The Improved Quantum Secret Sharing Protocol Based on Grover Algorithm

Zhuo Yu

University of Warwick, Physics Department, Coventry, England, CV4 7AL

Abstract—Quantum secret sharing (QSS) is a cryptographic protocol based on the uncertainty principle and quantum no-cloning theorem and is an essential aspect in quantum computing. This paper describes the Grover search algorithm and how to improve QSS protocol by Grover Algorithm. The QSS based on the Grover algorithm is more secure and easier to operate compared to old QSS protocols. Some scientists improved the security of the first QSS protocol based on QSA by changing the check mode. After that, a protocol with quite different procedures was proposed. The improved one enhances the feasibility of the protocol and it could also make sure that the communication is secure from the attacks.

1. Introduction
Secret sharing is a consequential topic in quantum information science. Nowadays, people pay more and more attention on the privacy and at the same time, there is a crisis of confidence in the society. Many people try their best to protect their own secrets, but want to gain others’ secrets. So the multi-party protocols are required. One of the most critical protocols is the secret sharing. In the secret sharing protocol, a boss splits the secret into several parts and sends them to the agents. As a result, any agent can not read the secret alone, and they must work together to get the secret. Quantum secret sharing was proposed in 1999 [1]. Compared to the Classical secret sharing, quantum secret sharing is more secure because the QSS is based on the uncertainty principle and quantum no-cloning theorem.

Quantum search algorithm is another crucial part of quantum computing. Due to the quantum superposition, the state of a qubit could be superposed. Then the system could complete several assignment simultaneously. This makes the efficiency of the quantum searching task much higher than that of the classical search, especially for the large space. For an unsorted database of size N, the QSA needs √N operation, while N steps are required to the target classically. The Grover algorithm is one of the most significant quantum searching algorithm and is discovered by Grover in 1996 [2]. The Grover algorithm can not ensure that the answer is true and it can only offer the correct outcome with a high probability. However, some scientists proposed an upgraded Grover algorithm that can achieve a 100% success rate [3].

Many scientists focus on QSS protocols based on the QSA since this kind of the protocols play an important role in quantum computation. Hsu tried to come up with a QSS protocol based on the QSA in 2003 [4]. But in 2010, Hao et al. published a eavesdropping and the solution in the Hsu’s protocol [5]. For these two protocols, the boss needs to prepare the initial state |S_i> and divide them into two parts, S_1 and S_2. Then the boss sends S_1 to one agent and sends S_2 to the other. However, there are some defects. For example, agents need to store photons, which is extremely challenging especially
when the time duration is long. Besides, face-to-face cooperation or the third party’s help is necessary [6]. This makes the process more complicated.

Some scientists introduced another QSS protocol based on the Grover algorithm. Two problems above are solved and the scientists proved that this protocol is secure [6]. The research on the improvement of this kind of protocols is necessary because it need to be optimized in order to make sure that it can be more practical and must be secure when there is eavesdropping.

2. Grover Algorithm

2.1. Process of the Grover Algorithm

The Grover’s quantum search algorithm is designed for the search task in an unsorted database with $2^n$ elements. This is followed by the detailed process.

1) The first step is to use a quantum oracle $O$ operation. An oracle can be considered as a “black box” operation. A target state should be chosen and the target state reverses in this step. But other states do not change.

2) Secondly, the Hadamard transformation is required. In this step, Hadamard gate is operated on every qubit. Hadamard gate could be represented as $\frac{1}{\sqrt{2}} (\vert 0 \rangle + \vert 1 \rangle)$. 

3) In the third step, $\vert 0 \rangle$ remains invariant and other states add -1 phase. This means $\vert 0 \rangle \rightarrow \vert 0 \rangle$, $\vert x \rangle \rightarrow -\vert x \rangle$ if $x$ does not equal 0. This step is equal to $2\vert 0 \rangle < 0 \rangle - I$.

4) The fourth step is repeating the second step.

In conclusion, a single grover iteration equals $G = (2\vert \psi \rangle < \psi \vert - I)O (1)$ where $\psi$ is the superposed state with equal weight.

2.2. Defects and Improvement of the Grover Algorithm

The Grover Algorithm has some drawbacks. For instance, the probability of finding the target can not be 1 and can only approach 1 for the standard Grover algorithm. But there are also some solutions. In 2001, G. L. Long came up with an improved Grover algorithm in which we could find the target state with certainty. In this improved version, the phase inversion is replaced by phase rotation [7].

3. Quantum Secret Sharing

In recent years, many scientists are working on quantum secret sharing and trying to combine the quantum search algorithm and quantum secret sharing. The following section will focus on some types of QSS based on the QSA, especially the advanced quantum secret sharing protocol based on the Grover algorithm. And there will also be some detailed comparison of these different protocols.

3.1. QSA-based Protocols

The first QSS protocol based on the QSA is for one boss and two agents and this is based on the two-qubit Grover algorithm. Firstly, the definition “threshold scheme” needs to be introduced. For a (k, n) threshold theme, there are n shares and it is enough to reconstruct the data by any k shares. In this protocol, a (2, 2) threshold scheme is used [4].

1) The initial states(or the carrier states) $\vert S_i \rangle$ (i = 1, 2, 3,...,16) should be prepared by the boss(Alice). Sixteen initial states are required and they are produced by $\vert + \rangle$, $\vert - \rangle$, $\vert +i \rangle$, $\vert -i \rangle$, where $\vert + \rangle = \frac{1}{\sqrt{2}} (\vert 0 \rangle + \vert 1 \rangle)$ (2), $\vert - \rangle = \frac{1}{\sqrt{2}} (\vert 0 \rangle - \vert 1 \rangle)$ (3), $\vert +i \rangle = \frac{1}{\sqrt{2}} (\vert 0 \rangle + i \vert 1 \rangle)$ (4)and $\vert -i \rangle = \frac{1}{\sqrt{2}} (\vert 0 \rangle - i \vert 1 \rangle)$ (5). Then Alice need to use the unitary operation $U_w$, which is equal to $(1-2\vert w \rangle < w \vert)$. So the code state is $\vert S_i \rangle = U_w \vert S_i \rangle$ (6).

2) Two qubits are sent by Alice to Bob and Eve. Bob and Eve should announce that they receive the qubits.

3) Alice need to confirm that the qubits are received through classical communication.

4) Alice publishes her carrier states $\vert S_i \rangle$.

5) Bob and Eve have to combine their qubits and perform a decoding operation in order to get the key state $\vert w \rangle$. According to the Alice’s announcement, Bob and Eve know the initial state, so they
could determine which operation should use. The decoding operation is \( 2|S_i><S_i| - 1 \) denoted as \( U_{S_i} \). Then the key state could be obtained with reference to the grover algorithm. The key states in this protocol are \(|00>, |01>, |10>, |11>\). The states \(|01>\) and \(|10>\) are the message states, which are used to encode, while the states \(|00>\) and \(|11>\) are used to detect the eavesdropping respectively.

(6) Bob and Eve need to make the measurement on their qubits respectively. Then they have to discuss whether or not their outcomes are perfectly correlated.

(7) If the results of Bob and Eve are perfectly correlated, they will both inform Alice through the classical channel. Then Alice needs to analysis that whether there is an eavesdropper. However, Hsu’s protocol is not secure theoretically. In 2010, Hao et al. proposed a dense-coding attack on Hsu’s protocol and they also gave an improved protocol [5]. The attack and solution will be discussed briefly.

Eve is assumed to be the dishonest agent in this attack here. Besides, the definition “Bell states” (or “EPR pairs”) should be introduced. The Bell states are two qubits with four entangled quantum states. And it is possible to create the Bell states via quantum circuits.

In this attack, Eve needs to block all the qubits from Alice. At the same time, Eve has to prepare an EPR pair in \( \frac{1}{\sqrt{2}}(|01> + |10>) \) and sends one of them to Bob, leaving himself another qubits. Since Bob actually receives the qubit (although it is the incorrect one), both Bob and Eve will make the announcement and Alice would confirm the reception. Then Alice announces the initial states in public. As a result, Eve obtains \(|S_i>\) and can decode through the operation \( U_{S_i} \). Eve could get the key states. Besides, Eve needs to transform the prepared qubit (the one of the EPR pair) into \(|S_i>\) by operations. In the following steps, all the results are correct and both Alice and Bob will not discover the eavesdropping.

Hao et al. also gave the solution of this attack. The check mode is changed. Instead of announcing the decoding operation, Alice asks Bob and Eve to measure their qubit in random basis which might be the plus-basis or the cross basis, or the circular basis. And both Bob and Eve should publish their measuring results. Alice will analysis whether their results conform to her code state and if the results accord with Alice’s states, then Alice could make sure that there is no cheating and the communication is secure.

### 3.2. An Enhanced QSS Protocol based on the Grover Algorithm

Although the protocol by Hao et al. improves the security, this version also has some problems during the procedure. For example, agents need to store the qubits from the boss, which is not convenient or even impossible. So Tseng et al. proposed an improved protocol (still based on the Grover algorithm) which could make the process more realistic [6].

In this enhanced version, Bob and Eve do not need to store photons. Instead, they need to prepare a random N-bits string, respectively. The two random strings are denoted as \( K_B \) and \( K_E \). And they have to prepare a sequence of photons respectively, represented as \( S_B \) and \( S_E \). The “0” in the string corresponds to \(|+>\) and the “1” corresponds to \(|->\). Apart from that, Bob and Eve need to prepare abundant decoy photons. The decoy photons should be randomly chosen from one of the four states which are \(|+>, |->, |0>, \) and \(|1>\). These prepared decoy photons are inserted into the sequence of photons, \( S_B \) and \( S_E \) in order to obtain a new sequence, denoted as \( S_B' \) and \( S_E' \). Then these two new sequences are sent to Alice.

Secondly, Alice is confirmed to receive the sequences. After that, there should be a security check. Bob and Eve need to publish the positions, bases and values of the decoy photons and Alice makes the measurement according to the agents’ announcement. If the error rate outstrips a threshold value, this means there exists an eavesdropper. Alice will stop the transmission and restart the communication. If the error rate is tolerable, the communication could continue.

In the third step, photons of \( S_B \) and \( S_C \) on the same position in the sequence could be combined by Alice to obtain two-qubit initial states, represented as \(|S>\). Alice has the secret, so she knows the \(|w>\). Alice is able to perform the correct operation \( U_w \) on the initial state. The secret “0” corresponds to the unitary operation \( U_{00} = I - 2|00><00| \) (7)or \( U_{11} = I - 2|11><11| \) (8). Otherwise, the corresponding
operation is \( U_{0|1} = I - 2|01><01| (9) \) or \( U_{1|0} = I - 2|10><10| (10) \). After that, operation \( U_S \), which equals \( 2|++><++|-I \), need to be performed. And then Alice measures in the Z basis and obtains the results. Measurement \(|00>\) or \(|11>\) leads to the result “0”, and otherwise, the measurement would lead to measurement “1”. After these procedures, Alice gets a N-bit string, denoted as \( MR_A \) and sends to Bob and Eve. Then Bob and Eve could decode the secret by computing \( K_B \oplus K_C \oplus MR_A \).

4. Security of the improved QSS protocol

Tseng et al. also proposed some attacks that might exist. The attacks could come from both the agents and eavesdroppers who do not take part in the activity. However, the agents could gain more information and they could cheat in the public discussion. So it is essential to focus on the insiders’ cheating. We could make sure that the protocol is secure if the attacks from the agents could be avoided [6]. In this section, the existing attacks by agents and solutions will be discussed and Eve will be assumed as the eavesdropper.

4.1. Existing Attacks and the solutions of the improved QSS

One of the existing attacks is the Intercept-and-Resend Attack [8]. Eve intercepts \( S_B' \) and resends the false photons to Alice. But it is extremely possible to be detected during the check procedure since Eve does not know the positions, bases and values of the decoy photons and there may be some errors. If there are copious errors, the eavesdropping will be discovered and the communication will stop.

The Entangle-and-Measure attack is another kind of existing attacks on this protocol [9], but it also have faults. In this attack, auxiliary photons are necessary. Eve should prepare some auxiliary photons, represented by \( E = \{ |E_1>, |E_2>, ... , |E_n> \} \). And Eve also needs to perform a unitary operation on the decoy photons in order to make the auxiliary photons be entangled with \( S_C' \). The consequence of the operation is below [6].

\[
U|0>|E_n> = a|0>|e_{00}> + b|1>|e_{01}> \quad (11),
\]

\[
U|1>|E_n> = c|0>|e_{10}> + d|1>|e_{11}> \quad (12),
\]

\[
U|+>|E_n> = \frac{1}{\sqrt{2}}(|+> + |->) (a|e_{00}> + b|e_{01}> + c|e_{10}> + d|e_{11}> ) + \frac{1}{\sqrt{2}}(|> - |->) (a|e_{00}> - b|e_{01}> + c|e_{10}> - d|e_{11}> ) \quad (13),
\]

\[
U|->|E_n> = \frac{1}{\sqrt{2}}(|+> + |->) (a|e_{00}> + b|e_{01}> - c|e_{10}> - d|e_{11}> ) + \frac{1}{\sqrt{2}}(|> - |->) (a|e_{00}> - b|e_{01}> - c|e_{10}> + d|e_{11}> ) \quad (14),
\]

where \( |a|^2 + |b|^2 + |c|^2 + |d|^2 = 1 \).

In order to eavesdrop without the detection, there are some conditions which are needed:

1. \( b \) should equal 0 ;
2. \( c \) should equal 0 ;
3. \( a|e_{00}> - b|e_{01}> + c|e_{10}> - d|e_{11}> = 0 \) (15);
4. \( a|e_{00}> + b|e_{01}> - c|e_{10}> - d|e_{11}> = 0 \) (16).

While if the first two conditions are satisfied, \( a|e_{00}> \) will be equal to \( d|e_{11}> \) according to the third condition. And then these two states can not be distinguished [6].

5. Conclusion

This paper concludes some quantum secret sharing protocols based on the Grover algorithm and how this kind of protocol is improved. Hsu starts the quantum secret sharing based on the quantum searching algorithm and this protocol was improved by Hao et al. Then the protocol proposed by Tseng et al. is not only secure from the existing attacks, but it also have some other advantages during the communication: the agents do not need to store photons and the secret of the boss is easy to decode for the agents. The QSS protocols based on QSA are vital for the quantum computation and can avoid some practical problems during the communication. This kind of protocols is useful and suitable for many situations. However, maybe there will be some attacks for this protocol, which should be discovered in the future.
Acknowledgments
The author would like to thank Dr. Ming-Deh A. Huang and my thesis advisor for the help.

References
[1] Hillery, M., Buek, V., Berthiaume, A., Quantum secret sharing [J] Phys. Rev. A, vol.59, no.3, 1829, 1999.
[2] Lov K. Grover, A fast quantum mechanical algorithm for database search [C] Proc. of the 28th annual ACM Symp on Theory of Computing. New York, USA: ACM Press, July 1996, pp.212-219.
[3] G. L. Long, Grover algorithm with zero theoretical failure rate [J] Phys. Rev. A, vol.64, 022307, 2001.
[4] Li-Yi Hsu, Quantum secret-sharing protocol based on Grover's algorithm [J] Phys. Rev. A, vol.68, 022306, 2003.
[5] Hao Liang, Li Junlin and Long Guilu, Eavesdropping in a quantum secret sharing protocol based on Grover algorithm and its solution [J] Science China Physics, Mechanics and Astronomy, vol.53, 2010, pp.491-495.
[6] Hsin-Yi Tseng, Chia-Wei Tsai, Tzonelih Hwang and Chuan-Ming Li, Quantum Secret Sharing Based on Quantum Search Algorithm [J] International Journal of Theoretical Physics, vol.51, 2012.
[7] Long Guilu, Li Yansong, Xiao Li, Tu Changcun and Sun Yang, Phase matching in quantum searching and the improved Grover algorithm [J] Nuclear Physics Review, vol.21, 2004, pp.114-116.
[8] Chun-Wei Yang, Chia-Wei Tsai and Tzonelih Hwang, Thwarting intercept-and-resend attack on Zhang’s quantum secret sharing using collective rotation noises [J] Quantum Information Processing, vol.11, 2012, pp.113-122.
[9] Chia-Wei Tsai, Shih-Hsueh Wang and Tzonelih Hwang, Comment on “N quantum channel are sufficient for multi-user quantum key distribution protocol between n users” [J] Optics Communications, vol.283, no.24, 2010, pp.5285-5286.