基于 GHZ 态的无酉操作多方量子秘密共享方案*

李文骞[1,2]，刘志昊[2]
(1. 南京森林警察学院 信息技术系，南京 210023；2. 东南大学 计算机科学与工程学院，南京 211189)

摘 要：为了简化多方量子秘密共享协议，利用 Greenberger-Horne-Zeilinger(GHZ)态和互补基特性，提出了一种简单高效的多方量子秘密共享方案。该方案无须进行任何酉操作，发送方与多个接收方之间只需一次量子通信，并使用互补基进行测量即可完成信道安全检测和秘密共享。除去少量用于检测量子信道安全的粒子，其余每个 GHZ 态粒子共享一个比特的经典信息。安全性分析表明该方案是安全可靠的。

关键词：量子安全通信；多方量子秘密共享；GHZ 态；安全性分析
中图分类号：TP309 **文献标志码**：A **文章编号**：1001-3695(2016)02-0491-04
doi:10.3969/j.issn.1001-3695.2016.02.040

Multiparty quantum secret sharing scheme without unitary operations based on GHZ states

Li Wenqian[1,2], Liu Zhihao[2]
(1. *Dept. of Information Technology, Nanjing Forest Police College, Nanjing* 210023, *China*; 2. *School of Computer Science & Engineering, Southeast University, Nanjing* 211189, *China*)

Abstract: Based on GHZ states and properties of mutually unbiased bases, this paper proposed a simple and effective multiparty quantum secret sharing protocol to simplify the current ones. Without any unitary operations, the sender and multiple receivers could implement security detection of quantum channel and quantum secret sharing by a one-step quantum communication and mutually unbiased bases measurement. Except a few particles which used to check the security of quantum channel, every GHZ state could be used to share 1-bit of information. The security analysis shows that the scheme is secure.

Key words: quantum secure communication; multiparty quantum secret sharing; GHZ states; security analysis

秘密共享是密码学的一个重要分支，其机制是(k,n)门限方案，即将秘密拆分成 n 份，每一个份额由不同的参与者管理，当且仅当 k 个以上参与者一同协作才能恢复秘密消息，k 个以下参与者无论如何均无法恢复秘密信息。量子秘密共享是经典秘密共享在量子领域的引申和发展，是利用量子作为信息载体，以量子力学的基本原理保证其安全性。自 1999 年 Hillery 等人[1]利用 Greenberger-Horne-Zeilinger(GHZ)态提出了第一个量子秘密共享协议后，越来越多的学者开始研究这个方向，主要集中在(n,n)门限方案的研究，从最初的三方量子秘密共享扩展到多方量子秘密共享，提出了若干量子秘密共享协议。这些协议按量子态性质大致可以分为两类，一类是基于纠缠态的量子秘密共享，如文献[1~13]；另一类是基于直积态的量子秘密共享，如文献[14~18]。上述协议都是基于(n,n)门限方案的研究，秘密发送者通过酉(幺正)操作将信息编码到量子态粒子中，共享方利用联合测量进行纠缠交换或进行酉(幺正)操作得到各自信息，最终通过信息协作完成秘密共享。

对于(k,n)门限方案的研究，由于量子纠缠是作用于纠缠态所有的粒子上，所以使用纠缠态来设计(k,n)门限方案较为困难。文献[19]对(k,n)门限方案的量子秘密共享进行了理论研究，指出设计这样的量子秘密共享实质上是构造某种特定的量子纠错码，这个结论为后续(k,n)门限方案的研究指明了方向。

本文利用 $n+1$ 位的 GHZ 纠缠态在互补基测量中所表现的数学关系，提出了一种(n,n)门限方案的多方量子秘密共享方案，其特点是无须任何酉操作和纠缠交换，若不计信道安全检测粒子，每个 GHZ 态粒子均共享一个比特的经典信息，其利用率为 100%。对于可能存在的攻击方式，文中给出了详细的安全性证明。

1 互补基和 GHZ 态

量子系统中一个量子态通常由一组标准正交基来表示。在二维量子系统中，常用的一组标准正交基为$\{|Z_0\rangle,|Z_1\rangle\}$，其中$|Z_0\rangle=|0\rangle$ $|Z_1\rangle=|1\rangle$，称为 Z 基。根据量子傅里叶变换，可构造出另一组标准正交基$\{|X_0\rangle,|X_1\rangle\}$，称为 X 基，如式(1)所示。

$$|X_i\rangle=F|Z_j\rangle=\frac{1}{\sqrt{2}}\sum_{k=0}^{1}e^{\frac{2\pi ijk}{2}}|Z_k\rangle=\frac{1}{\sqrt{2}}\sum_{k=0}^{1}e^{\pi ijk}|Z_k\rangle \tag{1}$$

其中：$0\leqslant j\leqslant 1$，F 为量子傅里叶变换。显而易见，X 基的基向量就是 Z 基中对应基向量的傅里叶变换。

$$|X_0\rangle=|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),|X_1\rangle=|-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

同样，经过量子傅里叶逆变换，Z 基中的任一基向量$|Z_j\rangle$

收稿日期：2014-10-19；**修回日期**：2014-11-29 **基金项目**：中央高校基本科研业务费专项资金项目(LGYB201411)；国家自然科学基金资助项目(61170321)；江苏省自然科学基金资助项目(BK20140651)

作者简介：李文骞(1979-)，男，江苏南京人，讲师，博士研究生，主要研究方向为量子可逆逻辑、量子安全通信(zxhflwq@sina.com)；刘志昊(1982-)，男，讲师，博士，主要研究方向为量子安全通信.

$(0\leqslant j\leqslant 1)$都可以用 X 基来表示,即

$$|Z_j\rangle = F^{-1}|X_j\rangle = \frac{1}{\sqrt{2}}\sum_{k=0}^{1} e^{\frac{-2\pi ijk}{2}}|X_k\rangle = \frac{1}{\sqrt{2}}\sum_{k=0}^{1} e^{-\pi ijk}|X_k\rangle \quad (2)$$

根据互补基[20,21](也称为相互无偏基)的概念,由于对任意的 $0\leqslant j,k\leqslant 1$ 都有

$$|\langle Z_j|X_k\rangle| = \frac{1}{\sqrt{2}} \quad (3)$$

所以 Z 和 X 基为互补基,这表明当一个量子态处于 Z 基(X 基)的本征态,用 X 基(Z 基)去测量时,得到的结果是完全随机的,只有选择相同的测量基去测量,才能够识别该量子态,得到正确的结果。GHZ 态是一类 3 粒子及以上的最大纠缠态。一个 $n+1$ 位的二维 GHZ 态$|\Phi\rangle$用 Z 基可以表示为

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\cdots 0\rangle_{01\cdots n} + |11\cdots 1\rangle_{01\cdots n}) = \frac{1}{\sqrt{2}}\sum_{j=0}^{1}|Z_j\rangle_0|Z_j\rangle_1\cdots|Z_j\rangle_n \quad (4)$$

若改为用 X 基表示则为

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\cdots 0\rangle_{01\cdots n} + |11\cdots 1\rangle_{01\cdots n}) = \frac{1}{\sqrt{2}}\sum_{j=0}^{1}|Z_j\rangle_0|Z_j\rangle_1\cdots|Z_j\rangle_n =$$
$$\frac{1}{\sqrt{2}}\sum_{j=0}^{1}\{(\frac{1}{\sqrt{2}}\sum_{k_0=0}^{1}e^{-\pi ijk_0}|X_{k_0}\rangle)(\frac{1}{\sqrt{2}}\sum_{k_1=0}^{1}e^{-\pi ijk_1}|X_{k_1}\rangle)\cdots$$
$$(\frac{1}{\sqrt{2}}\sum_{k_n=0}^{1}e^{-\pi ijk_n}|X_{k_n}\rangle)\} =$$
$$2^{-(n+2)/2}\sum_{j=0}^{1}\sum_{k_0,k_1,\cdots,k_n=0}^{1}e^{-\pi ij(k_0+k_1\cdots+k_n)}|X_{k_0}\rangle|X_{k_1}\rangle\cdots|X_{k_n}\rangle =$$
$$2^{-(n+2)/2}\sum_{k_0,k_1,\cdots,k_n=0}^{1}(\sum_{j=0}^{1}e^{-\pi ij(k_0+k_1\cdots+k_n)})|X_{k_0}\rangle|X_{k_1}\rangle\cdots|X_{k_n}\rangle \quad (5)$$

其中:$k_0+k_1+\cdots+k_n$ 为模 2 加法。令 $K=k_0+k_1+\cdots+k_n\pmod 2$,则对于 $k_i(0\leqslant i\leqslant n)$的所有可能的取值,$K$ 为 0 或者 1。根据欧拉公式,当 $K=0$ 时,$\sum_{j=0}^{1}e^{-\pi ij(k_0+k_1\cdots+k_n)}=2$;当 $K=1$ 时,$\sum_{j=0}^{1}e^{-\pi ij(k_0+k_1\cdots+k_n)}=0$。则式(5)化简为

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\cdots 0\rangle_{01\cdots n} + |11\cdots 1\rangle_{01\cdots n}) = \frac{1}{\sqrt{2}}\sum_{j=0}^{1}|Z_j\rangle_0|Z_j\rangle_1\cdots|Z_j\rangle_n =$$
$$2^{-(n+2)/2}\sum_{k_0,k_1,\cdots,k_n=0}^{1}(\sum_{j=0}^{1}e^{-\pi ij(k_0+k_1\cdots+k_n)})|X_{k_0}\rangle|X_{k_1}\rangle\cdots|X_{k_n}\rangle =$$
$$2^{-n/2}\sum_{\substack{k_0,k_1,\cdots,k_n=0\\ k_0+k_1+\cdots+k_n=0(\bmod 2)}}^{1}|X_{k_0}\rangle|X_{k_1}\rangle\cdots|X_{k_n}\rangle \quad (6)$$

由式(6)可得,对于 $n+1$ 位的二维 GHZ 态,如果用 Z 基去测量各个量子位,则每个量子位的测量结果相同;而用 X 基去测量各个量子位,令$|X_{k_i}\rangle$对应经典信息 $k_i(k_i\in\{0,1\},0\leqslant i\leqslant n)$,则得到$\sum_{i=0}^{n}k_i=0(\bmod 2)$。这也意味着,若有 $n+1$ 方各持有这个 GHZ 态的一个量子位,利用 X 基去测量,则它们的测量结果满足一个数学关系。例如一个 3 位 GHZ 态$|\Phi\rangle$用 Z 和 X 基表示如下:

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) = \frac{1}{\sqrt{2}}\sum_{j=0}^{1}|Z_j\rangle|Z_j\rangle|Z_j\rangle =$$
$$\frac{1}{2}(|X_0\rangle|X_0\rangle|X_0\rangle + |X_0\rangle|X_1\rangle|X_1\rangle +$$
$$|X_1\rangle|X_0\rangle|X_1\rangle + |X_1\rangle|X_1\rangle|X_0\rangle) \quad (7)$$

可以看出,若用 Z 基去测量$|\Phi\rangle$的各个量子位,则它们的结果是相同的;而用 X 基去测量时,无论测量结果处于哪一个量子态$|X_{k_0}\rangle|X_{k_1}\rangle|X_{k_2}\rangle$,都满足 $k_0+k_1+k_2=0(\bmod 2)$。

2 基于 GHZ 态的多方量子秘密共享方案

假设有秘密发送方 Alice 和 n 个接收方 $\text{Bob}_i(1\leqslant i\leqslant n)$,Alice 准备通过量子信道向 Bobs 发送一个长度为 M 的二进制信息串 Q,要求 n 个 Bobs 一起合作才能得到该信息,而少于 n 个 Bobs 时则得不到。利用式(6)的数学关系,构建一种无酉操作多方量子秘密共享方案,方案流程如图 1 所示。

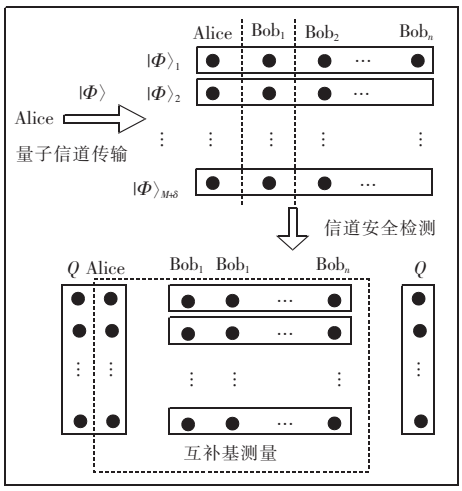


图 1 方案流程示意图

方案的步骤如下:

a) Alice 准备 $M+\delta$ 个 $n+1$ 位的 GHZ 态$|\Phi\rangle=\frac{1}{\sqrt{2}}(|00\cdots 0\rangle_{01\cdots n}+|11\cdots 1\rangle_{01\cdots n})$,并将这些 $n+1$ 位$|\Phi\rangle$按量子位的对应位置分别组成粒子序列 $S_0,S_1,\cdots,S_n$,$|S_i|=M+\delta(0\leqslant i\leqslant n)$,然后自己保留粒子序列 S_0,将其余的粒子序列 S_i 发送给对应的 $\text{Bob}_i(1\leqslant i\leqslant n)$。

b)待确认 Bobs 都收到对应的粒子序列后,Alice 进行量子信道安全检测。Alice 从自己的粒子序列 S_0 中随机抽取 δ 个粒子,并随机使用 Z 基$\{|0\rangle,|1\rangle\}$或 X 基$\{|X_0\rangle,|X_1\rangle\}$(其中$|X_0\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$,$|X_1\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$)进行测量。然后向 Bobs 公布 δ 个粒子在粒子序列中的位置以及使用的测量基,要求 $\text{Bob}_i(1\leqslant i\leqslant n)$使用相同的测量基对各自 S_i 中对应位置的粒子进行测量。

c) Alice 按随机顺序要求 $\text{Bob}_i(1\leqslant i\leqslant n)$向自己通告测量结果,当用 Z 基测量时,Alice 和 Bobs 对应粒子的测量结果应相同;当用 X 基测量时,Alice 和 Bobs 对应的量子态$|X_{k_i}\rangle$具有$\sum_{i=0}^{n}k_i=0(\bmod 2)$的关系式。Alice 根据自己和 Bobs 的测量结果以及上述关系,可以判断量子信道有无窃听。若测量错误率超过某个阈值,Alice 和 Bobs 放弃本次通信,否则继续执行下一步。

d)除去 δ 个检测粒子后,剩余的粒子串长度为 M,记为 $S'_0,S'_1,\cdots,S'_n$,$|S'_i|=M(0\leqslant i\leqslant n)$。Alice 和 Bobs 都使用 X 基对各自的粒子串 $S'_i(0\leqslant i\leqslant n)$进行测量,并令 S'_i 的第 j 位$(1\leqslant j\leqslant M)$粒子的测量结果$|X^j_{k_i}\rangle$对应经典信息 $k^j_i(k^j_i\in\{0,1\},0\leqslant i\leqslant n,1\leqslant j\leqslant M)$。然后 Alice 将自己的测量结果 k^j_0 与信息串 Q 中相应的位 $Q_j(1\leqslant j\leqslant M)$进行模 2 加法,即对于 $Q_j(1\leqslant j\leqslant M)$,Alice 进行计算 $k'^j_0=k^j_0+Q_j$,最后向 Bobs 宣布 k'^j_0。

e) Bobs 得到 k'^j_0 后,进行联合计算$\sum_{i=1}^{n}k^j_i+k'^j_0=\sum_{i=0}^{n}k^j_i+Q_j=Q_j$,从而得到二进制信息串 Q 第 j 位 $Q_j(1\leqslant j\leqslant M)$,进而可以得到整个消息 Q。可以看出,由于$\sum_{i=0}^{n}k_i=0(\bmod 2)$,所以只有所有的 Bobs 联合运算才能得到正确的消息 Q。

从上述方案可知,Alice 和 Bobs 不需要进行任何酉操作和纠缠交换,只需通过量子信道进行一次传输,并用 Z 或 X 基进行测量即可完成信道安全检测和秘密共享。除去少量用于检测量子信道安全的粒子,其余每个 GHZ 态粒子共享一个比特的经典信息。

3　安全性分析

方案的安全性是基于量子信道传输的安全性,如果粒子在传输中能够有效防范各种攻击,无法被攻击者窃取,那么多方秘密共享的安全性也得到了保证。事实上,就攻击能力而言,相对外部攻击者,内部攻击者本身就获得了秘密的部分信息,攻击危害性更大。同时,外部攻击者也可以看成是一个有限制性的内部攻击者。因此,安全性分析重点在讨论内部攻击者所采取的攻击。

假设 n 个 Bob 中有 t 个是不忠实的($1\leqslant t\leqslant n-1$),即他们在如实执行方案的同时有可能串通起来,对诚实参与者进行联合攻击,目的是获取诚实参与者的信息,进而得到秘密信息 Q。不失一般性,令 $\mathrm{Bob}_1\cdots\mathrm{Bob}_t$ 为不忠实参与者,如果想获得诚实参与者信息,他们唯一的机会是在步骤 a) Alice 进行粒子串分发时,进行攻击。由于方案只有这一次量子信道通信,所以对于不可见光攻击和木马攻击是免疫的。下面就攻击者们采用的截获—重发攻击和纠缠攻击来进行分析。

1)截获—重发攻击　对应于一个 GHZ 态的所有粒子,不忠实的参与者在收到 Alice 给自己的粒子同时,截获了发送给其余($n-t$)个诚实参与者的粒子,然后他们分发($n-t$)个假冒粒子给相应的诚实参与者,企图在不被察觉的情况下,利用手中的 n 个粒子,获得秘密信息 Q。为了逃避步骤 c)的检测,不忠实的参与者必须使得诚实参与者在步骤 b)的测量结果中满足步骤 c)的关系,唯一的策略就是测量这($n-t$)个粒子,并发送相同状态的粒子给诚实参与者。但是由于步骤 b)中的测量基由 Alice 随机选择,且等待所有的 Bobs 都收到粒子后才公布检测粒子的测量基,所以不忠实参与者只能随机选择 Z 或 X 基进行测量。同时,Bobs 是按随机顺序向 Alice 宣布自己的测量结果,因此,在这种情况下,不忠实参与者的测量行为势必会引入错误而被察觉。

2)纠缠攻击　根据 Stinespring Dilation 定理[22],不忠实的参与者的窃听操作可以通过作用在更大的希尔伯特(Hilbert)空间上的酉操作实现,即将酉算子 $\hat{E}$ 作用于诚实参与者的粒子和 s 位(s 取决于具体攻击策略)的辅助粒子 E 上,通过观测辅助粒子以达到获取诚实参与者信息的目的。因此,当酉算子 $\hat{E}$ 作用后,Alice 和 Bobs 的系统状态可以表示为

$$\hat{E}|\Phi\rangle|E\rangle=|\Phi'\rangle=\sum_{j_0,j_1,\cdots,j_n=0}^{1}a_{j_0j_1\cdots j_n}|j_0\rangle|j_1\rangle\cdots|j_n\rangle\otimes|\xi_{j_0j_1\cdots j_n}\rangle \tag{8}$$

其中:$|\xi_{j_0j_1\cdots j_n}\rangle$ 是不忠实参与者引入的 s 位辅助粒子的状态。为了在步骤 c)的检测中不引入错误,则 Alice 和 Bobs 用 Z 基测量时,结果应该相同,因此 $|\Phi'\rangle$ 状态应该为

$$|\Phi'\rangle=\sum_{j=0}^{1}a_j|j\rangle|j\rangle\cdots|j\rangle\otimes|\xi_j\rangle \tag{9}$$

其中:系数 a_j 满足归一化条件 $\sum_{j=0}^{1}a_j^*a_j=1$。

另一方面,用 X 基表示 $|\Phi'\rangle$ 状态则为

$$|\Phi'\rangle=2^{-n/2}\sum_{j=0}^{1}\sum_{k_0,k_1,\cdots,k_n=0}^{1}a_j\mathrm{e}^{-\pi ij(k_0+k_1\cdots+k_n)}|X_{k_0}\rangle|X_{k_1}\rangle\cdots|X_{k_n}\rangle\otimes|\xi_j\rangle=$$
$$2^{-n/2}\sum_{k_0,k_1,\cdots,k_n=0}^{1}\{|X_{k_0}\rangle|X_{k_1}\rangle\cdots|X_{k_n}\rangle\otimes\sum_{j=0}^{1}a_j\mathrm{e}^{-\pi ij(k_0+k_1\cdots+k_n)}|\xi_j\rangle\} \tag{10}$$

若在步骤 c)中不引入错误,则 Alice 和 Bobs 用 X 基测量时,结果应该为 $\sum_{i=0}^{n}k_i=0(\mathrm{mod}\ 2)$,因此式(10)中应没有满足 $\sum_{i=0}^{n}k_i=1(\mathrm{mod}\ 2)$ 关系的项:

$$2^{-n/2}\sum_{\substack{k_0,k_1,\cdots,k_n=0\\k_0+k_1\cdots+k_n=1}}^{1}\{|X_{k_0}\rangle|X_{k_1}\rangle\cdots|X_{k_n}\rangle\otimes\sum_{j=0}^{1}a_j\mathrm{e}^{-\pi ij(k_0+k_1\cdots+k_n)}|\xi_j\rangle\}=0 \tag{11}$$

即

$$2^{-n/2}\sum_{\substack{k_0,k_1,\cdots,k_n=0\\k_0+k_1\cdots+k_n=1}}^{1}\{|X_{k_0}\rangle|X_{k_1}\rangle\cdots|X_{k_n}\rangle\otimes(a_0|\xi_0\rangle-a_1|\xi_1\rangle)\}=0 \tag{12}$$

由此可得

$$a_0|\xi_0\rangle-a_1|\xi_1\rangle=0,a_0|\xi_0\rangle=a_1|\xi_1\rangle \tag{13}$$

依据式(13)和归一化条件 $\sum_{j=0}^{1}a_j^*a_j=1$,式(9)可改写为

$$|\Phi'\rangle=\left(\frac{1}{\sqrt{2}}\sum_{j=0}^{1}|j\rangle|j\rangle\cdots|j\rangle\right)\otimes|\xi_0\rangle=|\Phi\rangle\otimes|\xi_0\rangle \tag{14}$$

也就是说,如果想逃避步骤 c)的检测而不被察觉,那么不忠实参与者的辅助粒子与 GHZ 态组成的状态空间必定是张量积的关系,此时辅助粒子的密度算子为 $\rho_e=tr_\Phi(|\Phi\rangle|\xi_0\rangle\langle\xi_0|\langle\Phi|)=|\xi_0\rangle\langle\xi_0|$,von Neumann 熵 $S(\rho_e)=0$。这表明,如果不忠实参与者在不引入错误的情况下去观测辅助粒子,将不能获得任何结果。换句话说,如果不忠实参与者得到了诚实参与者的信息,那么在势必会引入错误能够在步骤 c)的检测中被发现。

此外,若攻击者不进行窃听攻击,仅仅通过步骤 d)中 Alice 宣布的信息进行推演,由于至少存在一位诚实参与者,攻击者无法得到诚实参与者的信息,所以不能正确推算出秘密消息。

综上说明,不忠实参与者无论采取何种攻击方式,只要得到了有效信息,那么攻击必定在信道安全检测中被发现,可知文中所提方案是安全的。

4　结束语

本文利用量子傅里叶变换构造了一对互补基,根据 GHZ 态在不同基底的表现形式,提出了一种简单高效的多方量子秘密共享方案。在该方案中,秘密发送方 Alice 准备一种 $n+1$ 位的 GHZ 态,并将其中 n 个量子位对应分发给 n 个参与方 Bobs;然后 Alice 和 Bobs 利用互补基 Z 和 X 基进行量子信道的安全检测,若无窃听存在,则进行量子态测量;最后 Bobs 依据测量结果和 Alice 公布的信息进行联合计算,完成秘密共享。在安全性分析中,列举了攻击者可能采用的攻击手段,利用 Stinespring Dilation 定理证明了方案的安全性。相对现有的多方量子秘密共享方案,本方案操作简单,只需进行量子态分发通信和互补基测量操作,就可以实现信道安全检测和秘密共享。除去信道安全检测粒子,每个 GHZ 态可完成 1-bit 的经典信息的秘密共享,且外部攻击者和不忠实参与方无法在不引入错误的情况下窃取秘密,实现了安全高效的多方秘密共享。

参考文献:

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

[2] Liu Weitao, Liang Linmei, Li Chengzu. Quantum secret sharing with two-particle entangled states[J]. Chinese Physics Letters, 2006,

23(12):3148-3151.

[3] Liu Weitao, Liang Linmei, Li Chengzu, *et al*. Scalable quantum secret sharing extended from quantum key distribution[J]. Chinese Physics Letters, 2007, 24(5): 1147-1150.

[4] Xia Yan, Song Jie, Song Heshan, *et al*. Multiparty quantum secret sharing via introducing auxiliary particles using a pure entangled state [J]. Communications in Theoretical Physics, 2008, 49(6): 1468-1472.

[5] Zhou Ping, Deng Fuguo, Zhou Hongyu. Probabilistic quantum entang-lement swapping and quantum secret sharing with high-dimensional pure entangled systems[J]. Physica Scripta, 2009, 79(3): 035005(1)-035005(5).

[6] Hsieh C R, Tasi C W, Hwang T. Quantum secret sharing using GHZ-like state [J]. International Journal of Quantum Information, 2010, 54(6): 1019-1022.

[7] 袁素真,孙志富,田俊龙. 基于 *N* 个有序纠缠光子对的量子机密共享方案[J]. 光子学报, 2011, 40(8): 1248-1252.

[8] Helwig W, Cui Wei, Riera A, *et al*. Absolute maximal entanglement and quantum secret sharing[J]. Physical Review A, 2012, 86(5): 052335(1)-052335(5).

[9] Massoud H D, Elham F. A novel and efficient multiparty quantum secret sharing scheme using entangled states [J]. Science China-Physics Mechanics & Astronomy, 2012, 55(10): 1828-1831.

[10] Shi Runhua, Zhong Hong. Multiparty quantum secret sharing with the pure entangled two-photon states [J]. Quantum Information Processing, 2012, 11(1): 161-169.

[11] Wang Wenhua, Cao Huaixin. An improved multiparty quantum secret sharing with Bell states and Bell measurement [J]. International Journal of Theoretical Physics, 2013, 52(9): 3238-3243.

[12] Wang Mingming, Chen Xiubo, Yang Yixian. Quantum secret sharing for general access structures based on multiparticle entanglements [J]. Quantum Information Processing, 2014, 13(2): 429-443.

[13] Liao Cihong, Yang Chunwei, Hwang T. Dynamic quantum secret sharing protocol based on GHZ state [J]. Quantum Information Processing, 2014, 13(8): 1907-1916.

[14] Guo Guoping, Guo Guangcan. Quantum secret sharing without entanglement[J]. Physics Letters A, 2003, 310(4): 247-251.

[15] Yan Fengli, Gao Ting. Quantum secret sharing between multiparty and multiparty without entanglement[J]. Physical Review A, 2005, 72(1): 012304(1)-012304(5).

[16] Hsu L Y, Li Cheming. Quantum secret sharing using product states [J]. Physical Review A, 2005, 71(2): 022321(1)-022321(9).

[17] Xu Juan, Chen Hanwu, Liu Zhihao. A simple and secure quantum secret sharing scheme based on product states[J]. International Journal of Quantum Information, 2012, 10(3): 1250031(1)-1250031(11).

[18] Xu Juan, Yuan Jiabin. Improvement and extension of quantum secret sharing using orthogonal product states[J]. International Journal of Quantum Information, 2014, 12(1): 1450008(1)-1450008(10).

[19] Gottesman D. Theory of quantum secret sharing[J]. Physical Review A, 2000, 61(4): 042311(1)-042311(8) .

[20] Wootters W K, Fields B D. Optimal state determination by mutually unbiased measurements [J]. Annals of Physics, 1989, 191(2): 363-381.

[21] Pittenger A O, Rubin M H. Mutually unbiased bases, generalized spin matrices and separability[J]. Linear Algebra and Its Applications, 2004, 390(2004): 255-278.

[22] Boström K, Felbinger T. Deterministic secure direct communication using entanglement[J]. Physical Review Letters, 2002, 89(18): 187902(1)-187902(4).