Quantum Information and Computation, Vol. 14, No. 7&8 (2014) 0589–0607

ROBUST VARIATIONS OF SECRET SHARING THROUGH NOISY QUANTUM CHANNEL

XIU-BO CHEN[a)d)], GANG XU[a)c)d)],YUAN SU[b)] and YI-XIAN YANG[a)]
[a)] *Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[b)] *School of Mathematical Sciences, Peking University, Beijing, 100871, China*
[c)] *School of Software Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[d)] *State Key Laboratory of Information Security (Institute of Information Engineering, Graduate University of Chinese Academy of Sciences), Beijing 100093, China*

Received April 20, 2012
Revised September 9, 2013

In this paper, the perfect secret sharing in quantum cryptography is investigated. On one hand, the security of a recent protocol [Adhikari et al. Quantum Inform. & Comput. 12 (2012) 0253-0261] is re-examined. We find that it violates the requirement of information theoretic security in the secret sharing and suffers from the information leakage. The cryptanalysis including several specific attack strategies are given, which shows that a dishonest participant can steal half or all of the secrets without being detected. On the other hand, we design a new quantum secret sharing protocol. The security of protocol is rigorously proved. It meets the fundamental requirement of information theoretic security. Furthermore, the security analysis including both the outside attacks and participant attacks is given in details. It is shown that our proposed protocol can achieve perfect secret sharing.

Keywords: Quantum secret sharing; Information leakage; Security
Communicated by: B Kane & H Zbinden

1. Introduction

Secret sharing is a significant branch of cryptography. In a secret sharing protocol, the dealer distributes the secret messages among several participants. Each one is allocated a share of the secret. The biggest merit of secret sharing is that the secret message can be recovered if and only if a sufficient number of shares are combined together. In other words, individual shares provide no useful information as to the value of secret key. Quantum secret sharing (QSS) is the quantum counterpart of secret sharing. In 1999, Hillery, Bužek and Berthiaume [1] proposed the first QSS protocol for sharing a private key using multi-particle GHZ states. Since then, QSS has been deeply researched both in theory [2, 3, 4] and experiment [5, 6].

In a QSS protocol, the security is particularly important. Up to now, many QSS protocols [7, 8, 9], which are originally concerned to be secure, have been successfully attacked by some subtle attack strategies. Generally, the security requirement of QSS protocol is much higher than the quantum key distribution (QKD) [10], because a number of participants are involved and not all of them are honest. For example, Liu et al [8] pointed out that the multiparty

quantum secret sharing (MQSS) protocol based on the GHZ state [9] is insecure. They found that an inside participant can deduce half of the sender's secret information directly just by his piece of secret. In order to resist this attack, an improvement was put forward. However, we [11] find that Liu et al's improved protocol is still insecure. We have presented three attack strategies, by which the eavesdropper can steal half or all of the secrets.

In this paper, we firstly introduce the requirement of information theoretic security in the protocol of perfect secret sharing. It provides theoretical basis for the cryptanalysis and design of secure QSS protocol. On one hand, we re-examine the security of a novel QSS protocol (NQC-QSS) proposed by Adhikari et al. [12]. One merit of NQC-QSS is that they focus on the secret sharing through noisy quantum channels, which is more suitable for realistic situation. Unfortunately, we find that the NQC-QSS cannot meet the requirement of information theoretic security. As a result, a dishonest participant has the chance to steal the secrets without being noticed by the legitimate members. We give the cryptanalysis including several specific attack strategies in details. On the other hand, we propose a new quantum secret sharing protocol. The security of protocol is rigorously proved. It meets the fundamental requirement of information theoretic security. Furthermore, by performing explicit security analysis including both the outside attacks and participant attacks, we show that our proposed protocol is perfect secret sharing. The rest of this paper is organized as follows. In Section 2, the requirement of information theoretic security is introduced, which is very useful for the cryptanalysis and design of QSS protocol. In Section 3, we briefly review and analyze the security of NQC-QSS protocol. Then, we propose a new QSS protocol in Section 4. The security analysis of the proposed protocol is also given in details. Finally, the paper is concluded in Section 5.

2. Requirement of information theoretic security

In this section, we give a brief introduction for the requirement of information theoretic security in the secret sharing protocol [13, 14]. Later in Sections 3 and 4, it will not only provide the theoretical basis for the cryptanalysis of NQC-QSS, but also contribute to a rigorous proof for the security of our proposed protocol.

Definition 1 (Access structure and authorized subset):

Denote $\mathcal{P}$ as the set of all the players participated in the secret sharing. Let Γ be a set of subsets of $\mathcal{P}$ (the powerset of $\mathcal{P}$). Each element in Γ are those subsets of participants that should be able to recover the secret successfully. Then, Γ is called an *access structure* and each element in Γ is called an *authorized subset*.

If Γ is an access structure, then $B \in \Gamma$ is a *minimal authorized subset* if $A \notin \Gamma$ whenever $A \subseteq B, A \neq B$. The set of minimal authorized subsets of Γ is denoted Γ_0 and is the basis of Γ.

□

Definition 2 (Distribution rule):

Let $\mathcal{K}$ be the key set, which contains all the possible values of secret. Denote $\mathcal{S}$ as the set of all partial information distributed to each participants. Then, a *distribution rule* is a function defined as $f : \mathcal{P} \to \mathcal{S}$. The function f represents a possible distribution of shares to the participants, where $f(P_i)$ is the share given to P_i, for $\forall P_i \in \mathcal{P}$.

Now, for each $k \in \mathcal{K}$, let $\mathcal{F}_k$ be a set of distribution rules corresponding to a particular

key k. Next, define F as the complete set of distribution rules, where $\mathcal{F} = \bigcup_{k\in\mathcal{K}}\mathcal{F}_k$. If $k \in \mathcal{K}$ is the value of the key that the dealer wishes to share, he will randomly choose a distribution $f \in \mathcal{F}_k$ in each round. Finally, given any subset of participants $B \subseteq \mathcal{P}$, define $S(B) = \{\bigcup_{P\in B} f(P) | f \in \mathcal{F} = \bigcup_{k\in\mathcal{K}}\mathcal{F}_k\}$. Thus, $S(B)$ is the set of possible distributions of shares to the participants in B.

□

Here, below is a formal definition of perfect secret sharing. This model is mathematically precise and easier for rigorous **proofs**.

Definition 3 (Perfect secret sharing): Suppose Γ is an access structure and $\mathcal{F} = \bigcup_{k\in\mathcal{K}}\mathcal{F}_k$ is a set of distribution rules. Then $\mathcal{F}$ is a *perfect secret sharing* protocol realizing Γ if and only if the following two properties are satisfied:

i) For any authorized subset $B \in \Gamma$, there do not exist two distribution rules $f \in \mathcal{F}_k$ and $f' \in \mathcal{F}_{k'}$ with $k \neq k'$, such that $\forall P \in B, f(P) = f'(P)$. In other words, any distribution of shares to the participants in an authorized subset $B \in \Gamma$ can be uniquely figured out.

ii) For any unauthorized subset $B \subseteq \mathcal{P}$ and for any distribution of shares $g_B \in S(B)$, it holds that $Pr[K = k|S(B) = g_B] = Pr[K = k]$. That is, given a particular share $g_B \in S(B)$, the posterior probability on K is the same as the priori probability. In other words, the knowledge of $g_B \in S(B)$ provides no help.

□

Attention should be paid that the above requirement of perfect secret sharing will naturally lead to information theoretic security. To prove this, we just calculate the conditional entropy $H(K|S(B))$ and find that it equals to the uncertainty of the secret itself, i.e. $H(K|S(B)) = H(K)$. Therefore, when talking about the perfect secret sharing, we will sometimes refer to information theoretic security instead.

In general, we measure the efficiency of a secret sharing protocol by the information rate, which is given as follows.

Definition 4 (Information rate): Suppose there is a perfect secret sharing protocol realizing an access structure Γ. The *information rate* for a participant $P_i \in \mathcal{P}$ is the ratio

$$\rho_i = \frac{log_2|\mathcal{K}|}{log_2|S(P_i)|}.$$

The *information rate* of the protocol is defined by $\rho = min\{p_i|P_i \in \mathcal{P}\}$.

□

Obviously, a high information rate is desirable for secret sharing. However, the following theorem states that the rate of a perfect secret sharing protocol cannot be too high.

Theorem (Requirement of information theoretic security in the secret sharing)

In any perfect secret sharing protocol realizing an access structure Γ and $\rho_i \in \{\rho_j|\forall B \in \Gamma_0, P_j \in B\}$, it holds $\rho_i \leq 1$. Thus, $\rho \leq 1$.

□

The above theorem serves as a fundamental requirement of information theoretic security in the perfect secret sharing. As a consequence of the above result, if the information rate $\rho_i > 1$ for any $\rho_i \in \{\rho_j|\forall B \in \Gamma_0, P_j \in B\}$, then the secret sharing protocol is certainly not information theoretic secure. In the following, we will make use of this theorem in the security analysis of NQC-QSS protocol and our new protocol.

3. Review and cryptanalysis of NQC-QSS

In Subsection 3.1, NQC-QSS is briefly reviewed, including both the noiseless and the noisy protocol. In Subsection 3.2, we point out the information leakage in NQC-QSS using the theorem of perfect secret sharing. Then, in order to see how the dishonest participant can steal the secret, we present some specific attack strategies in details.

3.1. *Review of NQC-QSS*

Here, we briefly review the Noiseless-NQC-QSS in Subsection 3.1.1, and Noisy-NQC-QSS in Subsection 3.1.2.

3.1.1. *Noiseless-NQC-QSS*

Noiseless-NQC-QSS mainly contains the following four steps.

Step I: Three participants, i.e., Alice, Bob and Charlie, share a pure GHZ state

$$|\psi\rangle_{ABC} = \frac{|000\rangle + |111\rangle}{\sqrt{2}} \tag{1}$$

Step II: Alice encodes two bits secret messages m_1m_2 by performing one of the unitary operations$\{I(00), \sigma_x(01), i\sigma_y(10), \sigma_z(11)\}$ on her qubit. Then, Alice sends her qubit to Bob.

Step III: The quantum state in Eq.(1) is transformed into one of the following states

$$\begin{aligned}
|\psi_{00}\rangle_{ABC} &= (I \otimes I \otimes I)|\psi\rangle_{ABC} = \tfrac{|000\rangle+|111\rangle}{\sqrt{2}} = \tfrac{|\Phi^+\rangle\otimes|+\rangle+|\Phi^-\rangle\otimes|-\rangle}{\sqrt{2}} \\
|\psi_{01}\rangle_{ABC} &= (\sigma_x \otimes I \otimes I)|\psi\rangle_{ABC} = \tfrac{|100\rangle+|011\rangle}{\sqrt{2}} = \tfrac{|\Psi^+\rangle\otimes|+\rangle-|\Psi^-\rangle\otimes|-\rangle}{\sqrt{2}} \\
|\psi_{10}\rangle_{ABC} &= (i\sigma_y \otimes I \otimes I)|\psi\rangle_{ABC} = \tfrac{|100\rangle-|011\rangle}{\sqrt{2}} = \tfrac{|\Psi^+\rangle\otimes|-\rangle-|\Psi^-\rangle\otimes|+\rangle}{\sqrt{2}} \\
|\psi_{11}\rangle_{ABC} &= (\sigma_z \otimes I \otimes I)|\psi\rangle_{ABC} = \tfrac{|000\rangle-|111\rangle}{\sqrt{2}} = \tfrac{|\Phi^+\rangle\otimes|-\rangle+|\Phi^-\rangle\otimes|+\rangle}{\sqrt{2}}
\end{aligned} \tag{2}$$

Here, $|\Phi^{\pm}\rangle = \frac{|00\rangle\pm|11\rangle}{\sqrt{2}}$, $|\Psi^{\pm}\rangle = \frac{|01\rangle\pm|10\rangle}{\sqrt{2}}$, and $|\pm\rangle = \frac{|0\rangle\pm|1\rangle}{\sqrt{2}}$.

Charlie performs a single-qubit measurement under the basis $\{|+\rangle, |-\rangle\}$. If Charlie agrees to help Bob unmask the secret, he transmits his measurement outcomes to Bob.

Step IV: Bob performs a Bell-state measurement on his two qubits. Then, according to Charlie's measurement outcomes, Bob can successfully obtain the secret messages m_1m_2, which are encoded by Alice.

3.1.2. *Noisy-NQC-QSS*

In Noisy-NQC-QSS protocol, the phase-damping channel is considered as the noisy channel. The Kraus representation of a phase-damping channel is given by the set of operators $E_0 = \sqrt{1-p}I$, $E_1 = \sqrt{p}|0\rangle\langle 0|$, $E_2 = \sqrt{p}|1\rangle\langle 1|$, where $0 < p < 1$. An alternative representation is

$$\varepsilon(\rho) = (1 - \frac{p}{2})\rho + \frac{p}{2}\sigma_z\rho\sigma_z. \tag{3}$$

Step I: Charlie prepares a three-qubit pure GHZ state. He keeps one qubit and sends the other two qubits through the phase-damping channels to Alice and Bob, respectively.

Step II: Alice encodes two bits information m_1m_2 by carrying out the unitary transforms $\{I(00), \sigma_x(01), i\sigma_y(10), \sigma_z(11)\}$ on her qubit. Then, she sends her qubit to Bob through the same phase-damping channel. As a result, the 3-qubit density operators become

$$\begin{aligned}
\rho_{00}^{BBC} &= \frac{|000\rangle\langle 000|+|111\rangle\langle 111|}{2} + \frac{(1-p)^3|000\rangle\langle 111|+|111\rangle\langle 000|}{2} \\
\rho_{01}^{BBC} &= \frac{|100\rangle\langle 100|+|011\rangle\langle 011|}{2} + \frac{(1-p)^3|100\rangle\langle 011|+|011\rangle\langle 100|}{2} \\
\rho_{10}^{BBC} &= \frac{|100\rangle\langle 100|+|011\rangle\langle 011|}{2} + \frac{(1-p)^3|100\rangle\langle 011|+|011\rangle\langle 100|}{2} \\
\rho_{11}^{BBC} &= \frac{|000\rangle\langle 000|+|111\rangle\langle 111|}{2} + \frac{(1-p)^3|000\rangle\langle 111|+|111\rangle\langle 000|}{2}
\end{aligned} \tag{4}$$

Step III: If Charlie is willing to help Bob, he performs a measurement on his qubit in the basis $\{|N+\rangle, |N-\rangle\}$, where $|N+\rangle = \alpha|0\rangle + \beta|1\rangle, |N-\rangle = \beta|0\rangle - \alpha|1\rangle$, and $\alpha^2 + \beta^2 = 1$. Thereafter, he sends the measurement outcomes to Bob.

Step IV: To recover the secret messages, Bob should firstly perform a projective measurements $P_1 = |00\rangle\langle 00| + |11\rangle\langle 11|$ and $P_2 = |01\rangle\langle 10| + |10\rangle\langle 10|$ to classify the quantum states into two classes. Then, he performs the POVM measurement to identify the secret state. The optimal POVM elements are

$$\Pi_1 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \qquad \Pi_2 = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \tag{5}$$

Finally, Bob can probabilistically reconstruct the secret messages m_1m_2 .

3.2. *Cryptanalysis of NQC-QSS*

In this subsection, we show that the design of NQC-QSS protocol violates the basic requirement of information theoretic security in perfect secret sharing. As a result, it suffers from the information leakage problem. Then, the cryptanalysis including several specific attack strategies are given, which shows that a dishonest participant can steal half or all of the secrets. The vulnerability of Noiseless-NQC-QSS is analyzed in Subsection 3.2.1. The cryptanalysis of Noisy-NQC-QSS is given in Subsection 3.2.2.

3.2.1. *Cryptanalysis of Noiseless-NQC-QSS*

In this subsection, the security of Noiseless-NQC-QSS is re-examined.

Firstly, it is shown that the distribution rule for Noiseless-NQC-QSS is not well designed. As a result, it suffers from the information leakage. Now, we give a theoretical proof of the information leakage in Noiseless-NQC-QSS. Let us begin with the following distribution rule.

Table 1. The distribution rule of Noiseless-NQC-QSS. Here, Bob's measurement result$\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ is denoted as classical bits $\{00, 10, 01, 11\}$, and Charlie's result $\{|+\rangle, |-\rangle\}$ is denoted as$\{0, 1\}$. $\mathcal{F}_k$ denotes the set of distribution rules corresponding to a particular key k.

	$\mathcal{F}_{00}$		$\mathcal{F}_{01}$		$\mathcal{F}_{10}$		$\mathcal{F}_{11}$	
Bob	00	10	01	11	01	11	00	10
Charlie	0	1	0	1	1	0	1	0

In Noiseless-NQC-QSS protocol, the secret is supposed to be recovered if and only if Bob and Charlie cooperate. Therefore, the basis of the access structure is $\Gamma_0 = \{\{Bob, Charlie\}\}$ and there exists only one authorized subset $B = \{Bob, Charlie\} \in \Gamma_0$. Now, we calculate the information rate of each participant in this minimal authorized subset

$$\begin{aligned} \rho_{Bob} &= \frac{log_2|\mathcal{K}|}{log_2|S(Bob)|} = \frac{log_2|Z_2^2|^2}{log_2|Z_2^2|^2} = 1 \\ \rho_{Charlie} &= \frac{log_2|\mathcal{K}|}{log_2|S(Charlie)|} = \frac{log_2|Z_2^2|^2}{log_2|Z_2^1|^2} = 2 > 1. \end{aligned} \tag{6}$$

One may find that the information rate of Charlie is overflowed, which violates the theorem of requirement of information theoretic security in Section 2. Thus, there exists some $k \in \mathcal{K}$, such that the distribution rules $\mathcal{F}_k$ leaks some information to Bob.

The above analysis does provide a theoretical clue for the information leakage in Noiseless-NQC-QSS. Next, in order to see how the dishonest participant can steal the secret, we give the specific attack strategies. It is shown that a dishonest participant can steal half or all of the secrets without being detected.

After Alice performs the unitary operations $\{I(00), \sigma_x(01), i\sigma_y(10), \sigma_z(11)\}$ on her particles, the quantum state will become one of the states shown in Eq.(2). We first calculate the reduced density operators on the particles in Bobs hand

$$\begin{aligned} \rho_{00}^{BB} &= \frac{|00\rangle\langle 00| + |11\rangle\langle 11|}{2}, \rho_{01}^{BB} = \frac{|10\rangle\langle 10| + |01\rangle\langle 01|}{2}, \\ \rho_{10}^{BB} &= \frac{|10\rangle\langle 10| + |01\rangle\langle 01|}{2}, \rho_{11}^{BB} = \frac{|00\rangle\langle 00| + |11\rangle\langle 11|}{2}. \end{aligned} \tag{7}$$

Bob's attack strategy is as follows.

(i) Bob divides the four operators $\{\rho_{00}^{BB}, \rho_{01}^{BB}, \rho_{10}^{BB}, \rho_{11}^{BB}\}$ into two subsets $S_1 = \{\rho_{00}^{BB}, \rho_{11}^{BB}\}$ and $S_2 = \{\rho_{01}^{BB}, \rho_{10}^{BB}\}$.

(ii) He makes measurement on his two particles under the basis $\{P_1 = |00\rangle\langle 00| + |11\rangle\langle 11|, P_2 = |01\rangle\langle 01| + |10\rangle\langle 10|\}$.

(iii) If the quantum state is projected into P_1, Bob can figure out the original secret messages are either 00 or 11. Therefore, one bit information $m_1 \oplus m_2 = 0$ is leaked. Similarly, if projector P_2 is obtained, one bit secret message $m_1 \oplus m_2 = 1$ can be stolen. Therefore, no matter what messages $m_1 m_2 = \{00, 01, 10, 11\}$ Alice chooses, Bob can successfully steal one bit secret $m_1 \oplus m_2$.

The above attack strategy shows that Bob can steal half of secret messages without Charlie's help. Now, we give an example. For instance, suppose that Alice's original secret messages are m=01001011. By means of the above attack strategy, Bob's measurement outcomes must be $P_2 P_1 P_2 P_1$. To elicit the secret messages, Bob obtains the secrets 01 (Certainly, it can be chosen as 10) if the projector P_1 is obtained. Otherwise, the secret messages are considered as 00 (Here, it can also be chosen as 11). Therefore, the secret messages obtained by Bob are 00100010. One can easily find that every 1 out of 2 bits is leaked. That is, half of Alice's secrets are stolen by Bob.

In cryptography, the security of a modern cryptosystem is highly related to the computational complexity of all the possible attacks. The higher computational complexity, the longer time it takes for code-breaking, and vice versa. Typically, the effective cryptanalysis of

a cryptography protocol often involves looking for an attack, which can remarkably decrease the computational complexity. For one example, a simple brute force attack against DES requires 1 known plaintext and 2^{55} decryptions, trying approximately half of the possible keys, before the correct key is found. However, a linear cryptanalysis attack against DES requires 2^{43} known plaintexts and approximately 2^{43} DES operations [15]. Thus, this is a considerable improvement on brute force attacks. For another example, consider the application of quantum Grover algorithm [16] in cryptanalysis. It can remarkably decrease the complexity of brute force attack from $O(N)$ to $O(\sqrt{N})$, with a high success probability. Thus, Grover algorithm is considered as an effective attack to cryptographic protocols. Now, let us consider the attack on NQC-QSS. In the noiseless NQC-QSS protocol, Bob can steal every 1 out of 2 bits. Therefore, to break a secret with n bits length, he only needs to search $\frac{n}{2}$ bits on average. Instead of making $O(N)$ attempts where $N = 2^n$, Bob can now recover the secret within $O(\sqrt{N})$ attempts using the leaked information, which remarkably decreases the computational complexity and the cost of the time for code-breaking. In fact, there are several other protocols in quantum cryptography, which suffers from the same security problems as the NQC-QSS. For one example, Lin et al. [17] show the Zhang et al.'s [18] multiparty QSS is insecure, in which the dishonest participant Charlie can illegally elicit half of Alices secrets. For other example, Sun et al. [19] find that an Eve in a quantum cryptography protocol [20] can steal 20% of sender's secrets. So, one should pay more attention to the strict security analysis in the design of cryptography protocol.

3.2.2. *Cryptanalysis of Noisy-NQC-QSS*

In this subsection, it will be shown that Noisy-NQC-QSS is vulnerable to both Bob's and Charlie's attack.

Case 1: Charlie's Attack

In the original Noisy-NQC-QSS protocol, the 3-qubit GHZ state is prepared by one of the participants, Charlie. However, if Charlie is dishonest, he may perform the participant attack during the process of secret sharing. We now present a simple and feasible attack strategy, in which Charlie can recover nearly all secrets without being noticed by Alice and Bob. The process of Charlies attack is shown in Figure1.

(S1) Charlie prepares a two-qubit pure Bell state $\rho^{A^*C^*} = [|\Phi^+\rangle\langle\Phi^+|]_{A^*C^*}$. He sends the fake particle A^* to Alice through the phase-damping channel, while keeping the particle C^* in his hand. At the same time, he randomly prepares a two-qubit mixed state $\rho^{B'B''+}$ or $\rho^{B'B''-}$.

$$\begin{aligned}\rho^{B'B''+} &= \tfrac{1}{2}[\alpha^2|00\rangle\langle 00| + \alpha^2|10\rangle\langle 10| + \beta^2|01\rangle\langle 01| + \beta^2|11\rangle\langle 11|]_{B'B''},\\ \rho^{B'B''-} &= \tfrac{1}{2}[\beta^2|00\rangle\langle 00| + \beta^2|10\rangle\langle 10| + \alpha^2|01\rangle\langle 01| + \alpha^2|11\rangle\langle 11|]_{B'B''},\end{aligned} \tag{8}$$

Thereafter, he sends the fake particle B' to Bob through the same phase-damping channel. The reason of choosing the states $\rho^{B'B''+}$ and $\rho^{B'B''-}$ is that they will not be interfered by the phase-damping channel, i.e.

$$\varepsilon(\rho^{B'B''+}) = \rho^{B'B''+}, \varepsilon(\rho^{B'B''-}) = \rho^{B'B''-} \tag{9}$$

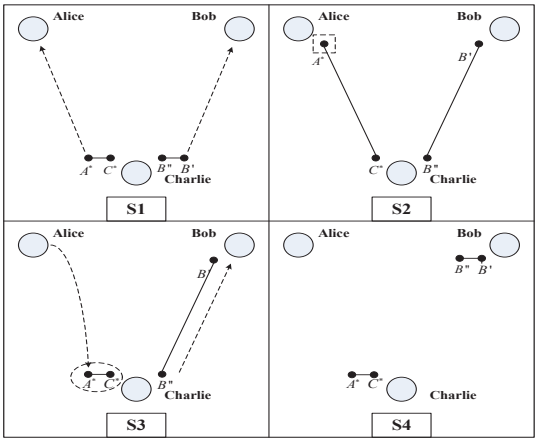

Fig. 1. Charlie's attack strategy. The gray circles are the participants Alice, Bob and Charlie. The black dots represent the qubits prepared by Charlie..

(S2) After receiving the particle A^*, Alice encodes her secret messages m_1m_2 by performing the unitary operations $\{I(00), \sigma_x(01), i\sigma_y(10), \sigma_z(11)\}$. Then, she sends the modified particle A^* to Bob.

(S3) Charlie eavesdrops on the phase-damping channel between Alice and bob, and intercepts the particle A^*.

Then, Charlie performs the projective measurement and POVM measurement to extract the secret messages. The measurement basis is the same as Step IV of Subsection 2.2. However, compared to the original Noisy-NQC-QSS protocol in which the extracted secret messages are $1 + (1 - p)^3$ bits, the amount of secret messages will increase to $1 + (1 - p)^2$ bits extracted by Charlie in this paper. So, it can be seen that the obtaining power of secret messages in the noisy quantum channel is higher than the normal communication in the original protocol. The main reason is that the number of transmission in the original protocol is 3 times in all, while only 2 times are needed in this attack.

(S4) Charlie sends the fake particle $B^{''}$ to Bob through the phase-damping channel. Then, the protocol continues according to Subsection 2.2.

It can be seen that Charlie's attack is feasible. On one hand, Charlie can successfully steal nearly all the secret messages by performing Steps (S1)-(S4). On the other hand, we will explain that the above attack will not be detected by the legitimate participants, i.e., Alice and Bob.

Firstly, we introduce the concept of trace distance [21], that is, $\delta(\rho, \sigma) = \frac{1}{2}||\rho - \sigma||_1 = \frac{1}{2}tr|\rho - \sigma|$. Given two states ρ and σ, the trace distance between them is closely related to the maximum distinguishing probability. If $\delta(\rho, \sigma) = 0$, the quantum states ρ and σ cannot be distinguished from each other. If $\delta(\rho, \sigma) = 1$, the states ρ and σ can be distinguished deterministically.

Although there is no security checking between legitimate participants in Noisy-NQC-QSS, it is very likely that the participant can check the security by himself. For example, Alice can

compare the fake qubit ρ^{A^*}, which comes from the attacker Charlie, with the original qubit ρ^A, which comes from the original Noisy-NQC-QSS protocol. In fact, there are the following equations

$$\rho^A = tr_{BC}(\rho^{ABC}) = tr_{BC}(\tfrac{1}{2}[|000\rangle\langle 000| + |111\rangle\langle 111|] + \tfrac{1-p}{2}[|000\rangle\langle 111| + |111\rangle\langle 000|]_{ABC}) = \tfrac{I}{2},$$
$$\rho^{A^*} = tr_{C^*}(\rho^{A^*C^*}) = tr_{C^*}(\tfrac{1}{2}[|00\rangle\langle 00| + |11\rangle\langle 11|] + \tfrac{1-p}{2}[|00\rangle\langle 11| + |11\rangle\langle 00|]_{A^*C^*}) = \tfrac{I}{2}, \tag{10}$$

It can be found that $\delta(\rho^A, \rho^{A^*}) = 0$. Thus, Alice can never distinguish the quantum states ρ^A and ρ^{A^*}. It means that Charlie's attack will not be noticed by sender Alice. As far as Bob is concerned, he may compare the fake qubits $\rho^{B^{'}B^{''}+}(\rho^{B^{'}B^{''}-})$ with the qubit $\rho^{BB+}(\rho^{BB-})$ if Charlie announces $|N+\rangle(|N-\rangle)$. However, there are

$$\rho^{BB+} = \frac{\langle N+|\frac{1}{4}\sum_{m_1m_2}\rho^{ABC}_{m_1m_2}|N+\rangle}{tr_{AB}\langle N+|\frac{1}{4}\sum_{m_1m_2}\rho^{ABC}_{m_1m_2}|N+\rangle} = \tfrac{1}{2}[\alpha^2|00\rangle\langle 00| + \alpha^2|10\rangle\langle 10| + \beta^2|01\rangle\langle 01| + \beta^2|11\rangle\langle 11|],$$
$$\rho^{BB-} = \frac{\langle N-|\frac{1}{4}\sum_{m_1m_2}\rho^{ABC}_{m_1m_2}|N-\rangle}{tr_{AB}\langle N-|\frac{1}{4}\sum_{m_1m_2}\rho^{ABC}_{m_1m_2}|N-\rangle} = \tfrac{1}{2}[\beta^2|00\rangle\langle 00| + \beta^2|10\rangle\langle 10| + \alpha^2|01\rangle\langle 01| + \alpha^2|11\rangle\langle 11|]. \tag{11}$$

One can easily verify that $\delta(\rho^{BB+}, \rho^{B^{'}B^{''}+}) = \delta(\rho^{BB-}, \rho^{B^{'}B^{''}-}) = 0$. It is impossible for Bob to distinguish the states $\{\rho^{BB+}, \rho^{B^{'}B^{''}+}\}$ and $\{\rho^{BB-}, \rho^{B^{'}B^{''}-}\}$. Therefore, the above attack strategy will not arouse Bob's suspicion. That is, Charlie's attack is feasible.

Case 2: Bob's Attack

By using the similar attack in Subsection 3.2.1, Bob can also steal partial secret messages in Noisy-NQC-QSS without Charlie's help. The similar attack is as follows.

After Bob has received particle A from Alice through the phase-damping channel, the density operators on the particles in his hand can be calculated by tracing out the particle C in Eq.(4). One can easily verify that Bob's quantum state is the same as the result in Noiseless-NQC-QSS, which is described by Eq.(7). To recover the secret messages without Charlie's help, he performs the attack according to Subsection 3.2.1. If the projector P_1 is got, Bob can figure out that the original secret messages are either 00 or 11. On the other hand, if the quantum state is projected to P_2, he guesses that Alice's secret messages are 01 or 10. Thus, Bob can partially steal Alice's secret messages.

4. The perfect QSS protocol

In the section, we investigate the perfect QSS protocol. A new Noiseless QSS protocol in Subsection 4.1 and a Noisy QSS protocol in Subsection 4.2 will be proposed. The security of our protocol will be analyzed rigorously in Subsection 4.3.

4.1. *A perfect Noiseless QSS protocol*

In this subsection, we propose a new Noiseless QSS protocol. The security loophole in the Noiseless-NQC-QSS is solved. We give our protocol as follows.

(TL-1) Pure GHZ states are shared by three parties. Let three parties, i.e., Alice, Bob and Charlie, securely share a group of pure GHZ states, which are randomly in $|\psi^I\rangle_{ABC} =$

$\frac{|000\rangle+|111\rangle}{\sqrt{2}}$ or $|\psi^X\rangle_{ABC} = \frac{|100\rangle+|011\rangle}{\sqrt{2}}$. The initial quantum states (either $|\psi^I\rangle$ or $|\psi^X\rangle$) are completely known to Alice. However, Bob and Charlie do not know the initial state.

(TL-2) Unitary operations are performed by Alice. Alice has the secret messages m, which has been denoted as the binary number. In this step, Alice encodes every two bits message by performing one of the unitary operations$\{I(00), H(01), i\sigma_y(10), H \cdot i\sigma_y(11)\}$ on the particle A in every pure GHZ state. Here, the unitary operations [22] are $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$, and $i\sigma_y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

As far as a GHZ quantum state is concerned, it can be transformed into one of the following cases

$$
\begin{aligned}
|\tilde{\psi}^I_{00}\rangle_{ABC} &= (I \otimes I \otimes I)|\psi^I\rangle_{ABC} = \tfrac{|000\rangle+|111\rangle}{\sqrt{2}} \\
|\tilde{\psi}^I_{01}\rangle_{ABC} &= (H \otimes I \otimes I)|\psi^I\rangle_{ABC} = \tfrac{|000\rangle+|100\rangle+|011\rangle-|111\rangle}{2} \\
|\tilde{\psi}^I_{10}\rangle_{ABC} &= (i\sigma_y \otimes I \otimes I)|\psi^I\rangle_{ABC} = \tfrac{-|100\rangle+|011\rangle}{\sqrt{2}} \\
|\tilde{\psi}^I_{11}\rangle_{ABC} &= (H \cdot i\sigma_y \otimes I \otimes I)|\psi^I\rangle_{ABC} = \tfrac{-|000\rangle+|100\rangle+|011\rangle+|111\rangle}{2}
\end{aligned}
\tag{12}
$$

$$
\begin{aligned}
|\tilde{\psi}^X_{00}\rangle_{ABC} &= (I \otimes I \otimes I)|\psi^X\rangle_{ABC} = \tfrac{|100\rangle+|011\rangle}{\sqrt{2}} \\
|\tilde{\psi}^X_{01}\rangle_{ABC} &= (H \otimes I \otimes I)|\psi^X\rangle_{ABC} = \tfrac{|000\rangle-|100\rangle+|011\rangle+|111\rangle}{2} \\
|\tilde{\psi}^X_{10}\rangle_{ABC} &= (i\sigma_y \otimes I \otimes I)|\psi^X\rangle_{ABC} = \tfrac{|000\rangle-|111\rangle}{\sqrt{2}} \\
|\tilde{\psi}^X_{11}\rangle_{ABC} &= (H \cdot i\sigma_y \otimes I \otimes I)|\psi^X\rangle_{ABC} = \tfrac{|000\rangle+|100\rangle-|011\rangle+|111\rangle}{2}
\end{aligned}
\tag{13}
$$

Alice then sends the qubit A to Bob. When sending the particles, she inserts a certain number of decoy-state particles which are randomly in one of four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

(TL-3) Security check is performed by Alice and Bob. Bob makes instant confirmation after he has received the particles from Alice. After that, Alice and Bob cooperate to check the security of the protocol. (i) Alice announces the positions and measurement basis ($\{|0\rangle, |1\rangle\}$or $\{|+\rangle, |-\rangle\}$) of the decoy-state particles. (ii) Bob measures these particles under the given basis and announces the results. (iii) Alice compares the measurement outcomes with the initial states of the decoy particles. If the error rate during the transmission is higher than the given threshold, Alice cancels this protocol and restarts.

(TL-4) Charlie performed a single-qubit measurement. The above states in Eqs.(12) and (13) can be re-written as

$$
\begin{aligned}
|\tilde{\psi}^I_{00}\rangle_{ABC} &= \frac{(|\tilde{\Phi}_{00}\rangle \otimes |+\rangle + \frac{(|\tilde{\Phi}_{01}\rangle - |\tilde{\Phi}_{11}\rangle)}{\sqrt{2}} \otimes |-\rangle}{\sqrt{2}}, \quad |\tilde{\psi}^I_{01}\rangle_{ABC} = \frac{(|\tilde{\Phi}_{01}\rangle \otimes |+\rangle + \frac{(|\tilde{\Phi}_{00}\rangle - |\tilde{\Phi}_{10}\rangle)}{\sqrt{2}} \otimes |-\rangle}{\sqrt{2}}, \\
|\tilde{\psi}^I_{10}\rangle_{ABC} &= \frac{(|\tilde{\Phi}_{10}\rangle \otimes |+\rangle - \frac{(|\tilde{\Phi}_{01}\rangle + |\tilde{\Phi}_{11}\rangle)}{\sqrt{2}} \otimes |-\rangle}{\sqrt{2}}, \quad |\tilde{\psi}^I_{11}\rangle_{ABC} = \frac{(|\tilde{\Phi}_{11}\rangle \otimes |+\rangle - \frac{(|\tilde{\Phi}_{10}\rangle + |\tilde{\Phi}_{00}\rangle)}{\sqrt{2}} \otimes |-\rangle}{\sqrt{2}}.
\end{aligned}
\tag{14}
$$

$$
\begin{aligned}
|\tilde{\psi}^X_{00}\rangle_{ABC} &= \frac{[\frac{(|\tilde{\Phi}_{01}\rangle)+|\tilde{\Phi}_{11}\rangle}{\sqrt{2}} \otimes |+\rangle - |\tilde{\Phi}_{10}\rangle \otimes |-\rangle]}{\sqrt{2}}, \quad |\tilde{\psi}^X_{01}\rangle_{ABC} = \frac{[\frac{(|\tilde{\Phi}_{00}\rangle)+|\tilde{\Phi}_{10}\rangle}{\sqrt{2}} \otimes |+\rangle - |\tilde{\Phi}_{11}\rangle \otimes |-\rangle]}{\sqrt{2}}, \\
|\tilde{\psi}^X_{10}\rangle_{ABC} &= \frac{[\frac{(|\tilde{\Phi}_{01}\rangle)-|\tilde{\Phi}_{11}\rangle}{\sqrt{2}} \otimes |+\rangle + |\tilde{\Phi}_{00}\rangle \otimes |-\rangle]}{\sqrt{2}}, \quad |\tilde{\psi}^X_{11}\rangle_{ABC} = \frac{[\frac{(|\tilde{\Phi}_{00}\rangle)-|\tilde{\Phi}_{10}\rangle}{\sqrt{2}} \otimes |+\rangle + |\tilde{\Phi}_{01}\rangle \otimes |-\rangle]}{\sqrt{2}}.
\end{aligned}
\tag{15}
$$

Here, $|\tilde{\Phi}_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, $|\tilde{\Phi}_{01}\rangle = \frac{|00\rangle+|10\rangle+|01\rangle-|11\rangle}{2}$, $|\tilde{\Phi}_{10}\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$ and $|\tilde{\Phi}_{11}\rangle = \frac{-|00\rangle+|10\rangle+|01\rangle+|11\rangle}{2}$.

At this stage, it is not possible for either Bob or Charlie to recover the secret messages independently. To recover the secret messages, Charlie performs a single-qubit measurement in the Hadamard basis $\{|+\rangle, |-\rangle\}$ and announces the measurement outcome. Meanwhile, Alice announces the initial GHZ states $|\psi^I\rangle$ or $|\psi^X\rangle$.

(TL-5) Bob performs a two-qubit measurement. According to the announcements from Alice and Charlie, Bob performs a two-qubit measurement on his particles. If the announcements from Alice and Charlie are $|\psi^I\rangle$ and $|+\rangle$ (or $|\psi^X\rangle$ and $|-\rangle$), Bob makes the measurement under the basis $MB_1 = \{|\tilde{\Phi}_{00}\rangle, |\tilde{\Phi}_{01}\rangle, |\tilde{\Phi}_{10}\rangle, |\tilde{\Phi}_{11}\rangle\}$. Otherwise, he performs projection measurement under the basis $MB_2 = \{\frac{|\tilde{\Phi}_{01}\rangle-|\tilde{\Phi}_{11}\rangle}{\sqrt{2}}, \frac{|\tilde{\Phi}_{00}\rangle-|\tilde{\Phi}_{10}\rangle}{\sqrt{2}}, \frac{|\tilde{\Phi}_{01}\rangle+|\tilde{\Phi}_{11}\rangle}{\sqrt{2}}, \frac{|\tilde{\Phi}_{10}\rangle+|\tilde{\Phi}_{00}\rangle}{\sqrt{2}}\}$. Finally, the two bits secret messages can be decoded according to the Table 2.

Table 2. The relations between the two bits secret messages, the announcement of Alice and Charlie, and the measurement outcomes of Bob.

Bob measurement basis	Alice and Charlie's announcement $\|\psi^I\rangle, \|+\rangle(00)$	Alice and Charlie's announcement $\|\psi^X\rangle, \|-\rangle(11)$
$\|\tilde{\Phi}_{00}\rangle(00)$	$I(00)$	$i\sigma_y(10)$
$\|\tilde{\Phi}_{01}\rangle(01)$	$H(01)$	$H \cdot i\sigma_y(11)$
$\|\tilde{\Phi}_{10}\rangle(10)$	$i\sigma_y(10)$	$I(00)$
$\|\tilde{\Phi}_{11}\rangle(11)$	$H \cdot i\sigma_y(11)$	$H(01)$
Bob measurement basis	Alice and Charlie's announcement $\|\psi^X\rangle, \|+\rangle(00)$	Alice and Charlie's announcement $\|\psi^I\rangle, \|-\rangle(11)$
$[\frac{\|\tilde{\Phi}_{01}\rangle-\|\tilde{\Phi}_{11}\rangle}{\sqrt{2}}(00)$	$i\sigma_y(10)$	$I(00)$
$\frac{\|\tilde{\Phi}_{00}\rangle-\|\tilde{\Phi}_{10}\rangle}{\sqrt{2}}(01)$	$H \cdot i\sigma_y(11)$	$H(01)$
$\frac{\|\tilde{\Phi}_{01}\rangle+\|\tilde{\Phi}_{11}\rangle}{\sqrt{2}}(10)$	$I(00)$	$i\sigma_y(10)$
$\frac{\|\tilde{\Phi}_{10}\rangle+\|\tilde{\Phi}_{00}\rangle}{\sqrt{2}}(11)$	$H(01)$	$H \cdot i\sigma_y(11)$

4.2. *A perfect Noisy QSS protocol*

In this subsection, we will investigate a Noisy QSS protocol, which can prevent the attacks in Section 3.2. Our Noisy QSS protocol through phase-damping channels is described as followings.

(TN-1) Mixed GHZ state shared by three parties. Since Alice serves as the dealer, she is supposed to perform the protocol faithfully. Let Alice prepare a group of pure GHZ states, which are randomly in $|\psi^I\rangle_{ABC} = \frac{|000\rangle+|111\rangle}{\sqrt{2}}$ or $|\psi^X\rangle_{ABC} = \frac{|100\rangle+|011\rangle}{\sqrt{2}}$. Thereafter, she keeps qubit A, while sends the qubits B and C to Bob and Charlie through the phase-damping channels, respectively.

When sending the sequences B and C, Alice inserts two different groups of decoy-state particles in two sequences. Similar to Step (TL-3), Alice checks the security of qubit transmission with Bob and Charlie, respectively. In fact, the above checking method is originated from BB84 QKD [10]. It can resist several attacks, such as the intercept-resend attack, the measurement-resend attack, the entanglement-measure attack and the denial-of-service (DOS) attack. Furthermore, the decoy technique is effective with both noise-free channel and noisy quantum channel. If the qubits are transmitted in a noiseless channel, a reasonable thresh-

old value can be calculated [23] to guarantee that the legitimate participants can distill the information.

(TN-2) Local unitary operation by Alice. In this step, Alice encodes every two bits message by carrying out the local unitary operations $\{I(00), H(01), i\sigma_y(10), H \cdot i\sigma_y(11)\}$ on the qubit A in every GHZ state. As far as a GHZ state is concerned, it is transformed into one of the following eight cases

$$\begin{aligned}
\rho_{00}^{ABC,I} &= \frac{|000\rangle\langle 000| + |111\rangle\langle 111|}{2} + \frac{(1-p)^2[|000\rangle\langle 111| + |111\rangle\langle 000|]}{2} \\
\rho_{01}^{ABC,I} &= \frac{[|000\rangle\langle 000| + |100\rangle\langle 000| + |000\rangle\langle 100| + |100\rangle\langle 100| + |011\rangle\langle 011| - |111\rangle\langle 011| - |011\rangle\langle 111| + |111\rangle\langle 111|]}{4} \\
&\quad + \frac{(1-p)^2[|000\rangle\langle 011| + |100\rangle\langle 011| - |000\rangle\langle 111| - |100\rangle\langle 111| + |011\rangle\langle 000| - |111\rangle\langle 000| + |011\rangle\langle 100| - |111\rangle\langle 100|]}{4} \\
\rho_{10}^{ABC,I} &= \frac{|100\rangle\langle 100| + |011\rangle\langle 011|}{2} - \frac{(1-p)^2|100\rangle\langle 011| + |011\rangle\langle 100|}{2} \\
\rho_{11}^{ABC,I} &= \frac{[|000\rangle\langle 000| - |100\rangle\langle 000| - |000\rangle\langle 100| + |100\rangle\langle 100| + |011\rangle\langle 011| + |111\rangle\langle 011| + |011\rangle\langle 111| + |111\rangle\langle 111|]}{4} \\
&\quad + \frac{(1-p)^2[-|000\rangle\langle 011| + |100\rangle\langle 011| - |000\rangle\langle 111| + |100\rangle\langle 111| - |011\rangle\langle 000| - |111\rangle\langle 000| + |011\rangle\langle 100| + |111\rangle\langle 100|]}{4}
\end{aligned} \tag{16}$$

$$\begin{aligned}
\rho_{00}^{ABC,X} &= \frac{|100\rangle\langle 100| + |011\rangle\langle 011|}{2} + \frac{(1-p)^2[|011\rangle\langle 100| + |100\rangle\langle 011|]}{2} \\
\rho_{01}^{ABC,X} &= \frac{[|000\rangle\langle 000| - |100\rangle\langle 000| - |000\rangle\langle 100| + |100\rangle\langle 100| + |011\rangle\langle 011| + |111\rangle\langle 011| + |011\rangle\langle 111| + |111\rangle\langle 111|]}{4} \\
&\quad + \frac{(1-p)^2[|011\rangle\langle 000| + |111\rangle\langle 000| - |011\rangle\langle 100| - |111\rangle\langle 100| + |000\rangle\langle 011| - |100\rangle\langle 011| + |000\rangle\langle 111| - |100\rangle\langle 111|]}{4} \\
\rho_{10}^{ABC,X} &= \frac{|000\rangle\langle 000| + |111\rangle\langle 111|}{2} - \frac{(1-p)^2|111\rangle\langle 000| + |000\rangle\langle 111|}{2} \\
\rho_{11}^{ABC,X} &= \frac{[|000\rangle\langle 000| + |100\rangle\langle 000| + |000\rangle\langle 100| + |100\rangle\langle 100| + |011\rangle\langle 011| - |111\rangle\langle 011| - |011\rangle\langle 111| + |111\rangle\langle 111|]}{4} \\
&\quad + \frac{(1-p)^2[-|011\rangle\langle 000| + |111\rangle\langle 000| - |011\rangle\langle 100| + |111\rangle\langle 100| - |000\rangle\langle 011| - |100\rangle\langle 011| + |000\rangle\langle 111| + |100\rangle\langle 111|]}{4}
\end{aligned} \tag{17}$$

After that, Alice sends the qubit A to Bob through the same phase-damping channel. While sending the particles, she inserts a number of decoy-state particles which are randomly in $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

(TN-3) Security check performed by Alice and Bob. Similar to Step (TL-3) and (TN-1), Alice and Bob cooperate to check the security of transmission.

(TN-4) Charlie performs a single-qubit measurement. After receiving the qubits from Alice, the quantum states in Bob and Charlie's hands become $\rho_{m_1 m_2}^{BBC,\{I,X\}}$. But it is impossible for either of them to decipher the secret independently. To help Bob recover the secret messages, Charlie performs a single-qubit measurement under the orthogonal basis $\{|N+\rangle, |N-\rangle\}$. Thereafter, he announces the measurement outcome. Alice should also publish the initial GHZ state $|\psi^I\rangle_{ABC}$ or $|\psi^X\rangle_{ABC}$ which is randomly chosen in Step (TN-1).

Without loss of generality, suppose that the GHZ state prepared by Alice is $|\psi^I\rangle_{ABC}$ and

Charlie's measurement outcome is $|N+\rangle$ (Please see the Appendix for all the other cases). Then, the particles in Bob's hand will become one of the following states

$$\begin{aligned}
\rho_{00}^{BB,I+} &= \alpha^2|00\rangle\langle 00| + \beta^2|11\rangle\langle 11| + (1-p)^3[\alpha\beta|00\rangle\langle 11| + \alpha\beta|11\rangle\langle 00|] \\
\rho_{01}^{BB,I+} &= \tfrac{1}{2}[\alpha^2|00\rangle\langle 00| + \alpha^2|10\rangle\langle 10| + \beta^2|01\rangle\langle 01| + \beta^2|11\rangle\langle 11|] \\
&\quad + \tfrac{1-p}{2}[\alpha^2|10\rangle\langle 00| + \alpha^2|00\rangle\langle 10| - \beta^2|11\rangle\langle 01| - \beta^2|01\rangle\langle 11|] \\
&\quad + \tfrac{(1-p)^2}{2}[\alpha\beta|00\rangle\langle 01| - \alpha\beta|10\rangle\langle 11| + \alpha\beta|01\rangle\langle 00| - \alpha\beta|11\rangle\langle 10|] \\
&\quad + \tfrac{(1-p)^3}{2}[\alpha\beta|10\rangle\langle 01| - \alpha\beta|00\rangle\langle 11| - \alpha\beta|11\rangle\langle 00| + \alpha\beta|01\rangle\langle 10|] \\
\rho_{10}^{BB,I+} &= \alpha^2|10\rangle\langle 10| + \beta^2|01\rangle\langle 01| - (1-p)^3[\alpha\beta|10\rangle\langle 01| + \alpha\beta|01\rangle\langle 10|] \\
\rho_{11}^{BB,I+} &= \tfrac{1}{2}[\alpha^2|00\rangle\langle 00| + \alpha^2|10\rangle\langle 10| + \beta^2|01\rangle\langle 01| + \beta^2|11\rangle\langle 11|] \\
&\quad + \tfrac{1-p}{2}[-\alpha^2|10\rangle\langle 00| - \alpha^2|00\rangle\langle 10| + \beta^2|11\rangle\langle 01| + \beta^2|01\rangle\langle 11|] \\
&\quad + \tfrac{(1-p)^2}{2}[-\alpha\beta|00\rangle\langle 01| + \alpha\beta|10\rangle\langle 11| - \alpha\beta|01\rangle\langle 00| + \alpha\beta|11\rangle\langle 10|] \\
&\quad + \tfrac{(1-p)^3}{2}[\alpha\beta|10\rangle\langle 01| - \alpha\beta|00\rangle\langle 11| - \alpha\beta|11\rangle\langle 00| + \alpha\beta|01\rangle\langle 10|]
\end{aligned} \tag{18}$$

(TN-5) Bob performs a two-qubit measurement. If Charlie and Alice announce $|\psi^I\rangle$ and $|N+\rangle$ (or $|\psi^X\rangle$ and $|N-\rangle$), Bob performs a two-qubit measurement under the basis $MB_1 = \{|\tilde{\Phi}_{00}\rangle, |\tilde{\Phi}_{01}\rangle, |\tilde{\Phi}_{10}\rangle, |\tilde{\Phi}_{11}\rangle\}$. Otherwise, he measures his particles under the orthogonal basis $MB_2 = \frac{|\tilde{\Phi}_{11}\rangle - |\tilde{\Phi}_{01}\rangle}{\sqrt{2}}, \frac{|\tilde{\Phi}_{00}\rangle - |\tilde{\Phi}_{10}\rangle}{\sqrt{2}}, \frac{|\tilde{\Phi}_{01}\rangle + |\tilde{\Phi}_{11}\rangle}{\sqrt{2}}, \frac{|\tilde{\Phi}_{10}\rangle + |\tilde{\Phi}_{00}\rangle}{\sqrt{2}}$.

We now calculate the average success probability as follows

$$\begin{aligned}
&P(success) \\
&= \textstyle\sum_{Me\{I,X\},Ne\{N+,N-\}} P(|\psi^M\rangle, |N\rangle) P(success||\psi^M\rangle, |N\rangle) \\
&= \tfrac{1}{4}[1 + 2\alpha\beta(1-p)^3] + \tfrac{1}{8}[2 - p + 2\alpha\beta(2-p)(1-p)^2] \\
&\leq \tfrac{1}{4}[1 + (1-p)^3] + \tfrac{1}{8}[2 - p + (2-p)(1-p)^2] \\
&= 1 + \tfrac{-3p^3 + 10p^2 - 12p}{8}
\end{aligned} \tag{19}$$

Here, the success probability is maximized if and only if $\alpha = \beta = \frac{1}{\sqrt{2}}$. The relations between the success probability and the channel parameter are presented in Figure 2.

4.3. *Security analysis of our QSS protocol*

Security is one of the most important issues for consideration in quantum cryptography, especially in QSS. We will prove the security of our protocol from the following four aspects.

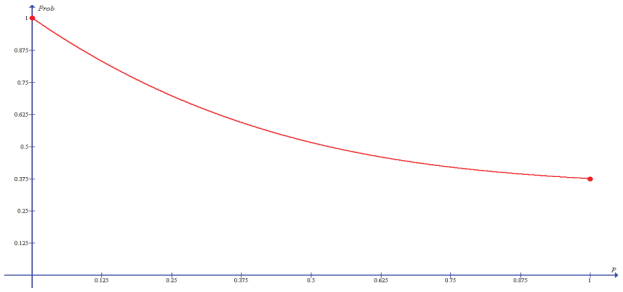

Fig. 2. The relations between the success probability (Prob) and the channel parameter (p)

(i) Meeting the requirement of information theoretic security

To prove the security of our QSS, we should first consider the fundamental requirement of information theoretic security. In our protocol, the information rate for each participant is

$$\rho_{Bob} = \frac{log_2|\mathcal{K}|}{log_2|S(Bob)|} = \rho_{Charlie} = \frac{log_2|\mathcal{K}|}{log_2|S(Charlie)|} = \frac{log_2|Z_2^2|}{log_2|Z_2^2|} = 1, \tag{20}$$

which further implies the information rate for the whole protocol. According to the theorem in Section 2, it is the maximum rate that can be achieved by perfect secret sharing. Thus, the proposed protocol has satisfied the basic requirement of information theoretic security in the secret sharing.

(ii)Security analysis of outside attack

In the proposed protocol, Alice inserts some decoy states to check the security of qubit transmission. This technique is enlightened by the well-known BB84 QKD [10], which has been proved unconditionally secure by several groups [24]. Specifically, an eavesdropper Eve may perform a general quantum operation, which can be described as an isometric extension to a larger Hilbert space $V \in Hom(\mathcal{H}_{Alice}, \mathcal{H}_{Alice} \otimes \mathcal{H}_{Eve})$. As a result, the state on the decoy states will be transformed into

$$\begin{aligned} V|0\rangle &= |0\rangle|e_{00}\rangle + |1\rangle|e_{01}\rangle; \qquad V|1\rangle = |0\rangle|e_{10}\rangle + |1\rangle|e_{11}\rangle; \\ V|+\rangle &= |0\rangle\tfrac{|e_{00}\rangle+|e_{10}\rangle}{\sqrt{2}} + |1\rangle\tfrac{|e_{01}\rangle+|e_{11}\rangle}{\sqrt{2}}; \quad V|-\rangle = |0\rangle\tfrac{|e_{00}\rangle-|e_{10}\rangle}{\sqrt{2}} + |1\rangle\tfrac{|e_{01}\rangle-|e_{11}\rangle}{\sqrt{2}}. \end{aligned} \tag{21}$$

To avoid being detected, the above states should always lie in the corresponding eigenspace of Pauli operator Z and X

$$\begin{aligned} ZV|0\rangle = V|0\rangle \Rightarrow |e_{01}\rangle = \mathbf{0}; \qquad ZV|1\rangle = -V|1\rangle \Rightarrow |e_{10}\rangle = \mathbf{0}; \\ XV|+\rangle = V|+\rangle \Rightarrow |e_{00}\rangle = |e_{11}\rangle = |e\rangle; \quad XV|-\rangle = -V|-\rangle \Rightarrow |e_{00}\rangle = |e_{11}\rangle = |e\rangle. \end{aligned} \tag{22}$$

Therefore, what Eve has got is just the blank state $|e\rangle$, which prevents her from stealing any useful information. Even in the presence of noisy quantum channel, a reasonable threshold can be devised to prevent all possible attacks [23]. Thus, any outside attacks will be detected with non-zero probability.

Besides, even if an outside attack happens, the eavesdropper not only obtains no useful information but also is detected in the security checking process. On one hand, the qubits in the distribution of GHZ states in Steps (TN-1) and (TL-1) do not carry any secret message.

If an eavesdropper appears, she learns nothing about the secret messages and will be noticed by the legitimate participants. Once the security checking passes, the fidelity of the GHZ state can be sufficiently verified. On the other hand, the quantum state of the transmitted qubit in Steps (TN-2) and (TL-2) is completely mixed, i.e. $tr_{BC}\rho^{ABC} = I/2$. Any outside eavesdropping attack is ineffective and will be detected in Steps (TN-3) and (TL-3).

Above all, our protocol is secure against outside attacks.

(iii)Security analysis of participant attack from Bob

In the following, the participant attack from Bob will be analyzed. Assume that Alice is honest, since she is the dealer of the secret sharing protocol. However, the participant Bob may try to steal the secret messages m_1m_2 by measuring his qubits and obtaining the result $\rho^{BB}_{m_1m_2}$. In our protocol, the quantum state on the particles in Bob's hand is

$$\begin{aligned}\rho^{BB}_{00} &= tr_C(\tfrac{1}{2}\rho^{BBC,I}_{00} + \tfrac{1}{2}\rho^{BBC,X}_{00}) \\ &= \tfrac{1}{4}(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|) \\ &= \rho^{BB}_{01} = \rho^{BB}_{10} = \rho^{BB}_{11}\end{aligned} \tag{23}$$

In this case, Bob can never distinguish the states $\rho^{BB}_{00}, \rho^{BB}_{01}, \rho^{BB}_{10}$ and ρ^{BB}_{11} without Charlie's help, as the Holevo bound [22] shows that the accessible information for him is no more than $S(\frac{1}{4}\sum_{m_1m_2}\rho^{BB}_{m_1m_2}) - \frac{1}{4}\sum_{m_1m_2}\rho^{BB}_{m_1m_2}) = 0$ *bit*.

For clarity, we now provide a proof by calculating the posterior probability from Bob's point of view. Let us first suppose that Bob chooses his measurement basis MB_1, MB_2 with probability $p(MB_1)$ and $p(MB_2)$, respectively. Then, given a certain key $\mathbf{K} = k$, the conditional probability of his share can be calculated as follows:

$$\begin{aligned}&p[\mathbf{S(Bob)} = 00|\mathbf{K} = 00] \\ &= p(MB_1)p[\mathbf{S(Bob)} = 00|\mathbf{K} = 00, MB_1] + p(MB_2)p[\mathbf{S(Bob)} = 00|\mathbf{K} = 00, MB_2] \\ &= p(MB_1)tr(|\tilde{\Phi}_{00}\rangle\langle\tilde{\Phi}_{00}|\tfrac{I}{4}) + p(MB_2)tr(\tfrac{|\tilde{\Phi}_{01}\rangle - |\tilde{\Phi}_{11}\rangle}{\sqrt{2}}\tfrac{\langle\tilde{\Phi}_{01}| - \langle\tilde{\Phi}_{11}|}{\sqrt{2}}\tfrac{I}{4}) \\ &= \tfrac{1}{4}(p(MB_1) + p(MB_2)) = \tfrac{1}{4} \\ &= p[\mathbf{S(Bob)} = 01|\mathbf{K} = 00] = \ldots = p[\mathbf{S(Bob)} = 11|\mathbf{K} = 11]\end{aligned} \tag{24}$$

Next, we compute the probability of the share in Bob's hand

$$\begin{aligned}p[\mathbf{S(Bob)} = 00] &= \sum_k p[\mathbf{K} = k]p[\mathbf{S(Bob)} = 00|\mathbf{K} = k] \\ &= \sum_k p[\mathbf{K} = k]\frac{1}{4} = \frac{1}{4} \\ &= p[\mathbf{S(Bob)} = 01] = p[\mathbf{S(Bob)} = 10] = p[\mathbf{S(Bob)} = 11]\end{aligned} \tag{25}$$

Finally, the posterior can be immediately obtained using the Bayes theorem

$$p[\mathbf{K} = k|\mathbf{S(Bob)} = g_B] = \frac{p[\mathbf{K} = k]p[\mathbf{S(Bob)} = g_B|\mathbf{K} = k]}{p[\mathbf{S(Bob)} = g_B]} = \frac{p[\mathbf{K} = k]\frac{1}{4}}{\frac{1}{4}} = p[\mathbf{K} = k] \tag{26}$$

Therefore, for the dishonest Bob alone, he can get no useful information about the value of the secret key.

(iv) Security analysis of participant attack from Charlie

In the QSS protocol, the participant Charlie may also attack NQC-QSS by performing some local operations on his qubit. However, if the other two particles are traced out, the quantum state of his qubit always lies in $\frac{I}{2}$.

$$\rho_{00}^{C,I} = tr_{AB}\rho_{00}^{BBC,I} = \frac{I}{2} = \rho_{00}^{C,X} = \rho_{01}^{C,I} = \ldots = \rho_{11}^{C,X} \tag{27}$$

Thus, by calculating the conditional probability

$$\begin{aligned} & p[\mathbf{S(Charlie)} = 00|\mathbf{K} = 00] \\ & = p[Alice\,chooses\,|\psi^I\rangle]p[Charlie\,gets\,|N+\rangle|\mathbf{K} = 00, Alice\,chooses\,|\psi^I\rangle] \\ & = \tfrac{1}{2}tr[|N+\rangle\langle N+|\tfrac{I}{2}] = \tfrac{1}{4} = p[\mathbf{S(Charlie)} = 01|\mathbf{K} = 00] \\ & = \ldots = p[\mathbf{S(Charlie)} = 11|\mathbf{K} = 11] \end{aligned} \tag{28}$$

the probability of Charlie's share

$$\begin{aligned} & p[\mathbf{S(Charlie)} = 00] = \sum_k p[\mathbf{K} = k]p[\mathbf{S(Charlie)} = 00|\mathbf{K} = k] = \frac{1}{4} \\ & = p[\mathbf{S(Charlie)} = 01] = p[\mathbf{S(Charlie)} = 10] = p[\mathbf{S(Charlie)} = 11] \end{aligned} \tag{29}$$

and the posterior probability

$$p[\mathbf{K} = k|\mathbf{S(Charlie)} = g_C] = \frac{p[\mathbf{K} = k]p[\mathbf{S(Charlie)} = g_C|\mathbf{K} = k]}{p[\mathbf{S(Charlie)} = g_C]} = p[\mathbf{K} = k] \tag{30}$$

one may find that Charlie's own share is independent of the secret key.

From the above analysis, the proposed protocol is secure.

5. Conclusions

In conclusion, the perfect secret sharing in quantum cryptography is investigated. On one hand, the security of NQC-QSS is re-examined. We find that it violates the requirement of information theoretic security in the secret sharing and suffers from the information leakage. The cryptanalysis including several specific attack strategies are given. For the Noiseless-NQC-QSS, the dishonest Bob can steal half of secrets by classifying $\{\rho_{00}^{BB}, \rho_{01}^{BB}, \rho_{10}^{BB}, \rho_{11}^{BB}\}$ into two subsets and performing appropriate projection measurement. As far as the Noisy-NQC-QSS is concerned, the information leakage becomes even worse. The attack strategy from the dishonest Bob is still feasible. Moreover, the participant Charlie can steal nearly all the secrets solely without being noticed by legitimate members. On the other hand, a new QSS protocol including both noiseless and noisy quantum channel is proposed. We rigorously prove the security of protocol. It meets the fundamental requirement of information theoretic security in perfect secret sharing. Furthermore, the security analysis including both the outside attacks and participant attacks is taken into consideration in details. It is shown that our new protocol is a perfect secret sharing.

Acknowledgements

Project supported by the National Natural Science Foundation of China (Nos. 61003287, 61170272, 61272514, 61121061), the Program for New Century Excellent Talents in University, the Specialized Research Fund for the Doctoral Program of Higher Education (20100005120002), the Fok Ying Tong Education Foundation (No. 131067) and the Fundamental Research Funds for the Central Universities (No. BUPT2012RC0221).

References

1. M. Hillery, V. Buzek, and A. Berthiaume, *Quantum secret sharing*, Phys. Rev. A 59, 1829 (1999).
2. D. Gottesman, *Theory of quantum secret sharing*, Phys. Rev. A 61, 042311 (2000).
3. S. K. Singh and R. Srikanth, *Generalized quantum secret sharing*, Phys. Rev. A 71, 012328 (2005).
4. X. B. Chen, X. X. Niu, X. J. Zhou, and Y. X. Yang, *Multi-party quantum secret sharing with single-particle quantum state to encode information*, Quantum Inf Process 12, 365 (2013).
5. W. Tittel, H. Zbinden, and N. Gisin, *Experimental demonstration of quantum secret sharing*, Phys. Rev. A 63, 042301 (2001).
6. A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, *Tripartite Quantum State Sharing*, Phys. Rev. Lett. 92, 177903 (2004).
7. G. Gao, *Cryptanalysis of multiparty quantum secret sharing with collective eavesdropping-check*, Opt. Commun, 283, 2997 (2010).
8. X. F. Liu and R. J. Pan, *Cryptanalysis of quantum secret sharing based on GHZ states*, Phys. Scr. 84, 045015 (2011).
9. T. Hwang, C. C. Hwang, and C. M. Li, *Multiparty quantum secret sharing based on GHZ states*, Phys. Scr. 83, 045004 (2011).
10. C. H. Bennett and G. Brassard., *Quantum cryptography: public-key distribution and coin tossing.* , *In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, IEEE, New York, Bangalore, India (1984) 175-179
11. X. B. Chen, S. Yang, Y. Su, and Y. X. Yang, *Cryptanalysis on the improved multiparty quantum secret sharing protocol based on the GHZ state*, Phys. Scr. 86, 055002 (2012).
12. S. Adhikadri, I. Chakrabarty, and P. Agrawal, *Probabilistic secret sharing sharing through noisy quantum channels*, Quantum Inform. & Comput. 12, 0253 (2012).
13. M. Ito, A. Saito, and T. Nishizeki, *Secret sharing scheme realizing general access structure*, Electronics and Communications in Japan, 72, 56 (1989).
14. J. Benaloh and J. Leichter, *Generalized secret sharing and monotone functions*, Lecture Notes in Computer, Lecture Notes in Computer Science (RYPTO'08) 403, 27 (1990).
15. P. Junod, *On the complexity of Matsui's attack*, Lecture Notes in Computer Science 2259, 199 (2001).
16. L. K. Grover, *A fast quantum mechanical algorithm for database search*, *In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, STOC, New York, NY, USA (1996).
17. S. Lin, Q. Y. Wen, F. Gao, and F. C. Zhu, *Improving the security of multiparty quantum secret sharing based on the improved Bostrom-Felbinger protocol*, Opt. Commun. 281, 4553 (2008).
18. Z. J. Zhang, G. Gao, X. Wang, L. F. Han, and S. H. Shi, *Multiparty quantum secret sharing based on the improved Bostrom-Felbinger protocol*, Opt. Commun. 281, 4553 (2008).
19. Y. Sun, Q. Y. Wen, F. Gao, and F. C. Zhu, *Robust variations of the Bennett-Brassard 1984 protocol against collective noise*, Phys. Rev. A 80, 032321 (2009).
20. A. Cabello, *Six-qubit permutation-based decoherence-free orthogonal basis*, Phys. Rev. A 75, 020301 (2007).
21. C. A. Fuchs and J. Van De Graaf, *Cryptographic distinguishability measures for quantum-mechanical states*, IEEE Transactions on Information Theory 45, 1216 (1999).

22. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge. (Cambridge University Press, 2000).
23. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum cryptography*, Reviews of Modern Physics 74, 145 (2002).
24. H. K. Lo and H. F. Chau, *Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances*, Science 283, 2050 (1999).

Appendix A

In the Step (TN-4) of Subsection 4.2, we have calculated the density operators of Bob's qubits when Alice's and Charlie's announcement $\{|\psi^I\rangle_{ABC}, |N+\rangle\}$. In this appendix, we will provide the calculation results for all the other cases, i.e.$\{|\psi^I\rangle_{ABC}, |N-\rangle\}$, $\{|\psi^X\rangle_{ABC}, |N+\rangle\}$ and $\{|\psi^X\rangle_{ABC}, |N-\rangle\}$

$$
\begin{aligned}
\rho_{00}^{BB,I-} &= \beta^2|00\rangle\langle 00| + \alpha^2|11\rangle\langle 11| - (1-p)^3[\alpha\beta|00\rangle\langle 11| + \alpha\beta|11\rangle\langle 00| \\
\rho_{01}^{BB,I-} &= \tfrac{1}{2}[\beta^2|00\rangle\langle 00| + \beta^2|10\rangle\langle 10| + \alpha^2|01\rangle\langle 01| + \alpha^2|11\rangle\langle 11|] \\
&\quad + \tfrac{1-p}{2}[\beta^2|10\rangle\langle 00| + \beta^2|00\rangle\langle 10| - \alpha^2|11\rangle\langle 01| - \alpha^2|01\rangle\langle 11|] \\
&\quad + \tfrac{(1-p)^2}{2}[-\alpha\beta|00\rangle\langle 01| + \alpha\beta|10\rangle\langle 11| - \alpha\beta|01\rangle\langle 00| + \alpha\beta|11\rangle\langle 10|] \\
&\quad + \tfrac{(1-p)^3}{2}[-\alpha\beta|10\rangle\langle 01| + \alpha\beta|00\rangle\langle 11| + \alpha\beta|11\rangle\langle 00| - \alpha\beta|01\rangle\langle 10|] \\
\rho_{10}^{BB,I-} &= \beta^2|10\rangle\langle 10| + \alpha^2|01\rangle\langle 01| + (1-p)^3[\alpha\beta|10\rangle\langle 01| + \alpha\beta|01\rangle\langle 10|] \\
\rho_{11}^{BB,I-} &= \tfrac{1}{2}[\beta^2|00\rangle\langle 00| + \beta^2|10\rangle\langle 10| + \alpha^2|01\rangle\langle 01| + \alpha^2|11\rangle\langle 11|] \\
&\quad + \tfrac{1-p}{2}[-\beta^2|10\rangle\langle 00| - \beta^2|00\rangle\langle 10| + \alpha^2|11\rangle\langle 01| + \alpha^2|01\rangle\langle 11|] \\
&\quad + \tfrac{(1-p)^2}{2}[\alpha\beta|00\rangle\langle 01| - \alpha\beta|10\rangle\langle 11| + \alpha\beta|01\rangle\langle 00| - \alpha\beta|11\rangle\langle 10|] \\
&\quad + \tfrac{(1-p)^3}{2}[-\alpha\beta|10\rangle\langle 01| + \alpha\beta|00\rangle\langle 11| + \alpha\beta|11\rangle\langle 00| - \alpha\beta|01\rangle\langle 10|]
\end{aligned}
\tag{A.1}
$$

$$
\begin{aligned}
\rho_{00}^{BB,X+} &= \alpha^2|10\rangle\langle 10| + \beta^2|01\rangle\langle 01| + (1-p)^3[\alpha\beta|01\rangle\langle 10| + \alpha\beta|10\rangle\langle 01|] \\
\rho_{01}^{BB,X+} &= \tfrac{1}{2}[\alpha^2|00\rangle\langle 00| + \alpha^2|10\rangle\langle 10| + \beta^2|01\rangle\langle 01| + \beta^2|11\rangle\langle 11|] \\
&\quad + \tfrac{1-p}{2}[-\alpha^2|10\rangle\langle 00| - \alpha^2|00\rangle\langle 10| + \beta^2|11\rangle\langle 01| + \beta^2|01\rangle\langle 11|] \\
&\quad + \tfrac{(1-p)^2}{2}[\alpha\beta|01\rangle\langle 00| - \alpha\beta|11\rangle\langle 10| + \alpha\beta|00\rangle\langle 01| - \alpha\beta|10\rangle\langle 11|] \\
&\quad + \tfrac{(1-p)^3}{2}[\alpha\beta|11\rangle\langle 00| - \alpha\beta|01\rangle\langle 10| - \alpha\beta|10\rangle\langle 01| + \alpha\beta|00\rangle\langle 11|] \\
\rho_{10}^{BB,X+} &= \alpha^2|00\rangle\langle 00| + \beta^2|11\rangle\langle 11| - (1-p)^3[\alpha\beta|11\rangle\langle 00| + \alpha\beta|00\rangle\langle 11|] \\
\rho_{11}^{BB,X+} &= \tfrac{1}{2}[\alpha^2|00\rangle\langle 00| + \alpha^2|10\rangle\langle 10| + \beta^2|01\rangle\langle 01| + \beta^2|11\rangle\langle 11|] \\
&\quad + \tfrac{1-p}{2}[\alpha^2|10\rangle\langle 00| + \alpha^2|00\rangle\langle 10| - \beta^2|11\rangle\langle 01| - \beta^2|01\rangle\langle 11|] \\
&\quad + \tfrac{(1-p)^2}{2}[-\alpha\beta|01\rangle\langle 00| + \alpha\beta|11\rangle\langle 10| - \alpha\beta|00\rangle\langle 01| + \alpha\beta|10\rangle\langle 11|] \\
&\quad + \tfrac{(1-p)^3}{2}[\alpha\beta|11\rangle\langle 00| - \alpha\beta|01\rangle\langle 10| - \alpha\beta|10\rangle\langle 01| + \alpha\beta|00\rangle\langle 11|]
\end{aligned}
\tag{A.2}
$$

$$
\begin{aligned}
\rho_{00}^{BB,X-} &= \beta^2|10\rangle\langle 10| + \alpha^2|01\rangle\langle 01| - (1-p)^3[\alpha\beta|01\rangle\langle 10| + \alpha\beta|10\rangle\langle 01|] \\
\rho_{01}^{BB,X-} &= \tfrac{1}{2}[\beta^2|00\rangle\langle 00| + \beta^2|10\rangle\langle 10| + \alpha^2|01\rangle\langle 01| + \alpha^2|11\rangle\langle 11|] \\
&\quad + \tfrac{1-p}{2}[-\beta^2|10\rangle\langle 00| - \beta^2|00\rangle\langle 10| + \alpha^2|11\rangle\langle 01| + \alpha^2|01\rangle\langle 11|] \\
&\quad + \tfrac{(1-p)^2}{2}[-\alpha\beta|01\rangle\langle 00| + \alpha\beta|11\rangle\langle 10| - \alpha\beta|00\rangle\langle 01| + \alpha\beta|10\rangle\langle 11|] \\
&\quad + \tfrac{(1-p)^3}{2}[-\alpha\beta|11\rangle\langle 00| + \alpha\beta|01\rangle\langle 10| + \alpha\beta|10\rangle\langle 01| - \alpha\beta|00\rangle\langle 11|] \\
\rho_{10}^{BB,X-} &= \beta^2|00\rangle\langle 00| + \alpha^2|11\rangle\langle 11| + (1-p)^3[\alpha\beta|11\rangle\langle 00| + \alpha\beta|00\rangle\langle 11|] \\
\rho_{11}^{BB,X-} &= \tfrac{1}{2}[\beta^2|00\rangle\langle 00| + \beta^2|10\rangle\langle 10| + \alpha^2|01\rangle\langle 01| + \alpha^2|11\rangle\langle 11|] \\
&\quad + \tfrac{1-p}{2}[\beta^2|10\rangle\langle 00| + \beta^2|00\rangle\langle 10| - \alpha^2|11\rangle\langle 01| - \alpha^2|01\rangle\langle 11|] \\
&\quad + \tfrac{(1-p)^2}{2}[\alpha\beta|01\rangle\langle 00| - \alpha\beta|11\rangle\langle 10| + \alpha\beta|00\rangle\langle 01| - \alpha\beta|10\rangle\langle 11|] \\
&\quad + \tfrac{(1-p)^3}{2}[-\alpha\beta|11\rangle\langle 00| + \alpha\beta|01\rangle\langle 10| + \alpha\beta|10\rangle\langle 01| - \alpha\beta|00\rangle\langle 11|]
\end{aligned}
\tag{A.3}
$$