轻量级的仲裁半量子秘密共享

王 晨
(西安工程大学 计算机科学学院,陕西 西安 710048)

摘 要:半量子秘密共享(SQSS)研究部分参与者只有有限的量子能力时,如何实现保密信息在合法参与者之间安全共享的问题。文中提出了两个新的半量子秘密共享方案,一个是基于单粒子的秘密共享方案,允许多个经典参与者在可信的第三方的帮助下共享密钥,其中经典参与者和第三方的量子能力都是有限的,该协议节约了量子资源,更易于实现;另一个是基于 Bell 态的半量子秘密共享方案,在不可信的第三方帮助下共享密钥,该协议具有更高的安全性。由于减少了参与者的量子设备需求,轻量级的仲裁量子秘密共享方案在未来的云量子场景下具有广泛的应用前景。

关键词:半量子;轻量级;量子秘密共享;可信第三方;云量子场景
中图分类号:TP31 **文献标识码**:A **文章编号**:1673-629X(2021)10-0111-05
doi:10.3969/j.issn.1673-629X.2021.10.019

Lightweight Mediated Semi-quantum Secret Sharing

WANG Chen
(School of Computer Science, Xi'an Polytechnic University, Xi'an 710048, China)

Abstract: Semi-quantum secret sharing (SQSS) studies how to realize the secure sharing of confidential information among legitimate participants when some participants have only limited quantum capabilities. Two new secret sharing scheme are proposed. One is the secret sharing scheme based on single particle, which allows multiple classic participants to share secret with the help of the trusted third party (TP). The quantum capacity of classic participants and the TP is limited. The agreement saves quantum resources and is easier to implement. The other is the secret sharing scheme based on Bell state, which shares the secret keys with the help of untrusted TP, with higher security. Since the protocol reduces the quantum device requirements of the participants, the lightweight arbitration quantum secret sharing scheme will be more practical in future cloud quantum scene.

Key words: semi-quantum; lightweight; quantum secret sharing; untrusted third party; cloud quantum scene

0 引 言

量子密码学的一个重要分支是量子秘密共享(QSS)[1]。量子秘密共享将秘密分发给多个参与者,只有授权参与者共同合作才可以恢复初始秘密。1999 年,Hillery 等人[1]提出的 Greenberger-Horne-Zeilinger(GHZ)态是第一个基于量子秘密共享方案;1999 年,Gottesman 等人[2]提出了量子秘密共享方案,秘密信息被划分为 n 份,任意 k 份都可以用于恢复秘密,并且证明了阈值方案存在的限制是来自量子不可克隆定理;2000 年,Gottesman[3]给出了量子秘密共享理论的一些重要结果,证明了具有一般访问结构的量子秘密共享方案存在的唯一限制是单调性和不可克隆定理;2001 年,Tittel 等人[4]提出了基于纠缠的量子秘密共享实验方案,利用参量下转换创建两个纠缠光子,模拟三量子比特 GHZ 态[1];2003 年,Guo 等人[5]提出了不使用纠缠态的量子秘密共享协议,其理论效率接近 100%;2004 年,Deng 等人[6]提出了基于测量的量子秘密共享方案,根据测量结果形成的字符串的奇偶性,给出共享秘密信息的显示表达式,该方案不仅可以保障协议的安全性,并且其效率渐近为 100%;2005 年,Ogawa 等人[7]提出了新的量子秘密共享方案,参与者无法从自己的秘密中获取任何量子秘密信息,该协议满足了机密性;2014 年,Liao 等人[8]提出具有添加新代理的简便方法,对撤销的代理进行诚实性检测;自此,其他量子秘密共享方案随后被提出。

尽管在最近几十年来出现了各种量子秘密共享协议,但是由于量子设备造价高昂,更可能的应用场景是只有少数的公司和政府机构能够拥有量子计算机。因此,如何降低量子能力是一个值得研究的领域。为了减轻协议的量子负担,2007 年 Boyer 等人提出了半量

收稿日期:2020-12-11 **修回日期**:2021-04-13
基金项目:陕西省创新基金项目(chx2020029)
作者简介:王 晨(1995-),女,硕士研究生,通信作者,研究方向为量子密码学。

子的想法[9],在 2009 年,Boyer 等人提出了半量子密钥分发协议,该协议被证明对窃听者是完全鲁棒的,无论对手做什么操作均会被检测到。这里的半量子环境是指,协议中部分参与者是量子方,具有无限量子能力;而另外一些参与方是经典方仅需要有限的量子能力,只执行以下几种操作:(1)在 Z 基上测量量子比特;(2)在 Z 基上制备量子比特,{| 0〉,| 1〉};(3)无干扰的反射量子比特;(4)通过不同的延迟线重新排列量子比特。随后,半量子密码协议得到了一定的发展。2010 年,Li 等人[10]提出了两种使用最大纠缠 GHZ 态的半量子秘密共享协议;2012 年,Wang 等人[11]通过使用两个粒子纠缠态进而提出了半量子秘密共享协议,经典的参与者只能执行制备粒子或者反射粒子的操作;2015 年,Xie 等人[12]提出了一种新的指定比特的半量子秘密共享协议,即量子参与者可以与经典参与者共享特定的消息;2018 年,Li 等人[13]提出了有限资源内的半量子秘密共享协议。

为了进一步减轻协议参与者的量子负担,可以引入第三方进行量子计算等操作。2015 年,Krawec[14]首次提出了仲裁半量子密钥分发协议,两个参与者在不可信量子第三方的协助下分发密钥。2018 年,Liu 等人[15]提出了经典方不需要测量能力的中介半量子密钥分发协议。2019 年,Tsai 等人[16]提出了轻量级的量子密钥分发协议,两个参与者和第三方都是经典用户,使用单向传输策略,提出的协议更实用。2019 年,Lin 等人[17]提出了新的中介半量子密钥分发协议,该协议允许两个经典参与者在不受信任的第三方帮助下共享秘密密钥。受上述研究启发[18-20],文中提出了轻量级的仲裁量子秘密共享方案,即量子方(可信或者不可信的第三方)和经典方的能力均是有限的,减少了量子开销,使该协议更加易于实现。

1 协议描述

1.1 第三方可信的半量子秘密共享协议

本节介绍了中介可信的量子秘密共享协议,提出的协议允许参与者 Alice(dealer)和 $n-1$ 个经典代理方 $Bob_1, Bob_2, \cdots, Bob_{n-1}$ 在第三方 TP 的帮助下共享密钥。TP 是诚实的,即 TP 必须严格遵守协议的规则。关于参与者有限的量子能力的具体描述在表 1 中给出。假设参与秘密共享协议共有 n 个参与者,Alice(dealer)需要在可信第三方 TP 的帮助下共享密钥 K 给 $n-1$ 个参与者,协议的具体执行内容如下:

(1)TP 随机地制备 δ 个 BB84 粒子 {| +〉,| −〉,| 0〉,| 1〉},并且发送给 Alice(δ 是一个固定参数,且 δ 远大于 n)。

(2)Alice 收到 TP 发送的粒子序列后,随机执行以下两种操作:

表 1 有限量子能力的具体描述

参与方	可执行操作
Alice(庄家)	在 Z 基上制备量子比特 在 Z 基上测量量子比特 无干扰的反射量子比特
$Bob_1, Bob_2, \cdots, Bob_{n-1}$(参与者)	在 Z 基上制备量子比特 在 Z 基上测量量子比特 无干扰的反射量子比特
TP(可信的第三方)	制备 BB84 粒子 测量 BB84 粒子 诚实执行协议

①Alice 以概率 p 对收到的粒子无干扰地反射给 Bob_1(CTRL);

②Alice 以概率 $1-p$ 丢弃收到的粒子,随机在 Z 基上重新制备量子比特({| 0〉,| 1〉}),并且发送给 Bob_1(SIFT)。

(3)Bob_1 收到来自 Alice 发送的粒子后,随机执行以下两种操作:

①反射:Bob_1 以概率 p 对收到的粒子无干扰地反射给 TP(CTRL)。

②测量重发:Bob_1 以概率 $1-p$ 对收到的粒子用 Z 基测量,并且随机在 Z 基上制备量子比特({| 0〉,| 1〉}),并且发送给 TP(SIFT)。

(4)TP 接收到 Bob_1 发送的粒子后,通知 Alice 和 Bob_1 进行窃听检测。Alice 和 Bob_1 在公共信道公布在哪个粒子位置上执行的 CTRL 操作,对 Alice 和 Bob_1 都选择执行 CTRL 的粒子进行测量,TP 测量结果应和初始态一致,若错误率高于阈值,则终止协议并重新开始。

(5)在 Bob_1 和 Alice 都选择 SIFT 操作的位置,这些粒子(以概率$(1-p)*(1-q)$)作为 Alice 共享给 Bob_1 的密钥 K_1 的编码量子比特({| 0〉,| 1〉,| 1〉,…,| 0〉} 分别代表 0,1 比特)。

(6)同理,Alice 和 $Bob_2, \cdots, Bob_{n-1}$ 在 TP 的帮助下共享密钥 $K_2 \cdots K_{n-1}$,重复步骤 1 ~ 5。最终,$K = K_1 \oplus K_2 \oplus \cdots \oplus K_{n-1}$ 作为所有参与者共享密钥,只有所有的 Bob 共同合作才能恢复该密钥。

1.2 中介不可信的半量子秘密共享协议

本节介绍了中介不可信的量子秘密共享协议,提出的协议中参与秘密共享协议的成员有 Alice(dealer)、Bob 和 Charlie,三个参与者在 TP 的帮助下共享密钥。TP 是不可信的,即必须验证 TP 的诚实性。关于参与者有限量子能力的具体描述在表 2 中给出。

假设 Alice 需要在不可信第三方帮助下共享密钥 K 给 Bob 和 Charlie,协议的具体内容如下:

(1)一个不可信的第三方 TP 生成 n 个 $|\Phi^+\rangle$ 态,其中 $|\Phi_i^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{12}$ 且 $i = 1, 2, \cdots, n$,第 i

个 $|\Phi^+\rangle$ 态用 $|\Phi_i^+\rangle$ 表示,并且发送生成的量子态给 Alice。

表 2　有限量子能力的具体描述

参与方	可执行操作
Alice(庄家)	制备 BB84 粒子 在 Z 基上制备和测量量子比特
Bob,Charlie (参与者)	在 Z 基上制备量子比特 在 Z 基上测量量子比特 无干扰的反射量子比特
TP(不可信的 第三方)	制备 Bell 态 测量 Bell 态

(2)Alice 收到量子序列后,将收到的量子序列划分为两个子序列 S_1,S_2,Alice 将共享给 Bob 和 Charlie 的密钥 K 插入 m 个 BB84 窃听检测粒子中,再将插入后的粒子序列插入两个子序列 S_1,S_2 中,记插入后量子序列为 S_1',S_2',将 S_1',S_2' 分别发送给 Bob 和 Charlie。

(3)Bob 和 Charlie 在收到 Alice 发送的量子序列后,随机执行两种操作:

①CTRL:以概率 p 对收到的粒子无干扰地反射给 TP;

②SIFT:以概率 $1-p$ 对收到的粒子用 Z 基测量并随机制备量子态发送给 TP。

(4)TP 收到来自 Bob 和 Charlie 的所有量子态并且按顺序存储,按照顺序结合收到的粒子进行 Bell 测量,并且公布测量结果及初始态,Bob 和 Charlie 计算选择 SIFT 的初始态且检测 SIFT 比特错误率。若 Z-SIFT 错误率高于预先设定的阈值 P_{SIFT},那么中止协议。

(5)Alice 公布插入窃听检测粒子的位置,Bob 和 Charlie 公布执行 Z-SIFT 操作的位置,TP 对比 Bob 和 Charlie 选择 CTRL 的量子态并且检测 CTRL 比特错误率。若 Z-SIFT 错误率高于预先设定的阈值 P_{CTRL},那么中止协议。

(6)Alice 随机选择插入窃听检测粒子中的 Z-SIFT 比特为密钥 K_1,K_2,通知 Bob 和 Charlie 公布剩余诱骗粒子为自身 Z-SIFT 粒子的测量结果。若 Z-SIFT 错误率高于预先设定的阈值 P_{TEST},那么协议中止。

(7)Bob 和 Charlie 记录未公布测量结果的 Z-SIFT 为 K_1,K_2,最终 $K_1 \oplus K_2$ 为共享密钥,只有 Bob 和 Charlie 合作才能恢复密钥。

1.3　中介可信的半量子秘密共享验证

本节中,中介可信的量子秘密共享协议允许参与者 Alice(dealer)和 2 个经典代理方 Bob_1,Bob_2 在 TP 的帮助下共享密钥。TP 是诚实的,即 TP 必须严格遵守协议的规则。假设参与秘密共享协议共有 3 个参与者,Alice(dealer)需要在可信第三方(TP)的帮助下共享密钥 K 给 2 个参与者,协议的具体执行内容如下:

(1)TP 随机地制备 20 个 BB84 粒子 $\{|+\rangle,|0\rangle,|-\rangle,|1\rangle,|-\rangle,|+\rangle,|0\rangle,|1\rangle,|1\rangle,|+\rangle,|-\rangle,|0\rangle,|+\rangle,|1\rangle,|-\rangle,|1\rangle,|0\rangle,|+\rangle,|-\rangle,|1\rangle\}$ 并且发送给 Alice。

(2)Alice 收到 TP 发送的粒子序列后,执行以下两种操作:

①Alice 对收到的粒子序列为奇数的粒子无干扰地反射给 Bob_1(CTRL);

②Alice 丢弃收到的其余粒子,随机在 Z 基上重新制备量子比特($\{|0\rangle,|1\rangle\}$),并且发送给 Bob_1(SIFT)。

操作后的粒子序列为 $\{|+\rangle,|0\rangle,|-\rangle,|1\rangle,|-\rangle,|0\rangle,|0\rangle,|1\rangle,|1\rangle,|0\rangle,|-\rangle,|0\rangle,|+\rangle,|1\rangle,|-\rangle,|1\rangle,|0\rangle,|1\rangle,|-\rangle,|1\rangle\}$。

Bob_1 收到来自 Alice 发送的粒子后,执行以下两种操作:

①Bob_1 对收到的粒子序列为 3 的倍数的粒子无干扰地反射给 TP(CTRL);

②测量重发:Bob_1 对收到的其余粒子用 Z 基测量,并且随机在 Z 基上制备量子比特($\{|0\rangle,|1\rangle\}$),并且发送给 TP(SIFT)。

操作后的粒子序列为 $\{|1\rangle,|0\rangle,|-\rangle,|1\rangle,|0\rangle,|0\rangle,|0\rangle,|1\rangle,|1\rangle,|0\rangle,|1\rangle,|0\rangle,|1\rangle,|1\rangle,|-\rangle,|1\rangle,|0\rangle,|0\rangle,|0\rangle,|1\rangle\}$。

(3)TP 接收到 Bob_1 发送的粒子后,通知 Alice 和 Bob_1 进行窃听检测。Alice 和 Bob_1 在公共信道公布在哪个粒子位置上执行的 CTRL 操作,对 Alice 和 Bob_1 都选择执行 CTRL 的粒子进行测量,TP 的测量结果应和初始态一致,最终检测粒子序列为 $\{|-\rangle,|1\rangle,|-\rangle\}$。

(4)在 Bob_1 和 Alice 都选择 SIFT 操作的位置,这些粒子作为 Alice 共享给 Bob_1 的密钥 K_1 的编码量子比特,($\{|0\rangle,|1\rangle\}$ 分别代表 0,1 比特),最终量子比特为 $\{|0\rangle,|1\rangle,|1\rangle,|0\rangle,|1\rangle,|1\rangle,|1\rangle\}$。

(5)TP 随机地制备 20 个 BB84 粒子 $\{|-\rangle,|0\rangle,|+\rangle,|0\rangle,|1\rangle,|+\rangle,|-\rangle,|1\rangle,|+\rangle,|0\rangle,|1\rangle,|+\rangle,|-\rangle,|0\rangle,|-\rangle,|0\rangle,|0\rangle,|-\rangle,|+\rangle,|0\rangle\}$ 并且发送给 Alice。

(6)Alice 收到 TP 发送的粒子序列后,执行以下两种操作:

①Alice 对收到的粒子序列为奇数的粒子无干扰地反射给 Bob_2(CTRL);

②Alice 丢弃收到的其余粒子,随机在 Z 基上重新制备量子比特($\{|0\rangle,|1\rangle\}$),并且发送给 Bob_2(SIFT)。

操作后的粒子序列为 $\{|-\rangle,|0\rangle,|+\rangle,|1\rangle,|1\rangle,|0\rangle,|-\rangle,|1\rangle,|+\rangle,|0\rangle,|1\rangle,|0\rangle,|-\rangle,$

$|1\rangle, |-\rangle, |0\rangle, |0\rangle, |1\rangle, |0\rangle, |0\rangle\}$ 。

Bob_2 收到来自 Alice 发送的粒子后,执行以下两种操作:

①Bob_2 对收到的粒子序列为 3 的倍数的粒子无干扰地反射给 TP(CTRL);

②测量重发:Bob_2 对收到的其余粒子用 Z 基测量,并且随机在 Z 基上制备量子比特($\{|0\rangle, |1\rangle\}$),并且发送给 TP(SIFT)。

操作后的粒子序列为$\{|1\rangle, |0\rangle, |+\rangle, |1\rangle, |1\rangle, |0\rangle, |1\rangle, |1\rangle, |+\rangle, |0\rangle, |1\rangle, |0\rangle, |-\rangle, |1\rangle, |-\rangle, |0\rangle, |0\rangle, |1\rangle, |0\rangle, |0\rangle\}$ 。

(7)TP 接收到 Bob_2 发送的粒子后,通知 Alice 和 Bob_2 进行窃听检测。Alice 和 Bob_2 在公共信道公布在哪个粒子位置上执行的 CTRL 操作,对 Alice 和 Bob_2 都选择执行 CTRL 的粒子进行测量,TP 的测量结果应和初始态一致,最终检测粒子序列为$\{|+\rangle, |+\rangle, |-\rangle\}$。

(8)在 Bob_2 和 Alice 都选择 SIFT 操作的位置,这些粒子作为 Alice 共享给 Bob_2 的密钥 K_2 的编码量子比特,($\{|0\rangle, |1\rangle\}$ 分别代表 0,1 比特),最终量子比特为$\{|0\rangle, |1\rangle, |1\rangle, |0\rangle, |1\rangle, |0\rangle, |0\rangle\}$ 。

(9)Alice 和 Bob_1,Bob_2 在 TP 的帮助下共享密钥 K_1,K_2,最终,$K = K_1 \oplus K_2$ 作为所有参与者共享密钥,最终共享密钥为$\{|0\rangle, |0\rangle, |0\rangle, |0\rangle, |0\rangle, |1\rangle, |1\rangle\}$,只有 Bob_1 和 Bob_2 共同合作才能恢复该密钥。

2 安全分析

2.1 特洛伊木马攻击

常见的木马攻击有两种:延迟光子木马攻击和隐形光子窃听。特洛伊木马攻击是一种常见的攻击,外部攻击者可能会将特洛伊木马光子插入 TP 发送的量子比特中,尝试通过特洛伊木马光子获得信息[21]。两个协议中,参与者可以引入光波过滤器来检测是否存在多光子信号,因而参与者收到的都是滤波器过滤后的具有合法波长的粒子,这样可以抵抗来自 Eve 的隐形光子窃听。

2.2 联合攻击

中介可信的半量子秘密共享协议中将证明一个或多个不诚实的参与者无法获得最终密钥[22-23]。在此,考虑最极端的情况,有一部分参与者是不诚实的,在这种情况下,不诚实方具有最大的权力。首先,若没有 Bob_1 的帮助下,$Bob_2 \cdots Bob_{n-1}$ 相互串通想获得最终的密钥。若是想知道 Bob_1 的密钥,只有检测发送给 Bob_1 的粒子,若是在 Alice 发送给 Bob_1 的过程中,他们不知道具体的位置,协议继续进行则成为拦截攻击,TP 会检测出;其次,若是在 Bob_1 发送给 TP 的过程中窃听,则没有意义。并且 $Bob_2 \cdots Bob_{n-1}$ 可相互独立,但是,这些信息仍然无法获取。因此,协议可以抵抗内部攻击。

中介不可信的半量子秘密共享协议中,因为第三方、Alice、Bob 和 Charlie 是互相检验诚实性,若一方不诚实,协议无法继续进行,因此可发现潜在的联合攻击。

2.3 外部攻击

外部攻击者(Eve)将执行一系列操作,以达到窃取密钥的目的。因此,存在拦截攻击,攻击者进行信息拦截攻击,外部攻击者 Eve 可能会尝试根据测量结果来拦截传输的量子比特,在中介可信的半量子秘密共享协议中,可以在第 3 步中从 Alice 发送给 Bob 的量子比特随机测量,测量这些量子比特后,Eve 会获得有关密钥的信息,将假的量子比特发送给 Bob,Bob 再将粒子发送给第三方(TP),第三方测量反射粒子,并计算错误率。在这里,Eve 测量重发的量子位不被发现的概率为 $\frac{1}{2}$,因为参数 δ 的数值较大,所以 Eve 只测量几个量子比特是不会影响协议的正常进行。假设 Eve 攻击了 l 个量子位,那么在第 4 步不被发现的概率为 $(\frac{1}{2})^y$。也就是说,Eve 攻击成功的概率为 $1-(\frac{1}{2})^y$。这意味着如果 l 足够大,则检测到攻击者的概率几乎接近 1。外部攻击者(Eve)还可以执行操作,使 Alice 共享给 Bob 的密钥没有意义,在本协议中,可以在第 3 步中从 Alice 发送给 Bob 的量子比特随机执行单一操作,假设 Eve 执行的 X 操作,$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$。Eve 可以不获取信息,仅仅恶意篡改协议的比特值,使用 X 运算来改变量子比特的状态。即可以将 $|0\rangle$ 或 $|1\rangle$ 更改为 $|1\rangle$ 或 $|0\rangle$,$|+\rangle$,$|-\rangle$ 态不会发生变化,其中 $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$,$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$。如果 Eve 仅仅攻击一个量子位,不被发现的概率为 $\frac{1}{2}$(因为 X 基的本征态为 $|+\rangle, |-\rangle$)。但是,因为参数 δ 的数值较大,所以 Eve 只修改几个量子比特是不会影响协议的正常进行。假设 Eve 攻击了 l 个量子位,那么在第 4 步不被发现的概率为 $(\frac{1}{2})^x$。也就是说,Eve 攻击成功的概率为 $1-(\frac{1}{2})^x$。这意味着如果 l 足够大,则检测到攻击者的概率几乎接近 1。所以本协议在受到外部攻击情况下,仍然是安全的。

3 结束语

和现有的协议相比较[24-25]:对于半量子环境,在测量重发和丢弃重发环境中设计该协议,协议中,参与

方都是“经典的”,经典参与者具有相同的量子能力,包括用 Z 基测量量子比特,以 Z 基制备量子比特,和无干扰反射量子比特。在量子资源方面,现有的半量子秘密共享协议中,量子方需要无限的量子能力,来保持协议的正常进行,在该方案中,对于第三方 TP 的量子能力要求也是有限的,参与者只需生成 Z 基的单个光子。降低了量子 TP 的量子能力,不需要完全的量子能力,这些使该协议更加实用和轻便。文中在的第三方 TP 的帮助下,提出了一种轻量级仲裁量子秘密共享方案,允许经典参与者在具有有限量子能力 TP 的帮助下共享密钥,因为 dealer 只需要生成 Z 基量子位的能力,经典参与者和 TP 的量子能力都是有限的,该协议节约了量子资源,提高了协议的实用性。尽管在半量子领域中共享密钥的无条件安全性仍然很困难[26-29],但是所提出的协议可免受各种众所周知的攻击。在这里,不增加 TP 量子能力的情况下,如何将参与者的能力降低也是一个有挑战的问题,需要进一步研究。

参考文献:

[1] HILLREY M, BUAEK V, BERTHIAUME A. Quantum secret sharing[J]. Physical Review A, 1999, 59(3): 1829-1834.

[2] CLEVE R, GOTTESMAN D, LO H. How to share a quantum secret[J]. Physical Review Letters, 1999, 83(3): 648-651.

[3] GOTTESMAN D. Theory of quantum secret sharing[J]. Physical Review A, 2000, 61(4): 042311.

[4] TITTEL W, ZBINDEN H, GISIN N. Experimental demonstration of quantum secret sharing[J]. Physical Review A, 2001, 63: 042301.

[5] GUO G P, GUO G C. Quantum secret sharing without entanglement[J]. Physics Letters A, 2003, 310(4): 247-251.

[6] LI X, LONG G L, DENG F G, et al. Efficient multiparty quantum-secret-sharing schemes[J]. Physical Review A. 2004, 69(5): 052307.

[7] OGAWA T, SASAKI A, IWAMOTO M, et al. Quantum secret sharing schemes and reversibility of quantum operations [J]. Physical Review A, 2005, 72(3): 032318.

[8] LIAO C H, YANG C W, HWANG T. Dynamic quantum secret sharing protocol based on GHZ state[J]. Quantum Information Processing, 2014, 13: 1907-1916.

[9] BOYER M, GELLES R, KENIGSBERG D, et al. Semi-quantum key distribution[J]. Physical Review A, 2009, 79(3): 032341.

[10] LI Q, CHAN W H, LONG D Y. Semi-quantum secret sharing using entangled states[J]. Physical Review A, 2010, 82(2): 022303.

[11] WANG J, ZHANG S, ZHANG Q, et al. Semi-quantum secret sharing using two-particle entangled state[J]. International Journal of Quantum Information, 2012, 10(5): 1250050.

[12] XIE C, LI L, QIU D. A novel semi-quantum secret sharing scheme of specific bits[J]. International Journal of Theoretical Physics, 2015, 54(10): 3819-3824.

[13] LI Z, LI Q, LIU C, et al. Limited resource semi-quantum secret sharing[J]. Quantum Information Processing, 2018, 17(10): 285.

[14] KRAWEC W O. Mediated semi-quantum key distribution [J]. Physical Review A. 2015, 91(3): 032323.

[15] LIU Z R, HWANG T. Mediated semi-quantum key distribution without invoking quantum measurement[J]. Annalen der Physik, 2018, 530: 1700206.

[16] TSAI C T, YANG C W, LEE N Y. Lightweight mediated semi-quantum key distribution protocol[J]. Modern Physics Letters A, 2019, 34: 1950281.

[17] LIN P H, TSAI C W, HWANG T. Mediated semi-quantum key distribution using single photons[J]. Annalen der Physik, 2019, 531(8): 1800347.

[18] LIU F, QIN S J, WEN Q Y. A quantum secret-sharing protocol with fairness[J]. Physica Scripta, 2014, 89(7): 075104.

[19] LIU L L, TSAI C W, HWANG T. Quantum secret sharing using symmetric W state[J]. International Journal of Theoretical Physics, 2012, 51: 2291-2306.

[20] LAU H K, WEEDBROOK C. Quantum secret sharing with continuous-variable cluster states[J]. Physical Review A, 2013, 88(4): 042313.

[21] LI L, QIU D, MATEUS P. Quantum secret sharing with classical Bobs[J]. Journal of Physics A: Mathematical and Theoretical, 2013, 46(4): 1-10.

[22] MARKHAM D, SANDERS B C. Graph states for quantum secret sharing[J]. Physical Review A, 2008, 78(4): 042309.

[23] YANG C W, HWANG T. Efficient key construction on semi-quantum secret sharing protocols[J]. International Journal of Quantum Information, 2013, 11(5): 1350052.

[24] YE C Q, YE T Y, HE D, et al. Multiparty semi-quantum secret sharing with d-level single-particle states[J]. International Journal of Theoretical Physics, 2019, 58(19): 3797-3814.

[25] QIN H, WALLACE K S, TSO R, et al. Rational quantum secret sharing[J]. Scientific Reports, 2019, 8(1): 11115.

[26] 王娅如,李富林,朱士信. 可验证的动态多秘密共享方案[J]. 合肥工业大学学报:自然科学版, 2019, 42(12): 1725-1728.

[27] 李梦慧,田有亮. 基于分组的理性秘密共享方案[J]. 密码学报, 2017, 4(3): 209-217.

[28] 刘　海,李兴华,田有亮,等. 理性公平的秘密共享方案[J]. 计算机学报, 2020, 43(8): 1517-1533.

[29] 茹秀娟,李俊州. 基于单向函数的多秘密共享方案[J]. 开封大学学报, 2013, 27(3): 94-96.