基于密集编码的多方与多方量子秘密共享

杜宇韬[①②] 鲍皖苏*[①] 管文强[②] 周 淳[①] 付向群[①]
[①](解放军信息工程大学 郑州 450004)
[②](解放军 72850 部队 济南 250031)

摘 要：该文针对多方与多方之间的秘密共享问题，通过对 Bell 态的两个粒子分别进行相位旋转局域操作，以及 Pauli 变换与 Hadamard 变换、I 变换之一复合的局域操作，基于密集编码思想提出一种新的多方与多方量子秘密共享协议。该协议不仅可以抵抗现有的攻击策略如密集编码攻击、纠缠交换攻击等，还可以抵抗代理成员的欺骗攻击，即具备可验证功能。同时，该协议还具有高效率、可动态更新子秘密和增减代理成员等特点。

关键词：密码学；量子秘密共享；密集编码；可验证
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2013)11-2623-07
DOI: 10.3724/SP.J.1146.2013.00164

Multiparty-to-multiparty Quantum Secret Sharing Based on Dense-coding

Du Yu-tao[①②] Bao Wan-su[①] Guan Wen-qiang[②] Zhou Chun[①] Fu Xiang-qun[①]
[①](*PLA Information Engineering University*, *Zhengzhou* 450004, *China*)
[②](*Unit* 72850 *of the PLA*, *Ji'nan* 250031, *China*)

Abstract: To solve the problem of secret sharing between multiparty and multiparty, a new multiparty-to-multiparty quantum secret sharing protocol is proposed based on dense-coding. It performs different local operations on different photons of the Bell state, choosing separately from the random phase shift operations and the combinations of Pauli operations and either Hadamard operation or I operation. This protocol can resist not only the existing attacks such as the dense-coding attack and the entanglement-swapping attack, but also the cheating attack from the agent, which is viewed as verifiability. Meanwhile, the protocol is also high-efficient and can change the sub-secrets and the group of agents dynamically.

Key words: Cryptography; Quantum Secret Sharing (QSS); Dense-coding; Verifiability

1 引言

量子秘密共享(Quantum Secret Sharing, QSS)是量子密码的一个重要研究方向，它允许分发者利用量子资源将秘密信息拆分为若干份子秘密发送给多个代理成员，只有被授权的成员组合才能恢复该秘密；或者多个代理成员可利用量子资源将各自的子秘密发送给分发者进行秘密合成，从而使双方建立起共同的秘密信息。1999 年，Hillery 等人[1]利用 GHZ 态提出了第 1 个 QSS 协议，首次将秘密共享引入到量子密码领域，并且基于量子力学原理提高了秘密共享的安全性。此后各类QSS协议层出不穷，相关研究在理论与实验上均取得了诸多重要的成果[2−10]。

QSS 的理论研究分为设计与分析两个方向，二者相辅相成。在设计方面，其研究目标是设计安全、高效和易于实现的QSS协议。根据不同的应用场景，QSS 协议可以有多种分类。例如按照秘密信息的类型，QSS 协议可分为共享经典信息[1,3−10]和共享量子态信息[1,2]两种；按照秘密分发者的数目，QSS 协议可分为一方与多方[1−5]和多方与多方[6−10]两种。在分析方面，其研究目标主要是针对现有 QSS 协议存在的安全性漏洞提出各种攻击策略，使得攻击者可以在不引入错误的情况下得到部分或全部的秘密信息。由于不同的 QSS 协议可能出现不同的缺陷，因此相应的攻击策略也是多种多样的。毫无疑问，一个安全的 QSS 协议必须经得起各种攻击策略的考验。

2005 年，Yan 等人[6]基于单光子提出一种多方与多方 QSS 协议，实现了群组间的秘密共享：A 组成员共同创造一个秘密信息 M 发送给 B 组成员，后者只有在全体成员合作的情况下才可以恢复出该秘密。此后，各种多方与多方的 QSS 协议被相继提出[7−10]，而针对此类协议的攻击策略也陆续出

2013-01-29 收到，2013-04-15 改回
*通信作者：鲍皖苏 2010thzz@sina.com

现[11−14]。在设计方面，目前此类协议主要有基于单光子[6−9,11−13]与基于Bell态和Bell测量[10,14]两种实现方式。前者的编码效率不高，对 1 个量子比特的编码操作只能传输 1 bit 经典信息；后者的量子态利用率较低，例如 n 方与 m 方之间共享 2 bit 经典信息需要消耗 $n+m$ 对 Bell 态。此外，具备参数动态更新功能的 QSS 已成为新的研究热点[15]，而现有的多方与多方QSS协议均不能更新子秘密或者增减代理成员。在分析方面，针对此类协议的攻击策略主要有截获重发攻击、纠缠交换攻击[16]和密集编码攻击[17]等。此外，一种成员欺骗攻击[18]引起了人们的关注：不诚实者 Eve 在恢复秘密时可提供假的子秘密，使得其它成员无法恢复出秘密信息，而他自己可利用真的子秘密纠错而独自得到秘密。只有具备可验证功能的QSS协议[18]可通过验证子秘密是否真实来抵抗此类攻击策略，而现有的多方与多方 QSS 协议尚不具备该功能。

本文通过对 Bell 态的两个粒子分别进行相位旋转局域操作以及 Pauli 变换与 Hadamard 变换、I 变换之一复合的局域操作，并且基于密集编码思想[19]提出了一种对经典信息的多方与多方 QSS 协议。在安全性方面，由于不需回传粒子给 A 组成员且 B 组的相位旋转操作集合 $S=\{\boldsymbol{U}(0),\boldsymbol{U}(2\pi/3),\boldsymbol{U}(4\pi/3)\}$ 可限制内部攻击者的假操作声明，因此该协议可抵抗纠缠交换攻击；由于 B 组所使用酉操作集合 S 的元素对 Bell 态一个粒子进行不同的局域操作，其结果两两非正交而不能可靠区分[20]，从而使密集编码攻击失效；由于不诚实者 Eve 进行欺骗攻击时无法从错误的测量结果中恢复出秘密，因此该协议具备可验证功能。在性能方面，由于采用了密集编码思想，该协议可通过对 1 个量子比特的编码传输 2 bit 经典信息，并且在 n 方与 m 方之间共享 2 bit 经典信息只需消耗一对 Bell 态，从而显著地提高了协议效率；由于对 Bell 态的两个粒子分别进行的局域操作彼此独立，该协议可动态地更新子秘密和增减代理成员。

2 协议描述

设成员组 $A=\{\text{Alice}_1,\text{Alice}_2,\cdots,\text{Alice}_n\}$，成员组 $B=\{\text{Bob}_1,\text{Bob}_2,\cdots,\text{Bob}_m\}$。$A$ 组成员共同创造出秘密信息 M，协议目的是将该秘密传递给 B 组，并使得只有当 B 组全体成员合作时才可恢复出秘密，而各组中的部分成员或者两组的部分成员联合起来均无法得到该秘密。本协议不考虑信道损耗。具体步骤为：

(1) A 组的 Alice_1 从 $\left\{\left|\phi^+\right\rangle,\left|\phi^-\right\rangle,\left|\psi^+\right\rangle,\left|\psi^-\right\rangle\right\}$ 中随机选择制备 k 对 Bell 态 $\left|\varphi_1\right\rangle_{th},\left|\varphi_2\right\rangle_{th},\cdots,\left|\varphi_k\right\rangle_{th}$，并将每个 Bell 态中的粒子 t 组成 T 序列，粒子 h 组成 H 序列(粒子的对应顺序一致)。之后 Alice_1 存储 H 序列，而将 T 序列发送给 B 组的 Bob_1。其中

$$\left|\phi^{\pm}\right\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle),\quad \left|\psi^{\pm}\right\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle) \tag{1}$$

(2) Bob_1 收到 T 序列后，首先使用光子数目分离器(Photon Number Splitter, PNS: 50=50)或光子分束器(Photon Beam Splitter, PBS: 50=50)，检测是否存在多粒子攻击；使用特定波长的滤波器或者隔离器，检测是否存在不可见光子攻击[8]。如果存在以上攻击则协议中止，反之继续。确定 T 序列均为单光子后，Bob_1 从相位旋转操作集合 $S=\{\boldsymbol{U}(0),\boldsymbol{U}(2\pi/3),\boldsymbol{U}(4\pi/3)\}$ 中随机选择 $\boldsymbol{U}(\alpha)$ 对 T 序列的粒子分别实施操作得到 T_1 序列，并记录操作信息作为其子秘密。其中

$$\boldsymbol{U}(\alpha)=\begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix},\quad \alpha\in\left\{0,\frac{2\pi}{3},\frac{4\pi}{3}\right\} \tag{2}$$

操作结束后，Bob_1 将 T_1 序列发送给 Bob_2。

(3)如图 1 所示，$\text{Bob}_j(j=2,\cdots,m)$ 与 Bob_1 类似地对 T_{j-1} 序列的粒子进行操作，之后发送给 Bob_{j+1}。当 Bob_m 操作完毕后，存储 T_m 序列，并通过经典信道告知 Alice_1：B 组全体成员操作完毕。

(4) Alice_1 得到通知后，生成一组二进制数 $M_1=(m_1^1,m_1^2,\cdots,m_1^{2l})$，其中 $l\le k$。按照连续两个字符 (m_1^{2f-1},m_1^{2f}) (其中 $f=1,2,\cdots,l$)为一组依次对 H 序列的粒子用 Pauli 变换 $\{I,\sigma_z,\sigma_x,i\sigma_y\}$ 进行编码操作："00"对应 I，"01"对应 σ_z，"10"对应 σ_x，"11"对应 $i\sigma_y$。之后 Alice_1 再随机选择 I 变换或 Hadamard 变换(简称 H 变换)对其进行基变换得到 H_1 序列并记录其操作信息。其中

$$\left.\begin{aligned}&I=|0\rangle\langle0|+|1\rangle\langle1|,\quad \sigma_z=|0\rangle\langle0|-|1\rangle\langle1|\\ &\sigma_x=|1\rangle\langle0|+|0\rangle\langle1|,\quad i\sigma_y=|0\rangle\langle1|-|1\rangle\langle0|\\ &H=\frac{1}{\sqrt{2}}(|0\rangle\langle0|-|1\rangle\langle1|+|0\rangle\langle1|+|1\rangle\langle0|)\end{aligned}\right\} \tag{3}$$

Alice_1 操作完毕后，将 H_1 序列发送给 Alice_2。

(5)收到 $\text{Alice}_{i-1}(i=2,\cdots,n)$ 发来的 H_{i-1} 序列后，Alice_i 先确定其是否为单光子序列(同样使用光子数目分离器等设备)。检测通过后，Alice_i 也生成一组二进制数 $M_i=(m_i^1,m_i^2,\cdots,m_i^{2l})$，与 Alice_1 类似地对 H_{i-1} 序列的粒子进行编码操作以及基变换并记录其操作信息，之后将 H_i 序列发送给 Alice_{i+1}。当 Alice_n 操作完毕后，秘密 M 作为 A 组全体成员复合操作信息的一部分已经生成。设 A 组全体成员对 H 序列的

第 f 个粒子 h^f ($f=1,2,\cdots,l$)的复合操作为 $\boldsymbol{N}^f$，易知 $\boldsymbol{N}^f \in \{I,\sigma_z,\sigma_x,i\sigma_y,H,H\cdot\sigma_z,H\cdot\sigma_x,H\cdot i\sigma_y\}$。对该集合的元素进行二进制编码：

在表 1 中，元素编码的左边 1 bit 表示 A 组成员的基变换信息：当 A 组全体成员对粒子 h^f 实施 H 变换的次数是偶数时为 0，是奇数时为 1。而后 2 bit 就是 A 组成员所共同生成的秘密信息 $M^f=(m^{2f-1},m^{2f})$。因此 $M=(M^1,M^2,\cdots,M^l)=(m^1,m^2,\cdots,m^{2l})$。之后，$\text{Alice}_n$ 将 H_n 序列发送给 Bob_m。

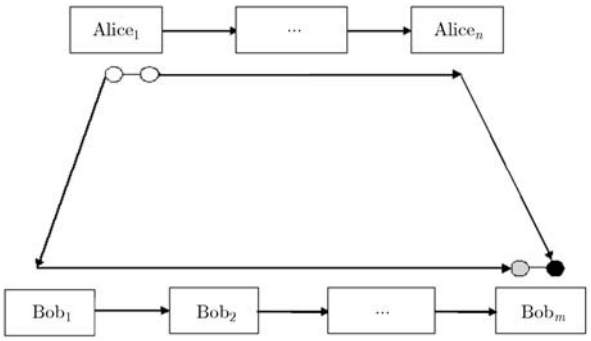
表 1 A 组成员的复合操作编码表

I	σ_z	σ_x	$i\sigma_y$	H	$H\cdot\sigma_z$	$H\cdot\sigma_x$	$H\cdot i\sigma_y$
000	001	010	011	100	101	110	111

(6) Bob_m 收到 H_n 序列后，首先由全体 B 组成员和 A 组成员一道进行窃听检测。首先，B 组成员让 Bob_m 将手中的 T_m 序列和 H_n 序列发给某个随机指定的成员 $\text{Bob}_j(j=1,2,\cdots,m)$，并任选 k_1 个位置要求 A 组公布其对 H_n 序列相应粒子的基变换信息。之后，Bob_j 汇总对 T_m 序列相应粒子的全部操作记录以推算出其复合操作，从而对其粒子实施逆操作；同时根据 A 组的反馈，对 H_n 序列的相应粒子进行基变换操作(当 A 组成员所实施 H 变换的次数为奇数时执行 H 变换；为偶数时执行 I 变换)。最后，Bob_j 在 Bell 基 $\left\{\left|\phi^+\right\rangle,\left|\phi^-\right\rangle,\left|\psi^+\right\rangle,\left|\psi^-\right\rangle\right\}$ 下对 T_m 序列和 H_n 序列中相应位置的粒子进行联合测量，并将测量结果返回 A 组。A 组成员再根据其结果与手中的信息，判断 H 序列在传输过程中是否存在攻击行为。存在则中止协议；反之则 Alice_1 公布所有 Bell 态的初态信息，同时 A 组全体成员公布其基变换信息。

恢复秘密时，B 组成员可随机指定 $\text{Bob}_j(j=1,\cdots,m)$ 收集其它成员的操作记录从而对 T_m 序列的剩余粒子进行相应的逆复合操作；同时根据 A 组的反馈对 H_n 序列的剩余粒子作基变换操作(同上)。之后 Bob_j 在 Bell 基下对两个序列对应位置的粒子进行联合测量，根据所有的测量结果与初态信息，推断出 A 组成员所生成的秘密信息 M。

下面给出该协议结构示意图，如图 1 所示。



表示 Alice_1 所制备的 Bell 态

表示 B 组成员与 A 组成员对该 Bell 态的两个粒子分别进行相位旋转局域操作(对左侧粒子)和编码操作与基变换操作复合的局域操作(对右侧粒子)后所得的新纠缠态

图 1 基于密集编码的 n 方与 m 方 QSS 协议结构图

3　正确性分析

本协议的整个过程可分为以下 3 个阶段：一是预计算阶段(包括步骤(1), (2), (3)), B 组成员从集合 S 中随机选择对 T 序列的粒子实施相位旋转操作。二是秘密生成阶段(包括步骤(4), (5)), A 组成员依次对 H 序列的粒子进行编码操作和基变换操作，从而生成秘密信息。三是秘密恢复阶段(即步骤(6))，B 组成员分别对 T_m 序列和 H_n 序列的粒子进行逆变换，最后在 Bell 基下对两个序列的对应粒子进行联合测量，从而得到 A 组的秘密。下面分析本协议的正确性。

不妨设 Alice_1 所制备的 Bell 态为 $\left|\phi^+\right\rangle_{th}$。在预计算阶段，当 Alice_1 将粒子 t 传递给 B 组成员后，设 $\text{Bob}_j(j=1,\cdots,m)$ 对其实施的相位旋转操作为 $\boldsymbol{U}_j\in S=\{\boldsymbol{U}(0),\boldsymbol{U}(2\pi/3),\boldsymbol{U}(4\pi/3)\}$。当 B 组全体成员操作完毕后，整个 Bell 态变化为

$$\prod_{j=1}^{m}(\boldsymbol{U}_j\otimes I)\left|\phi^+\right\rangle_{th}=(\boldsymbol{U}\otimes I)\left|\phi^+\right\rangle_{th} \tag{4}$$

其中 $\boldsymbol{U}=\prod_{j=1}^{m}\boldsymbol{U}_j$。

在秘密生成阶段，设 A 组的 $\text{Alice}_i(i=1,\cdots,n)$ 对粒子 h 所实施的 Pauli 变换与基变换(随机选择 I 变换或 H 变换)的复合操作为 $\boldsymbol{N}_i\in\{I,\sigma_z,\sigma_x,i\sigma_y,H,H\cdot\sigma_z,H\cdot\sigma_x,H\cdot i\sigma_y\}$。当 A 组全体成员操作完毕后，新纠缠态变化为

$$\begin{aligned}&\prod_{i=1}^{n}(I\otimes\boldsymbol{N}_i)\cdot(\boldsymbol{U}\otimes I)|\phi^+\rangle_{th}\\&\quad=(\boldsymbol{U}\otimes\prod_{i=1}^{n}\boldsymbol{N}_i)\phi^+\rangle_{th}=(\boldsymbol{U}\otimes\boldsymbol{N})\left|\phi^+\right\rangle_{th}\end{aligned} \tag{5}$$

其中 $\boldsymbol{N}=\prod_{i=1}^{n}\boldsymbol{N}_i$。

易知集合 $\{I,\sigma_z,\sigma_x,i\sigma_y,H,H\cdot\sigma_z,H\cdot\sigma_x,H\cdot i\sigma_y\}$ 对复合运算封闭(不考虑整体符号)，因此 A 组全体成员的复合操作 N 也属于该集合。根据表 1 可知，N 的二进制编码中左边 1 bit 表示 A 组成员的基变换信息，而后 2 bit 表示 A 组成员所共同生成的秘密信息 M。当 A 组成员需要恢复出 M 时，可指定一人汇总每个成员的复合操作信息 $\boldsymbol{N}_i(i=1,\cdots,n)$，

按照原先的操作顺序作乘法得到 N，再查表 1 即可得到。而当 B 组成员需要恢复出 M 时，他们可进行相应的酉操作和测量，根据其测量结果和 Alice_1 公布的初态信息，推断出对应的 Pauli 操作，再根据编码规则得到 M。下面证明这两种方式所得到的结果一致。

在秘密恢复阶段，B 组成员首先对粒子 t 实施逆复合操作 $\boldsymbol{U}^{-1}$。设 $\text{Bob}_j(j=1,\cdots,m)$ 的逆相位旋转操作为 $\boldsymbol{U}_j^{-1}$，其中 $\boldsymbol{U}_j^{-1}\cdot\boldsymbol{U}_j=I$。由于相位旋转操作集合 S 对复合运算构成交换群：设 $\forall\alpha,\beta\in\{0,2\pi/3,4\pi/3\}$，易知 $\boldsymbol{U}(\alpha)\cdot\boldsymbol{U}(\beta)=\boldsymbol{U}(\beta)\cdot\boldsymbol{U}(\alpha)=\boldsymbol{U}(\alpha+\beta)$，$\boldsymbol{U}(0)=I$ 是其单位元，且 $\boldsymbol{U}^{-1}(\alpha)\in S$。因此，新纠缠态可表示为

$$(\boldsymbol{U}^{-1}\otimes I)\cdot(\boldsymbol{U}\otimes\boldsymbol{N})\left|\phi^+\right\rangle_{th}=(\prod_{j=1}^{m}(\boldsymbol{U}_j^{-1}\cdot\boldsymbol{U}_j)\otimes\boldsymbol{N})\left|\phi^+\right\rangle_{th}=(I\otimes\boldsymbol{N})\left|\phi^+\right\rangle_{th}\quad(6)$$

之后 B 组成员将该纠缠态恢复到 Bell 基下。根据式(6)，此时纠缠态上只有 A 组全体成员的复合操作 N。设对 $\left|\phi^+\right\rangle_{th}$ 的粒子 h 的操作为 $\boldsymbol{N}\in\{I,\sigma_z,\sigma_x,i\sigma_y,H,H\cdot\sigma_z,H\cdot\sigma_x,H\cdot i\sigma_y\}$ 时，新纠缠态相应地处于 $\left\{\left|\phi^+\right\rangle_{th},\left|\phi^-\right\rangle_{th},\left|\psi^+\right\rangle_{th},\left|\psi^-\right\rangle_{th},|\xi\rangle_{th},|\eta\rangle_{th},|\chi\rangle_{th},|\varsigma\rangle_{th}\right\}$ 之一。收到 A 组成员的基变换信息后，B 组成员可根据其奇偶性判断出 A 组的复合操作 N 属于 $\{I,\sigma_z,\sigma_x,i\sigma_y\}$ 或 $\{H,H\cdot\sigma_z,H\cdot\sigma_x,H\cdot i\sigma_y\}$，从而进行相应的基变换操作：当 A 组成员实施 H 变换次数为偶数时，纠缠态处于 $\left\{\left|\phi^+\right\rangle_{th},\left|\phi^-\right\rangle_{th},\left|\psi^+\right\rangle_{th},\left|\psi^-\right\rangle_{th}\right\}$ 之一，执行 I 变换；当其为奇数时，纠缠态处于以下状态之一：

$$\left.\begin{aligned}|\xi\rangle_{th}&=(I\otimes H)\left|\phi^+\right\rangle_{th},\ |\eta\rangle_{th}=(I\otimes H)\left|\phi^-\right\rangle_{th}\\|\chi\rangle_{th}&=(I\otimes H)\left|\psi^+\right\rangle_{th},\ |\varsigma\rangle_{th}=(I\otimes H)\left|\psi^-\right\rangle_{th}\end{aligned}\right\}\quad(7)$$

此时再对粒子 h 执行 H 变换。从而将该纠缠态恢复到 Bell 基 $\left\{\left|\phi^+\right\rangle,\left|\phi^-\right\rangle,\left|\psi^+\right\rangle,\left|\psi^-\right\rangle\right\}$ 下。

最后 B 组成员在 Bell 基下对纠缠态进行联合测量，根据 Alice_1 提供的初态信息 $\left|\phi^+\right\rangle_{th}$ 与 4 种可能的测量结果 $\left\{\left|\phi^+\right\rangle_{th},\left|\phi^-\right\rangle_{th},\left|\psi^+\right\rangle_{th},\left|\psi^-\right\rangle_{th}\right\}$，推断出对应的 Pauli 变换 $\{I,\sigma_z,\sigma_x,i\sigma_y\}$，例如 $(I\otimes\sigma_z)\left|\phi^+\right\rangle=\left|\phi^-\right\rangle$。再根据编码规则：$I$ 对应“00”，σ_z 对应“01”，σ_x 对应“10”，$i\sigma_y$ 对应“11”，B 组成员可得到 2 bit 经典信息(00, 01, 10 或 11)。从表 1 中可知，该结果就是 A 组成员所共同生成的秘密 M。因此，两组成员用不同方式恢复出的秘密信息完全相同。

4 安全性分析

对 QSS 协议的安全性分析，既要考虑外部窃听者的攻击行为，也要考虑内部攻击者的威胁。本文对攻击者的能力规定为：攻击者只受到量子力学基本原理的约束，其计算能力无限，可截获但无法修改协议中传递的经典信息。

此外，QSS 协议的安全性根本上取决于两个条件[20]：一是代理成员的酉操作信息(即子秘密)不可泄漏；二是未授权的成员组合对秘密信息不可恢复。因此，只要能确保子秘密与秘密信息的安全性，QSS 协议就是安全的[20]。本协议已利用光子分束器等设备排除了从现实设施存在漏洞出发的各种攻击手段，因此下面将从理论角度入手分别分析子秘密和秘密信息的安全性。

4.1 子秘密的安全性

对子秘密进行攻击的理论基础为：攻击者可通过测量来区分不同酉操作下的量子态，从而窃取代理成员的酉操作信息，即其子秘密。其中典型的攻击策略有附加粒子纠缠攻击[16]、密集编码攻击[17]等。由于前者会引入错误被窃听检测环节所察觉，因此下面对后一种攻击策略进行分析。

抗密集编码攻击性 在密集编码攻击策略[17]中，内部或外部攻击者 Eve 可截获从 Alice_i(或 Bob_j)处发送给 Alice_{i+1}(或 Bob_{j+1})的 H 序列(或 T 序列)，并用自行伪造的 Bell 态的一个粒子组成的 H' 序列(或 T' 序列)进行替换并照常发送。当 Alice_{i+1}(或 Bob_{j+1})对 H' 序列(或 T' 序列)操作完毕并发送给下一名成员时，Eve 再将其截获并联合伪造 Bell 态的另一组粒子进行投影测量。根据测量结果 Eve 对原 H 序列(或 T 序列)做相同的酉操作并发送给下一名成员。此时，Eve 可在不被察觉的前提下成功获取 Alice_{i+1}(或 Bob_{j+1})的子秘密信息。

本协议可以抵抗此类攻击策略。文献[4]已经证明了对 Bell 态的粒子 t 进行 Pauli 变换与 H 变换、I 变换之一复合的局域操作，所得的量子态非正交，不能通过投影测量进行区分。因此，A 组成员对 Bell 态的粒子 h 进行不同的酉操作，其结果也不可区分。下面证明 B 组成员对 Bell 态的粒子 t 进行不同的酉操作，其结果同样不能通过投影测量进行区分。

定理 相位旋转操作集合 $S=\{\boldsymbol{U}(0),\boldsymbol{U}(2\pi/3),\boldsymbol{U}(4\pi/3)\}$ 中的元素分别作用在 $\left\{\left|\phi^+\right\rangle,\left|\phi^-\right\rangle,\left|\psi^+\right\rangle,\left|\psi^-\right\rangle\right\}$ 中任意 Bell 态的一个粒子上，所得量子态在投影测量下不可区分。

证明 以 $\left|\phi^+\right\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$ 为例，对其第 1

个粒子用集合 S 的元素分别进行操作：

$$\boldsymbol{U}(\alpha)\otimes I\left|\phi^+\right\rangle=\frac{1}{\sqrt{2}}(\cos\alpha|00\rangle-\sin\alpha|01\rangle+\sin\alpha|10\rangle+\cos\alpha|11\rangle) \tag{8}$$

当 $\alpha=0$ 时，

$$\boldsymbol{U}(0)\otimes I\left|\phi^+\right\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)=\left|\phi^+\right\rangle \tag{9}$$

当 $\alpha=\frac{2}{3}\pi$ 时，

$$\begin{aligned}&\boldsymbol{U}\left(\frac{2}{3}\pi\right)\otimes I|\phi^+\rangle\\&=\frac{1}{\sqrt{2}}\left(\frac{1}{2}|00\rangle+\frac{\sqrt{3}}{2}|01\rangle-\frac{\sqrt{3}}{2}|10\rangle+\frac{1}{2}|11\rangle\right)\\&=\frac{1}{2}\left|\phi^+\right\rangle+\frac{\sqrt{3}}{2}\left|\psi^-\right\rangle\triangleq|\delta\rangle\end{aligned} \tag{10}$$

当 $\alpha=\frac{4}{3}\pi$ 时，

$$\begin{aligned}&\boldsymbol{U}\left(\frac{4}{3}\pi\right)\otimes I|\phi^+\rangle\\&=\frac{1}{\sqrt{2}}\left(\frac{1}{2}|00\rangle-\frac{\sqrt{3}}{2}|01\rangle+\frac{\sqrt{3}}{2}|10\rangle+\frac{1}{2}|11\rangle\right)\\&=\frac{1}{2}\left|\phi^+\right\rangle-\frac{\sqrt{3}}{2}\left|\psi^-\right\rangle\triangleq|\beta\rangle\end{aligned} \tag{11}$$

而这 3 个 Bell 态两两内积均非零：

$$\left|\langle\delta|\beta\rangle\right|=\left|\left\langle\delta\middle|\phi^+\right\rangle\right|=\left|\left\langle\phi^+\middle|\beta\right\rangle\right|=\frac{1}{2}\neq0 \tag{12}$$

由于其两两非正交，无法通过投影测量进行区分。对 $\left|\phi^-\right\rangle,\left|\psi^+\right\rangle$ 和 $\left|\psi^-\right\rangle$ 的操作结果同理可证。

证毕

值得一提的是，如果将其中的投影测量换成 POVM 测量，则攻击者可无误地区分非正交的量子态。然而这种无误性是以一定概率得不到任何信息为代价的。同时该攻击行为在窃听检测中会引入一定概率的错误，从而无法通过检测。因此，攻击者对子秘密的攻击无法成功。

4.2 秘密信息的安全性

对秘密信息的攻击策略主要有 3 类：一是截获重发攻击[16]，二是纠缠交换攻击[16]，三是子秘密欺骗攻击[18]。其中第 1 类攻击(包括两组部分成员联合的情况)在窃听检测中可被察觉，下面只对后两类进行分析。

4.2.1 抗纠缠交换攻击性　在纠缠交换攻击策略[16]中，内部攻击者 Eve(或成员组合)可截获协议中的传输粒子(称为粒子 t)，并利用自行伪造的 Bell 态(例如 $\left|\psi^-\right\rangle_{t'h'}$)的粒子 t' 替换其发送给分发方。当分发方将秘密编码在粒子 t' 上发送回代理方时，Eve 与接收粒子 t' 的代理成员合谋或者直接将粒子 t' 截获，联合 $\left|\psi^-\right\rangle_{t'h'}$ 的另一个粒子 h' 进行 Bell 测量，从而窃取秘密信息。当窃听检测时，Eve 对粒子 t 和粒子 h' 进行 Bell 测量，利用纠缠交换原理宣布恰当的假操作即可通过检测。这种攻击策略简单而高效，往往能使攻击者获得全部秘密而不被发现。

纠缠交换攻击成功的条件有二：一是协议要求代理方将粒子 t 在操作后传回分发者手中，从而内部攻击者可以发送假粒子 t' 进行替换；二是内部攻击者所宣布的假操作包含在协议约定的酉操作集合中，使其谎言能够通过窃听检测。因此，抵抗纠缠交换攻击的有效手段也有两种：一是修改 QSS 协议的结构，不让粒子 t 回传到分发者处，使得攻击者无法进行假粒子替换；二是限制内部攻击者的操作声明，使其无法通过宣布假操作而逃脱检测[20]：设假操作集合为 S'，原协议约定的酉操作集合 S 的所有元素及其可能的乘积构成群(S)，则有 $S'\not\subset(S)$。

本协议采用了新的结构，A 组成员不要求 B 组成员回传粒子 t，并且在窃听检测通过后才公布初态信息；同时 B 组成员选用的相位旋转操作集合 $\{\boldsymbol{U}(0),\boldsymbol{U}(2\pi/3),\boldsymbol{U}(4\pi/3)\}$ 可有效限制内部攻击者的操作声明[20]。因此，B 组中不诚实者将无法通过发送假粒子和声明假操作来骗取 A 组的秘密，从而杜绝了纠缠交换攻击发生的可能性。因此本协议可以抵抗纠缠交换攻击。

4.2.2 抗成员欺骗攻击性　成员欺骗攻击[18]是指：在秘密恢复阶段，不诚实者 Eve 提供假的子秘密使得秘密无法正确恢复，而她可以利用真的子秘密纠错，从而独自得到秘密。目前大多数 QSS 协议[1–13]均无法抵抗这种攻击策略，通常是假定参与者诚实执行协议而没有欺骗。只有具有可验证功能的 QSS 协议[18]可通过验证子秘密是否真实来抵抗此类攻击策略，而现有的多方与多方 QSS 协议尚不具备该功能。

本协议所采用的相位旋转操作集合 $\{\boldsymbol{U}(0),\boldsymbol{U}(2\pi/3),\boldsymbol{U}(4\pi/3)\}$，可起到抵抗 B 组不诚实者的欺骗攻击的作用。不妨设 Alice_1 所制备的 Bell 态为 $\left|\phi^+\right\rangle_{th}$，Eve 是 B 组的不诚实者，她在预计算阶段对粒子 t 的操作为 $\boldsymbol{U}(\alpha)\in\{\boldsymbol{U}(0),\boldsymbol{U}(2\pi/3),\boldsymbol{U}(4\pi/3)\}$。而在秘密恢复阶段，她提供错误的逆操作 $\boldsymbol{U}(\beta)\neq\boldsymbol{U}^{-1}(\alpha)$。假设协议中其他成员均诚实操作，当 B 组成员对粒子 h 作基变换操作后，整个纠缠态变化为

$$(\boldsymbol{U}(\beta)\cdot\boldsymbol{U}(\alpha)\otimes\boldsymbol{N}')\left|\phi^+\right\rangle_{th}\neq(I\otimes\boldsymbol{N}')\left|\phi^+\right\rangle_{th},\quad\boldsymbol{N}'\in\{I,\sigma_x,\sigma_z,i\sigma_y\} \tag{13}$$

此时，该纠缠态处于 $\left\{\left(\left|\phi^+\right\rangle+\sqrt{3}\left|\psi^-\right\rangle\right)\middle/2,\ \left(\left|\phi^-\right\rangle+\sqrt{3}\left|\psi^+\right\rangle\right)\middle/2,\ \left(\left|\psi^-\right\rangle+\sqrt{3}\left|\phi^+\right\rangle\right)\middle/2,\left(\left|\psi^+\right\rangle+\sqrt{3}\left|\phi^-\right\rangle\right)\middle/2\right\}$

或 $\left\{\left(\left|\phi^+\right\rangle-\sqrt{3}\left|\psi^-\right\rangle\right)/2,\ \left(\left|\phi^-\right\rangle-\sqrt{3}\left|\psi^+\right\rangle\right)/2,\ \left(\left|\psi^-\right\rangle-\sqrt{3}\left|\phi^+\right\rangle\right)/2,\left(\left|\psi^+\right\rangle-\sqrt{3}\left|\phi^-\right\rangle\right)/2\right\}$ 下，显然这两组基与 Bell 基并不正交。根据测不准原理，B 组成员进行 Bell 测量后其结果必然出现错误。如果该错误出现在窃听检测中，则协议中止；即使在检测中未出现，Eve 也无法从随机分布的错误结果中恢复出秘密。因此本协议具备可验证功能。

5 性能分析

5.1 高效性

相比现有的多方与多方 QSS 协议，本协议提高了编码效率和量子态资源利用率，整体上提高了协议的执行效率。

首先，本协议采用了密集编码思想，可通过对 1 个量子比特的操作传输 2 bit 经典信息。而已有的基于单光子的 n 方与 m 方 QSS 协议[6−9,11−13]中，对 1 个量子比特的操作只能传输 1 bit 经典信息，因此本协议更为高效。

其次，本协议的量子态利用率比已有的多方与多方 QSS 协议更高。对于基于 Bell 态和 Bell 测量的 n 方与 m 方 QSS 协议[10]而言，前者传输 2 bit 经典信息需要消耗 $m+n$ 对 Bell 态，而本协议只需要 1 对。另外，由于本协议只需采用一次窃听检测，且抽样检测的量子态同样可用于传输秘密，从而既减少了协议的交互次数，同时量子态利用率也达到了 100%。本文协议与几种典型协议的效率对比如表 2 所示。

5.2 参数更新

现有的 QSS 协议大都无法解决参数更新问题，即动态更新子秘密或者增减代理成员[15]。本协议采用了对 Bell 态的两个粒子分别进行不同酉操作的方法和可交换的相位旋转操作集合 S，可以满足上述需求。不失一般性，设 Alice_1 所制备的 Bell 态为 $\left|\phi^+\right\rangle_{th}$，$B$ 组全体成员对粒子 t 实施的复合操作为 U，A 组全体成员对粒子 h 实施的复合操作为 N。此时，新纠缠态 $|\varphi\rangle_{th}$ 为

$$(\boldsymbol{U}\otimes\boldsymbol{N})\left|\phi^+\right\rangle_{th}=|\varphi\rangle_{th},\ \boldsymbol{U}=\prod_{i=1}^{m}\boldsymbol{U}_i \tag{14}$$

在 Alice_n 将粒子 h 发送给 Bob_m 之前：

(1)某个 B 组成员(如 Bob_j)要求更新自己的子秘密 $\boldsymbol{U}_j(j=1,2,\cdots,n)$。$\text{Bob}_j$ 首先让 Bob_m 将粒子 t 传给自己，之后对其实施酉操作 $\boldsymbol{U}_j^{'}\cdot\boldsymbol{U}_j^{-1}$ 即可将子秘密更新为 $\boldsymbol{U}_j^{'}$：

$$(\boldsymbol{U}_j^{'}\cdot\boldsymbol{U}_j^{-1}\otimes I)|\varphi\rangle_{th}=(\boldsymbol{U}'\otimes\boldsymbol{N})\left|\phi^+\right\rangle_{th},\quad \boldsymbol{U}'=\boldsymbol{U}_j^{'}\cdot\prod_{i=1,i\neq j}^{m}\boldsymbol{U}_i \tag{15}$$

(2)某个 B 组成员(如 Bob_j)要求离开协议。Bob_j 首先让 Bob_m 将粒子 t 传给自己，之后对其实施酉操作 $\boldsymbol{U}_j^{-1}$ 即可去除其子秘密信息：

$$(\boldsymbol{U}_j^{-1}\otimes I)|\varphi\rangle_{th}=(\boldsymbol{U}'\otimes\boldsymbol{N})\left|\phi^+\right\rangle_{th},\ \boldsymbol{U}'=\prod_{i=1,i\neq j}^{m}\boldsymbol{U}_i \tag{16}$$

类似地，如果 B 组有新成员(如 Bob_{m+1})要求加入协议，他首先要求 Bob_m 将粒子 t 传给自己，之后对其实施酉操作 $\boldsymbol{U}_{m+1}$ 即可注入子秘密：

$$(\boldsymbol{U}_{m+1}\otimes I)|\varphi\rangle_{th}=(\boldsymbol{U}'\otimes\boldsymbol{N})\left|\phi^+\right\rangle_{th},\ \boldsymbol{U}'=\prod_{i=1}^{m+1}\boldsymbol{U}_i \tag{17}$$

综上，本协议具备动态更新子秘密或者增减代理成员的功能。

6 结束语

本文基于密集编码思想提出了一种新的多方与多方 QSS 协议，在提高安全性的同时，还具备高效率、动态更新子秘密和增减代理成员等特点。本协议所涉及的量子态与酉操作在目前实验条件下均不难实现。随着量子密码的飞速发展，设计更加安全、高效和功能多样的 QSS 协议还存在很多后续问题有待解决，值得人们进一步关注。

表 2 本文协议与几种典型协议的效率对比

	文献[6]协议	文献[7]方案	文献[8]协议	文献[10]协议	本文协议
总粒子数	$2mk+k'$	$2mk+k'$	$2k+k'$	$2k(m+n)+k'$	$2k$
编码效率	100%	100%	100%	无	200%
量子态利用率	$2k/(2mk+k')$	$2k/(2mk+k')$	$2k/(2k+k')$	$2k/[2k(m+n)+k']$	100%

注：编码效率＝秘密信息比特数/编码操作的量子比特数，量子态利用率＝经典信息比特数/总粒子数。为便于比较，设各协议中秘密信息比特数为 $2k$，各协议中用于窃听检测的样本粒子数为 k'。

参 考 文 献

[1] Hillery M, Buzek V, and Berthiaume A. Quantum secret sharing[J]. *Physical Review A*, 1999, 59(3): 1829−1834.

[2] Cleve R, Gottesman D, and Lo H K. How to share a quantum

secret[J]. *Physical Review Letters*, 1999, 83(3): 648–651.

[3] Guo Guo-ping and Guo Guang-can. Quantum secret sharing without entanglement[J]. *Physics Letters A*, 2003, 310(4): 247–251.

[4] Zhang Zhan-jun. Multiparty quantum secret sharing protocol of secure direct communication[J]. *Physics Letters A*, 2005, 342(1–2): 60–68.

[5] Liu Bin, Gao Fei, and Wen Qiao-yan. Eavesdropping and improvement to multiparty quantum secret sharing with collective eavesdropping-check[J]. *International Journal of Theoretical Physics*, 2012, 51(4): 1211–1223.

[6] Yan Feng-lin and Gao Ting. Quantum secret sharing between multiparty and multiparty without entanglement[J]. *Physical Review A*, 2005, 72(1): 2304–2309.

[7] Han Lian-fang, Liu Yi-min, Shi Shou-hua, *et al*.. Efficient multiparty-to-multiparty quantum secret sharing via continuous variable operations[J]. *Chinese Physics Letters*, 2007, 24(12): 3312–3315.

[8] Yan Feng-lin, Gao Ting, and Li You-cheng. Quantum secret sharing protocol between multiparty and multiparty with single photons and unitary transformations[J]. *Chinese Physics Letters*, 2008, 25(4): 1187–1190.

[9] 张盛, 张守林, 王剑, 等. 基于压缩态的多方与多方量子秘密共享[J]. 中国科学: 物理学力学天文学, 2011, 41(7): 855–861.
Zhang Sheng, Zhang Shou-lin, Wang Jian, *et al*.. Quantum secret sharing between multiparty and multiparty with squeezed state[J]. *SCIENCE CHINA Physica, Mechanica & Astronomica*, 2011, 41(7): 855–861.

[10] Shi Run-hua, Huang Liu-sheng, Yang Wei, *et al*.. Quantum secret sharing between multiparty and multiparty with Bell states and Bell measurements[J]. *SCIENCE CHINA Physics, Mechanics & Astronomy*, 2010, 53(12): 2238–2244.

[11] Li Chuan-ming, Chang Chi-chao, and Hwang T. Comment on "quantum secret sharing between multiparty and multiparty without entanglement"[J]. *Physical Review A*, 2006, 73(1): 016301.

[12] Han Lian-fang, Liu Yi-min, Shi Shou-hua, *et al*.. Improving the security of a quantum secret sharing protocol between multiparty and multiparty without entanglement[J]. *Physics Letters A*, 2007, 361(1/2): 24–28.

[13] Zhu Zhen-chao and Zhang Yu-qing. Cryptanalysis and improvement of a quantum secret sharing protocol between multiparty and multiparty with single photons and unitary transformations[J]. *Chinese Physics Letters*, 2010, 27(6): 060303(1–3).

[14] Wang Tian-yin, Wen Qiao-yan, and Zhu Fu-chen. Cryptanalysis of multiparty quantum secret sharing with Bell states and Bell measurements[J]. *Optical Communications*, 2011, 284(6): 1711–1713.

[15] Jia Heng-yue, Wen Qiao-yan, Gao Fei, *et al*.. Dynamic quantum secret sharing[J]. *Physics Letters A*, 2012, 376(10/11): 1035–1041.

[16] 秦素娟. 量子秘密分享协议的设计与分析[D]. [博士论文], 北京: 北京邮电大学, 2008.
Qin Su-juan. Research on protocols of quantum secret sharing: design and analysis[D]. [Ph. D. dissertation], Beijing: Beijing University of Posts and Telecommunications, 2008.

[17] Gao Fei, Qin Su-juan, Guo Fen-zhou, *et al*.. Dense-coding attack on three-party quantum key distribution protocols[J]. *IEEE Journal of Quantum Electronics*, 2011, 47(5): 630–635.

[18] Yang Yu-guang, Teng Yi-wei, Chai Hai-ping, *et al*.. Verifiable quantum (k, n)-threshold secret key sharing[J]. *International Journal of Theoretical Physics*, 2011, 50(3): 792–798.

[19] Bennett C H and Wiesner S J. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states[J]. *Physical Review Letters*, 1992, 69(20): 2881–2884.

[20] Wang Tian-yin and Wen Qiao-yan. Security of a kind of quantum secret sharing with single photons[J]. *Quantum Information & Computation*, 2011, 11(5): 434–443.

杜宇韬：　男，1985 年生，硕士生，研究方向为量子密码.

鲍皖苏：　男，1966 年生，教授，主要研究方向为序列密码、公钥密码、量子密码.

管文强：　男，1974 年生，工程师，主要研究方向为计算机应用.