Multiparty Quantum Key Agreement Based on Quantum Search Algorithm

Hao Cao, Wenping Ma

Quantum key agreement is an important topic that the shared key must be negotiated equally by all participants, and any nontrivial subset of participants cannot fully determine the shared key. To date, the embed modes of subkey in all the previously proposed quantum key agreement protocols are based on either BB84 or entangled states. The research of the quantum key agreement protocol based on quantum search algorithms is still blank. In this paper, on the basis of investigating the properties of quantum search algorithms, we propose the first quantum key agreement protocol whose embed mode of subkey is based on a quantum search algorithm known as Grover's algorithm. A novel example of protocols with 5 – party is presented. The efficiency analysis shows that our protocol is prior to existing MQKA protocols. Furthermore it is secure against both external attack and internal attacks.

Since the first quantum key distribution (QKD) protocol known as BB84 was proposed by Bennett and Brassard in 1984, quantum cryptography has been attracted more and more attention, and many kinds of schemes such as QKD, quantum secret sharing (QSS), quantum direct communication (QDC), quantum privacy comparison (QPC), have been proposed. Especially, QKD has received wide attention because of its numerous applications in quantum communication. Different from the classic cryptography schemes, quantum protocols that are based on the principles of quantum mechanics, could provide unconditionally security. Hence, quantum cryptography is innately superior to the classic cryptography.

Another very important topic named Quantum key agreement (QKA) also received widespread concerns. Compared with QKD protocols in which one participant distributes a predetermined secret key to the other participants, QKA protocols require that all participants need to negotiate mutually and equally to derive a common secret key, and any unauthorized users cannot extract the key through illegal means. Hence, the justice and fairness can be better reflected in the procession of QKA protocols because all participants are involved in the selection of the target key K and their contribution to it are equal. In 2004, the firstly QKA protocol (ZZX protocol) based on Einstein - Podolsky - Rosen (EPR) pairs was proposed by Zhou, Zeng and Xiong. However, in 2009, Tsai and Hwang pointed out that ZZX protocol is not a fair QKA because one party could fully determine the target key without being detected, and they proposed an improvement one (TH protocol). Unfortunately, TH protocol is also not a really QKA because the shared key is produced based on random measurement results without negotiation. In 2004, based on maximally entangled states, Hsueh and Chen also proposed a QKA protocol (HC protocol). In 2011, Chong, Tsai and Hwang claimed that HC protocol is susceptible to eavesdropping attack and internal attacks. In 2010, Chong and Hwang proposed the first successful QKA protocol (CH protocol) based on BB84 by using the technique of delayed measurement. In 2013, Liu, Gao, Huang and Wen proposed the first secure multiparty quantum key agreement (MQKA) protocol (LGHW protocol) by utilizing single particles. In the same year, Sun, Zhang and Wang et al improved the LGHW protocol and the efficiency is improved obviously. Subsequently, several QKA and MQKA protocols were proposed.

Furthermore, quantum search algorithms (QSA) are also a research focus in quantum theory, and are famous for the Grover’s algorithm. The target could be probabilistic found in an unsorted database by executing the Grover’s algorithm which is faster than the best known classical search algorithms. Grover’s algorithm plays an important role in quantum computation and quantum communication. Recently, based on the ideas of QSA, some quantum protocols, liking QSS, QPC and QDC, have been proposed.

1Xidian University, State Key Laboratory of Integrated Service Networks, Xi’an, 710071, China. 2University of Science and Technology of Anhui, School of Information and Network Engineering, Chuzhou, 233001, China. Correspondence and requests for materials should be addressed to H.C. (email: caohao2000854@163.com)
As far as I know, all existing QKA protocols are based on either BB84 or entangled states, and the QKA protocol based on QSA has not yet appeared. The research of the QKA protocol based on QSA still is blank. This study proposes a MQKA protocol based on QSA for the first time. In the proposed scheme, the idea of quantum dense coding is used. Each participant encodes his or her secret key by a unitary operation, and makes a two-particle quantum measurement to extract the common key. The security and efficiency analysis shows that our protocol is prior to existing MQKA protocols. The rest of our paper is structured as follows. Section 2 introduces some notions and properties of QSA. Section 3 describes the presented protocol in detail, the correctness of it is showed, and a novel example with 5-party protocol is presented. Section 4 analyzes the proposed scheme and compares it to other schemes. Finally, the conclusion of this paper is given in section 5.

**Results**

**Preliminaries.** Here we tackle some notations and properties of the Quantum Search Algorithm (QSA) with two quantum particles input. Owing to that Grover’s QSA is one of the most famous of all the QSAs, we only discuss the notations and properties of it.

The Grover’s QSA can be described as follows. Let the database be a two-particle quantum state $|S\rangle = |++\rangle$, and $w \in \{00, 01, 10, 11\}$ be the search target. One can perform two specific unitary operations on $|S\rangle = |++\rangle$ repeatedly to find the target. Here, we firstly give some notations adopted in this article.

Let $w \in \{00, 01, 10, 11\}$, define $|S_w\rangle$ as follows:

$$|S_w\rangle = \begin{cases} |++\rangle, & w = 00, \\ |--\rangle, & w = 01, \\ |+-\rangle, & w = 10, \\ |--\rangle, & w = 11. \end{cases}$$

(1)

Two specific unitary operations can be described as follows.

$$U_w = I - 2|w\rangle\langle w|$$

(2)

$$U_S = 2|S\rangle\langle S| - I$$

(3)

where $w \in \{00, 01, 10, 11\}$ and $S \in \{++, --, +-, -+\}$.

Grover’s QSA possesses two special properties as follows.

**Property 1.** Ref. 32 Let $w_1 \in \{00, 01, 10, 11\}$ ($i = 1, 2, 3, 4$). Then $U_{w_3} U_{w_2} U_{w_1} |S_{00}\rangle = \pm U_{w_1} |S_{00}\rangle$ if and only if $w_3 \oplus w_2 \oplus w_1 = w_4$. 

**Property 2.** Ref. 14 Let $v, w_2, w_3 \in \{00, 01, 10, 11\}$. Then $U_v U_{w_3} |S_w\rangle = \pm w_2$, if only if $w_1 \oplus v = w_2$.

The following Theorem 1 and Theorem 2 generalize the Property 1 and property 2 from $|S_{00}\rangle$ to $|S_w\rangle$ with any $w \in \{00, 01, 10, 11\}$ separately.

**Theorem 1.** Let $w, w_1 \in \{00, 01, 10, 11\}$ ($i = 1, 2, 3, 4$), then $U_{w_3} U_{w_2} U_{w_1} |S_w\rangle = \mp U_{w_3} |S_w\rangle$ if and only if $w_3 \oplus w_2 \oplus w_1 = w_4$. More generally, let $n$ be an odd positive integer, and $w, v, w_i \in \{00, 01, 10, 11\}$ ($i = 1, 2, \ldots, n$), then $U_{w_3} U_{w_2} \cdots U_{w_1} |S_w\rangle = \pm U_{w_1} |S_w\rangle$ if and only if $w_n \oplus w_{n-1} \oplus \cdots \oplus w_1 = v$.

**Proof.** (1) Firstly, we show that $U_{w_3} U_{w_2} U_{w_1} |S_w\rangle = \pm U_{w_3} |S_w\rangle$ if and only if $w_3 \oplus w_2 \oplus w_1 = w_4$.

(a) If $w_3 \oplus w_2 \oplus w_1 = w_4$ and $w_3 = w_4$, then $w_5 = w_6$, and it is obviously that $U_{w_3} U_{w_2} U_{w_1} |S_w\rangle = \pm U_{w_1} |S_w\rangle$. Similarly to the cases $w_3 = w_5$ and $w_1 = w_2$.

(b) If $w_3 \oplus w_2 \oplus w_1 = w_4$ and $w_3$, $w_2$ and $w_1$ are different from each other, then $|w_3\rangle, |w_2\rangle, |w_1\rangle$ and $|w_4\rangle$ are orthogonal to each other because of the relation $w_3 \oplus w_2 \oplus w_1 = w_4$. In this case, we can get

$$|S_w\rangle = \langle w_3, S_w\rangle |w_3\rangle + \langle w_2, S_w\rangle |w_2\rangle + \langle w_1, S_w\rangle |w_1\rangle + \langle w_4, S_w\rangle |w_4\rangle$$

Hence,

$$U_{w_3} U_{w_2} U_{w_1} |S_w\rangle = \langle w_3, S_w\rangle |(I - 2|w_3\rangle\langle w_3|)(I - 2|w_2\rangle\langle w_2|)(I - 2|w_1\rangle\langle w_1|)S_w\rangle = \pm |S_w\rangle - 2\langle w_3, S_w\rangle |w_3\rangle - 2\langle w_2, S_w\rangle |w_2\rangle - 2\langle w_1, S_w\rangle |w_1\rangle = -(|S_w\rangle - 2\langle w_4, S_w\rangle |w_4\rangle) = - U_{w_3} |S_w\rangle$$

(4)

(c) If $w_3 \oplus w_2 \oplus w_1 = w_4$, let us show that $U_{w_3} U_{w_2} U_{w_1} |S_w\rangle = \pm U_{w_3} |S_w\rangle$.

Denote $w_3 \oplus w_2 \oplus w_1 = w_6$. From (a) and (b), we can easily get $U_{w_3} U_{w_2} U_{w_1} |S_w\rangle = \pm U_{w_3} |S_w\rangle$. Suppose the equation $U_{w_3} U_{w_2} U_{w_1} |S_w\rangle = \pm U_{w_3} |S_w\rangle$ holds, then $U_{w_6} |S_w\rangle = U_{w_3} |S_w\rangle$ or $U_{w_3} |S_w\rangle = - U_{w_3} |S_w\rangle$.

In the former case, we have
\[ U_{w_1}S_{w_1} = U_{w_1}|S_w \]
\[ \Rightarrow |S_w| - 2\{w_0, S_w\}|w_0\} = |S_w| - 2\{w_4, S_w\}|w_4\}
\[ \Rightarrow \{w_0, S_w\}|w_0\} - \{w_4, S_w\}|w_4\} = 0 \]
\[ \Rightarrow \{w_0, S_w\} = \{w_4, S_w\} = 0 \]

a contradiction to the fact that \( \{v, S_w\} = \pm \frac{1}{2} \) for any \( v \in \{00, 01, 10, 11\} \). The same conclusion of the second case can be got similarly. Hence, \( U_{w_1}U_{w_2}U_{w_3}|S_w\} = \pm U_{w_1}|S_w\} \).

From (a), (b) and (c), we can get \( U_{w_1}U_{w_2}U_{w_3} = \pm U_{w_1} \) if and only if \( w_3 \oplus w_2 \oplus w_1 = w_0 \).

(2) Secondly, we show that \( U_{w_1}U_{w_2} \cdots U_{w_n}|S_w\} = \pm U_{w_1}|S_w\} \) if and only if \( w_1 \oplus w_{n-1} \oplus \cdots \oplus w_1 = v \). We will give the proof by using the mathematical induction to the odd positive integer \( \eta \).

(a) \( \eta = 1 \), the result is trivial.

(b) Suppose that the result is correct in the case of \( \eta = k \), where \( k \) is a positive odd integer. That is to say, \( U_{w_1}U_{w_2} \cdots U_{w_n}|S_w\} = \pm U_{w_1}|S_w\} \) if and only if \( w_1 \oplus w_{n-1} \oplus \cdots \oplus w_1 = v \), where \( v = w_1 \oplus w_{n-1} \oplus \cdots \oplus w_1 \). When \( \eta = k + 2 \), we have

\[ U_{w_1}U_{w_2} \cdots U_{w_n}U_{w_1}|S_w\} = \pm U_{w_1}|S_w\} \] if and only if \( w_1 \oplus w_{n-1} \oplus \cdots \oplus w_1 = v \).

**Theorem 2.** Let \( w, v, w_o, w_l \in \{00, 01, 10, 11\} \). Then \( U_{w_1}U_{w_2}U_{w_3}|S_w\} = \pm w_o \) if and only if \( v \oplus w_l \oplus w_o = w_o \).

The correctness of **Theorem 2** could be verified for each value of the tuples \( (w, v, w_o, w_l) \in \{00, 01, 10, 11\}^4 \) one by one.

From **Theorem 1** and **Theorem 2**, we can get **Theorem 3** at once.

**Theorem 3.** Let \( \eta \) be an odd positive integer, and \( w, v, w_l \in \{00, 01, 10, 11\} \), where \( i = 0, 1, \ldots, \eta \). Then \( U_{w_1}U_{w_2} \cdots U_{w_n}|S_w\} = \pm w_o \) if and only if \( v \oplus w_0 \oplus w_{n-1} \oplus \cdots \oplus w_1 = w_o \).

**Theorem 4.** Let \( w, w_0, w_1, w_2 \in \{00, 01, 10, 11\} \). Then \( U_{w_1}U_{w_2}U_{w_3}|S_w\} = \pm S_{w_2} \) if and only if \( w \oplus w_2 \oplus w_1 = w_0 \).

More generally, let \( \eta \) be a positive even integer, and \( w, w_1 \in \{00, 01, 10, 11\} \) \((i = 0, 1, \ldots, \eta)\), then \( U_{w_1}U_{w_2} \cdots U_{w_n}|S_w\} = \pm S_{w_2} \) if and only if \( w \oplus w_2 \oplus w_{n-1} \oplus \cdots \oplus w_1 = w_0 \).

**Proof.** (1) Firstly, we show that \( U_{w_1}U_{w_2}U_{w_3}|S_w\} = \pm S_{w_2} \) if and only if \( w \oplus w_2 \oplus w_1 = w_0 \).

(a) If \( w_1 = w_o \), the result is trivial.

(b) If \( w_i = w_o \), suppose \( \{w_1, w_2, w_3, w_4\} = \{00, 01, 10, 11\} \), then \( |w_1|, |w_2|, |w_3| \) and \( |w_4| \) are orthogonal to each other. In this case, we can get

\[ |S_w| = \{w_p, S_w\}|w_1\} + \{w_2, S_w\}|w_2\} + \{w_3, S_w\}|w_3\} + \{w_4, S_w\}|w_4\} \]

Now, we show that there exists \( w_0 \in \{00, 01, 10, 11\} \) such that \( U_{w_1}U_{w_2}U_{w_3}|S_w\} = \pm S_{w_2} \).

\[ U_{w_1}U_{w_2}U_{w_3}|S_w\} = 2|S_w| - 2\{w_0, S_w\}|w_0\} = 2\{w_2, S_w\}|w_2\} = 2\{w_3, S_w\}|w_3\} = 2\{w_4, S_w\}|w_4\} \]

Hence, we can select a proper \( w_o \in \{00, 01, 10, 11\} \) such that \( U_{w_1}U_{w_2}U_{w_3}|S_w\} = \pm S_{w_2} \) and we can easily get the relation \( w \oplus w_2 \oplus w_1 = w_o \) from Table 1.

(2) From (1) and **Theorem 1**, we can easily get the correction of the proposition that \( U_{w_1}U_{w_2} \cdots U_{w_n}|S_w\} = \pm S_{w_2} \) if and only if \( w \oplus w_2 \oplus w_{n-1} \oplus \cdots \oplus w_1 = w_0 \) by using the mathematical induction similar to the proof of (2) in **Theorem 1**.
The Proposed QKA Protocol. Suppose that there are $N$ ($N \geq 2$) participants $P_0$, $P_1$, $P_2$, ..., and $P_{N-1}$, and each of them generate a random sequence with length $2n$ as his or her secret key firstly.

\[
K_0 = (k_{0,0}, k_{0,2}, ..., k_{0,2n})
\]
\[
K_1 = (k_{1,0}, k_{1,2}, ..., k_{1,2n})
\]
\[
K_2 = ...
\]
\[
K_{N-1} = (k_{N-1,0}, k_{N-1,2}, ..., k_{N-1,2n})
\]

where the element $k_{i,j} \in \{0, 1\}$ ($i = 0, 1, ..., N - 1; j = 1, 2, ..., 2n$). Next, $P_0$, $P_1$, $P_2$, ..., and $P_{N-1}$ want to negotiate a common key $K_0 \oplus K_1 \oplus K_2 \oplus \cdots \oplus K_{N-1}$, where $\oplus$ denotes the bitwise Exclusive OR. Now, The detailed description of the proposed MQKA protocol can be seen in Fig. 1 and the following explanation.

The Detailed Description of MQKA. Step 1 Initialization Phase. Each participant $P_i$ selects two random sequences $S_i$ and $V_i$ with length $2n$, and prepares a two-particle quantum state sequence $S_{i+1}$ according to the random sequence $S_i$.

\[
S_i = (s_{i,0}, s_{i,2}, ..., s_{i,2n}) \Rightarrow S_{i+1} = (s_{i+1,0}, s_{i+1,2}, ..., s_{i+1,2n})
\]

\[
V_i = (v_{i,0}, v_{i,2}, ..., v_{i,2n})
\]
Next, $P_i$ performs unitary operations $U_{v_{i,1}v_{i,2}}(t = 1, 2, \ldots, n)$ on every state $|S_{i,t-1}^{v_{i,1}v_{i,2}}\rangle$ and the resulted sequence be denoted as $S_{i,t}$. He also generates $kn$ ($k$ is the detection rate) decoy particles from $|0\rangle, |1\rangle$ or $|+, \rangle$, $|-\rangle$), and gets a new sequence $S_{i,t+1}$ by inserting them into the sequence $S_{i,t}$. Meanwhile, $P_i$ records the initial states and corresponding positions of every checking particles, and then sends the sequence $S_{i,t+1}$ to the next participant $P_{i+1}$, where $+$ denotes modulo $N$ addition.

In addition, it is important to note that the decoy particles could be inserted into $S_{i,t+1}$ randomly. For example, suppose $S_{i,t+1} = |(ab), (cd), (ef), (gh)\rangle$ and the decoy sequence is $\{0\}, \{+\}, \{0\}, \{0\}$ for $S_{i,t}$ with position $1, 3, 4, 6, 8, 10, 11, 15$, then $S_{i,t+1} = |(00), (0), (0), (0), (1), (1), (1), (1)\rangle$ can be seen in equation (2). $P_{i+1}$ will get a new sequence $S_{i,t+1}$ by inserting the decoy particles into $S_{i,t+1}$ similar to Step 1, and send it to $P_{i+2}$.

Step 2 Eavesdropping Checking Phase. After confirming that all $P_{i,t}$ have received the sequence $S_{i,t}^{v_{i,1}v_{i,2}}$, $P_i$ and $P_{i+1}$ can calculate the error probability by comparing the measurement results with the initial states of decoy particles. If the error ratio exceeds the predetermined threshold value, $P_i$ declares that the communication is invalid. Otherwise, the process continues to Step 3.

Step 3 Encoding Phase. By deleting the decoy states from $S_{i,t}$, $P_{i+1}$ can get the sequence $S_{i,t+1}$. Then according to the private key $K_{i,t+1}$, $P_{i+1}$ performs unitary operations $U_{k_{i,t+1}k_{i,t+2}}(t = 1, 2, \ldots, n)$ on every two-particle state in $S_{i,t+1}$, and denotes the resulted sequence as $S_{i,t+2}$. Here the definition of $U_{k_{i,t+1}k_{i,t+2}}$ can be seen in equation (2). $P_{i+1}$ will get a new sequence $S_{i,t+1}$ by inserting the decoy particles into $S_{i,t+1}$ similar to Step 1, and send it to $P_{i+2}$.

Step 4 Encoding Recursively Phase. After confirming that $P_{i+2}$ has received the sequence $S_{i,t+2}$, $P_{i+1}$ and $P_{i+2}$ execute eavesdropping checking mentioned in Step 2. If the error ratio exceeds the predetermined threshold value, $P_i$ declares that the communication is invalid. Otherwise, the process continues. $P_{i+1}$ execute Encoding Phase similar to $P_{i+1}$ in Step 3.

$P_{i+1}, \ldots, P_{i-1}$ execute eavesdropping checking mentioned in Step 2 and Encoding Phase similar to $P_{i+1}$ in Step 3.

Step 5 Extracting Common Key Phase. When $P_i$ has received the sequence $S_{i,t}$ from $P_{i-1}$, he firstly does eavesdropping checking with $P_{i-1}$. Then he will obtain the sequence $S_{i,t}$ by deleting the decoy particles from $S_{i,t}$. Next, $P_i$ performs unitary operation $U_{k_{i-1}k_{i-2}}$ on the corresponding two-particle state in the sequence $S_{i,t}$ according the sequence $S_{i,t+1} = (|S_{i,t+1}^{v_{i,1}v_{i,2}}\rangle, |S_{i,t+2}^{v_{i,1}v_{i,2}}\rangle, \ldots, |S_{i,t+n}^{v_{i,1}v_{i,2}}\rangle)$, and takes measurements on every resulted two-particle state with basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ if $N$ is odd, or $|+, \rangle, |-, +\rangle, |+, -\rangle, |-, +\rangle$ if $N$ is even.

(i) If $N$ is odd, denote the sequence of measured result as $S_{W_i} = (|w_{i,1}^{v_{i,1}v_{i,2}}\rangle, |w_{i,3}^{v_{i,1}v_{i,2}}\rangle, \ldots, |w_{i,2n-1}^{v_{i,1}v_{i,2}}\rangle)$. Then $P_i$ computes

$$[K_i] = [W_i] \oplus [V_i] \oplus K_i$$

(ii) If $N$ is even, denote the sequence of measured result as $S_{W_i} = (|S_{W_i}^{v_{i,1}v_{i,2}}\rangle, |S_{W_i}^{v_{i,1}v_{i,2}}\rangle, \ldots, |S_{W_i}^{v_{i,1}v_{i,2}}\rangle)$. Then $P_i$ computes

$$[K_i] = [W_i] \oplus [V_i] \oplus [K_i] \oplus S_i$$

where $W_i = (|w_{i,1}^{v_{i,1}v_{i,2}}\rangle, |w_{i,3}^{v_{i,1}v_{i,2}}\rangle, \ldots, |w_{i,2n-1}^{v_{i,1}v_{i,2}}\rangle, \ldots, |w_{i,2n-2}^{v_{i,1}v_{i,2}}\rangle)$.

The $2n - bit$ sequence $[K_i]$ is the target common key $[K]$ of the $N$ participants.

**Correctness of The Proposed Protocol.** Now, we show that $K = [K_0] = [K_1] = \cdots = [K_{N-1}]$.

In fact, the sequence $W_i$ defined in step 5 can be got by using Theorem 3 or Theorem 4 separately. Namely, after performed unitary operations $U_{S_{i,t}^{k_{i-1}k_{i-2}}} \cdots U_{S_{i,t+n}^{k_{i-1}k_{i-2}}} U_{S_{i,t+n}^{k_{i-1}k_{i-2}}} \cdots U_{S_{i,t}^{k_{i-1}k_{i-2}}} |S_{i,t}^{v_{i,1}v_{i,2}}\rangle$, i.e., $P_n, P_{n-1}, \ldots, P_{i+1}$ perform unitary operations defined by equation (2) on the two-particle state $|S_{i,t}^{v_{i,1}v_{i,2}}\rangle$ separately, and $P_i$ performs the operation defined by equation (3) at last.

(i) If $N$ is odd, then we can get the conclusion that the $t-\text{th}$ two-particle state mentioned in (4) will be in $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, and the state of (4) equals $|w_{i,1}^{v_{i,1}v_{i,2}}\rangle$ by using Theorem 3. Furthermore, we can also get

$$w_{i,2t-1}^{v_{i,1}v_{i,2}} = v_{i,2t-1}^{v_{i,1}v_{i,2}} \oplus k_{i,1}^{v_{i,1}v_{i,2}} \oplus k_{i,2}^{v_{i,1}v_{i,2}} \oplus k_{i,3}^{v_{i,1}v_{i,2}} \oplus \cdots \oplus k_{i,2t-2}^{v_{i,1}v_{i,2}}$$
Then, \[ W_I = V_I \oplus K_{i+1} \oplus K_{i+2} \oplus \cdots \oplus K_{i-1} = V_I \oplus K_8 \oplus K_4 \oplus \cdots \oplus K_{i-1} \oplus K_{i+1} \oplus \cdots \oplus K_{N-1} \]

Hence, \[ [K_i] = W_I \oplus V_I \oplus K_i = K_0 \oplus K_1 \oplus K_2 \oplus \cdots \oplus K_{N-1} \]

(ii) If \( N \) is even, then we can get the conclusion that the \( t - th \) two-particle state mentioned in (4) will be in \([|+\rangle, |+\rangle, |+\rangle, |+\rangle\]

and the state of (4) equals \( |Sw_{i,2t-1}w_{i,2t}\rangle \) by using Theorem 4. Furthermore, we can also get

\[ w_{i,2t-1}w_{i,2t} = v_{i,2t-1}v_{i,2t} \oplus k_{i,1+1,2t-1}k_{i,1+1,2t} \oplus k_{i,1+2,2t-1}k_{i,1+2,2t} \oplus \cdots \oplus k_{i,1-1,2t-1}k_{i,1-1,2t} \oplus s_{i,2t-1} s_{i,2t} \]

Then, \[ W_I = V_I \oplus K_{i+1} \oplus K_{i+2} \oplus \cdots \oplus K_{i-1} \oplus S_I \]

\[ = V_I \oplus S_I \oplus K_0 \oplus K_1 \oplus \cdots \oplus K_{i-1} \oplus K_{i+1} \oplus \cdots \oplus K_{N-1} \]

Hence, \[ [K_i] = W_I \oplus V_I \oplus K_i \oplus S_I = K_0 \oplus K_1 \oplus K_2 \oplus \cdots \oplus K_{N-1} \]

From (i) (ii), we can know that all participants obtain the target common key sequence successfully, i.e.

\[ [K] = [K_3] = \cdots = [K_{N-1}] = K_0 \oplus K_1 \oplus K_2 \oplus \cdots \oplus K_{N-1} \]

An Example of The Proposed Protocol with \( N = 5 \). In the following, we will give an example of five-party quantum key agreement protocol without considering eavesdropping checking. Suppose \( P_0, P_1, P_2, P_3, \) and \( P_4 \) want to negotiate a common sequence with length 6 as the target key. Firstly, they select their private key separately as follows.

\[
\begin{align*}
K_0 &= (k_{0,1}, k_{0,2}, \ldots, k_{0,6}) = (100101) \\
K_1 &= (k_{1,1}, k_{1,2}, \ldots, k_{1,6}) = (010110) \\
K_2 &= (k_{2,1}, k_{2,2}, \ldots, k_{2,6}) = (010111) \\
K_3 &= (k_{3,1}, k_{3,2}, \ldots, k_{3,6}) = (011111) \\
K_4 &= (k_{4,1}, k_{4,2}, \ldots, k_{4,6}) = (011101)
\end{align*}
\]

Next, they run the protocol.

Step 1 Initialization Phase. \( P_i \) selects two random sequences \( V_i \) and \( S_i \) with length \( 2n \), and prepares a two-particle quantum state sequence \( S_{i+1} \) according to the random sequence \( S_r \).

\[
\begin{align*}
S_0 &= (s_{0,1}, s_{0,2}, \ldots, s_{0,6}) = (100100) \Rightarrow \\
S_{0,1} &= (|s_{0,1}, s_{0,2}\rangle, |s_{0,1}, s_{0,2}\rangle, |s_{0,1}, s_{0,2}\rangle) = (|+\rangle, |+\rangle, |+\rangle) \\
S_1 &= (s_{1,1}, s_{1,2}, \ldots, s_{1,6}) = (011011) \Rightarrow \\
S_{1,2} &= (|s_{1,1}, s_{1,2}\rangle, |s_{1,1}, s_{1,2}\rangle, |s_{1,1}, s_{1,2}\rangle) = (|+\rangle, |+\rangle, |+\rangle) \\
S_2 &= (s_{2,1}, s_{2,2}, \ldots, s_{2,6}) = (110000) \Rightarrow \\
S_{2,3} &= (|s_{2,1}, s_{2,2}\rangle, |s_{2,1}, s_{2,2}\rangle, |s_{2,1}, s_{2,2}\rangle) = (|+\rangle, |+\rangle, |+\rangle) \\
S_3 &= (s_{3,1}, s_{3,2}, \ldots, s_{3,6}) = (010111) \Rightarrow \\
S_{3,4} &= (|s_{3,1}, s_{3,2}\rangle, |s_{3,1}, s_{3,2}\rangle, |s_{3,1}, s_{3,2}\rangle) = (|+\rangle, |+\rangle, |+\rangle) \\
S_4 &= (s_{4,1}, s_{4,2}, \ldots, s_{4,6}) = (110111) \Rightarrow \\
S_{4,0} &= (|s_{4,1}, s_{4,2}\rangle, |s_{4,1}, s_{4,2}\rangle, |s_{4,1}, s_{4,2}\rangle) = (|+\rangle, |+\rangle, |+\rangle)
\end{align*}
\]

\[
\begin{align*}
V_0 &= (v_{0,1}, v_{0,2}, \ldots, v_{0,6}) = (010110) \\
V_1 &= (v_{1,1}, v_{1,2}, \ldots, v_{1,6}) = (111000) \\
V_2 &= (v_{2,1}, v_{2,2}, \ldots, v_{2,6}) = (001101) \\
V_3 &= (v_{3,1}, v_{3,2}, \ldots, v_{3,6}) = (001001) \\
V_4 &= (v_{4,1}, v_{4,2}, \ldots, v_{4,6}) = (111011)
\end{align*}
\]
Next, $P_o$ performs unitary operations $U_{t=1,2,3}$ on every state $|S_{t=1,2,3}\rangle$ ($t = 1, 2, 3$), and the resulted sequence be denoted as $S_{0-3}, P_0, P_1, P_2, P_3$ and $P_t$ perform the same operations similarly. $P_0$ (or $P_1$ or $P_2$ or $P_3$) sends $S_{0-1}$ (or $S_{1-2}$ or $S_{2-3}$ or $S_{3-4}$ or $S_{4-0}$) to $P_1$ (or $P_2$ or $P_3$ or $P_4$ or $P_0$).

Step 2 Encoding Phase and Encoding Recursively Phase. $P_1$ (or $P_2$ or $P_3$ or $P_4$ or $P_0$) encodes $S_{0-1}$ (or $S_{1-2}$ or $S_{2-3}$ or $S_{3-4}$ or $S_{4-0}$) by using a unitary operation according to his private key.

$$S_{0-1} = (U_{01} |0\rangle, U_{01} |1\rangle, U_{01} |0\rangle, U_{01} |1\rangle) \Rightarrow$$
$$S_{0-2} = (U_{01} U_{01} |0\rangle, U_{01} U_{01} |1\rangle, U_{01} U_{01} |0\rangle, U_{01} U_{01} |1\rangle) \text{(Encoded by } K_1)$$
$$S_{1-2} = (U_{11} |0\rangle, U_{11} |1\rangle, U_{11} |0\rangle, U_{11} |1\rangle) \Rightarrow$$
$$S_{1-3} = (U_{01} U_{11} |0\rangle, U_{01} U_{11} |1\rangle, U_{01} U_{11} |0\rangle, U_{01} U_{11} |1\rangle) \text{(Encoded by } K_2)$$
$$S_{2-3} = (U_{00} |0\rangle, U_{00} |1\rangle, U_{00} |0\rangle, U_{00} |1\rangle) \Rightarrow$$
$$S_{2-4} = (U_{01} U_{10} |0\rangle, U_{01} U_{10} |1\rangle, U_{01} U_{10} |0\rangle, U_{01} U_{10} |1\rangle) \text{(Encoded by } K_3)$$
$$S_{3-4} = (U_{00} |0\rangle, U_{00} |1\rangle, U_{00} |0\rangle, U_{00} |1\rangle) \Rightarrow$$
$$S_{4-1} = (U_{10} U_{11} |0\rangle, U_{10} U_{11} |1\rangle, U_{10} U_{11} |0\rangle, U_{10} U_{11} |1\rangle) \text{(Encoded by } K_0)$$

The encoding process continues until $P_0$ has received the sequence $S_{0-0}$ Encoded by $K_1, K_2, K_3,$ and $K_4)$ separately. $S_{0-0}, S_{1-1}, S_{2-2}, S_{3-3}$ and $S_{4-4}$ can be represented as follows.

$$S_{0-0} = (U_{01} U_{11} U_{01} U_{01} |0\rangle, U_{01} U_{11} U_{01} U_{01} |1\rangle, U_{01} U_{11} U_{01} U_{01} |0\rangle, U_{01} U_{11} U_{01} U_{01} |1\rangle)$$
$$S_{1-1} = (U_{00} U_{00} U_{00} U_{00} |0\rangle, U_{00} U_{00} U_{00} U_{00} |1\rangle, U_{00} U_{00} U_{00} U_{00} |0\rangle, U_{00} U_{00} U_{00} U_{00} |1\rangle)$$
$$S_{2-2} = (U_{11} U_{11} U_{11} U_{11} |0\rangle, U_{11} U_{11} U_{11} U_{11} |1\rangle, U_{11} U_{11} U_{11} U_{11} |0\rangle, U_{11} U_{11} U_{11} U_{11} |1\rangle)$$
$$S_{3-3} = (U_{01} U_{10} U_{01} U_{10} |0\rangle, U_{01} U_{10} U_{01} U_{10} |1\rangle, U_{01} U_{10} U_{01} U_{10} |0\rangle, U_{01} U_{10} U_{01} U_{10} |1\rangle)$$
$$S_{4-4} = (U_{11} U_{11} U_{11} U_{11} |0\rangle, U_{11} U_{11} U_{11} U_{11} |1\rangle, U_{11} U_{11} U_{11} U_{11} |0\rangle, U_{11} U_{11} U_{11} U_{11} |1\rangle)$$

Step 3 Extracting Common Key Phase. $P_o$ (or $P_1$ or $P_2$ or $P_3$ or $P_4$) performs unitary operations decided by $S_{0-1}$ (or $S_{1-2}$ or $S_{2-3}$ or $S_{3-4}$ or $S_{4-0}$) on $S_{0-0}$ (or $S_{1-1}$ or $S_{2-2}$ or $S_{3-3}$ or $S_{4-4}$), and takes measurements on every two-particle state of the resulted sequence with basis $\{|00\rangle, |10\rangle, |01\rangle, |11\rangle\}$ because $N = 5$ is odd. Then the measurement results of $P_o$ (or $P_1$ or $P_2$ or $P_3$ or $P_4$) will be

$$S_{W_0} = (\{01\}, \{11\}, \{00\}) \Rightarrow W_0 = 011100$$
$$S_{W_1} = (\{11\}, \{11\}, \{10\}) \Rightarrow W_1 = 111110$$
$$S_{W_2} = (\{10\}, \{11\}, \{01\}) \Rightarrow W_2 = 101101$$
$$S_{W_3} = (\{11\}, \{11\}, \{01\}) \Rightarrow W_3 = 111101$$
$$S_{W_4} = (\{01\}, \{01\}, \{00\}) \Rightarrow W_4 = 010100$$

At last, $P_0$ computes $K = [K_0] = W_0 \oplus V_0 \oplus K_0 = (001011)$, and it is easy to verify that $[K_0] = K_0 \oplus K_0 \oplus K_0 \oplus K_0 \oplus K_0$. $P_1, P_2, P_3$ and $P_4$ can also obtain the target common key sequence $K = [K_0] = [K_1] = K_2$ similar to $P_o$.

Security Analysis of The Proposed Protocol. In this section, we will show that the proposed MQKA protocol is secure against external and internal attacks. The external attacks contains intercept-resend attack and entangling attack. Without loss of generality, we only consider the circumstance that there are only three participants named $P_o, P_1$ and $P_2$ in the proposed scheme, and it is similar to other cases. Here, we suppose that an eavesdropper named Eve wants to eavesdrop the target common key of $P_o, P_1$ and $P_2$ without being detected.

Firstly, let us discuss the intercept-resend attack. Suppose that $P_o$ prepares a two-particle quantum state sequence $S_{0-1}$, according to a random sequence $S'$ with length $2n$. $P_o$ inserts $2n$ decoy particles into it and sends the new sequence $S'_{0-1}$ to $P_r$. If Eve intercepts the sequence and re-sends a fake sequence prepared beforehand instead of $S'_{0-1}$, then she wants to obtain the operations performed by $P_r$ through the eavesdropping sequence. However, Eve will be detected with probability $1 - \left(\frac{1}{2}\right)^n$ in the eavesdropping check phase by $P_o$ and $P_r$ because she does not know about the positions and basis of decoy particles. Hence, Eve will be detected with probability converging to 1 when $n$ is large enough. Similar to the intercept-resend attack in the channel between $P_1$ and $P_2$ or $P_2$ and $P_o$.

Secondly, let us discuss the entangling attack. Suppose Eve intercepts a transmitting particles to the sequence $S'_{0-1}$, and performs a unitary operation $U_e$ on the intercepted particles to entangle an ancillary particles $|E\rangle$ prepared beforehand. The unitary operation $U_e$ can be defined by the following equations:

$$U_e(0) = a(0) |e_0\rangle + b(1) |e_0\rangle$$
$$U_e(1) = c(0) |e_0\rangle + d(1) |e_1\rangle$$
Table 2. Comparison between the existed five MQKA protocols with our protocol.

| Protocol            | Number of Measurements | Number of Unitary Operations | Security against Internal Attack |
|---------------------|------------------------|-----------------------------|---------------------------------|
| LGHW protocol       | (k + 1)(N − 1)         | 0                          | Secure                          |
| SZ protocol         | (k + 1)N              | 0                          | Insecure                        |
| SZWYZL protocol     | (2kN + 2k + 3)N       | N²                         | Secure                          |
| SYW protocol        | (k + 1)N              | (N − 1)N                   | Secure                          |
| SZWLL protocol      | (2kN + 1)N            | (N − 1)N                   | Insecure                        |
| Our protocol        | (2kN + 1)N            | (N + 1)N                   | Secure                          |

where |e₀₀⟩, |e₁₀⟩, |e₁₁⟩ and |e₁₂⟩ are pure states decided by the unitary operation $U_a$, and the amplitude a, b, c and d satisfy $|a|^2 + |b|^2 = 1$ and $|c|^2 + |d|^2 = 1$. Then it is easy to get:

$$U_e(|+⟩ + |⟩) = \frac{1}{\sqrt{2}} \left( a|0⟩ |e₀₀⟩ + b|1⟩ |e₀₁⟩ + c|0⟩ |e₁₀⟩ + d|1⟩ |e₁₁⟩ \right)$$

$$= \frac{1}{\sqrt{2}} \left( |a|e₀₀⟩ + |b|e₀₁⟩ + |c|e₁₀⟩ + |d|e₁₁⟩ \right)$$

$$= \frac{1}{\sqrt{2}} \left( |a|e₀₀⟩ - |b|e₀₁⟩ + |c|e₁₀⟩ - |d|e₁₁⟩ \right)$$

$$U_e(|−⟩ - |⟩) = \frac{1}{\sqrt{2}} \left( a|0⟩ |e₀₀⟩ + b|1⟩ |e₀₁⟩ - c|0⟩ |e₁₀⟩ - d|1⟩ |e₁₁⟩ \right)$$

$$= \frac{1}{\sqrt{2}} \left( |a|e₀₀⟩ + |b|e₀₁⟩ - |c|e₁₀⟩ - |d|e₁₁⟩ \right)$$

$$= \frac{1}{\sqrt{2}} \left( |a|e₀₀⟩ - |b|e₀₁⟩ - |c|e₁₀⟩ + |d|e₁₁⟩ \right)$$

If the decoy particle belongs to |{0⟩, 1⟩}, in order to pass the eavesdropping checking phase, Eve has to set $b = c = 0$ which implies that $a = d = 1$. Then Eve cannot distinguish |e₀₀⟩ from |e₁₁⟩, and cannot get any useful information. Hence the entangling attack cannot work in the proposed scheme.

Thirdly, let us discuss the internal attack. Without loss of generality, suppose the dishonest participants, $P_1$ and $P_2$, want to cooperate to determine the target common key alone by illegal means. In the encoding process $P_1 → P_2 → P_2 → P_2$, $P_2$ does not leak any information. In the encoding process $P_1 → P_2 → P_2 → P_2$, $P_2$ encodes the two-particle states by his private key in the last step, and meanwhile, he has already obtained the information of the $P_1’s$ and $P_1’s$ private keys from $S_{e−d}$. So we only need to consider the encoding process $P_1 → P_2 → P_2 → P_2$. Firstly, $P_1$ sends $S_2$ to $P_2$. Meanwhile, he also sends his private information $S_1$ and $V_2$ to $P_2$. Secondly, after the eavesdropping checking phase between $P_1$ and $P_1$, $P_1$ perform unitary operations defined by equation (3) according to the $P_1’s$ private information $S_1$. Next, $P_1$ takes measurements on the two-particle state in the resulted sequence with the basis $|+⟩, |−⟩,|+⟩,|−⟩$. At last, $P_1$ eavesdrops $P_1’s$ private key successfully from the value of the measurement results, $S_2$ and $V_2$. Even so, $P_1$ and $P_2$ still cannot determine the target common key alone. In fact, it is obvious that the only way to the $P_1$ to get the target key sequence is to compute $W_0 ⊗ V_0 ⊗ K_0 ⊗ S_0$ and the information of $V_0$ and $S_0$ is only known to $P_0$. Suppose that $P_1$ and $P_2$ embed new private key in the process $P_1 → P_2 → P_2 → P_2$, then the behavior of them only affects the value of $W_0$ because of that $P_1$ and $P_2$ know nothing about $V_0$ and $S_0$. Therefore, the final key $[K_0]$ of $P_0$ will be different from the final key $[K_0]$ and $[K_0]$. Hence, $P_0, P_1$ and $P_2$ cannot obtain the target common key sequence. In a word, $P_1$ and $P_2$ cannot determine the target common key alone by illegal means, and the proposed protocol is secure against internal attack.

**Efficiency Comparison with Existing Protocol.** In this section, we will compare the proposed MQKA protocols with five existing MQKA protocols in the following four aspects: number of qubit measurements, number of unitary operations, qubit efficiency and security against internal attack. The five existing MQKA protocols are “LGHW protocol”20, “SZ protocol”21, “SZWYZL protocol”26, “SYW protocol”28, and “SZWLL protocol”29. The qubit efficiency can be defined as $\eta = \frac{1}{2^b}$, where $c$ is the length of target common key sequence, $q$ is the number of qubits used in transmission and security checking, and “b” is the number of used classical bits. We only compare the internal attack because the internal attackers are the most powerful attackers in the multi-party protocols usually. Suppose the five protocols just mentioned will produce $2 − n$ bit target common key sequence, i.e., $c = 2$. The parameter comparison can be seen in Table 2.

(i) LGHW protocol. The protocol is secure from internal attack, because it is based on BB84 and all participants transmit their privacy secret only once. However, the efficiency $\frac{1}{(k + 1)N(N − 1)}$ is too low and the number of measurements is larger than others.
(ii) SZ protocol. The efficiency and the number of measurements are both not good. More important, it is susceptible to internal attacks owing to an attack strategy proposed by Liu et al.

(iii) SZWYZL protocol. Any participant’s modification can be detected by others because the protocol is based on cluster states. Hence, it is secure from internal attack. Besides, I think the efficiency analysed by authors in ref. 26 is not objective. In fact, the efficiency of the number of measurements and unitary operations are all better than SZWYZL protocol.

(iv) SYW protocol. The protocol is similar to SZWYZL protocol, so it is secure for internal attack. The parameters of efficiency, the number of measurements and unitary operations, are all better than SZWYZL protocol.

(v) SZWLL protocol. The protocol is an improvement on LHGW protocol, and it is much more efficient than any other secure protocols. However, it is susceptible to internal attacks. Without loss of generality, we consider three-party protocol. Suppose the dishonest participants, $P_1$ and $P_2$, want to cooperate to obtain the private key of $P_k$. Consider the message encoding phase in the process $P_1 \rightarrow P_0 \rightarrow P_2 \rightarrow P_k$. Firstly, $P_1$ pre-agreed a common final key $[K]$ with $P_1$, tells the original state of the photon in the sequence $S_2$ to $P_2$. Secondly, after eavesdropping check between $P_1$ and $P_0$, $P_1$ takes measures on $S_0$ with basis $\{0\}, \{1\}$, and obtains the privacy $k_0$ according to $S_2$. Thirdly, $P_1$ sends $k_1$ and $k_0$ to $P_2$. At last, $P_2$ encodes $S_1$ according to $[K] \oplus k_1$. Hence, $P_0$, $P_1$ and $P_2$ obtain the final key $[K]$ only determined by $P_1$ and $P_2$ only.

(vi) Our protocol. Firstly, our protocol is secure against internal attack. Secondly, The number of measurements is better than LHGW protocol and SZWYZL protocol, but worse than SYW protocol. The unitary operations is not better than LHGW protocol, SZWYZL protocol and SYW protocol. However, the efficiency of our protocol is better than any other secure protocols.

Discussion

In this paper, we propose the first multiparty QKA protocol based on a quantum search algorithm known as Grover’s algorithm. Firstly, we generalize the properties of quantum search algorithms. Secondly, using the generalized properties of QSA, we propose a multiparty QKA protocol. Next, a 5-party protocol novel example is presented. At last, the security and efficiency analysis shows that our protocol is prior to existing MQKA protocols.

References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: public-key distribution and coin tossing [C]. Proceedings of IEEE International Conference on Computer System and Signal Processing 175–179 (1984).
2. Lo, H. K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances[J]. Science 283, 2050C2056 (1999).
3. Lo, H. K., Ma, X. & Chen, K. Decoy state quantum key distribution. Phys. Rev. Lett. 94, 230504 (2005).
4. Li, H. Statistical-fluctuation analysis for quantum key distribution with consideration of after-pulse contributions. Phys. Rev. A. 92, 062344 (2015).
5. Hillery, M., Buzek, V. & Berthiaume, A. Quantum secret sharing. Phys. Rev. A. 59, 1829C1834 (1999).
6. Hsu, L. Y. Quantum secret-sharing protocol based on Grover’s algorithm. Phys. Rev. A. 68, 022306 (2003).
7. Yang, Y., jia, X. et al. Verifiable quantum (k, n)-threshold secret sharing. Quantum Inf Process 11, 1619C1625 (2012).
8. Liao, C., Yang, C. & Hwang, T. Dynamic quantum secret sharing scheme based on GHZ state. Quantum Inf Process 13, 1907C1916 (2014).
9. Qin, H. W. & Dai, Y. W. d-Dimensional quantum state sharing with a one-time pad. Quantum Inf Process 15, 1689C1701 (2016).
10. Deng, E. G. & Long, G. L. Secure direct communication with a quantum one-time pad. Phys. Rev. A. 69, 052319 (2004).
11. Tong, H. Y., Tsai, C. W. & Hwang, T. Controlled deterministic secure quantum communication based on quantum search algorithm. Int. J. Theor. Phys. 51, 2447C2454 (2012).
12. Li, Y. & Nie, L. Asymmetric bidirectional controlled teleportation by using six-qubit cluster state. Int. J. Theor. Phys. 55, 1C9 (2016).
13. Costa, D., Almeida, N. G. & Villas-Boas, C. J. Secure quantum communication using classical correlated channel. Quantum Inf Process 15, 4303C4311 (2016).
14. Zhang, W. W., Li, D. et al. Quantum private comparison based on quantum search algorithm. Int. J. Theor. Phys. 52, 1466C1473 (2013).
15. Guo, F. Z. & Gao, F. Quantum private comparison protocol based on entanglement swapping of d-level bell states. Quantum Inf Process 12, 2793C2802 (2013).
16. Zhuo, N., Zeng, G. & Xiong, J. Quantum key agreement protocol. Electronics Letters 40, 1149C1150 (2004).
17. Tsai, C. & Hwang, T. On quantum key agreement protocol. Technical Report (C-S-I-E, NCKU, Taiwan), ROC (2009).
18. Chong, S. K., Tsai, C. W. & Hwang, T. Improvement on Quantum key agreement protocol with maximally entangled states? Int. J. Theor. Phys. 50, 1793C1802 (2011).
19. Chong, S. K. & Hwang, T. Quantum key agreement protocol based on BB84. Opt. Commun. 283, 1192C1195 (2010).
20. Liu, B., Gao, F. et al. Multi-party quantum key agreement with single particles. Quantum Inf Process 12, 3411C3420 (2013).
21. Shi, R. H. & Zhong, H. Multi-party quantum key agreement with bell states and bell measurements. Quantum Inf Process 12, 921C932 (2013).
22. Shen, D. S., Ma, W. P. & Wang, L. Two-party quantum key agreement with four-qubit cluster states. Quantum Inf Process 13, 2313C2324 (2014).
23. Xu, G. B., Wen, Q. Y. et al. Novel multi-party quantum key agreement protocol with GHZ states. Quantum Inf Process 13, 2587C2594 (2014).
24. Huang, W., Wen, Q. Y. et al. Quantum key agreement with epr pairs and single-particle measurements. Quantum Inf Process 13, 649C663 (2014).
25. Shukla, C., Alam, N. & Pathak, A. Protocols of quantum key agreement solely using bell states and bell measurement. Quantum Inf Process 13, 2391C2405 (2014).
26. Sun, Z., Zhang, C. et al. Multi-party quantum key agreement by an entangled six-qubit state. Int. J. Theor. Phys. 55, 1920C1929 (2016).
27. Hsueh, C. C. & Chen, C. Y. Quantum key agreement protocol with maximal entangled states. Proceedings of the 14th Information Security Conference (National Taiwan University of Science and Technology. Taipei IISC 2004), 236C2242 (2004).
28. Sun, Z., Yu, J. & Wang, P. Efficient multi-party quantum key agreement by cluster states. Quantum Inf Process 15, 373C384 (2016).
29. Sun, Z., Zhang, C. et al. Improvements on fliparty quantum key agreement with single particles? Quantum Inf Process 12, 3411C3420 (2013).
30. Grover, L. K. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **79**, 325 (1997).
31. Wang, C., Hao, L. et al. Quantum direct communication based on quantum search algorithm. *Int. J. Quantum Inf.* **8**, 443–450 (2010).
32. Tseng, H. Y., Tsai, C. W. & Hwang, T. Controlled deterministic secure quantum communication based on quantum search algorithm. *Int. J. Theor. Phys.* **51**, 2447–2454 (2012).

**Acknowledgements**

This work is partially supported by National Science Foundation of China under grant No. 61373171, The 111 Project under grant No. B08038, and The Key Project of Science Research of Anhui Province (Quantum key agreement protocol based on entangled state).

**Author Contributions**

Cao, H. designed the scheme. Cao, H. and Ma, W. did security analysis and efficiency comparison. All authors wrote and reviewed the manuscript.

**Additional Information**

**Competing Interests:** The authors declare no competing financial interests.

**How to cite this article:** Cao, H. and Ma, W. Multiparty Quantum Key Agreement Based on Quantum Search Algorithm. *Sci. Rep.* **7**, 45046; doi: 10.1038/srep45046 (2017).

**Publisher’s note:** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This work is licensed under a Creative Commons Attribution 4.0 International License. The images or other third party material in this article are included in the article’s Creative Commons license, unless indicated otherwise in the credit line; if the material is not included under the Creative Commons license, users will need to obtain permission from the license holder to reproduce the material. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/

© The Author(s) 2017