Dual Compressible Hybrid Quantum Secret Sharing Schemes based on Extended Unitary Operations

Hong Lai[a,b], Mehmet A. Orgun[a], Liyin Xue[c], Jinghua Xiao[b] and Josef Pieprzyk[a]

[a]Department of Computing, Macquarie University, Sydney, NSW 2109, Australia;
[b]School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China;
[c]Corporate Analytics, The Australian Taxation Office, Sydney NSW 2000, Australia;

ABSTRACT

A crucial issue with hybrid quantum secret sharing schemes is the amount of data that is allocated to the participants. The smaller the amount of allocated data, the better the performance of a scheme. Moreover, quantum data is very hard and expensive to deal with, therefore, it is desirable to use as little quantum data as possible. To achieve this goal, we first construct extended unitary operations by the tensor product of $n, n \geq 2$, basic unitary operations, and then by using those extended operations, we design two quantum secret sharing schemes. The resulting dual compressible hybrid quantum secret sharing schemes, in which classical data play a complementary role to quantum data, range from threshold to access structure. Compared with the existing hybrid quantum secret sharing schemes, our proposed schemes not only reduce the number of quantum participants, but also the number of particles and the size of classical shares. To be exact, the number of particles that are used to carry quantum data is reduced to 1 while the size of classical secret shares also is also reduced to $\frac{l-2}{m-1}$ based on $((m+1, n'))$ threshold and to $\frac{l-2}{r_2}$ (where r_2 is the number of maximal unqualified sets) based on adversary structure. Consequently, our proposed schemes can greatly reduce the cost and difficulty of generating and storing EPR pairs and lower the risk of transmitting encoded particles.

Keywords: dual compressible hybrid quantum secret sharing schemes, extended unitary operations, access structure, $((m+1, n'))$ threshold, adversary structure

1. INTRODUCTION

Secret sharing is a critical primitive for building secure channels in a multi-party setting including many applications in business, commerce and military such as missile launch codes, shared bank accounts, preserving data privacy. It was proposed by Shamir[1] and Blakley[2] in 1979 independently. However, without quantum mechanics, secret sharing can just be done under the assumption that a certain computational problem is hard. As digital communication can be easily eavesdropped, tampered with and copied, it is necessary and significant to consider the secrecy of information anticipating future algorithmic and computational discoveries which could break the secrecy of past secrets, violating the secrecy of the confidential channel.

Quantum secret sharing(QSS), is a natural extension of the classical secret sharing, which is able to detect eavesdropping due to the fact that quantum mechanics remains an accurate description of the laws of nature. Hillery et al.[3] proposed the first quantum secret sharing scheme by using a three-photon entangled GHZ state in 1999. Subsequently, Karlsson et al.[4] proposed another QSS scheme with a two-photon polarization entangled state. Since these two QSS schemes[3,4] were presented, many authors[5–27] have proposed a variety of quantum secret sharing schemes. Though these quantum secret sharing (QSS) schemes can be used to share a secret and they are secure against any future algorithmic or computational improvements, all the share-holders must be capable of carrying and processing quantum information. Besides, quantum information is fragile in nature.

There have been several proposals for hybrid secret sharing schemes where both quantum and classical data are used. Nascimento et al.[28] proposed a quantum secret sharing scheme by using quantum encryption. That is, let $|\psi\rangle$ be a quantum state consisting of n particles and K a random sequence of classical bits of length $2n$, then assign to each particle of $|\psi\rangle$ two classical bits of K that determine which transformation is performed on the

Further author information: (Send correspondence to Hong Lai) E-mail: hong.lai@students.mq.edu.au

Quantum Information and Computation XII, edited by Eric Donkor, Andrew R. Pirich, Howard E. Brandt, Michael R. Frey, Samuel J. Lomonaco, Jr., John M. Myers, Proc. of SPIE Vol. 9123, 912309

respective particle. For instance, 00 corresponds to applying the identity mapping I, 01 to the Pauli X operator, 10 to the Pauli Z operator and 11 to the Pauli Y operator. After this encryption, the resulting state $|\widehat{\psi}\rangle$ is a complete mixture and no information can be gained from it. Only if one has the classical key K, can the original state $|\psi\rangle$ be obtained from $|\widehat{\psi}\rangle$. Later on, Singh et al.[29] extended and improved Nascimeto et al.'s scheme, and further proposed some approaches for sharing a quantum secret in a hybrid way, that is, certain participants have only classical shares and the remaining participants have (possibly multiple) quantum shares. In 2011, Fortescue et al.[30] proposed a construction for perfect quantum secret sharing schemes based on imperfect "ramp" secret sharing combined with classical encryption, in which the individual participants' shares are split into quantum and classical components, allowing the former to be of lower dimension than the secret itself, and hence reducing the communication cost of quantum secret sharing. However, the total amount of quantum data allocated is not necessarily decreased in these three hybrid quantum secret sharing schemes.[28–30]

As we know, an important issue existing in hybrid quantum secret sharing schemes is the amount of data that is allocated to the participants. The smaller the amount of allocated data, the better the performance of a scheme. Furthermore, as quantum data is very difficult and costly to cope with, it is desirable to use as little quantum data as possible. To address the issue, we first extend the four basic local unitary operations by the tensor product of $n, n \geq 2$, basic unitary operations to $2^{2n}, n \geq 2$, unitary operations that are still composed of the four basic local unitary operations. Extended unitary operations are then used in the design of two hybrid quantum secret sharing schemes. In fact, in 2012, Chou et al.[31] extended the four basic local unitary operations to 16 unitary operations and further proposed an enhanced multiparty quantum secret sharing of classical messages to enhance the transmission efficiency of the whole protocol. Later, Chou et al.[32] considered using GHZ-State for multiparty quantum secret sharing without a code table associated with the same idea used in.[31]

Inspired by Nascimeto et al., Singh et al., Fortescue et al. and Chou et al.,[28–32] we propose two dual compressible hybrid quantum secret sharing schemes using extended unitary operations, which aim at reducing the number of particles and quantum participants and the size of classical shares while maintaining the security of hybrid quantum secret sharing. In our proposed schemes, we stipulate that there is only one unique quantum participant called Bob; he first prepares $\lambda' + 1$ EPR pairs (where λ' is the number that can provide an analysis of the error). All of the 1st particles from each EPR pair are to form a photon sequence S_H and all of the 2nd particles from each EPR pair are to form a photon sequence S_T. Then Bob keeps the sequence S_H and sends the sequence S_T to Alice via a quantum channel. After confirming that the quantum channel is secure, Alice performs the correct transition operation on a particle from an EPR pair and sends the encoded particle to Bob (here, we assume that only Alice and Bob know the measured basic operations corresponding to particular transition operations respectively as all the extended unitary operations boil down to the four basic unitary operations eventually). Meanwhile the corresponding classical bits are transmitted to classical participants in various ways via the classical channel.

When comparing with Fortescue et al.'s, Nascimeto et al.'s and Singh et al's schemes, our schemes have the following four advantages:

(1) Not only can our schemes reduce the number of quantum participants, but also the number of particles and the size of classical shares. To be exact, the number of particles that are used to carry quantum data is reduced to 1 while the size of classical secret shares is also reduced to $\frac{l-2}{m-1}$ based on $((m+1, n'))$ threshold hybrid quantum secret sharing and to $\frac{l-2}{r_2}$ (where r_2 is the number of maximum unqualified sets) based on adversary structure. Consequently, our proposed schemes can greatly reduce the cost and difficulty of generating and storing EPR pairs and lower the risk of transmitting encoded particles. Also, our schemes can enhance the efficiency of secret sharing.

(2) In our proposed schemes, even if Eve can obtain all the transmitted classical data and quantum data, she is not able to obtain any information about the shared secrets. Because, first, she does not know the second particles which are always kept by Bob; second, she does not know which basic unitary operations correspond to which transition operations.

(3) Due to (2), our schemes are more secure in the face of various attacks such as the photon number attack, the entangle-measure attack, the trojan horse attack and the faked states attack.

(4) Quantum shares and classical shares do not have a direct relationship with the shared secret, but can determine the secret cooperatively. Moreover, owing to the compressibility of quantum data, our schemes are easier, cheaper and more practical to implement in real life.

The remainder of this paper is organized as follows. In Section 2, we describe the extended unitary operations in detail. We also define hybrid quantum secret sharing, and provide required definitions and then present the exact schemes in Section 3. We then discuss the features and the security of our schemes in Section 4. Conclusions are discussed in Section 5.

2. BACKGROUND

In this section, we introduce the concepts of EPR pairs, four basic local operations, and the extended unitary operations and their applications in quantum secret sharing.

2.1 EPR pairs[33]

An EPR pair is in one of the four Bell states shown as follows:

$|\psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)$; $|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$;

$|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$; $|\phi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B)$.

2.2 Four basic local unitary operations

Four basic local unitary operations $U_{00}, U_{01}, U_{10}, U_{11}$ are listed as follows:

$U_{00} = U_0 = |0\rangle\langle 0| + |1\rangle\langle 1|$; $U_{01} = U_1 = |0\rangle\langle 0| - |1\rangle\langle 1|$;

$U_{10} = U_2 = |0\rangle\langle 1| + |1\rangle\langle 0|$; $U_{11} = U_3 = |0\rangle\langle 1| - |1\rangle\langle 0|$.

The subscripts 00, 01, 10, 11 are two bits of messages denoted by the corresponding unitary operations. U_1, U_2, U_3 are Pauli operators.

2.3 Extended unitary operations

We consider $2^{2n}, n \geq 2$, unitary operations in a general way where each operation is the result of the tensor product of $n, n \geq 2$, basic unitary operations defined as follows:

$$U_{b_1b_2b_3b_4\ldots b_{2n-1}b_{2n}} = U_{b_1b_2} \otimes U_{b_3b_4} \otimes \ldots \otimes U_{b_{2n-1}b_{2n}} \tag{1}$$

where $b_1 \ldots b_{2n}$ represents any $2n$ bit values.

Definition 1. Extended unitary operations. For $\forall n \in \mathbb{N}, n \geq 2$, any unitary operation constructed as in (1) is called an $n-$extended unitary operation.

Lemma 1. When the four local unitary operations are used to transform any one of the Bell states, the outcomes are as follows: $U_{00}|\psi^-\rangle = U_0|\psi^-\rangle = |\psi^-\rangle$, $U_{01}|\psi^-\rangle = U_1|\psi^-\rangle = |\psi^+\rangle$, $U_{10}|\psi^-\rangle = U_2|\psi^-\rangle = |\phi^-\rangle$, $U_{11}|\psi^-\rangle = U_3|\psi^-\rangle = |\phi^+\rangle$. Then for composite operations when they are used to transform any one of the Bell states, the following equations hold:

$U_0U_i = U_i, i = 1, 2, 3; U_1U_2 = U_3$.

$U_1U_3 = U_2, U_2U_3 = U_1$.

$U_0U_1U_2 = U_3$, $U_0U_1U_3 = U_2$.

$U_0U_2U_3 = U_1$, $U_1U_2U_3 = U_0$.

$U_0U_1U_2U_3 = U_0$.

$(U_0)^n = U_0; (U_i)^{2n} = U_0, n \in \mathbb{N}^\star, i = 1, 2, 3$.

$(U_0U_i)^{2n} = U_0, (U_0U_i)^{2n+1} = U_i, n \in \mathbb{N}^\star, i = 1, 2, 3$.

Next, we see two particular examples using the construction of extended unitary operations.

We first consider 2−extended unitary operations by Definition 1.

$U_{0000} = U_{00} \otimes U_{00}$, $U_{0001} = U_{00} \otimes U_{01}$,

$U_{0010} = U_{00} \otimes U_{10}$, $U_{0011} = U_{00} \otimes U_{11}$,

$\vdots$

$U_{1100} = U_{11} \otimes U_{00}$, $U_{1101} = U_{11} \otimes U_{01}$,

$U_{1110} = U_{11} \otimes U_{10}$, $U_{1111} = U_{11} \otimes U_{11}$.

The 2−extended unitary operations can be used to transform one of the Bell states into any Bell states as follows:

$U_{0000}|\psi^-\rangle = U_{00} \otimes U_{00}|\psi^-\rangle = U_{00}|\psi^-\rangle = |\psi^-\rangle$,

$U_{0001}|\psi^-\rangle = U_{00} \otimes U_{01}|\psi^-\rangle = U_{00}|\psi^+\rangle = |\psi^+\rangle$,

$U_{0010}|\psi^-\rangle = U_{00} \otimes U_{10}|\psi^-\rangle = U_{00}|\phi^-\rangle = |\phi^-\rangle$,

$U_{0011}|\psi^-\rangle = U_{00} \otimes U_{11}|\psi^-\rangle = U_{00}|\phi^+\rangle = |\phi^+\rangle$,

$\vdots$

$U_{1100}|\psi^-\rangle = U_{11} \otimes U_{00}|\psi^-\rangle = U_{11}|\psi^-\rangle = |\phi^+\rangle$,

$U_{1101}|\psi^-\rangle = U_{11} \otimes U_{01}|\psi^-\rangle = U_{11}|\psi^+\rangle = |\phi^-\rangle$,

$U_{1110}|\psi^-\rangle = U_{11} \otimes U_{10}|\psi^-\rangle = U_{11}|\phi^-\rangle = |\psi^+\rangle$,

$U_{1111}|\psi^-\rangle = U_{11} \otimes U_{11}|\psi^-\rangle = U_{11}|\phi^+\rangle = |\psi^-\rangle$.

We can then group the 2−extended unitary operations based on their outcomes as follows:

$U_{0000}|\psi^-\rangle = U_{0101}|\psi^-\rangle = U_{1010}|\psi^-\rangle = U_{1111}|\psi^-\rangle = U_{00}|\psi^-\rangle = |\psi^-\rangle$;

$U_{0001}|\psi^-\rangle = U_{0100}|\psi^-\rangle = U_{1011}|\psi^-\rangle = U_{1110}|\psi^-\rangle = U_{01}|\psi^-\rangle = |\psi^+\rangle$;

$U_{0010}|\psi^-\rangle = U_{0111}|\psi^-\rangle = U_{1000}|\psi^-\rangle = U_{1101}|\psi^-\rangle = U_{10}|\psi^-\rangle = |\phi^-\rangle$;

$U_{0011}|\psi^-\rangle = U_{0110}|\psi^-\rangle = U_{1001}|\psi^-\rangle = U_{1100}|\psi^-\rangle = U_{11}|\psi^-\rangle = |\phi^+\rangle$.

And they are abbreviated as follows:

$U_{0000} = U_{0101} = U_{1010} = U_{1111} = U_{00} = |0\rangle\langle 0| + |1\rangle\langle 1|$

$U_{0001} = U_{0100} = U_{1011} = U_{1110} = U_{01} = |0\rangle\langle 0| - |1\rangle\langle 1|$

$U_{0010} = U_{0111} = U_{1000} = U_{1101} = U_{10} = |1\rangle\langle 0| + |0\rangle\langle 1|$

$U_{0011} = U_{0110} = U_{1001} = U_{1100} = U_{11} = |1\rangle\langle 0| - |0\rangle\langle 1|$

For 3−extended unitary operations, the similar abbreviation can be obtained as follows:

$U_{000000} = U_{000101} = U_{001010} = U_{001111} = U_{010001} = U_{010100} = U_{011011} = U_{011110} = U_{100010} = U_{100111} = U_{101000} = U_{101101} = U_{110011} = U_{111001} = U_{110110} = U_{111100} = U_{0000} = U_{0101} = U_{1010} = U_{1111} = U_{00} = |0\rangle\langle 0| + |1\rangle\langle 1|$

$U_{000001} = U_{000100} = U_{001011} = U_{010101} = U_{011010} = U_{011111} = U_{100011} = U_{100110} = U_{101001} = U_{101100} = U_{110010} = U_{110111} = U_{111000} = U_{101100} = U_{111101} = U_{010000} = U_{1011} = U_{0100} = U_{1110} = U_{0001} = U_{01} = |0\rangle\langle 0| - |1\rangle\langle 1|$

$U_{000010} = U_{000111} = U_{111110} = U_{001000} = U_{001101} = U_{010011} = U_{010110} = U_{011001} = U_{011100} = U_{100000} = U_{100101} = U_{101010} = U_{101111} = U_{110001} = U_{110100} = U_{111011} = U_{1101} = U_{0010} = U_{1000} = U_{0111} = U_{10} = |1\rangle\langle 0| + |0\rangle\langle 1|$

$U_{000011} = U_{000110} = U_{001001} = U_{001100} = U_{010010} = U_{010111} = U_{011000} = U_{011101} = U_{100001} = U_{100100} = U_{101011} = U_{101110} = U_{110000} = U_{110101} = U_{111010} = U_{111111} = U_{0110} = U_{1001} = U_{0011} = U_{1100} = U_{11} = |1\rangle\langle 0| - |0\rangle\langle 1|$

From the general pattern observed from the above equations, we can obtain the following Theorem.

Theorem 1. For any $n \geq 2$, when the 2^{2n} $n-$extended unitary operations are used to transform any one of the Bell states, the final outcomes boil down to the four basic local unitary operations that are used (the proof is given in Appendix A).

Definition 2. Transition operations and ultimate operations. For a given $n, n \geq 2$, if $U_{b_{i_1}b_{i_2}\ldots b_{i_{2n-1}}b_{i_{2n}}}|\psi^-\rangle = U_{b_{j_1}b_{j_2}\ldots b_{j_{2n-3}}b_{j_{2n-2}}}|\psi^-\rangle = |\psi^-\rangle$, where $b_{i_1}b_{i_2}\ldots b_{i_{2n-1}}b_{i_{2n}}$, $b_{j_1}b_{j_2}\ldots b_{j_{2n-3}}b_{j_{2n-2}}$ represent any $2n$ and $2n-2$ bit values respectively, then $U_{b_{j_1}b_{j_2}\ldots b_{j_{2n-3}}b_{j_{2n-2}}}$ is called the transition operation of $U_{b_{i_1}b_{i_2}\ldots b_{i_{2n-1}}b_{i_{2n}}}$. Meanwhile, $U_{b_{i_1}b_{i_2}\ldots b_{i_{2n-1}}b_{i_{2n}}}$ is called the ultimate operation of $U_{b_{j_1}b_{j_2}\ldots b_{j_{2n-3}}b_{j_{2n-2}}}$.

Definition 3. Control bits. According to Lemma 1, for given $n-$extend
-ed unitary operations, $n \geq 2$, every 2^{2n-2} $n-$extended unitary operations have the same outcomes when all the 2^{2n} $n-$extended unitary operations are used to transform an identical Bell state . The 2^{2n-2}, $n-$extended unitary operations are listed with matching sequence numbers that are denoted by the bit values. The bit values are called the control bits.

Definition 4. Corresponding classical bits. The bit values obtained by applying XOR to the bit values from the subscript of the transition operation and the control bits are called the corresponding classical bits.

According to Definition 2, for $2-$extended unitary operations, U_{00} is the transition operation of ultimate operation U_{0000}. Likewise, for $3-$extended unitary operations, $U_{0000}, U_{0101}, U_{1010}, U_{1111}$ are the transition operation of ultimate operations $U_{000000}, U_{000101}, U_{001010}, U_{001111}, U_{010001}, U_{010100}, U_{011011}$, $U_{011110}, U_{100010}, U_{100111}, U_{101000}, U_{101101}, U_{110011}, U_{111001}, U_{110110}, U_{111100}$.

We use an algorithm called build_tables (see Appendix B) to generate a collation table for any given $n \geq 2$. The tables are made up by following the rules: (1) The first column of all tables is composed of $U_{00}, U_{01}, U_{10}, U_{11}$. (2) If the size of the secret is $2n$, then the first rank consists of $\underbrace{0000\cdots0000}_{2n-2}$, $\underbrace{0000\cdots0001}_{2n-2}$, ..., $\underbrace{1111\cdots1111}_{2n-2}$.

Therefore, according to the algorithm, when $n = 2$, we can make the corresponding collation table (see Table 1). When $n = 3$, the corresponding collation table is given in Table C.2 in Appendix C.

Table 1. Collation table for $n = 2$, where BUO denotes basic unitary operation.

	Control bits			
BUO	00	01	10	11
U_{00}	U_{0000}	U_{0101}	U_{1010}	U_{1111}
U_{01}	U_{1011}	U_{0100}	U_{1110}	U_{0001}
U_{10}	U_{1101}	U_{0010}	U_{1000}	U_{0111}
U_{11}	U_{0110}	U_{1001}	U_{0011}	U_{1100}

3. HYBRID QUANTUM SECRET SHARING SCHEMES USING EXTENDED UNITARY OPERATIONS

In this section, we first provide some definitions, and then the corresponding schemes are presented.

Definition 5. A QSS is said to be hybrid only when a sufficient number of quantum participants with their quantum shares and enough classical participants with their classical shares together can recover a secret.

In hybrid quantum secret sharing (HQSS) schemes, the secret shares are composed of quantum and classical shares. We name the former q-shares and the latter c-shares. A participant who holds only c-shares is called a c-participant and a participant who holds only q-shares is named a q-participant.

3.1 Dual compressible $((m+1, n'))$ threshold hybrid quantum secret sharing scheme

In this subsection, we present a definition and a theorem for hybrid quantum secret sharing based on $((m+1, n'))$ threshold, that is, there are exactly one q-participant and $n'-1$ c-participants. Moreover, only when the q-participant and at least $m \leq n'-1$ c-participants cooperate, the secret can be recovered.

3.1.1 A definition and a theorem based on $((m+1,n'))$ threshold

Definition 6. A HQSS achieving $((m+1,n'))$ among a set of participants $\mathbb{P}=\{P_1,P_2,\ldots,P_{n'}\}$ is said to be dual compressible threshold HQSS if only one q-participant with one q-share and at least m c-participants with c-shares with the size of $\frac{l}{m-1}$ can share a secret cooperatively, where l is the length of the shared secret.

According to definition 6, we can obtain the following theorem. It formalizes the scenario when new participants join in.

Theorem 2. A $((m+1,n'))$-HQSS can be inflated only conformally, i.e. to threshold schemes having the form $((m+\lambda+1,n'+\lambda))$ where λ ($\lambda\in\mathbb{N}$) are all new c-participants (the proof is given in Appendix A).

3.1.2 The proposed scheme

In this subsection, we propose a dual compressible $((m+1,n'))$ hybrid quantum secret sharing scheme in which we assume that: 1) Bob is the q-participant and $Charlie_1,...,Charlie_{n'-1}$ are $n'-1$ c-participants. 2) Alice and Bob agree that each of the four basic unitary operations corresponds to a particular transition operation in advance. 3) The shared secret is $s_A=\{s_A^1,s_A^2,\ldots,s_A^l\}, l=2n, s_A^{i_1}\in\{0,1\}, i_1=1,2,\ldots,l$. 4) Classical channels are supposed to be authenticated classical channels.

(1) Bob first prepares $\lambda'+1$ EPR pairs (Where λ' is the number that can provide an analysis of the error.) Every EPR pair is supposed to be $|\psi^-\rangle_{h_jt_j}=\frac{1}{\sqrt{2}}(|0\rangle_{h_j}|1\rangle_{t_j}-|1\rangle_{h_j}|0\rangle_{j_j})$. All of the 1st particles of each EPR pair are to form a photon sequence S_H and all of the 2nd particles of each EPR pair are to form a photon sequence S_T. Then Bob keeps the sequence S_H and sends the sequence S_T to Alice via a quantum channel.

(2) After receiving the sequence S_T from Bob, Alice first finds the correct $n-$extended unitary operation in terms of the shared secret $s_A=\{s_A^1,s_A^2,\ldots,s_A^l\}$, which can be determined by the transition operation $U_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}}}$ and control bits. Then Alice performs the transition operation $U_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}}}$ on particle t_j. Under the transition operation, this state can be changed to one of the following states according to Theorem 1:

$$U^{t_j}_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}}}|\psi^-\rangle=U^{t_j}_{00}|\psi^-\rangle=|\psi^-\rangle;$$

$$U^{t_j}_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}}}|\psi^-\rangle=U^{t_j}_{01}|\psi^-\rangle=|\psi^+\rangle;$$

$$U^{t_j}_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}}}|\psi^-\rangle=U^{t_j}_{10}|\psi^-\rangle=|\phi^-\rangle;$$

$$U^{t_j}_{b_{i_1}b_{i_2}b_{i_3}b_{i_4}\ldots b_{i_{2n-3}}b_{i_{2n-2}}}|\psi^-\rangle=U^{t_j}_{11}|\psi^-\rangle=|\phi^+\rangle.$$

where the superscript t_j denotes the photon on which unitary operation is performed.

(3) In order to check eavesdropping in this transmission, Alice randomly chooses some particles from remaining S_T to detect eavesdropping and performs one of the four basic unitary operations on them at random. Then Alice transmits these encoded particles to Bob while telling him the positions of the these particles and the type of the basic unitary operations on them. Bob performs Bell-basis measurement on the encoded particles and their counterparts from S_H. Bob computes the error rates by checking the EPR pairs from which Alice chose particles. If the error rates of the chosen EPR pairs are lower than the predefined value, Alice transmits the encoded particle t'_j to the q-participant Bob via a quantum channel. Otherwise, Alice continues to check the quantum channel in the same way until the qubit t'_j encoded by the transition operation is sent to Bob safely.

(4) Then Alice allocates the corresponding classical bits obtained by applying XOR to the bit values from the subscript of the transition operation and the control bits with the size of $2n-2$ to the $n'-1$ c-participants $Charlie_1,...,Charlie_{n'-1}$ through a classical channel in the following way.

(5) Let c denote the corresponding classical bits, Alice allocates c in the way that used in,[34] which is as follows:

1. Alice cuts the corresponding classical bits into $m-1$ pieces. These pieces are denoted as $c_1,c_2,\ldots,c_{m-1}$ and $c=c_1\shortparallel c_2\shortparallel\ldots\shortparallel c_{m-1}$ where each $c_{i_2}, i_2=1,2,\ldots,m-1$, is the binary representation of a decimal number.

2. Alice allocates the corresponding classical bits in the following way:

2.1 Choose a prime p, $p > max(c_{max}, n' - 1)$, where $c_{max} = max\{c_1, c_2, ..., c_{m-1}\}$.

2.2 Randomly and uniformly choose a number $a_1 \in Z_p$ and generate a polynomial: $f_1(x) = a_1 x + c_1$.

2.3 Sample $f_1(x)$ at two points $A_{c_1 1} = f_1(1)$ and $A_{c_1 2} = f_1(2)$ which represent two shares of c_1.

2.4 Do for $2 \leq i_2 \leq (m-1)$.

(a) Generate a polynomial

$f_{i_2}(x) = A_{c_{i_2-1} i_2} x^{i_2} + A_{c_{i_2-1}(i_2-1)} x^{i_2-1} + \cdots + A_{c_{i_2-1}1} x + c_{i_2}$

(b) Sample $f_{i_2}(x)$ to create new shares.

i. If $i_2 < m-1$, sample at $i_2 + 1$ points such that

$A_{c_{i_2}1} = f_{i_2}(1)$, $A_{c_{i_2}2} = f_{i_2}(2)$, ..., $A_{c_{i_2}(i_2+1)} = f_{i_2}(i_2 + 1)$.

ii. If $i_2 = m-1$, sample at $n' - 1$ points such that

$A_1 = f_{i_2}(1)$, $A_2 = f_{i_2}(2)$, ..., $A_{n'-1} = f_{i_2}(n' - 1)$

(c) Delete old shares: $A_{c_{i_2-1}1}, \cdots, A_{c_{i_2-1} i_2}$.

2.5 The final $n' - 1$ shares are given by (i_2, A_{i_2}), for $1 \leq i_2 \leq n' - 1$.

(6) A group of the q-participant and any m c-participants together are able to reconstruct the secret. First, the q-participant measures (h_j, t'_j) to obtain the transition operation in terms of their agreement. Then, the m c-participants interpolate their m shares (i_2, A_{i_2}) to generate the polynomial of degree $m-1$ and thus obtain the corresponding classical bits.

$f(x) = c_{\alpha_{m-1}} x^{m-1} + c_{\alpha_{m-2}} x^{m-2} + \cdots + c_{\alpha_1} x + c_{m-1}$.

Hence, the control bits can be obtained by applying the XOR operation on the corresponding classical bits and bit values knowing from the subscript of the transition operation. Finally, they can recover the ultimate operation by checking the algorithm build_table, that is, Alice's secret $s_A = \{s_A^1, s_A^2, \ldots, s_A^l\}$.

It is worth noting that the dual compressible threshold hybrid quantum secret sharing scheme can be easily converted into a $((m+1, n'))$ threshold hybrid quantum multi-secret sharing scheme. But $c_1, c_2, ..., c_{m-1}$ correspond to $s_1, s_2, \ldots, s_{m-1}$. The rest of the processes remain unchanged.

3.2 Dual compressible Hybrid quantum secret sharing scheme based on adversary structure

In this section, a dual compressible hybrid quantum secret sharing scheme based on adversary structure is presented, in which all participants from any minimal qualified set can recover the secret.

3.2.1 Definitions and a theorem based on access structure and adversary structure

Let $\mathbb{P} = \{P_1, P_2, \ldots, P_{n'}\}$ be the set of participants. Let $\alpha \subseteq \mathbb{P}$. α is called a qualified set if the q-participant and any designated c-participants in α together can recover the secret; otherwise, it is called an unqualified set. An access structure, denoted by Γ, is a collection of qualified subsets of $\mathbb{P}$ satisfying the monotone ascending property: for any $A' \in \Gamma$ and $A \in 2^{\mathbb{P}}$, $A' \subseteq A$ implies $A \in \Gamma$. An adversary structure, denoted by $\mathbb{A}$, is a collection of unqualified subsets of $\mathbb{P}$ satisfying the monotone descending property: for any $A' \in \mathbb{A}$ and $A \in 2^{\mathbb{P}}, A \subseteq A'$ implies $A \in \mathbb{A}$.

By the definition of qualified and unqualified subsets, for any given access structure Γ and adversary structure $\mathbb{A}$ over $\mathbb{P}$, we have that $\Gamma \cap \mathbb{A} = \emptyset$. Because of the monotone properties, for any access structure Γ and any adversary structure $\mathbb{A}$, it is sufficient to consider the minimum access structure:

$$\Gamma_{min} = \{A \in \Gamma \mid \forall B \subset A \Rightarrow B \notin \Gamma\},$$

and the maximum adversary structure:

$$\mathbb{A}_{max} = \{B \in \mathbb{A} \mid \forall A \supset B \Rightarrow A \notin \mathbb{A}\}.$$

In this paper, we consider the complete situation, that is $\mathbb{A} \bigcup \Gamma = 2^{\mathbb{P}}$.[35]

Based on the above-mentioned concepts, Definition 7 and Theorem 3 are presented as follows.

Definition 7. A HQSS achieving the minimum access structure $\Gamma_{min} = \{\alpha_1, \alpha_2, \ldots, \alpha_{r_1}\}$ (where $\alpha_{j_1}, j_1 = 1, 2, \ldots, r_1$ is a minimal qualified set of participants) with its maximum adversary structure $\mathbb{A}_{max} = \{\beta_1, \beta_2, \ldots, \beta_{r_2}\}$ (where $\beta_{j_2}, j_2 = 1, 2, \ldots, r_2$ is a maximal unqualified set of participants) among a set of participants $\mathbb{P} = \{P_1, P_2, \ldots, P_{n'}\}$ is said to be dual compressible if only one q-participant with one q-share and all c-participants from $\alpha_{j_1} (j_1 = 1, 2, \ldots, r_1)$ who hold the c-shares with the size of $\frac{l-2}{r_2}$ can share a secret cooperatively.

According to definition 7, we can obtain the following theorem 3. It formalizes the scenario when new participants join in.

Theorem 3. A HQSS achieving the minimum access structure $\Gamma_{min} = \{\alpha_1, \alpha_2, \ldots, \alpha_{r_1}\}$ (where $\alpha_{j_1}, j_1 = 1, 2, \ldots, r_1$, is a minimal qualified set of participants.) among a set of participants $\mathbb{P} = \{P_1, P_2, \ldots, P_{n'}\}$ can be always inflatable (the proof is given in Appendix A).

3.2.2 Notation

In this dual compressible hybrid quantum secret sharing, we use the following notation.

Alice: a trusted dealer who wants to share the corresponding classical bits among the c-participants;

$\mathbb{P}$: $\mathbb{P} = \{P_1, P_2, \ldots, P_{n'}\}$ is the set of all the participants;

c: the corresponding shared classical bits;

Γ_{min}: $\Gamma_{min} = \{\alpha_1, \alpha_2, \ldots, \alpha_{r_1}\}$ is the minimum access structure corresponding to c ;

$\mathbb{A}_{max}$: $\mathbb{A}_{max} = \{\beta_1, \beta_2, \ldots, \beta_{r_2}\}$ is the maximum adversary structure corresponding to c;

$c_1, c_2, \ldots, c_{r_2}$: the pieces of c;

r_2: $r_2 = |\mathbb{A}_{max}|$, that is, the number of elements in $\mathbb{A}_{max}$.

3.2.3 The Alice's phase

The first three steps (1)-(3) in the scheme are the same as those in section 3.1.2 as they just involve Alice and Bob. Steps (4)-(6) are similar that used in,[35] which is as follows:

(4) Alice selects H: a suitable strongly collision-free hash function, which takes as input a binary string of an arbitrary length, and produces as output a binary string of a fixed length q, where q is the length of the pieces of the corresponding classical bits, and computes $H(c_{i_3})$.

(5) Alice computes:

$x_1 = c_1 \oplus H(c_2)$, $x_2 = c_2 \oplus H(c_3)$, ..., $x_{r_2-1} = c_{r_2-1} \oplus H(c_{r_2})$, $x_{r_2} = H(x_1) \oplus H(x_2) \oplus \ldots \oplus H(x_{r_2-1}) \oplus c_{r_2}$.

Then Alice generates $n' - 1$ identical arrays $H_{i_3} = \{x_1, x_2, \ldots, x_{r_2}\}$, for $i_3 = 1, 2, \ldots, n' - 1$.

(6) Alice allocates c-shares in such a way that each participant in $\mathbb{A}_1$ has no secret share x_1, each participant in $\mathbb{A}_2$ has no secret share x_2, ..., and each participant in $\mathbb{A}_{r_2}$ has no secret share x_{r_2}. Then Alice distributes the remaining c-shares in H_{i_3} to the c-participant P_{i_3}, for $i_3 = 1, 2, \ldots, n' - 1$, secretly.

Note that even if the number of participants is large, it is still possible to obtain the minimum access structure and the maximum adversary structure using linear codes (see[36]).

3.2.4 The recovery phase

Suppose a group of participants from α_{j_1} want to recover the secret.

C-participants from α_{j_1} delete the redundant x_{i_3}, for $i_3 = 1, 2, \ldots, r_2$ and compute:

$c_{r_2} = H(x_1) \oplus H(x_2) \oplus \ldots \oplus H(x_{r_2-1}) \oplus x_{r_2}$, $c_{r_2-1} = x_{r-1} \oplus H(c_{r_2})$, ..., $c_2 = x_2 \oplus H(c_3)$, $c_1 = x_1 \oplus H(c_2)$.

So, the c-participants from α_{j_1} recover $c = c_1 \shortparallel c_2 \shortparallel \cdots \shortparallel c_{r_2-1} \shortparallel c_{r_2}$ while the q-participant obtains the transition operation by measuring (h_j, t'_j). Consequently, they can recover the ultimate operation by checking the algorithm build_table, that is, Alice's secret $s_A = \{s_A^1, s_A^2, \ldots, s_A^l\}$.

Likewise, it is worth noting that the dual compressible quantum secret sharing scheme based on adversary structure can be easily converted into a hybrid quantum multi-secret sharing scheme based on adversary structure. The scheme can be realized by just considering every piece of classical bits of a secret in section 3.2 as the classical bits of every single secret.

4. THE FEATURES AND THE SECURITY ANALYSIS OF OUR SCHEME

As is known, on the one hand, classical secret sharing schemes cannot address the problem of eavesdropping and their security is guaranteed by the difficulty of computation, which might be susceptible to the strong ability of quantum computation. Fortunately, quantum secret sharing can address this issue and eavesdropping detection simultaneously. On the other hand, quantum data is much more prohibitive and difficult to cope with than classical data. Hence, we have proposed two dual compressible hybrid quantum secret sharing schemes, which make full use of the advantages of classical secret sharing schemes and quantum secret sharing schemes. These schemes can be surprisingly easy to implement because they just need to perform the correct transition operation on an EPR pair and to allocate the corresponding classical messages. Though collation tables are required in our schemes, this is easily achieved by an algorithm.

Recursive way is used to implement dual compressible hybrid quantum secret sharing based on $((m+1, n'))$ threshold and adversary structure. That is to say, just one q-participant with q-share and at least m c-participants (or all participants from any minimal qualified set with c-shares with the size of $\frac{l-2}{r_2}$) with c-shares with the size of $\frac{l-2}{m-1}$ can share one secret in a secure way. The obvious merit of the schemes is that they can curtail the cost of generating, transmitting and storing EPR pairs and classical bits. Moreover, a hybrid quantum multi-secret sharing scheme can be designed in the same way, i.e., one q-participant and any m or over m c-participants can share $m-1$ secrets simultaneously.

The existing classical secret sharing schemes, whose security is ensured by hard mathematical problems, may be compromised by the advances in computing technology. However, our proposed hybrid quantum secret sharing schemes are free from the strong ability of quantum computation. Because in our hybrid schemes the shared secret is determined by classical data and quantum data simultaneously, that is, the shared secret cannot be obtained by either classical data or quantum data alone. On the other hand, in our hybrid schemes, it is much simpler and faster to allocate quantum secret shares without weakening the security in contrast to quantum secret sharing. Compared with the existing hybrid quantum secret sharing schemes,[28–30] not only does the number of q-participants drop, but also the number of particles needed and the size of c-shares reduce. Most importantly, even if Eve is able to obtain all the classical messages, our proposed schemes are still secure. Because in our schemes, the c-participants do not know the transition operation used by Alice. Then, if these c-participants want to obtain the secret, they have to guess the used transition operation and the basic unitary operation. The probability of a successful guess is $\frac{1}{2^{2n-2}} \times \frac{1}{2^2} = \frac{1}{2^{2n}}$ which is in fact equal to the probability of conventional quantum secret sharing schemes. Moreover, the distribution of q-shares is the same as that in quantum secret sharing schemes. That is to say, the security of transmitting one particle can match that of n particles. Therefore, when conventional quantum secret sharing schemes are secure, our proposed hybrid quantum secret sharing schemes are also secure.

APPENDIX A. THE PROOF FOR THEOREMS

Theorem 1. For any $n \geq 2$, when the 2^{2n} $n-$extended unitary operations are used to transform any one of the Bell states, the final outcomes boil down to the four basic local unitary operations that are used.

Proof. We prove the theorem using induction as follows.

(1) As is shown above, when $n = 2$, the conclusion holds.

(2) Assume that the conclusion holds for $(n-1)-$extended unitary operations. Then $n-$extended unitary operations can be written as follows:

$$U_{\underbrace{0000\cdots0000}_{2n}} = U_{00} \otimes U_{\underbrace{0000\cdots0000}_{2n-2}},$$

$$U_{\underbrace{0000\cdots0001}_{2n}} = U_{00} \otimes U_{\underbrace{0000\cdots0001}_{2n-2}},$$

$\ldots,$

$$U_{\underbrace{1111\cdots1110}_{2n}} = U_{11} \otimes U_{\underbrace{11111\cdots1110}_{2n-2}},$$

$$U_{\underbrace{1111\cdots1111}_{2n}} = U_{11} \otimes U_{\underbrace{1111\cdots1111}_{2n-2}}.$$

Because $(n-1)-$extended unitary operations boil down to the four basic local unitary operations that are used, and then according to Lemma 1, $U_0U_i = U_i, i = 1, 2, 3; U_1U_2 = U_3, U_1U_3 = U_2, U_2U_3 = U_1$. Hence, we can obtain that $n-$extended unitary operations boil down to the four basic local unitary operations that are used as well.

Theorem 2. A $((m+1, n'))$-HQSS can be inflated only conformally, i.e. to threshold schemes having the form $((m+\lambda+1, n'+\lambda))$ where λ ($\lambda \in \mathbb{N}$) are all new c-participants.

Proof. As the given conformally-HQSS meets the no-cloning theorem, then obviously does the $((m+\lambda_m+1, n'+\lambda_{n'}))$-HQSS, where $\lambda_m \geq \lambda_{n'} \geq 0$ and $m+\lambda_m+1 \leq n'+\lambda_{n'}$. Moreover, according to Lemma 1 of Ref,[28] a restriction of the $((m+\lambda_m+1, n'+\lambda_{n'}))$-QTS by λ c-participants necessarily yields a conformally reduced, $((m+\lambda_m+1-\lambda, n'+\lambda_{n'}-\lambda))$-QTS. The restricted scheme has a different access structure from $((m+1, n'))$ unless $\lambda_m = \lambda_{n'} = \lambda$. Hence, just a conformal inflation of $((m+1, n'))$-HQSS is possible, where it is inflated to a $((m+\lambda+1, n'+\lambda))$-HQSS by the addition of λ c-participants.

Theorem 3. A HQSS achieving the minimum access structure $\Gamma_{min} = \{\alpha_1, \alpha_2, \ldots, \alpha_{r_1}\}$ (where $\alpha_{j_1}, j_1 = 1, 2, \ldots, r_1$, is a minimal qualified set of participants.) among a set of participants $\mathbb{P} = \{P_1, P_2, \ldots, P_{n'}\}$ can be always inflatable.

Proof. Suppose that m new c-participants $P_{n'+1}, P_{n'+2}, \ldots, P_{n'+m}$ are added into $\mathbb{P}$ to form $\mathbb{P}' = \{P_1, P_2, \ldots, P_{n'+m}\}$. The new minimum access structure $\Gamma'_{min} = \{\alpha'_1, \alpha'_2, \ldots, \alpha'_{r_1}\}$ can be achieved by adding any new c-participants to any of the $\alpha_{j_1}, j_1 = 1, 2, \ldots, r_1$. The corresponding classical bits are shared among $n'+m-1$ c-participants in terms of the classical scheme performing Γ'. To recover the secret, the q-participant from $\alpha'_{j_1}, j_1 = 1, 2, \ldots, r_1$ can obtain the transition operation and all the c-participants from $\alpha'_{j_1}, j_1 = 1, 2, \ldots, r_1$ can reconstruct the corresponding classical bits. The shared secret is obtained through the q-participant's and c-participants' collaboration. Hence, the new scheme HQSS (Γ') is an inflatable one of the given scheme HQSS (Γ).

APPENDIX B. ALGORITHM FOR BUILD_TABLES

Algorithm: build_tables

Algorithm: build_tables
input: n; **output:** collation table Q

```
for all 2^(2*n) n−extended unitary operations;
   s=cell(1,2^(2*n));
   for i=1:2^(2*n)
        s(i) = {num2str(dec2bin(i−1,2*n))};
        for j=1:n
             str=char(s(i));
             x(j)=bin2dec(str((2*j−1):2*j));
        for j=1:n−1
             [y]=fun(x(j),x(j+1));
             x(j+1)=y;
        z(i)=x(n);
A=sym(zeros(1,2^(2*n−2))); atr=1; B=sym(zeros(1,2^(2*n−2))); btr=1;
C=sym(zeros(1,2^(2*n−2))); ctr=1; D=sym(zeros(1,2^(2*n−2))); dtr=1;
for i=1:2^(2*n)
   if z(i)==0
      A(1,atr)=sym(['U',num2str(dec2bin(i−1,2*n))]);
      atr=atr+1;
  elseif  z(i)==1
      B(1,btr)=sym(['U',num2str(dec2bin(i−1,2*n))]);
      btr=btr+1;
  elseif  z(i)==2
      C(1,ctr)=sym(['U',num2str(dec2bin(i−1,2*n))]);
      ctr=ctr+1;
  elseif  z(i)==3
      D(1,dtr)=sym(['U',num2str(dec2bin(i−1,2*n))]);
      dtr=dtr+1;
P=[A;B;C;D]; M=sym(zeros(4,2^(2*n−2)+1));
for i=1:4
   M(i,1)=sym(['U',num2str(dec2bin(i−1,2))]);
for j=2: 2^(2*n−2)+1
   M(i,j)=P(i,j−1);
Q=sym(zeros(1,2^(2*n−2)+1));
len=length(num2str(dec2bin(2^(2*n−2)−1))); Q(1,1)='BUO';
for j=2:
2^(2*n−2)+1
   Q(1,j)=sym([num2str(dec2bin(j−2,len))]);
return Q
```

APPENDIX C. COLLATION TABLE FOR $N = 3$

Table 2. Collation table for $n = 3$, where BUO denotes basic unitary operation.

BUO	Control bits							
	0000	0001	0010	0011	0100	0101	0110	0111
	1000	1001	1010	1011	1100	1101	1110	1111
U_{00}	U_{000000}	U_{000101}	U_{001010}	U_{001111}	U_{010001}	U_{010100}	U_{011011}	U_{011110}
	U_{100010}	U_{100111}	U_{101000}	U_{101101}	U_{110011}	U_{111001}	U_{110110}	U_{111100}
U_{01}	U_{000001}	U_{000100}	U_{001011}	U_{010101}	U_{011010}	U_{011111}	U_{100011}	U_{100110}
	U_{101001}	U_{101100}	U_{110010}	U_{110111}	U_{111000}	U_{101100}	U_{111101}	U_{010000}
U_{10}	U_{000010}	U_{000111}	U_{111110}	U_{001000}	U_{001101}	U_{010011}	U_{010110}	U_{011001}
	U_{011100}	U_{100000}	U_{100101}	U_{101010}	U_{101111}	U_{110001}	U_{110100}	U_{111011}
U_{11}	U_{000011}	U_{000110}	U_{001001}	U_{001100}	U_{010010}	U_{010111}	U_{011000}	U_{011101}
	U_{100001}	U_{100100}	U_{101011}	U_{101110}	U_{110000}	U_{110101}	U_{111010}	U_{111111}

ACKNOWLEDGMENTS

Hong Lai has been supported in part by an International Macquarie University Research Excellence Scholarship (iMQRES). This work is also supported by the National Basic Research Program of China (973 Program) (Grant No. 2010CB923200), the National Natural Science Foundation of China (No. 61377067). The work is also supported by Fund of State Key Laboratory of Information Photonics and Optical Communications (Beijing University of Posts and Telecommunications), P. R. China.

REFERENCES

[1] Shamir, A., "How to share a secret," *Commun. ACM.* **22 (11)**, 612–613 (1979).
[2] Blakley, G. R., "Safeguarding cryptographic keys," in [*Proceedings of National Computer Conference*], Montvale, N., ed., *AFI-PS Press* **48**, 313–317 (1979).
[3] Hillery, M., B. V. and Berthiaume, A., "Quantum secret sharing," *Phys. Rev. A.* **59**, 1829–1834 (1999).
[4] Cleve, R., G. D. and Lo, H. K., "How to share a quantunm secrte," *Phys. Rev. Lett.* **83**, 648–652 (1999).
[5] Boström, K. and Felbinger, T., "Deterministic secure direct communication using entanglement," *Phys. Rev. Lett.* , 89–93 (2002).
[6] S., B., "Teleportation and secret sharing with pure entangled states," *Phys. Rev. A.* **62**, 012308–012320 (2000).
[7] Tittel, W., Z. H. and Gisin, N., "Experimental demonstration of quantum secret sharing," *Phys. Rev. A.* **63**, 042301–042306 (2001).
[8] D., G., "Theory of quantum secret sharing," *Phys. Rev. A.* **61**, 042311 (2000).
[9] Karlsson, A., K. M. and Imoto, N., "Quantum entanlement for secret sharing and secret splitting," *Phys. Rev. A.* **59**, 162–168 (1999).
[10] Xiao, L., L. G. L. D. F. G. and Pan, J. W., "Efficient multiparty quantum-secret-sharing schemes," *Phys. Rev. A.* **69**, 052307–052311 (2004).
[11] Zhang, Z. J, L. Y. and Man, Z., "Multiparty quantum secret sharing," *Physical Review A* **71**(4), 044301 (2005).
[12] Tokunaga, Y., O. T. and N., I., "quantum cryptography," *Phys. Rev. A.* **71**, 012314–012323 (2005).
[13] Zhang, Z. J. and Man, Z., "Multiparty quantum secret sharing of classical messages based on entanglement swapping," *Phys. Rev. A.* **72**, 022303–022306 (2005).
[14] Benaloh, J. and Leichter, J., "Secret sharing and monotone functions," *Proc. Crypto'88* **27**, 022303–022306 (1990).

[15] Wang, C., e. a., "secure direct communication with high-dimension quantum superdense coding," *Phys. Rev. A.* **71**, 044305 (2005).
[16] Cai, Q.Y., L. B., "Improving the capacity of the *boströem* k-felbinger protocol," *Phys. Rev. A.* **69**, 054301–054303 (2004).
[17] Lin, Q., C. W. H. L. D. Y., "Semiquantum secret sharing using entangled states," *Phys. Rev. A.* **82**, 022303–022308 (2010).
[18] Gheorghiu, V., "Generalized semiquantum secret sharing schemes," *Phys. Rev. A.* **85**, 052309–052319 (2012).
[19] Sarvepalli, P. and Raussendorf, R., "Matroids and quantum-secret-sharing scheme," *Phys. Rev. A.* **81**, 052333–052341 (2010).
[20] Han, L. F., L. Y. M. L. J. Z. Z. J., "Multiparty quantum secret sharing of secure direct communication using single photons," *Optics Communications* **281**, 2690–2694 (2008).
[21] Markham, D. and Sanders, B. C., "Graph states for quantum secret sharing," *arXiv:0808.1532.[quant-ph]* (2011).
[22] Marin, A. and Markham, D., "On the equivalence between sharing quantum and classical secrets and error correct," *arXiv:1205.4182v1 [quant-ph]* (2012).
[23] Dehkordi, M. H. and Fattahi, E., "Threshold quantum secret sharing between multiparty and multiparty using greenberger-horne-zeilinger," *Quantum Inf Process* **12**, 1299–1306 (2013).
[24] Duan, X. J., Z. R. and Li, X., "Efficient fault-tolerant quantum secret sharing over two collective channel," *International Journal of Quantum Inf.* **8**, 1347–1354 (2010).
[25] An, N. B., ", effivtive and flexible multiparty quantum secret sharing," *Commu in Phys* **2**, 65–74 (2008).
[26] Yang, Y. G., J. X. W. H. Y. and Zhang, H., "Verifiable quantum (k, n) threshold secret sharing," *Quantum Inf Process* **11**, 1619–1625 (2012).
[27] Lin, J. and Hwang, T., "New circular quantum secret sharing for remote agents," *Quantum Inf Process* **12**, 685–697 (2013).
[28] Anderson, C. A. N, J. M. Q. and Hideki, I., "Improving quantum secret-sharing schemes," *Phys. Rev. A* **64**, 042311–042515 (2001).
[29] Singh, S. D.and Srikanth, R., "Generalized quantum secret sharing," *Phys. Rev. A* **71**, 012328–012334 (2005).
[30] Fortescue, B. and Gour, G., "Reducing the quantum communication cost of quantum secret sharing," *IEEE Trans on Inf Theory* **58(10)**, 6659–6666 (2012).
[31] Chou, Y. H., C. C. Y. F. R. K. C. H. C. and Lin, F., "Enhanced multiparty quantum secret sharing of classical messages by using engtanglement swapping," *IET* **6(2)**, 84–92 (2011).
[32] Chou, Y. H., C. S. M. L. Y. T. C. C. Y. and Chao, H. C., "Using ghz-state for multiparty quantum secret sharing without code table," *The computer journal advance access* , 1–9 (2012).
[33] Bennett, C. H. and Wiesner, S. J., "Communication via one- and two- particle operators on einstein-podolsky-rosen states," *Phys. Rev. Lett.* **69**, 2881–2884 (1992).
[34] Parakh, A., K. S., "efficient secret sharing for implicit data security," *Inform. Sci.* , 33541 (2011).
[35] Lai, H., X. J. H. L. L. X. and Yang, Y. X., "Recursive hiding of biometrics-based secret sharing scheme using adversary structure," *Information Processing Letters* **112**, 683–687 (2012).
[36] Ding, C. S., K. D. and Ling, S., "Secret sharing with a class of ternary codes," *Theoret. Comput. Sci.* **246**, 285–298 (2000).

PROCEEDINGS OF SPIE

Quantum Information and Computation XII

Eric Donkor
Andrew R. Pirich
Howard E. Brandt
Michael R. Frey
Samuel J. Lomonaco Jr.
John M. Myers
Editors

8–9 May 2014
Baltimore, Maryland, United States

Sponsored and Published by
SPIE

Volume 9123

Proceedings of SPIE 0277-786X, V. 9123

SPIE is an international society advancing an interdisciplinary approach to the science and application of light.

Quantum Information and Computation XII, edited by Eric Donkor, Andrew R. Pirich, Howard E. Brandt, Michael R. Frey, Samuel J. Lomonaco, Jr., John M. Myers, Proc. of SPIE Vol. 9123, 912301

The papers included in this volume were part of the technical conference cited on the cover and title page. Papers were selected and subject to review by the editors and conference program committee. Some conference presentations may not be available for publication. The papers published in these proceedings reflect the work and thoughts of the authors and are published herein as submitted. The publisher is not responsible for the validity of the information or for any outcomes resulting from reliance thereon.

Please use the following format to cite material from this book:
Author(s), "Title of Paper," in *Quantum Information and Computation XII*, edited by Eric Donkor, Andrew R. Pirich, Howard E. Brandt, Michael R. Frey, Samuel J. Lomonaco Jr., John M. Myers, Proceedings of SPIE Vol. 9123 (SPIE, Bellingham, WA, 2014) Article CID Number.

ISSN: 0277-786X
ISBN: 9781628410600

Published by
SPIE
P.O. Box 10, Bellingham, Washington 98227-0010 USA
Telephone +1 360 676 3290 (Pacific Time)· Fax +1 360 647 1445
SPIE.org

Printed in the United States of America.

Publication of record for individual papers is online in the SPIE Digital Library.

SPIEDigitalLibrary.org

Paper Numbering: Proceedings of SPIE follow an e-First publication model, with papers published first online and then in print and on CD-ROM. Papers are published as they are submitted and meet publication criteria. A unique, consistent, permanent citation identifier (CID) number is assigned to each article at the time of the first publication. Utilization of CIDs allows articles to be fully citable as soon as they are published online, and connects the same identifier to all online, print, and electronic versions of the publication. SPIE uses a six-digit CID article numbering system in which:

- The first four digits correspond to the SPIE volume number.
- The last two digits indicate publication order within the volume using a Base 36 numbering system employing both numerals and letters. These two-number sets start with 00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 0A, 0B ... 0Z, followed by 10-1Z, 20-2Z, etc.

The CID Number appears on each page of the manuscript. The complete citation is used on the first page, and an abbreviated version on subsequent pages. Numbers in the index correspond to the last two digits of the six-digit CID Number.

Contents

Conference Committee

Symposium Chair

David A. Whelan, Boeing Defense, Space, and Security (United States)

Symposium Co-chair

Wolfgang Schade, Technische Universität Clausthal (Germany) and Fraunhofer Heinrich-Hertz-Institut (Germany)

Conference Chairs

Eric Donkor, University of Connecticut (United States)
Andrew R. Pirich, ACP Consulting (United States)
Howard E. Brandt, U.S. Army Research Laboratory (United States)

Conference Co-chairs

Michael R. Frey, Bucknell University (United States)
Samuel J. Lomonaco Jr., University of Maryland, Baltimore County (United States)
John M. Myers, Harvard University (United States)

Conference Program Committee

Paul M. Alsing, Air Force Research Laboratory (United States)
Chip Brig Elliott, Raytheon BBN Technologies (United States)
Reinhard K. Erdmann, Air Force Research Laboratory (United States)
Michael L. Fanto, Air Force Research Laboratory (United States)
Michael J. Hayduk, Air Force Research Laboratory (United States)
Louis H. Kauffman, University of Illinois at Chicago (United States)
Vladimir E. Korepin, Stony Brook University (United States)
Alexander V. Sergienko, Boston University (United States)
Tai Tsun Wu, Harvard University (United States)

Session Chairs

1 QKD, Cryptography I
Paul M. Alsing, Air Force Research Laboratory (United States)
Louis H. Kauffman, University of Illinois at Chicago (United States)

2 QKD, Cryptography II
Michael R. Frey, Bucknell University (United States)
Paul M. Alsing, Air Force Research Laboratory (United States)