基于秘密认证的可验证量子秘密共享协议

杜宇韬 鲍皖苏* 李 坦

(信息工程大学 郑州 450001)

摘 要：该文针对量子秘密共享协议难以抵抗内部成员欺骗攻击的问题，采用秘密认证的方法提出可验证量子秘密共享协议的一般性模型，基于Bell态双粒子变换提出一种新验证算法，并以此给出一个新的可验证量子秘密共享协议。与现有的量子秘密共享协议的验证算法相比，新验证算法既能有效抵抗内部成员欺骗攻击等典型的攻击策略，又可大幅提升协议效率，而且可以与现有量子秘密共享协议相结合，具备很好的可扩展性。

关键词：量子秘密共享；欺骗攻击；可验证

中图分类号：TN918; TP309 **文献标识码**：A **文章编号**：1009-5896(2021)01-0212-06

DOI: 10.11999/JEIT190901

Verifiable Quantum Secret Sharing Protocol Based on Secret Authentication

DU Yutao BAO Wansu LI Tan

(*Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: To solve the problem that Quantum Secret Sharing (QSS) protocol is difficult to resist inner-cheating attack, by utilizing the method of secret message authentication to present a general model of verifiable quantum secret sharing protocols, a new verification algorithm is proposed based on the two-particle transform of Bell states, and then a new verifiable quantum secret sharing protocol is proposed. Compared with the verification algorithms of the existing verifiable quantum secret sharing protocol, the new verification algorithm can not only resist effectively the typical attack strategies such as the inner-cheating attack, but also improves greatly the efficiency of the protocol, and has good scalability which can be combined with the existing quantum secret sharing protocols.

Key words: Quantum Secret Sharing (QSS); Cheating attack; Verifiability

1 引言

众所周知，量子密码协议是基于量子力学原理而设计的一类特殊密码协议，近几十年来始终是密码学领域的研究热点。量子秘密共享(Quantum Secret Sharing, QSS)作为经典秘密共享[1]在量子密码领域的延伸，是量子密码协议的一个重要研究方向，它允许秘密分发者将秘密信息拆分为若干份子秘密，借助量子态为载体分发给多个代理成员；只有代理成员集合中的授权子集可以恢复秘密，而非授权子集得不到任何信息[2]。经典秘密共享在对秘密或密钥(例如核武器的管控与发射、金库管理等)进行分散管理方面拥有不可替代的重要作用。相比之下，QSS协议基于量子力学原理能够更为有效地抵抗窃听者的攻击行为，因此具有极大的研究价值。自从1999年Hillery等人[3]基于GHZ态提出了第1个QSS协议以来，各种类型的QSS协议[2–21]层出不穷，相关研究已取得许多重要的成果。

现有的QSS协议通常假设：在恢复秘密时每个代理成员均诚实执行协议，从而正确恢复秘密信息。然而，现实中可能存在一种欺骗攻击：不诚实者此时可提供假的子秘密，使得其他成员无法恢复出秘密，而他则可通过纠错独自窃取秘密[13]。类似于经典秘密共享，抵抗欺骗攻击最有效的是可验证QSS协议。2002年，Crépeau等人[5]基于量子编码理论提出了第1个可验证QSS协议，可通过验证子秘密信息而防止不诚实者的欺骗行为，但是其协议效率很低。目前，已有的可验证QSS协议主要有两种类型：一是在设计QSS协议时就采用抗欺骗攻击的机制，如2018年Du等人[2]提出的动态QSS协议中通过选用相移操作[14]而阻止不诚实者窃取秘密，然而该方法可扩展性差，不能移植于其它QSS协议；二是在秘密恢复环节增加验证算法，如2011年Yang等人[10]基于后验证机制提出的一个可验证QSS协

收稿日期：2019-11-08；改回日期：2020-08-04；网络出版：2020-08-20
*通信作者： 鲍皖苏 bws@qiclab.cn

议，该机制具有较好的扩展性，因此后来的一些可验证QSS方案[11,15]均采用方式。但是，此类协议虽能够察觉欺骗行为却不能阻止攻击者得到秘密；另外采用验证子秘密的方式，其验证算法的执行效率偏低。因此，能否设计出既可有效抵抗欺骗攻击，又具备高效性和可扩展性的验证算法，是研究可验证QSS协议的焦点问题。

本文首先给出基于秘密认证的可验证QSS协议的一般性模型，之后利用Bell态双粒子变换[2]提出一种新验证算法，并结合一个现有的QSS方案给出一个新的对经典信息的可验证QSS协议。新协议采用认证秘密消息的方法，使得代理成员中的欺骗者无法利用验证环节得到任何秘密信息；基于Bell态双粒子变换的测量非局域关联性，使得欺骗者无法篡改或伪造验证信息。在效率方面，新验证算法所需的量子比特数约为$4H_k(l)$，与现有的可验证QSS协议的验证算法相比，其量子态消耗量大幅减少，从而提高了协议效率。另外，新验证算法具备很强的可扩展性，可与任意QSS协议相结合，得到不同的可验证QSS协议。

本文的组织结构与安排：第2节为基于秘密认证的可验证QSS协议的一般模型；第3节为基于Bell态双粒子变换的可验证QSS协议；第4节为验证算法安全性分析；第5节为验证算法效率分析；第6节为结束语。

2　基于秘密认证的可验证QSS协议的一般性模型

可验证QSS协议通常是在普通QSS协议上附加一个用于检验秘密或子秘密正确性的验证算法而构成的[11]。本文基于秘密认证给出一个可验证QSS协议的一般性模型。假设秘密分发者为Alice，其秘密信息为$M=(m_1,m_2,\cdots,m_l)$，代理成员集合为$\{\mathrm{Bob}_1,\mathrm{Bob}_2,\cdots,\mathrm{Bob}_n\}$，协议结构可分为以下4个阶段：

(1) 初始化阶段：Alice或某个代理成员首先制备若干个量子态(或者双方根据需要使用QKD技术事先协商会话密钥)。

(2) 秘密分发阶段：Alice与代理成员以量子态为载体进行信息交互，共同运行秘密分发算法，实现将秘密M拆分为若干份子秘密$(M_1,M_2,\cdots,M_n)$给n个代理成员的目的。通常采用两种实现方式：一是Alice将M拆分为若干份子秘密$(M_1,M_2,\cdots,M_n)$分发给n个成员；二是全体代理成员$(\mathrm{Bob}_1,\mathrm{Bob}_2,\cdots,\mathrm{Bob}_n)$自行生成其子秘密$(M_1,M_2,\cdots,M_n)$，并最终汇总至Alice处得到秘密$M$(通常为随机数)，从而实现密钥共享。

此外，Alice与代理成员需要执行窃听检测(包括两方或多方联合窃听检测等)，以确保承载秘密信息的量子态在传输时未遭受攻击(来自内部或外部)。如果存在攻击行为，则Alice或某个代理成员立即宣布中止协议，结果作废；反之，则接受此次秘密共享的结果。

(3) 秘密恢复阶段：当代理成员需要恢复秘密M时，由某个授权子集的代理成员共同执行秘密恢复算法：首先推举出(或随机选出)某个成员(如Bob_i)，其他成员将其子秘密交给Bob_i，由其执行秘密恢复算法，并通过量子态测量而得到信息M'。假设每个成员都诚实地执行协议，则恢复出的M'为Alice所共享的秘密M。

(4) 验证阶段：Bob_i执行验证算法来排查可能的欺骗攻击：得到M'后，Bob_i先不公布，而是联合Alice验证M'是否正确(通过可认证信道来交互信息)。如果Bob_i利用验证算法发现由$M_i(i=1,2,\cdots,k$且$k\le n)$所恢复出的M'与秘密M并不相同，则证明某个M_i(或若干个)不正确，秘密恢复环节存在欺骗攻击，此时Bob_i向其他代理成员宣布M'无效并销毁M'。反之，则证明M'有效，此时Bob_i公布M'为协议所共享的秘密信息M。

需要指出的是，这里所给出的是可验证QSS协议在理想条件下的一般性模型，暂不考虑实际环境中存在的器件不完美和信道损耗等情况。

3　基于Bell态双粒子变换的可验证QSS协议

秘密共享协议通常利用某种公钥算法来实现对秘密信息的完整性认证[22,23]，从而得到可验证秘密共享协议。本文基于Bell态双粒子变换[2]和杂凑函数[24]提出一种新的验证算法，并以2019年宋云[13]提出的QSS方案为例(新验证算法可与任意QSS协议结合)，结合新验证算法给出新的可验证QSS协议。

3.1　QSS方案描述

假设秘密分发者为Alice，其秘密信息为M，代理方成员集合为$\{\mathrm{Bob}_1,\mathrm{Bob}_2\}$。宋云[13]方案简述如下：

(1) 初始化阶段：Alice制备一列GHZ态，每个GHZ态随机地处于$|\mathrm{GHZ}_{000}\rangle_{123}$和$|\mathrm{GHZ}_{100}\rangle_{123}$，其中，

$$\left.\begin{aligned}|\mathrm{GHZ}_{000}\rangle_{123}&=\frac{1}{\sqrt{2}}(|000\rangle_{123}+|111\rangle_{123})\\|\mathrm{GHZ}_{100}\rangle_{123}&=\frac{1}{\sqrt{2}}(|000\rangle_{123}-|111\rangle_{123})\end{aligned}\right\}\quad(1)$$

(2) 秘密分发阶段：Alice保留每个GHZ态中的第1个粒子，并将其它粒子依序分别发送给Bob_1和Bob_2。Bob_1和Bob_2收到相应的粒子序列后，首先与Alice一起进行联合窃听检测(采用随机抽样法，详

见文献[13])。

窃听检测通过后，Alice, Bob_1和Bob_2分别对手中剩余的粒子进行测量。当Bob_1随机选基对剩余粒子测量完毕后，立即告诉Bob_2其测量基信息；而Bob_2则选择相同基测量手中粒子。双方将测量结果转化为二进制数(测量结果$|+x\rangle$和$|+y\rangle$对应1，而$|-x\rangle$和$|-y\rangle$对应0)，从而得到各自密钥(设为K_1和K_2)。另外，测量基信息也转化为比特串K_a。编码规则：当选基B_x或B_y测量第i个粒子时，K_a的第i个比特为0或1。

同时，Alice选用测量基$B_x=\{|+x\rangle,|-x\rangle\}$测量其剩余的粒子，并将测量结果编码为二进制数$k$($|+x\rangle$对应1，而$|-x\rangle$对应0)。另外，假设$|\mathrm{GHZ}_{000}\rangle_{123}$代表1而$|\mathrm{GHZ}_{100}\rangle_{123}$代表0，Alice可从窃听检测后剩余的纠缠对中得到一个比特串$K_{A'}$[13]。因此，Alice的密钥为$K{=}K_{A'}\oplus K_a\oplus k$(用于加密秘密信息$M$)。

(3) 秘密恢复阶段：Bob_1和Bob_2可以利用模2加运算$K_1\oplus K_2$，合作恢复出Alice的密钥K，从而得到秘密M。

3.2 验证算法描述

新验证算法是本文重点，这里采用更一般性的表述：设$\{\mathrm{Bob}_1,\mathrm{Bob}_2,\cdots,\mathrm{Bob}_k\}(k\le n)$是可恢复秘密的某个授权子集，$\mathrm{Bob}_i(1\le i\le k)$是该子集所推举出(或随机选出)的某个成员。验证算法描述如下：

(1) 代理成员Bob_i在恢复出信息M'后暂不公布，而是向秘密分发者Alice发出共同验证秘密信息的申请，同时自行制备f对Bell态$|\varphi_1\rangle_{sh},|\varphi_2\rangle_{sh},\cdots,|\varphi_k\rangle_{sh}$，其中，

$$|\varphi_j\rangle_{sh}=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle),\ j=1,2,\cdots,k \tag{2}$$

Bob_i将每对Bell态中的粒子s依序组成一个单量子序列(称为S序列)，每个粒子h按与S序列一致的顺序组成另一个单量子序列(称为H序列)。之后，Bob_i保存H序列，而对S序列粒子依序实施酉操作$\boldsymbol{U}(\alpha)$。这里的$\boldsymbol{U}(\alpha)$从三元相位旋转操作集合$\{\boldsymbol{U}(0),\boldsymbol{U}(2\pi/3),\cdots,\boldsymbol{U}(4\pi/3)\}$[14]中随机选择，其具体形式见式(3)

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

操作完成后，S序列被记为S_1序列。Bob_i此时记录好该酉操作信息，同时把之前的H序列发给Alice。

(2) 收到H序列粒子后，Alice首先检测H序列是否为单光子序列：一是使用光子数分离器(Photon Number Splitter, PNS)或光子分束器(Photon Beam Splitter, PBS)排查潜在的多粒子攻击，二是使用固定波长的滤波器或者隔离器，排查潜在的不可见光子攻击[2]。如果检测未通过，则宣布H序列受到了攻击并中止算法，反之，则继续执行余下的步骤。

确认H序列为单光子序列后，Alice再联合Bob_i进行窃听检测：Alice随机选用水平垂直基或对角基对H序列中的任意f_1个粒子进行单光子测量，之后将测量结果与对应位置信息发给Bob_i。Bob_i据此可对S_1序列中的对应粒子使用一致的测量基进行测量。根据两组测量结果，可以判断H序列的传送过程是否存在截取重发攻击。如果检测未通过，则宣布H序列受到了攻击并中止算法，反之，则继续执行余下的步骤。

(3) 完成上述的检测后，Alice选用约定的Hash函数$H_k(x)$[24]计算式(4)所示的Hash值

$$R_A=H_k(M||\mathrm{ID}_A||\mathrm{ID}_B||T) \tag{4}$$

式中，ID_A为Alice的公开身份数据，ID_B为Bob_i的公开身份数据，T为Alice收到H序列的时间信息，而密钥k可利用QKD技术提前分发。为便于后续操作，这里假设Hash值R_A为二进制数。

而后，Alice将R_A进行连续两两比特的分组，约定每一组比特数对应一个Pauli操作(选自$\{I,\sigma_z,\sigma_x,i\sigma_y\}$)：“00”对应$I$，“01”对应$\sigma_z$，“10”对应$\sigma_x$，“11”对应$i\sigma_y$。此时，Alice对$H$序列中通过检测的剩余粒子分别实施由$R_A$值所决定的Pauli操作。得到的新序列称为$H_1$序列，并发还给$\mathrm{Bob}_i$。

(4) 收到H_1序列后，Bob_i根据其保存的酉操作信息对剩余的S_1序列粒子实施逆相位旋转操作$U(\alpha)^{-1}$，之后将S_1序列和H_1序列的对应粒子合并执行Bell测量，根据测量结果推测出Alice的Hash值R_A。

此时，Bob_i验证式(5)是否成立，以此判断在秘密恢复阶段所得到的M'是否就是秘密M

$$R_A=H_k(M'||\mathrm{ID}_A||\mathrm{ID}_B||T) \tag{5}$$

如果式(5)不成立，证明必有成员在秘密恢复环节说谎，此时Bob_i向所有代理成员宣布在秘密恢复阶段存在欺骗攻击，M'作废且算法中止；反之则确认M'有效，并向其他代理成员公布该结果。

3.3 验证算法的正确性

该验证算法的基本思想是验证双方利用相同的Hash函数$H_k(x)$[24]分别生成两个Hash值，利用Bell态双粒子变换来确保对Hash值的安全传输，通过比较两个Hash值的异同来判断秘密M和恢复信息M'的异同，从而排查潜在的欺骗攻击以实现验证功能。

假设Alice由ID_A, ID_B, T以及秘密信息M所生

成的Hash值$R_A = H_k(M||\mathrm{ID}_A||\mathrm{ID}_B||T)$, Bob_i由ID_A, ID_B, T以及恢复出的信息M'所生成的Hash值$R'_A = H_k(M'||\mathrm{ID}_A||\mathrm{ID}_B||T)$。如果$M$等于$M'$，则所计算出的$R_A$也必然与$R'_A$相等；否则二者互不相等。从式(6)可以表示出这个逻辑关系

$$\left.\begin{array}{l} R_A = R'_A \Leftrightarrow M{=}M' \\ R_A \neq R'_A \Leftrightarrow M \neq M' \end{array}\right\} \tag{6}$$

4　验证算法安全性分析

新验证算法能够确保代理成员中的不诚实者(如Eve)在服从量子力学基本原理的前提下无法成功实施欺骗攻击和伪造攻击，同时也能够抵抗一些典型攻击策略(例如Bell态替换攻击等)。

4.1　抗欺骗攻击性

欺骗攻击是指：不诚实者Eve在恢复秘密时发送假的子秘密给Bob_i，使得执行秘密恢复算法的Bob_i无法恢复出真正的秘密M，即恢复出的M'与M并不相等，而Eve可对M'纠错从而独自获取秘密M。

然而，根据Hash函数具有“雪崩效应”的特点[24]，可知当消息有1个比特发生改变时，其对应的Hash值将会有大约1/2的比特位发生改变[24]。因此，即使Eve仅改动其子秘密的一小部分(使得M'和M的差别也很小)，由M'所计算出的$H(M'||\mathrm{ID}_A||\mathrm{ID}_B||T)$也将与$R_A$(由$M$计算出)产生较大差别，因此$\mathrm{Bob}_i$通过对比可轻易察觉到攻击行为，从而宣布存在欺骗攻击并将M'作废。因此，Eve实施欺骗攻击无法成功。

4.2　抗伪造攻击性

攻击者Eve可以用Alice的身份通过Hash函数伪造假的R_A发给Bob_i，以此通过验证算法的检测。这里Eve可能会选择两个时机：

第1种情况，在Bob_i发送H序列给Alice的过程中，Eve可以将其截获并发送一个伪造的H'序列给Alice；当Alice将R_A编码在H'序列上发回给Bob_i时，Eve可以再截获H'序列并通过Bell测量窃取R_A，之后对手中的H序列粒子实施假的编码操作并发回给Bob_i，借此来隐藏其欺骗行为。然而，新验证算法是基于Bell态双粒子变换[2]，Bob_i在H序列发给Alice前就已经对S序列的所有粒子实施了相位旋转操作$\boldsymbol{U}(\alpha)$。此时，每一对Bell态均随机地处于式(7)中的3组基(彼此互不正交)之下Eve即使截获了H序列，由于不知道Bob_i对S序列粒子的操作信息$\boldsymbol{U}(\alpha)$，因此其伪造的H'序列在验证算法第2步窃听检测就会被发现。因此，第1种可能的伪造攻击无效。

$$\left.\begin{array}{l} \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\} \\ \left\{\frac{1}{2}(|\phi^+\rangle + \sqrt{3}|\psi^-\rangle), \frac{1}{2}(|\phi^-\rangle + \sqrt{3}|\psi^+\rangle), \frac{1}{2}(|\psi^-\rangle + \sqrt{3}|\phi^+\rangle), \frac{1}{2}(|\psi^+\rangle + \sqrt{3}|\phi^-\rangle)\right\} \\ \left\{\frac{1}{2}(|\phi^+\rangle - \sqrt{3}|\psi^-\rangle), \frac{1}{2}(|\phi^-\rangle - \sqrt{3}|\psi^+\rangle), \frac{1}{2}(|\psi^-\rangle - \sqrt{3}|\phi^+\rangle), \frac{1}{2}(|\psi^+\rangle - \sqrt{3}|\phi^-\rangle)\right\} \end{array}\right\} \tag{7}$$

第2种情况，在Alice将已编码的H_1序列发回Bob_i时，Eve可截获H_1序列并实施相应的变换操作以实现伪造攻击。然而，Eve在验证算法结束前既无法知道秘密M，也无法得到Bob_i所恢复出的信息M'。因此，她无法推测出恰当的$H(M'||\mathrm{ID}_A||\mathrm{ID}_B||T)$来通过验证算法，第2种可能的伪造攻击也无效。

综上，攻击者Eve对该验证算法的伪造攻击不可能成功。

4.3　抗Bell态替换攻击性

在大多数QSS协议中，不诚实者Eve通常使用该攻击策略[20]而窃取其他成员的子秘密信息[2]。而在新验证算法中，Eve也可能用该策略窃取Alice的R_A并且隐藏攻击行为：Eve首先制备大量的Bell态(均为$|\psi^-\rangle$)并将其分成两个粒子序列(不妨设为T'序列和H'序列)；当Bob_i发送H序列给Alice时，Eve截获H序列并发送H'序列(相同粒子数)给Alice；当Alice将R_A编码在H'序列上发回给Bob_i时，Eve可以再将其截获并利用Bell测量窃取R_A，之后伪造假的R_A发给Bob_i。在窃听检测环节，Eve可对手中相应的T'序列和H序列粒子进行Bell测量，通过纠缠交换避免其攻击行为被发现。

然而，当Alice收到伪造的H'序列后，首先会对其中任意f_1个粒子进行单光子测量(随机选基)，完毕后才会向Bob_i告知测量结果和对应位置。此时，由于Eve无法事先知道哪些位置的粒子被测量，因此已经无法通过纠缠交换而隐藏自己。而H'序列粒子与Bob_i的S序列粒子不存在纠缠关联，所以Alice与Bob_i必然会察觉到潜在的攻击行为并中止算法。

另外，假设Eve提前对相应的T'序列和H序列粒子进行Bell测量，使得发送给Alice的H'序列粒子与Bob_i手中对应的S序列粒子建立起最大纠缠。但是，新纠缠态与原纠缠态之间仍相差一个随机的Pauli操作[24]，而Alice在窃听检测通过前不会对粒子进行编码操作，则Bob_i仍然可根据测量结果以3/4的概率察觉到攻击行为，从而中止算法。

综上，攻击者Eve对该验证算法的Bell态替换攻击不可能成功。

5 验证算法效率分析

本文给出的可验证QSS协议基于秘密认证的思想，与现有的基于子秘密认证的可验证QSS协议相比，其验证算法所需要执行的操作次数大幅减少，验证环节消耗的量子态数目也大幅减少。

现有的可验证QSS协议中比较典型的有2011年的Yang协议[11]和2018年的Lu协议[15]，其共同特点为：第一，均为(d,n)门限方案($d\leq n$)；第二，均进行子秘密认证，即若每个子秘密都通过验证才可确保无欺骗攻击。为便于比较，设秘密M的二进制比特数为l，执行秘密恢复环节的代理成员人数为n(此时d=n)，因此Yang协议[11]和Lu协议[15]在验证环节所需的验证次数为n次，所消耗的量子比特数约为$n(n-1)l$。

而本文的可验证QSS协议是验证秘密信息M，验证次数仅为1(Bob$_i$验证Hash值R_A与R'_A是否相等)，而验证算法所需的量子比特数计算如下：首先，经典信息$(M||\mathrm{ID}_A||\mathrm{ID}_B||T)$的二进制比特数可视为$l$(通常ID$_A$, ID$_B$和$T$的比特数远小于$M$的比特数，可忽略)，则其生成的$R_A=H_k(M||\mathrm{ID}_A||\mathrm{ID}_B||T)$的比特数约为$H_k(l)$(根据文献[24]，$H_k(l)\approx 2(k-k_1)$，其中$k_1$极小)，同样地$R'_A=H(M'||\mathrm{ID}_A||\mathrm{ID}_B||T)$的比特数也约为$H_k(l)$，因此验证算法使用Bell态双粒子变换[2]传输$R_A$的总粒子数约为$2H_k(l)$(用于窃听检测的粒子数可忽略)。另外，验证算法事先利用QKD技术分发密钥，则其所需的量子比特数约为$2k$(可视作$2H_k(l)$)。综上，本文协议的总量子比特数约为$4H_k(l)$。与Yang协议[11]和Lu协议[15]相比，其量子态消耗量非常小。

本文协议的验证算法与Yang协议[11]和Lu协议[15]的验证算法在效率方面的对比见表1。

6 结束语

本文首先给出一个可验证QSS协议的一般性模型，并基于Bell态双粒子变换提出一种新的验证算法，从而给出一个对经典信息的可验证QSS协议。新验证算法能够抵抗欺骗攻击等典型攻击策略，且进一步提升了协议效率。值得一提的是，新验证算法可以与任意QSS协议相结合，其适用性非常广泛。

表 1 新协议与现有协议的验证算法效率对比

	Yang协议[11]	Lu协议[15]	本文协议
验证内容	子秘密	子秘密	秘密
验证次数	n	n	1
验证所需量子比特数	$n(n-1)l$	$n(n-1)l$	$4H_k(l)$

注：为便于比较，统一假设各协议中秘密信息比特数为l，代理成员人数为n。另外，新协议中$k<l$。

参 考 文 献

[1] SHAMIR A. How to share a secret[J]. *Communications of the ACM*, 1979, 22(11): 612–613. doi: 10.1145/359168.359176.

[2] DU Yutao and BAO Wansu. Dynamic quantum secret sharing protocol based on two-particle transform of Bell states[J]. *Chinese Physics B*, 2018, 27(8): 080304. doi: 10.1088/1674-1056/27/8/080304.

[3] HILLERY M, BUŽEK V, and BERTHIAUME A. Quantum secret sharing[J]. *Physical Review A*, 1999, 59(3): 1829–1834. doi: 10.1103/PhysRevA.59.1829.

[4] CLEVE R, GOTTESMAN D, and LO H K. How to share a quantum secret[J]. *Physical Review Letters*, 1999, 83(3): 648–651. doi: 10.1103/PhysRevLett.83.648.

[5] CRÉPEAU C, GOTTESMAN D, and SMITH A. Secure multi-party quantum computation[C]. The 34th Annual ACM Symposium on Theory of Computing, Montréal, Canada, 2002: 643–652.

[6] GUO Guoping and GUO Guangcan. Quantum secret sharing without entanglement[J]. *Physics Letters A*, 2003, 310(4): 247–251. doi: 10.1016/S0375-9601(03)00074-4.

[7] ZHANG Zhanjun. Multiparty quantum secret sharing of secure direct communication[J]. *Physics Letters A*, 2005, 342(1/2): 60–66.

[8] YAN Fengli and GAO Ting. Quantum secret sharing between multiparty and multiparty without entanglement[J]. *Physical Review A*, 2005, 72(1): 012304. doi: 10.1103/PhysRevA.72.012304.

[9] LIU Hongwei, MA Haiqiang, WEI Kejin, *et al*. Multi-group dynamic quantum secret sharing with single photons[J]. *Physics Letters A*, 2016, 380(31/32): 2349–2353. doi: 10.1016/j.physleta.2016.05.032.

[10] YANG Yuguang, TENG Yiwei, CHAI Haiping, *et al*. Verifiable quantum (k, n)-threshold secret key sharing[J]. *International Journal of Theoretical Physics*, 2011, 50(3): 792–798. doi: 10.1007/s10773-010-0616-7.

[11] YANG Yuguang, JIA Xin, WANG Hongyang, *et al*. Verifiable quantum (k, n)-threshold secret sharing[J]. *Quantum Information Processing*, 2011, 11(6): 1619–1625. doi: 10.1007/s11128-011-0323-1.

[12] SONG Yun, LI Zhihui, and LI Yongming. A dynamic multiparty quantum direct secret sharing based on generalized GHZ states[J]. *Quantum Information Processing*, 2018, 17(9): 244. doi: 10.1007/s11128-018-1970-2.

[13] 宋云. 基于GHZ态局域测量的量子秘密共享[J]. 电子学报, 2019, 47(7): 1443–1448. doi: 10.3969/j.issn.0372-2112.

2019.07.007.

SONG Yun. Quantum secret sharing based on GHZ states local measurements[J]. *Acta Electronica Sinica*, 2019, 47(7): 1443–1448. doi: 10.3969/j.issn.0372-2112.2019.07.007.

[14] DU Yutao and BAO Wansu. Multiparty quantum secret sharing scheme based on the phase shift operations[J]. *Optics Communications*, 2013, 308: 159–163. doi: 10.1016/j.optcom.2013.06.014.

[15] LU Changbin, MIAO Fuyou, HOU Junpeng, *et al*. Verifiable threshold quantum secret sharing with sequential communication[J]. *Quantum Information Processing*, 2018, 17(11): 310. doi: 10.1007/s11128-018-2059-7.

[16] BAI Chenming, LI Zhihui, and LI Yongming. Sequential quantum secret sharing using a single qudit[J]. *Communications in Theoretical Physics*, 2018, 69(5): 513–518. doi: 10.1088/0253-6102/69/5/513.

[17] YE Chongqiang and YE Tianyu. Circular semi-quantum secret sharing using single particles[J]. *Communications in Theoretical Physics*, 2018, 70(6): 661–671. doi: 10.1088/0253-6102/70/6/661.

[18] YANG Yuguang, GAO Shang, LI Dan, *et al*. Three-party quantum secret sharing against collective noise[J]. *Quantum Information Processing*, 2019, 18(7): 215. doi: 10.1007/s11128-019-2319-1.

[19] WANG Yu, TIAN Caixing, SU Qi, *et al*. Measurement-device-independent quantum secret sharing and quantum conference based on Gaussian cluster state[J]. *Science China Information Sciences*, 2019, 62(7): 72501. doi: 10.1007/s11432-018-9705-x.

[20] 许娟, 陈汉武, 刘文杰, 等. 无纠缠量子秘密共享中酉操作的选择[J]. 中国科学: 信息科学, 2011, 54(9): 1837–1842. doi: 10.1007/s11432-011-4240-9.

XU Juan, CHEN Hanwu, LIU Wenjie, *et al*. Selection of unitary operations in quantum secret sharing without entanglement[J]. *Science China Information Sciences*, 2011, 54(9): 1837–1842. doi: 10.1007/s11432-011-4240-9.

[21] 黄鹏, 周南润, 刘晔. 基于多目标量子远程通信的秘密共享协议[J]. 通信学报, 2008, 29(3): 114–118. doi: 10.3321/j.issn:1000-436X.2008.03.018.

HUANG Peng, ZHOU Nanrun, and LIU Ye. Secret sharing protocol based on multi-target quantum teleportation[J]. *Journal on Communications*, 2008, 29(3): 114–118. doi: 10.3321/j.issn:1000-436X.2008.03.018.

[22] 魏春艳, 蔡晓秋, 王天银, 等. 基于量子不经意密钥传输的量子匿名认证密钥交换协议[J]. 电子与信息学报, 2020, 42(2): 341–347. doi: 10.11999/JEIT190679.

WEI Chunyan, CAI Xiaoqiu, WANG Tianyin, *et al*. Quantum anonymous authenticated key exchange protocol based on quantum oblivious Key transfer[J]. *Journal of Electronics & Information Technology*, 2020, 42(2): 341–347. doi: 10.11999/JEIT190679.

[23] 施荣华, 冯艳艳, 石金晶. 基于正则图上量子游走的仲裁量子签名方案[J]. 电子与信息学报, 2020, 42(1): 89–97. doi: 10.11999/JEIT190597.

SHI Ronghua, FENG Yanyan, and SHI Jinjing. Arbitrated quantum signature scheme with quantum walks on regular graphs[J]. *Journal of Electronics & Information Technology*, 2020, 42(1): 89–97. doi: 10.11999/JEIT190597.

[24] 李宏伟. 量子密钥分配协议的安全性分析[D]. [硕士论文], 解放军信息工程大学, 2009.

LI Hongwei. Security proof of quantum key distribution[D]. [Master dissertation], PLA Information Engineering University, 2009.

杜宇韬：男，1985年生，讲师，主要研究方向为量子密码和量子计算.

鲍皖苏：男，1966年生，教授，主要研究方向为公钥密码、量子密码和量子计算.

李　坦：男，1991年生，博士，主要研究方向为量子计算和量子密码.

责任编辑：马秀强