中国科学: 物理学 力学 天文学 2025 年 第 55 卷 第 1 期: 210311
SCIENTIA SINICA Physica, Mechanica & Astronomica physcn.scichina.com
《中国科学》杂志社 SCIENCE CHINA PRESS
论 文

半量子群代理盲签名

谈笑, 甘志刚, 叶天语*

浙江工商大学信息与电子工程学院, 杭州 310018
*联系人, E-mail: yetianyu@zjgsu.edu.cn

收稿日期: 2024-05-07; 接受日期: 2024-06-20; 网络出版日期: 2024-10-29
国家自然科学基金(编号: 62071430)资助项目

摘要 本文提出了半量子群代理盲签名方案, 其中签名验证者和部分代理签名者仅配备部分量子能力. 该方案在保证原始消息拥有者的原始消息内容对原始签名者、签名验证者、代理签名组和帮助完成签名过程的可信第三方都是盲的基础上实现原始签名者授权代理签名组对其进行签名. 经详细证实, 该方案拥有不可伪造性、不可否认性、完全的盲性以及安全性. 由于签名验证者和部分代理签名者都仅配备部分量子能力, 比起许多已被提出的量子群代理盲签名方案, 该方案具有更广泛的签名应用场景.

关键词 半量子群代理盲签名, 盲性, 不可伪造性, 不可否认性

PACS: 03.67.Dd, 03.67.Hk, 03.67.Pp

1 引言

加密技术中的数字签名[1], 旨在确保电子文件或数据的完整性与来源的可信性, 可有效避免文件遭到篡改或伪造. 其操作流程大致如下: 首先, 信息的发送方会使用个人私钥对文件的哈希值进行加密, 从而产生一个独一无二的数字签名; 随后, 接收方利用发送方提供的公钥来对数字签名进行解密, 以此来检验文件的完整性与真实性. 数字签名技术在多个领域发挥着关键作用, 被广泛应用于电子商务、网络安全以及数字证书等多个行业.

量子密码学依托于量子力学的基本原理, 最早由Bennett与Brassard[2]于1984年提出. 量子签名技术可被看作是量子密码学与经典数字签名技术的结合体. 经典数字签名凭靠求解数学问题的高复杂性获得高安全性, 但这种安全性在强大的量子并行计算面前很可能将不复存在. 与之相对, 量子签名技术可抵御来自具有高度并行处理能力的量子计算机的潜在威胁. 至今, 量子签名技术已经衍生出多个子领域, 包括量子仲裁签名[3–8]、量子盲签名[9,10]、量子代理签名[11]以及量子代理盲签名[12–21]等. 其中, 量子代理盲签名要求在确保消息内容不被泄露给除代理签名者之外的任何人的前提下, 代理签名者代表原始签名者完成对信息进行签名. 量子代理盲签名技术可被视为量子盲签名和量子代理签名技术的结合. 根据参与签名过程的代理签名者的数量, 量子代理盲签名可被进一步细分为量子

引用格式: 谈笑, 甘志刚, 叶天语. 半量子群代理盲签名. 中国科学: 物理学 力学 天文学, 2025, 55: 210311
Tan X, Gan Z G, Ye T Y. Semiquantum group proxy blind signature (in Chinese). Sci Sin-Phys Mech Astron, 2025, 55: 210311, doi: 10.1360/SSPMA-2024-0169

© 2024 《中国科学》杂志社

单代理盲签名和量子群代理盲签名. 文献[12–14,19]的协议都属于量子单代理盲签名协议, 文献[15–18,20,21]的协议都属于量子群代理盲签名协议.

2007年, Boyer等人[22]构造了半量子密码方案. 半量子密码方案往往存在半量子参与者; 半量子参与者只拥有部分的量子能力, 即只能利用Z基(即$\{|0\rangle, |1\rangle\}$)测量粒子、制备粒子处于Z基、通过量子信道传送粒子以及置乱粒子[22,23]. 随后, 半量子密码很快被融入到量子数字签名从而诞生了半量子数字签名. 已有少数几种半量子签名方案[24–31]被提出. 2019年, Zhao等人[24]设计了一种基于W态量子隐形传态的带两个签名者的半量子双签名方案. 2020年, Zheng等人[25]构造了一个新颖的使用量子游走和隐形传态的半量子代理签名方案; Chen等人[26]构造了一个基于四粒子团簇态的仲裁半量子签名方案. 2021年, Xia等人[27]利用五粒子GHZ态设计了一种半量子盲签名方案; Chen和Yan[28]利用Bell态纠缠交换设计了一个半量子盲签名方案. 2022年, 王俊辉等人[29]构造了抗集体噪声半量子盲签名方案. 2023年, Zhang等人[30]利用类GHZ态构造了半量子指定验证者签名方案. 2024年, 谈笑和叶天语[31]提出了一种基于χ态量子隐形传态的半量子代理盲签名方案. 半量子群代理盲签名协议的研究鲜有报道.

基于以上分析, 本文构造了半量子群代理盲签名方案. 因签名验证者和部分代理签名者仅配备有限量子能力, 与已有的许多量子群代理盲签名方案相比, 本方案具有更广泛的签名应用场景.

2 协议描述

二维量子系统的4个Bell态被定义为

$$\left|\phi_{u_1,u_2}\right\rangle = \frac{1}{\sqrt{2}}\sum_{j=0}^{1}(-1)^{ju_1}\left|j, j\oplus u_2\right\rangle, \tag{1}$$

其中, u_1, $u_2\in\{0,1\}$, 符号"$\oplus$"表示异或操作. 二维量子系统的两个酉操作被定义为

$$U_\beta = \sum_{j=0}^{1}\left|j\right\rangle\left\langle j\oplus\beta\right|, \tag{2}$$

其中, $\beta\in\{0,1\}$.

二维量子系统的n粒子GHZ态被定义为

$$\left|G\right\rangle_{123\ldots n} = \frac{1}{\sqrt{2}}\left(\underbrace{|0\rangle|0\rangle\ldots|0\rangle}_{n} + \alpha\underbrace{|1\rangle|1\rangle\ldots|1\rangle}_{n}\right)_{123\ldots n}, \tag{3}$$

其中, $\alpha\in\{-1, 1\}$. 根据文献[21]可知推理1.

推理1 在对式(3)的粒子1到粒子n都进行X基测量后, 如果所有测量结果中的$|-\rangle$的个数为偶数, 则有$\alpha=1$; 如果所有测量结果中的$|-\rangle$的个数为奇数, 则有$\alpha=-1$.

这里, X基为$\{|+\rangle, |-\rangle\}$, $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.

假设Alice持有原始的待签名消息, Bob是需外授签名权的原始签名者, Charlie的作用是核验签名是否有效, Trent扮演起到帮助作用的可信第三方, David是接受Bob签名权的代理签名人小组, 其小组成员为David$_j$, 其中j=1,2,⋯,n. 其中, Alice, Bob, Trent和David$_Q$ = {David$_1$, David$_2$, ⋯, David$_t$}配备全部量子能力, Charlie和David$_C$ = {David$_{t+1}$, David$_{t+2}$, ⋯, David$_n$}仅配备部分量子能力, 其中$t\in$N$_+$且$0<t<n$, N$_+$为正整数集.

为了实现"Alice的原始消息对其他人具有盲性且David组接受Bob授权对其完成签名"这一目标, 本文提出一个新颖的半量子群代理盲签名方案.

2.1 第一阶段: 初始化过程

步骤1: David$_Q$组中的David$_i$和Trent使用安全的量子密钥分配方案[2]建立拥有q个比特的密钥序列, 其中i=1,2,⋯,t. David$_C$组中的David$_r$和Trent使用安全的半量子密钥分配方案[22]建立拥有q个比特的密钥序列, 其中$r=t+1, t+2, \cdots, n$. 为简单起见, David$_j$和Trent建立的长度为q的密钥序列被记为k_{D_jT}, 其中 $k_{D_jT} = \left(k_{D_jT_1}, k_{D_jT_2}, \ldots, k_{D_jT_q}\right)$, $k_{D_jT_x}\in\{0,1\}$, x=1, 2,⋯, q, j=1, 2, ⋯, n.

Charlie和Trent使用半量子密钥分配方案[22]建立拥有qn个比特的密钥序列$k_{TC} = \left(k_{TC_1}, k_{TC_2}, \ldots, k_{TC_{qn}}\right)$, 其中$k_{TC_y}\in\{0,1\}$, y=1,2,⋯, qn.

步骤2: Alice的待签名消息记为g=(g_1, g_2, ⋯, g_q), 其中$g_x\in\{0,1\}$, x=1,2,⋯,q. Alice随机生成一个长度为q的经典序列l=(l_1, l_2, ⋯, l_q), 其中$l_x\in\{0,1\}$, x=1, 2, ⋯, q. Alice通过计算$m_x = g_x\oplus l_x$得到经典盲消息m=(m_1, m_2, ⋯, m_q), 其中$m_x\in\{0,1\}$, x=1,2,⋯,q. Alice计算$H_1(m)$, 并将其发送给Charlie, 其中$H_1(\cdot)$为仅由Alice和Charlie

之间共享的抗碰撞单向哈希函数.

2.2 第二阶段: 盲化过程

首先, Alice根据m制备$n-t+1$份相同的量子态序列$M=\left(\left|m_1\right\rangle,\left|m_2\right\rangle,...,\left|m_q\right\rangle\right)$. 接着, Alice制备$n-t+1$份不同的由数量足够多的随机处于$\left\{\left|0\right\rangle,\left|1\right\rangle,\left|+\right\rangle,\left|-\right\rangle\right\}$的诱骗粒子构成的诱骗粒子序列, 并将每份诱骗粒子序列随机插入M得到M'. 最后, Alice将1份M'发送给David$_1$, 将$n-t$份M'发送给David$_C$组, David$_C$组中的David$_r$每人收到一份M'. 这里, $\left|m_x\right\rangle\in\left\{\left|0\right\rangle,\left|1\right\rangle\right\}$, x=1,2,⋯,q, r=t+1, t+2, ⋯, n.

2.3 第三阶段: 授权与签名过程

步骤1: David$_1$和David$_C$组分别与Alice合作进行窃听检测.

(1) 在David$_1$宣布接收到自己那份M'后, Alice公布M'中诱骗粒子的位置及其制备基. David$_1$采取Alice的制备基去测量诱骗粒子, 并告知Alice测量结果. Alice判断David$_1$的测量结果和相应诱骗粒子的初态之间的一致性来统计错误率. 当错误率高得不合理时, 通信将被提前结束; 否则, 通信将被继续下去.

(2) 在David$_C$组中的David$_r$从Alice那里收到自己那份M'后, Alice公布M'中诱骗粒子的位置. 对于每个诱骗粒子, David$_r$随机采取SIFT操作或CTRL操作. David$_r$置乱发给Alice的粒子. Alice公布用Z基制备的诱骗粒子的位置. 这里, SIFT操作为用Z基测量, CTRL操作为不干扰地反射回去, r=t+1, t+2, ⋯, n.

David$_r$公布进行CTRL操作的粒子的位置及其发给Alice的顺序. Alice采取相应的制备基测量它们并统计相应的错误率. 当错误率高得不合理时, 通信将被提前结束; 否则, 通信将被继续下去.

David$_r$宣布自己的Z基测量结果. Alice统计自己以Z基制备且被David$_r$施加SIFT操作的诱骗粒子的错误率. 当错误率高得不合理时, 通信将被提前结束; 否则, 通信将被继续下去.

步骤2: David$_1$和David$_C$组都恢复出M, 然后向Bob请求授权签名.

步骤3: Bob制备qn个Bell态$\left|\phi_{0,0}\right\rangle_{12}=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle+\left|11\right\rangle\right)_{12}$. 令$W_1$和$W_2$分别代表这些Bell态的所有粒子1和所有粒子2组成的粒子序列. Bob将W_2分成n组, 第j组为$W_2^j=\left(\left|\phi_j^1\right\rangle_2,\left|\phi_j^2\right\rangle_2,\ \ldots,\left|\phi_j^q\right\rangle_2\right)$, 其中$\left|\phi_j^x\right\rangle_2$为第$j$组第$x$个$\left|\phi_{0,0}\right\rangle_{12}$的粒子2. 这里, j=1,2,⋯,n, x=1,2,⋯,q. Bob制备数量足够多的随机处于$\left\{\left|0\right\rangle,\left|1\right\rangle,\left|+\right\rangle,\left|-\right\rangle\right\}$的诱骗粒子, 将它们随机插入$W_2{}^j$中得到$W_2^{j\prime}$, 并将$W_2^{j\prime}$发送给David$_j$进行签名授权, 其中$j$=1,2,⋯,$n$.

步骤4: 在David$_j$收到$W_2^{j\prime}$后, David$_j$与Bob进行与步骤1相同的窃听检测. 在通过所有安全检测后, David组开始进行签名. 这里, j=1,2,⋯,n.

情形1: David$_Q$组签名

(1) David$_1$利用Z基测量手中的M并根据以下规则制备$M_D=\left(\left|m_{D_1}\right\rangle,\left|m_{D_2}\right\rangle,\ \ ...,\left|m_{D_q}\right\rangle\right)$, 其中$\left|m_{D_x}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle+a_x\left|1\right\rangle\right)$, $a_x\in\{-1,1\}$, x=1,2,⋯,q: 如果$\left|m_x\right\rangle=\left|0\right\rangle$, 那么David$_1$制备$\left|m_{D_x}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle+\left|1\right\rangle\right)$; 如果$\left|m_x\right\rangle=\left|1\right\rangle$, 那么David$_1$制备$\left|m_{D_x}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle-\left|1\right\rangle\right)$. 同时, David$_2$, David$_3$, ⋯, David$_t$各自制备$q$个$\left|0\right\rangle$. 此时, 由David$_1$, David$_2$, ⋯, David$_t$手中所有第$x$个粒子构成的复合系统的状态为

$$\varphi(x)=\left(\left|m_{D_x}\right\rangle\underbrace{\left|0\right\rangle\left|0\right\rangle...\left|0\right\rangle}_{t-1}\right)_{b_{x1}b_{x2}b_{x3}...b_{xt}}$$
$$=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle\underbrace{\left|0\right\rangle\left|0\right\rangle...\left|0\right\rangle}_{t-1}+a_x\left|1\right\rangle\underbrace{\left|0\right\rangle\left|0\right\rangle...\left|0\right\rangle}_{t-1}\right)_{b_{x1}b_{x2}b_{x3}...b_{xt}},$$

其中, x=1,2,⋯,q. David$_1$以粒子b_{x1}为控制量子比特、以粒子b_{x2}, b_{x3}, ⋯, b_{xt}为目标量子比特实施$t-1$次控制非操作 (即 CNOT $=\left|00\right\rangle\left\langle00\right|+\left|11\right\rangle\left\langle10\right|+\left|01\right\rangle\left\langle01\right|+\left|10\right\rangle\left\langle11\right|$) 得到

$$\varphi'(x)=\frac{1}{\sqrt{2}}\left(\underbrace{\left|0\right\rangle\left|0\right\rangle...\left|0\right\rangle}_{t}+a_x\underbrace{\left|1\right\rangle\left|1\right\rangle...\left|1\right\rangle}_{t}\right)_{b_{x1}b_{x2}b_{x3}...b_{xt}},$$

其中x=1,2,⋯,q.

(2) David$_1$用X基测量粒子b_{x1}, 其中x=1,2,⋯,q. 如果David$_1$对粒子b_{x1}的测量结果为$\left|+\right\rangle$, 那么David$_1$令d_{x1}=0; 如果David$_1$对粒子b_{x1}的测量结果为$\left|-\right\rangle$, 那么

David$_1$令d_{x1}=1. David$_1$用k_{D_1T}加密自己的签名d_1得到$E_{k_{D_1T}}(d_1)$, 其中d_1=(d_{11}, d_{21}, ⋯, d_{q1}). David$_1$对W_2^1的$|\phi_1^x\rangle_2$实施$U_{d_{x1}}$得到$P_{1x}=U_{d_{x1}}|\phi_1^x\rangle_2$, 其中$x$=1,2,⋯,$q$. 然后, David$_1$制备数量足够多的随机处于$\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$的诱骗粒子, 将它们随机插入$P_1$中得到$P_1'$, 并将$P_1'$发送给David$_2$, 其中$P_1$=($P_{11}$, P_{12},⋯,P_{1q}).

对于v=2,3,⋯,t−1: 在David$_v$从David$_{v-1}$收到P'_{v-1}后, 他们一起进行与步骤1-(1)类似的窃听检测. 在通过安全检测后, David$_v$用X基测量粒子b_{xv}, 其中x=1,2,⋯,q. 如果David$_v$对粒子b_{xv}的测量结果为$|+\rangle$, 那么David$_v$令d_{xv}=0; 如果David$_v$对粒子b_{xv}的测量结果为$|-\rangle$, 那么David$_v$令d_{xv}=1. David$_v$用k_{D_vT}加密自己的签名d_v得到$E_{k_{D_vT}}(d_v)$, 其中d_v=(d_{1v},d_{2v},⋯,d_{qv}). David$_v$对$P_{(v-1)x}$实施$U_{d_{xv}}$得到$P_{vx}=U_{d_{xv}}\cdots U_{d_{x2}}U_{d_{x1}}|\phi_1^x\rangle_2$, 其中$x$=1,2,⋯,$q$. 然后, David$_v$制备数量足够多的随机处于$\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$的诱骗粒子, 将它们随机插入$P_v$中得到$P'_v$, 并将$P'_v$发送给David$_{v+1}$, 其中$P_v$=($P_{v1}$,$P_{v2}$,⋯, P_{vq}). 最后, David$_v$制备数量足够多的随机处于$\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$的诱骗粒子, 将它们随机插入$W_2^v$中得到$W_2^{v\prime\prime}$, 并将$W_2^{v\prime\prime}$发送给Trent.

David$_t$用X基测量粒子b_{xt}, 其中x=1,2,⋯,q. 如果David$_t$对粒子b_{xt}的测量结果为$|+\rangle$, 那么David$_t$令d_{xt}=0; 如果David$_t$对粒子b_{xt}的测量结果为$|-\rangle$, 那么David$_t$令d_{xt}=1. David$_t$用k_{D_tT}加密自己的签名d_t得到$E_{k_{D_tT}}(d_t)$, 其中d_t=(d_{1t},d_{2t},⋯,d_{qt}). David$_t$对$P_{(t-1)x}$实施$U_{d_{xt}}$得到$P_{tx}=U_{d_{xt}}\cdots U_{d_{x2}}U_{d_{x1}}|\phi_1^x\rangle_2$, 其中$x$=1,2,⋯,$q$. David$_t$制备数量足够多的随机处于$\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$的诱骗粒子, 将它们随机插入$P_t$中得到$P_t'$, 并将$P'_t$发送给Trent, 其中$P_t$=($P_{t1}$,$P_{t2}$,⋯,$P_{tq}$). 最后, David$_t$制备数量足够多的随机处于$\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$的诱骗粒子, 将它们随机插入$W_2^t$中得到$W_2^{t\prime\prime}$, 并将$W_2^{t\prime\prime}$发送给Trent.

(3) David$_Q$组对签名产生方法保密. David$_Q$组加密后的签名为$S_Q=\left(E_{k_{D_1T}}(d_1),E_{k_{D_2T}}(d_2),\ \ ...,E_{k_{D_tT}}(d_t)\right.$. David$_Q$组将$S_Q$发送给Trent.

情形2: David$_C$组签名

(1) David$_r$利用Z基测量手中的M将其恢复为经典消息m, 其中r=t+1,t+2,⋯,n. 记David$_r$拥有的m为m_r=(m_{1r},m_{2r},⋯,m_{qr}), 其中$m_{xr}\in\{0,1\}$, x=1,2,⋯,q, r=t+1,t+2⋯,n. 然后, David$_r$用Z基测量手中的$|\phi_r^x\rangle_2$, 其中x=1,2,⋯,q, r=t+1,t+2⋯,n. 如果对$|\phi_r^x\rangle_2$的测量结果为$|0\rangle$, 那么David$_r$令$\lambda_r^x=0$; 如果对$|\phi_r^x\rangle_2$的测量结果为$|1\rangle$, 那么David$_r$令$\lambda_r^x=1$. 记$\lambda_r=\left(\lambda_r^1,\lambda_r^2,...,\lambda_r^q\right)$, 其中$\lambda_r^x\in\{0,1\}$, 其中$x$=1,2,⋯,$q$, r=t+1,t+2⋯,n. David$_r$根据表1的规则产生自己的签名d_r=(d_{1r},d_{2r},⋯,d_{qr})并对规则保密, 其中$d_{xr}\in\{0,1\}$.

(2) David$_r$用k_{D_rT}加密d_r得到$E_{k_{D_rT}}(d_r)$, 其中r=t+1,t+2⋯,n. 至此, David$_C$组加密后的签名为$S_C=\left(E_{k_{D_{t+1}T}}(d_{t+1}),E_{k_{D_{t+2}T}}(d_{t+2}),\ ...,E_{k_{D_nT}}(d_n)\right)$. David$_C$组将$S_C$发送给Trent.

(3) 在计算一次$H_2(m_r)$后, David$_C$组将其结果告知Trent, 其中$H_2(\cdot)$为David$_C$组与Trent共享的抗碰撞单向哈希函数.

2.4 第四阶段: 验证过程

步骤1: Trent用k_{D_iT}解密$E_{k_{D_iT}}(d_i)$得到d_i, 其中i = 1, 2,⋯,t. Trent用k_{D_rT}解密$E_{k_{D_rT}}(d_r)$得到d_r, 其中r=t+1, t+2⋯,n.

步骤2: Trent和David$_t$一起进行与第三阶段步骤1-(1)类似的窃听检测. 在通过安全检测后, Trent得到P_t.

步骤3: Trent计算$\text{sum}_x=d_{x1}\oplus d_{x2}\oplus\cdots\oplus d_{xt}$, 其中$x$=1,2,⋯,$q$. 当sum$_x$=0时, Trent得到$m'_x=0$, 并不对$P_{tx}$施加任何操作; 当sum$_x$=1时, Trent得到$m'_x=1$, 并对$P_{tx}$施加$U_1$. 这样, Trent得到$m'=\left\{m'_1,m'_2,...,m'_q\right\}$, 其中$m'_x\in\{0,1\}$, x=1,2,⋯,q. Trent计算$H_2(m')$, 并比较$H_2(m_r)$和$H_2(m')$是否相等. 如果$H_2(m_r)$=$H_2(m')$, 那么Trent公布flag=0并继续协议; 如果$H_2(m_r)\neq H_2(m')$, 那么Trent公布flag=1并重新开始协议.

步骤4: Trent自己手中现有的粒子P_{t1},P_{t2},⋯,P_{tq}组

表 1 David$_r$产生d_r的规则

Table 1 David$_r$'s rule of generating d_r

λ_r^x	m_{xr}	d_{xr}
0	0	$\lambda_r^x \oplus m_{xr} \oplus k_{D_rT_x}$
	1	$\lambda_r^x \oplus m_{xr} \oplus \overline{k}_{D_rT_x}$
1	0	$\lambda_r^x \oplus m_{xr} \oplus k_{D_rT_x}$
	1	$\lambda_r^x \oplus m_{xr} \oplus \overline{k}_{D_rT_x}$

成量子态序列$\psi_1=\left(\psi_1^1,\psi_1^2,...,\psi_1^q\right)$, 其中$\psi_1^x\in\left\{|0\rangle,|1\rangle\right\}$为Trent手中的粒子$P_{tx}$, x=1,2,⋯,q.

Trent和David$_v$一起对W_2^v"进行与第三阶段步骤1-(1)类似的窃听检测. 在通过安全检测后, Trent得到W_2^v. 这里, v=2,3,⋯,t−1.

Trent和David$_t$一起对W_2^t"进行与第三阶段步骤1-(1)类似的窃听检测. 在通过安全检测后, Trent得到W_2^t. Trent根据d_{xr}和$k_{D_rT_x}$制备ψ_r^x: 如果$d_{xr}=k_{D_rT_x}$, 那么Trent制备$\psi_r^x=|0\rangle$; 如果$d_{xr}=\overline{k}_{D_rT_x}$, 那么Trent制备$\psi_r^x=|1\rangle$. 因此, Trent得到$\psi_r=\left(\psi_r^1,\psi_r^2,...,\psi_r^q\right)$. 这里, r=t+1,t+2⋯,n, x=1,2,⋯,q.

Trent让ψ_1, W_2^v, W_2^t和ψ_r一起组成量子态序列$\psi=\left(\psi_1,W_2^2,W_2^3,...,W_2^{t-1},\psi_{t+1},\psi_{t+2},\ldots,\psi_n\right)$, 其中$v$=2,3,⋯,$t$−1, r=t+1,t+2,⋯,n.

Trent制备数量足够多的随机处于$\left\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\right\}$的诱骗粒子, 将它们随机插入$\psi$中得到$\psi'$, 并将$\psi'$发送给Charlie.

步骤5: Trent用k_{TC}加密S得到$E_{k_{TC}}(S)$将其发送给Charlie, 其中S=[S_Q, S_C]. Trent根据m'制备相应量子态序列$M^*=\left(|m'_1\rangle,|m'_2\rangle,...,|m'_q\rangle\right)$, 然后制备数量足够多的随机处于$\left\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\right\}$的诱骗粒子, 并将它们随机插入$M^*$中得到$M^{*\prime}$, 最后将$M^{*\prime}$发送给Charlie.

步骤6: Charlie利用k_{TC}将从Trent接收到的$E_{k_{TC}}(S)$进行解密得到S.

步骤7: Bob制备数量足够多的随机处于$\left\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\right\}$的诱骗粒子, 将它们插入$W_1$中得到$W_1'$, 并将$W_1'$发送给Charlie.

步骤8: Charlie和Trent对ψ'一起进行与第三阶段步骤1-(2)类似的窃听检测. 在通过安全检测后, Charlie得到ψ.

Charlie和Bob一起对W_1'进行与第三阶段步骤1-(2)类似的窃听检测. 在通过安全检测后, Charlie得到W_1. Charlie用Z基分别测量ψ和W_1中的所有粒子, 并将ψ中的粒子的测量结果与W_1中对应粒子的测量结果进行比较. 如果存在ψ中的粒子的测量结果与W_1中对应粒子的测量结果不一致, 那么Charlie宣布签名无效; 反之, Charlie继续检验签名.

步骤9: Charlie和Trent一起对$M^{*\prime}$进行与第三阶段步骤1-(2)类似的窃听检测. 在通过安全检测后, Charlie得到M^*. Charlie利用Z基测量M^*恢复出m'. Charlie比较$H_1(m')$和$H_1(m)$. 如果$H_1(m')$=$H_1(m)$, 那么Charlie接受签名; 如果$H_1(m')\neq H_1(m)$, Charlie拒绝接受签名.

为清晰起见, 将本文协议的流程描绘在图1中, 其中David组的签名过程描绘在图2中.

3 正确性分析

这部分对本文协议的正确性进行分析.

在David$_Q$组签名时, David$_1$以粒子b_{x1}为控制量子比特、以粒子$b_{x2},b_{x3},\cdots,b_{xt}$为目标量子比特实施$t$−1次CNOT操作得到

$$\varphi'(x)=\frac{1}{\sqrt{2}}\left(\underbrace{|0\rangle|0\rangle...|0\rangle}_{t}+a_x\underbrace{|1\rangle|1\rangle...|1\rangle}_{t}\right)_{b_{x1}b_{x2}b_{x3}...b_{xt}},$$

其中x=1,2,⋯,q; 然后, David$_i$用X基测量粒子b_{xi}, 其中x=1,2,⋯,q, i=1,2,⋯,t; 如果David$_i$对粒子b_{xt}的测量结果为$|+\rangle$, 那么David$_i$令d_{xi}=0, 如果David$_i$对粒子b_{xi}的测量结果为$|-\rangle$, 那么David$_i$令d_{xi}=1. 根据推理1可得: 如果David$_1$, David$_2$, ⋯, David$_t$对粒子$b_{x1},b_{x2},\cdots,b_{xt}$的所有$X$基测量结果中的$|-\rangle$的个数为偶数, 即$d_{x1},d_{x2},\cdots,d_{xt}$中1的个数为偶数, 则有$a_x$=1, 对应于$|m_x\rangle=|0\rangle$; 如果David$_1$, David$_2$, ⋯, David$_t$对粒子$b_{x1},b_{x2},\cdots,b_{xt}$的所有$X$基测量结果中的$|-\rangle$的个数为奇数, 即$d_{x1},d_{x2},\cdots,d_{xt}$中1的个数为奇数, 则有$a_x$=−1, 对应于$|m_x\rangle=|1\rangle$. 在验证阶段的步骤3, Trent计算$\mathrm{sum}_x=d_{x1}\oplus d_{x2}\oplus\ldots\oplus d_{xt}$. 当$d_{x1},d_{x2},\cdots,d_{xt}$中1

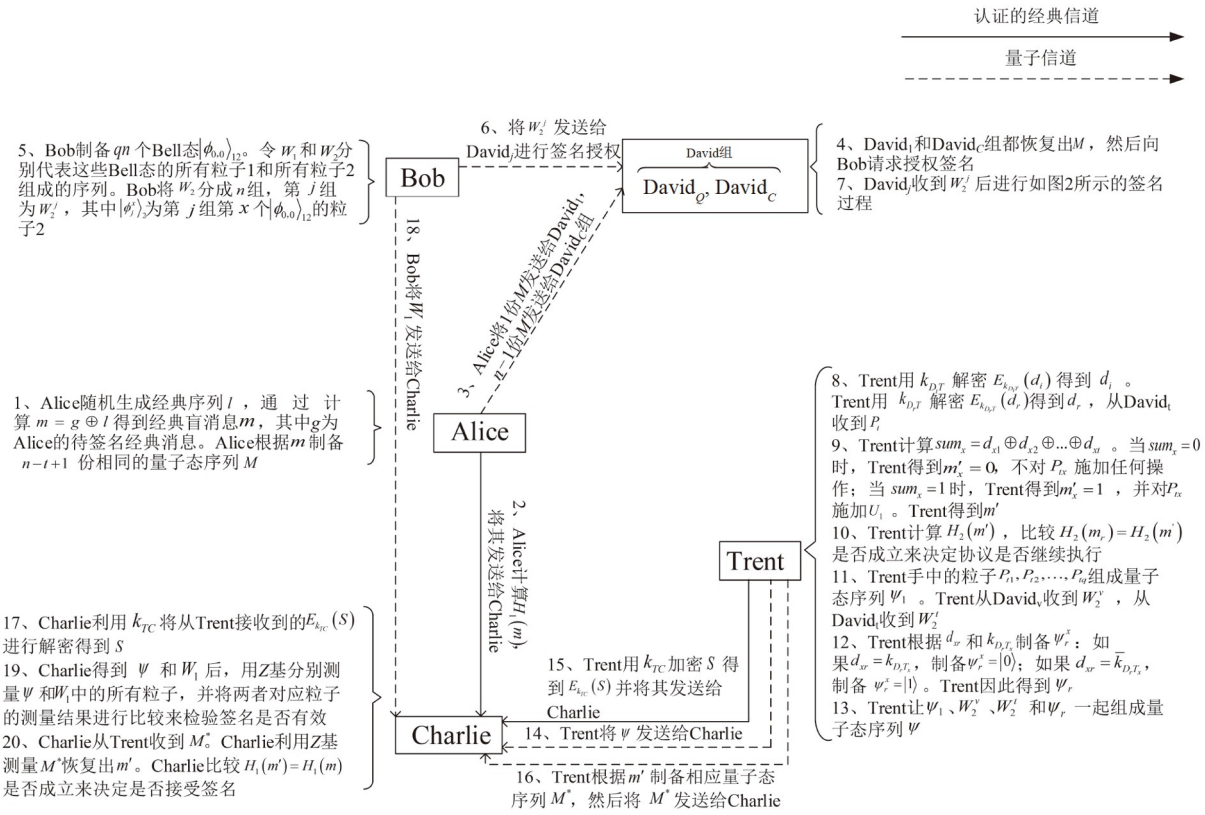


图 1 本文方案的流程图

Figure 1 Flow chart of this scheme.

的个数为偶数时, 有sum$_x$=0, 那么Trent得到$m'_x=0$, 并不对P_{tx}施加任何操作; 当$d_{x1},d_{x2},\cdots,d_{xt}$中1的个数为奇数时, 有sum$_x$=1时, Trent得到$m'_x=1$, 并对$P_{tx}$施加$U_1$. 如果协议的步骤都正常进行, 显然应该存在$H_2(m_r)=H_2(m')$和$H_1(m')=H_1(m)$, 而且在Trent的操作后, P_{tx}的状态会被还原成$|\phi_1^x\rangle_2$.

在David$_C$组签名时, David$_r$恢复出m_{xr}, 通过Z基测量手中的$|\phi_r^x\rangle_2$产生λ_r^x: 如果对$|\phi_r^x\rangle_2$的Z基测量结果为$|0\rangle$, 那么David$_r$令$\lambda_r^x=0$, 如果对$|\phi_r^x\rangle_2$的Z基测量结果为$|1\rangle$, 那么David$_r$令$\lambda_r^x=1$. 这里, x=1,2,$\cdots$,q, r=t+1, t+2$\cdots$,n. 然后, David$_r$根据表1生成d_{xr}. 根据表1, 当$\lambda_r^x=0$和m_{xr}=0时, 有$d_{xr}=\lambda_r^x\oplus m_{xr}\oplus k_{D_rT_x}=k_{D_rT_x}$; 当$\lambda_r^x=0$和$m_{xr}$=1时, 有$d_{xr}=\lambda_r^x\oplus m_{xr}\oplus\overline{k}_{D_rT_x}=k_{D_rT_x}$; 当$\lambda_r^x=1$和$m_{xr}$=0时, 有$d_{xr}=\lambda_r^x\oplus m_{xr}\oplus k_{D_rT_x}=\overline{k}_{D_rT_x}$; 当$\lambda_r^x=1$和$m_{xr}$=1时, 有$d_{xr}=\lambda_r^x\oplus m_{xr}\oplus\overline{k}_{D_rT_x}=\overline{k}_{D_rT_x}$. 因此, 当$\lambda_r^x=0$时, 有$d_{xr}=k_{D_rT_x}$; 当$\lambda_r^x=1$时, 有$d_{xr}=\overline{k}_{D_rT_x}$. 在验证阶段的步骤4, Trent根据$d_{xr}$和$k_{D_rT_x}$制备$\psi_r^x$: 如果$d_{xr}=k_{D_rT_x}$, 那么Trent制备$\psi_r^x=|0\rangle$, 对应于David$_r$对$|\phi_r^x\rangle_2$的$Z$基测量结果为$|0\rangle$; 如果$d_{xr}=\overline{k}_{D_rT_x}$, 那么Trent制备$\psi_r^x=|1\rangle$, 对应于David$_r$对$|\phi_r^x\rangle_2$的$Z$基测量结果为$|1\rangle$. 如果协议的步骤都正常进行, 根据$|\phi_{0,0}\rangle_{12}$的两个粒子间的纠缠相关性, 在验证阶段的步骤8中, Charlie对ψ中的粒子的Z基测量结果将与Charlie对W_1中对应粒子的测量结果相同.

4 性能分析

(1) 安全性

在本文协议中, Alice将1份M'发送给David$_1$; Bob将$W_2^{i\prime}$发送给David$_Q$组中的David$_i$, 其中i=1,2,$\cdots$,t; David$_1$将P'_1发送给David$_2$, David$_v$将P'_v发送给David$_{v+1}$,

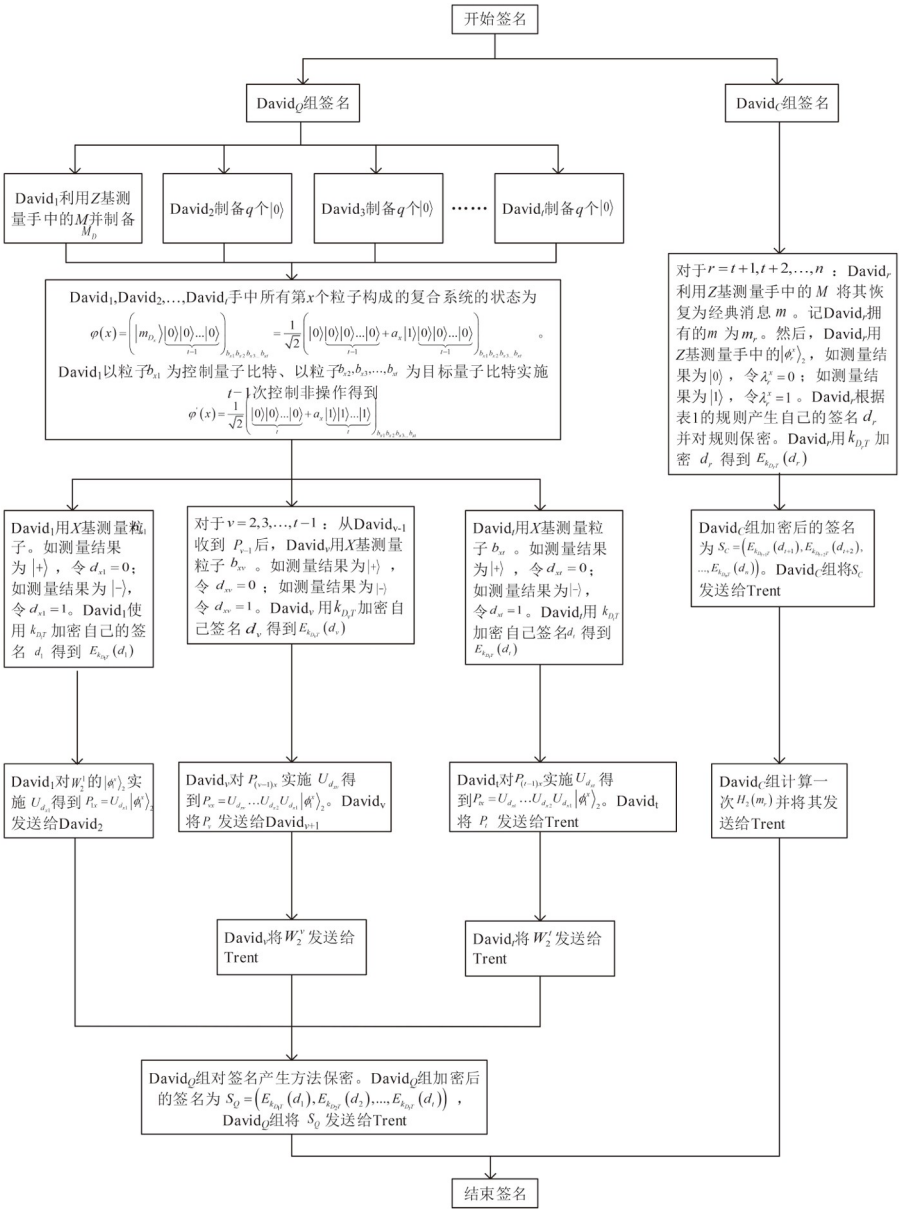


图 2 David组的签名过程

Figure 2 David group's signature process.

David$_v$将W_2^{v}″发送给Trent, 其中v=2,3,⋯,t−1; David$_t$将P'_t发送给Trent, 并将W_2^{t}″发送给Trent. 这些粒子传输过程都利用诱骗光子技术[32,33]来保证传输安全性. 诱骗光子窃听检测方法可被视为文献[2]方案的窃听检测方法的变种, 而后者已被文献[34]证明对窃听者Eve发起的攻击具有无条件安全性.

在本文协议中, Alice将n−t份M'发送给David$_C$组, David$_C$组中的David$_r$每人收到一份M', 其中r=t+1, t+2, ⋯,n; Bob将W_2^{r}′发送给David$_C$组中的David$_r$, 其中r=t+1,t+2, ⋯,n; Trent将ψ'发送给Charlie, 并将M^{*}′发送给Charlie; Bob将W_1'发送给Charlie. 这些粒子传输过程采用的窃听检测方法与文献[23]的随机置乱半量子密钥分配方案的窃听检测方法一样, 而后者已被文献[23]证明具有完全鲁棒性.

可以得出结论, 本文涉及的粒子传输过程的安全性都能得到保证.

(2) 盲性

在本文协议中, Alice通过l加密g得到m. 尽管David$_1$和David$_C$组在窃听检测后都恢复出了M, 但David$_1$和David$_C$组并不知道l, 因此, g对于David$_1$和David$_C$组是盲的.

Trent通过计算sum$_x$来得到m'. 尽管在理想情况下存在$m'=m$, 然而Trent无法获得l, 从而也无法进一步得到g. 因此, g对于Trent也是盲的.

本文方案使用诱骗粒子技术[32,33]来保障M'从Alice被传送到David$_1$的安全性, 从而使得Eve不能不留痕迹地获取M'来进一步得到m, 更不要说得到g. 本文方案采用文献[23]的随机置乱半量子密钥分配方案的窃听检测方法来保障M'从Alice被传送到David$_C$组的安全性, 从而使得Eve不能不留痕迹地获取M'来解密出m, 更不要说获取g. 本文方案同样采用文献[23]的随机置乱半量子密钥分配方案的窃听检测方法来保障$M^{*\prime}$从Trent被传送到Charlie的安全性, 从而使得Eve不能不留痕迹地获取$M^{*\prime}$来进一步得到M^*, 更不要说获取g. 而且, 即使拦截到Alice传向Charlie的$H_1(m)$, 由于$H_1(\cdot)$具有单向性, Eve还无法获取m, 更别提g. 另外, 即使拦截到David$_C$组传向Trent的$H_2(m_r)$, 由于$H_2(\cdot)$具有单向性, Eve还无法获取m_r, 更别提g. 现可得出, g对于Eve也是盲的.

(3) 不可伪造性

根据签名产生流程, 除了David组外, 攻击者无法知道d_1, d_v, d_t, d_r并伪造它们, 其中v=2,3,⋯,$t-1$, r=t+1, t+2⋯,n.

除Trent和David$_j$外, 任何攻击者都不能获得k_{D_jT}, 其中j=1,2,⋯,n; 即使拦截到从David$_Q$组传向Trent的S_Q和从David$_C$组传向Trent的S_C, 攻击者也不能分别解密出d_1, d_v, d_t以及d_r, 并不能进一步伪造签名, 其中v=2,3,⋯, $t-1$, r=t+1,t+2,⋯,n. 同样地, 除Charlie和Trent外, 任何攻击者都不能获得k_{TC}; 即使拦截到从Trent传向Charlie的$E_{k_{TC}}(S)$, 攻击者也不能推导出S并进一步伪造签名.

(4) 不可否认性

首先说明Bob不能否认对David组的签名授权. Charlie检验签名需要从Trent处得到ψ, 而ψ是由签名过程所产生, 特别是签名过程需要Bob将$W_2^{j\prime}$发送给David$_j$作为授权, 其中j=1,2,⋯,n. 因此, 在Charlie用Z基测量W_1和ψ中的所有粒子并证实签名有效时, Bob无法否认将签名权外授给David组.

接着说明David组无法否认生成签名. Charlie检验签名需要先得到ψ, 其中$\psi=\left(\psi_1, W_2^2, W_2^3, ..., W_2^{t-1}, W_2^t, \psi_{t+1}, \psi_{t+2}, \cdots, \psi_n\right)$. ψ_1是由Trent根据自己手中现有的粒子P_{t1},P_{t2},⋯,P_{tq}而组成的量子态序列, P_{t1},P_{t2},⋯,P_{tq}是由Trent根据sum$_x$得到, sum$_x$是由d_i得到, 其中x=1,2,⋯, q, i=1,2,⋯,t; $\left(W_2^2, W_2^3, ..., W_2^t\right)$由Trent从David$_v$和David$_t$获得, 其中$v$=2,3,⋯,$t-1$; 因此, David$_Q$组不能否认生成签名. $(\psi_{t+1}, \psi_{t+2}, \cdots, \psi_n)$是由Trent根据$d_{xr}$和$k_{D_rT_x}$制备, 其中$r$=$t$+1,$t$+2⋯,$n$, x=1,2,⋯,q, 因此, David$_C$组不能否认通过表1的规则生成签名.

最后说明Trent无法否认签名的接受. Charlie需得到ψ来检验签名是否有效, 而ψ是由Trent传送过来; 当Charlie证实签名有效时, Trent无法否认对David组签名的接受.

5 讨论和结论

量子通信方案的量子比特效率被定义为[35]

$$\gamma=\frac{\delta}{\sigma+\rho}, \tag{4}$$

其中, δ为签名长度, σ为所花费的量子比特的数量, ρ为所花费的经典比特的数量. 本文在计算量子比特效率时将安全检测花费的所有资源忽略.

在本文方案中, David$_Q$组的签名为(d_1,d_2,⋯,d_t), David$_C$组的签名为(d_{t+1},d_{t+2},⋯,d_n), 因此有δ=nq. Alice需根据m制备$n-t+1$份M, 并将1份M发送给David$_1$, 将$n-t$份M发送给David$_C$组; Bob需制备nq个Bell态$\left|\phi_{0,\ 0}\right\rangle_{12}=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle+\left|11\right\rangle\right)_{12}$; David$_1$需利用$Z$基测量手中的$M$并制备$M_D$; David$_2$, David$_3$, ⋯, David$_t$需各自制备$q$个$\left|0\right\rangle$; Trent需根据$d_{xr}$和$k_{D_rT_x}$制备$\psi_r^x$, 其中$r$=$t$+1,$t$+2,⋯, n, x=1,2,⋯,q; Trent根据m'制备M^*; David$_Q$组中的David$_i$和Trent使用文献[2]的方法建立k_{D_iT}, 其中i=1,2,⋯,t; David$_C$组中的David$_r$和Trent使用文献[22]的方法建立k_{D_rT}, 其中r=t+1,t+2,⋯,n; Charlie和Trent使用文献[22]的方法建立k_{TC}; 因此, 有σ=($n-t$+1)q+2nq+q+($t-1$)q+($n-t$)q+q+4tq+8($n-t$)q+8nq=(20n−5t+2)q. Alice计算$H_1(m)$, 并将其发送给Charlie; David$_Q$组将S_Q发送给

表 2 本文方案与文献[24,27,31]的半量子签名方案的对比

Table 2 Comparison of this scheme and semiquantum signature schemes of refs. [24,27,31]

参数	文献[24]	文献[27]	文献[31]	本文
量子资源	单粒子态、W态	单粒子态、五粒子GHZ态	单粒子态、χ态	单粒子态、Bell态
半量子通信者	验证者	验证者	原始签名者和验证者	部分代理签名者和验证者
待签名消息持有人数	2	1	1	1
代理签名人数	0	0	1	n
安全检测	否	是	是	是
量子通信者的量子测量	Z基测量、三粒子量子纠缠态测量	Z基测量	Z基测量、Bell基测量	Z基测量
是否预建立密钥	是	是	是	是
是否利用量子隐形传态	是	否	是	否
通信效率	$\frac{1}{31}$	$\frac{1}{29}$	$\frac{2n}{34n+l}$	$\frac{nq}{(22n-5t+2)q+f_1+f_2}$

Trent; David$_C$组将S_C发送给Trent; David$_C$组计算一次$H_2(m_r)$并将其发送给Trent; Trent用k_{TC}加密S得到$E_{k_{TC}}(S)$将其发送给Charlie; 因此, 有$\rho=f_1+nq+nq+f_2=2nq+f_1+f_2$, 其中$f_1$是$H_1(m)$的长度, f_2是$H_2(m_r)$的长度. 综上所述, 本文方案的量子比特效率为

$$\gamma=\frac{nq}{(20n-5t+2)q+(2nq+f_1+f_2)}=\frac{nq}{(22n-5t+2)q+f_1+f_2}.$$

接下来将本文协议与之前的3个半量子签名方案进行详细比较, 并将比较结果汇总在表2中. 根据文献[31]的计算, 文献[24,27,31]的量子比特效率分别为2/31, 1/29和$2n/34n+l$. 可得出: (1) 在量子资源上, 本文方案超过了文献[24,27,31]的方案, 这是因为Bell态比W态、五粒子GHZ态和χ态都更容易制备; (2) 文献[24,27]方案都为半量子盲签名方案, 不属于半量子代理盲签名方案; 文献[31]的方案属于半量子单代理盲签名方案; 本文方案存在n个代理签名人, 属于半量子群代理盲签名方案; (3) 文献[24]的方案不对量子传输进行安全检测, 存在安全隐患; 本文方案对量子传输都进行了安全检测, 会有更高的安全性; (4) 对于量子参与方的量子测量, 本文方案胜过文献[24,31]的方案, 这是因为Z测量比三粒子量子纠缠态测量和Bell基测量都更容易实现; (5) 对于量子隐形传态的使用, 本文方案胜过文献[24,31]的方案, 这是因为本文方案不需要复杂的量子隐形传态过程.

总之, 本文提出了一个新颖的签名验证者和部分代理签名者都仅配备有限量子能力的半量子群代理盲签名方案. 本文方案满足不可伪造性、不可否认性、完全的盲性、安全性这些要求. 与已有的许多量子群代理盲签名方案相比, 本文方案会具有更广泛的签名实际应用场景.

参考文献

1 Diffie W, Hellman M. New directions in cryptography. IEEE Trans Inform Theor, 1975, 22: 644–654

2 Bennett C H, Brassard G. Quantum cryptography: Public-key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. Bangalore: IEEE, 1984. 175–179

3 Zeng G, Keitel C H. Arbitrated quantum-signature scheme. Phys Rev A, 2001, 65: 042312

4 Lü X, Feng D G. An arbitrated quantum message signature scheme. In: Proceeding of the First International Conference on Computational and Information Science. Berlin, Heidelberg: Springer-Verlag, 2004. 1054–1060

5 Li Q, Li C, Long D, et al. Efficient arbitrated quantum signature and its proof of security. Quantum Inf Process, 2013, 12: 2427–2439

6 Liu F, Qin S J, Huang W. An arbitrated quantum signature with Bell states. Int J Theor Phys, 2014, 53: 1569–1579

7 Ma H, Li F, Mao N, et al. Network-based arbitrated quantum signature scheme with graph state. Int J Theor Phys, 2017, 56: 2551–2561
8 Ding L, Xin X, Yang Q, et al. Security analysis and improvements of XOR arbitrated quantum signature-based GHZ state. Mod Phys Lett A, 2022, 37: 2250008
9 Zhu H, Zhang Y, Li Z. Efficient quantum blind signature scheme based on quantum fourier transform. Int J Theor Phys, 2021, 60: 2311–2321
10 Deng Z M, Lu D J, Chen T, et al. Quantum (t, m, n) threshold group blind signature scheme with flexible number of participants. Int J Theor Phys, 2023, 62: 201
11 Wang T Y, Wei Z L. One-time proxy signature based on quantum cryptography. Quantum Inf Process, 2012, 11: 455–463
12 Li C, Xu G, Chen Y, et al. A new anti-quantum proxy blind signature for blockchain-enabled internet of things. Comput Mater Continua, 2019, 61: 711–726
13 Wen X, Chen Y, Fang J. An inter-bank E-payment protocol based on quantum proxy blind signature. Quantum Inf Process, 2013, 12: 549–558
14 Zhang L, Li S, Zhang K J, et al. Cryptanalysis and improvement of some quantum proxy blind signature schemes. Int J Theor Phys, 2019, 58: 1047–1059
15 Niu X F, Zhang J Z, Xie S C, et al. A third-party E-payment protocol based on quantum multi-proxy blind signature. Int J Theor Phys, 2018, 57: 2563–2573
16 Wang Z, Li J, Chen X B, et al. Quantum multi-proxy strong blind signature based on block blind coding. Quantum Inf Process, 2022, 21: 386
17 Xue Y, Yin A, Xing K. A quantum multi-proxy blind signature scheme based on d-dimensional GHZ States. Int J Theor Phys, 2023, 62: 265
18 Lan L, Lu R, Zhong J, et al. A secure quantum proxy group signature scheme based on three-qubit entangled states. Int J Theor Phys, 2024, 63: 59
19 Cao H J, Yu Y F, Song Q, et al. A quantum proxy weak blind signature scheme based on controlled quantum teleportation. Int J Theor Phys, 2015, 54: 1325–1333
20 Niu X F, Zhang J Z, Xie S C. A quantum multi-proxy blind signature scheme based on entangled four-qubit cluster state. Commun Theor Phys, 2018, 70: 043
21 Yu J, Zhang J. Quantum (t, n) threshold proxy blind signature scheme based on Bell states. Int J Theor Phys, 2022, 61: 207
22 Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob. Phys Rev Lett, 2007, 99: 140501
23 Boyer M, Gelles R, Kenigsberg D, et al. Semiquantum key distribution. Phys Rev A, 2009, 79: 032341
24 Zhao X Q, Chen H Y, Wang Y Q, et al. Semi-quantum bi-signature scheme based on W states. Int J Theor Phys, 2019, 58: 3239–3251
25 Zheng T, Chang Y, Yan L, et al. Semi-quantum proxy signature scheme with quantum walk-based teleportation. Int J Theor Phys, 2020, 59: 3145–3155
26 Chen L Y, Liao Q, Tan R C, et al. Offline arbitrated semi-quantum signature scheme with four-particle cluster state. Int J Theor Phys, 2020, 59: 3685–3695
27 Xia C, Li H, Hu J. A semi-quantum blind signature protocol based on five-particle GHZ state. Eur Phys J Plus, 2021, 136: 633
28 Chen B C, Yan L L. Quantum and semi-quantum blind signature schemes based on entanglement swapping. Int J Theor Phys, 2021, 60: 4006–4014
29 Wang J H, Li Y X, Guo H, et al. Semi-quantum blind signature against collective noise (in Chinese). Laser Optoelectron Prog, 2022, 59: 1927001 [王俊辉, 李云霞, 郭瀚, 等. 免疫集体噪声的半量子盲签名协议. 激光与光电子学进展, 2022, 59: 1927001]
30 Zhang L, Zhang J H, Xin X J, et al. Semi-quantum designated verifier signature scheme. Int J Theor Phys, 2023, 62: 254
31 Tan X, Ye T Y. Semiquantum proxy blind signature based on quantum teleportation (in Chinese). Sci Sin-Phys Mech Astron, 2024, 54: 230313 [谈笑, 叶天语. 基于量子隐形传态的半量子代理盲签名. 中国科学: 物理学 力学 天文学, 2024, 54: 230313]
32 Li C Y, Zhou H Y, Wang Y, et al. Secure quantum key distribution network with Bell states and local unitary operations. Chin Phys Lett, 2005, 22: 1049–1052
33 Li C Y, Li X H, Deng F G, et al. Efficient quantum cryptography network without entanglement and quantum memory. Chin Phys Lett, 2006, 23: 2896–2899
34 Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett, 2000, 85: 441–444
35 Cabello A. Quantum key distribution in the Holevo limit. Phys Rev Lett, 2000, 85: 5635–5638

Semiquantum group proxy blind signature

TAN Xiao, GAN ZhiGang & YE TianYu*

College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, China
**Corresponding author (email: yetianyu@zjgsu.edu.cn)*

In this study, we propose the semiquantum group proxy blind signature scheme, in which the signature verifier and some proxy signers only possess limited quantum capabilities. On the basis that the original message content of the original message owner is blind to the original signer, the signature verifier, the proxy signature group and the trusted third party helping complete the signing process, this scheme can accomplish the goal of the original singer authorizing the proxy signature group to sign this original message. This scheme is proved to have unforgeability, non-repudiation, complete blindness and security. Since the signature verifier and some proxy signers only possess limited quantum capabilities, compared with many existing quantum group proxy blind signature protocols, this scheme has a wider range of signature application scenarios.

semiquantum group proxy blind signature, blindness, unforgeability, non-repudiation

PACS: 03.67.Dd, 03.67.Hk, 03.67.Pp

doi: 10.1360/SSPMA-2024-0169