21] G. M. D'Ariano and P. L. Presti, Quantum Tomography for Measuring Experimentally the Matrix Elements of an Arbitrary Quantum Operation, [Phys. Rev. Lett. 86](#), 4195 (2001).
- [22] C. E. Shannon, A mathematical theory of communication, [Mob. Comput. Commun. Rev. 5](#), 3 (2001).