物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

一个基于三粒子部分纠缠态的量子广播多重盲签名协议

张维 韩正甫

Quantum broadcasting multiple blind signature protocol based on three-particle partial entanglement

Zhang Wei Han Zheng-Fu

引用信息 Citation: Acta Physica Sinica, 68, 070301 (2019) DOI: 10.7498/aps.68.20182044
在线阅读 View online: https://doi.org/10.7498/aps.68.20182044
当期内容 View table of contents: http://wulixb.iphy.ac.cn

一个基于三粒子部分纠缠态的量子广播多重盲签名协议*

张 维 1)2)† 韩 正 甫 2)

1) (黔南民族师范学院数学与统计学院, 复杂系统与计算智能重点实验室, 都匀 558000)

2) (中国科学技术大学, 中科院量子信息重点实验室, 合肥 230026)

(2018 年 11 月 18 日收到; 2019 年 1 月 18 日收到修改稿)

最近有研究者提出了一个基于三粒子最大纠缠态 GHZ 态的量子广播多重盲签名协议, 它能满足一个重要消息需要多人签发, 但出于隐私保护要求每一个签名者都不能获取消息的具体内容这一应用需求, 并有望应用于电子银行系统. 本文给出了一个基于三粒子部分纠缠态的量子广播多重盲签名协议, 与原协议相比, 该协议用三粒子部分纠缠态代替三粒子极大纠缠 GHZ 态, 并且能不降低协议的安全性. 新协议不再依赖于极大纠缠态, 仅仅需要在通信参与者之间分享部分纠缠态就可以完成该签名方案, 这在一定程度上节约了纠缠资源, 降低了协议的实现条件, 提高了协议的可应用性. 这也充分体现了多体部分纠缠态也可以作为一种量子资源来实现既定的量子通信任务.

关键词: 量子广播多重盲签名协议, 三粒子部分纠缠态, 哈希函数

PACS: 03.65.–w, 03.67.–a, 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.68.20182044

1 前 言

经典签名是对手写签名的模拟, 并已经被广泛应用于电子商务、电子政务和电子支付等领域, 它的安全性基于一些数学上的难解问题假设, 如大数分解问题和离散对数问题等. 很不幸的是, 1994 年 Shor[1] 发现了多项式时间的量子因数分解算法, 该算法能够快速地实现大整数的因数分解. 因此, 以 RSA 为代表的公钥密码系统在量子计算机面前将没有任何保密性可言, 量子计算机可以在瞬间攻破它. 相比于经典签名, 量子签名是一种基于未知量子态不可克隆定理和海森堡测不准原理等基本物理属性之上的签名协议. 特别是有一些量子签名协议已经在理论上被证明是无条件安全的[2,3]. 因此, 量子签名受到了越来越多研究者的关注, 成为量子密码的一个重要分支. 量子签名协议有望在量子时代里取代经典签名, 广泛应用于电子商务、电子政务和电子支付等领域. 研究者们也参照经典签名设计出了一些与之对应的量子签名协议.

2001 年, Gottesman 和 Chuang[4] 基于量子单向函数和量子交换测试给出了第一个量子签名协议, 并指出该协议是可以抵御量子攻击的. 从那之后, 量子签名迅速蓬勃发展起来, 各种不同类型的量子签名协议相继被提出. 如 2002 年, Zeng 和 Keitel[5] 提出了一个基于 GHZ 纠缠态的量子仲裁

* 国家自然科学基金 (批准号: 11847083, 61602532)、贵州省科技厅基础研究计划 (批准号: 黔科合基础 [2019]1296)、贵州省教育厅青年科技人才成长计划 (批准号: 黔教合 KY 字 [2018]426)、黔南州科技计划 (批准号: 黔南科合工字 (2017)9 号)、黔南民族师范学院科研创新基金专项计划 (批准号: QNSY2018BS015) 和黔南民族师范学院高层次人才研究专项计划 (批准号: QNSYRC201716) 资助的课题.

† 通信作者. E-mail: wzhang01@ustc.edu.cn

签名协议; 2009 年, Li 等[6] 给出了一个基于贝尔态的量子仲裁签名协议, 与 Zeng 和 Keitel 提出的协议相比, 不仅可以节约纠缠资源还提高了签名的效率; 2010 年, Zou 和 Qiu[7] 给出了一个不需要使用量子纠缠的量子仲裁签名协议. 随着人们对量子签名研究的深入, 针对不同的应用需求, 提出了不同类型的量子签名协议, 如量子代理签名[8–12]、量子群签名[13–17]、量子盲签名[18–21] 和量子多重签名[22,23] 等.

一个安全的量子签名协议必须满足不可伪造和不能抵赖两方面的要求. 所谓不可伪造指的是除了合法的签名者以外, 任何人不能伪造签名者的签名, 包括签名协议的参与者 (消息发送者或接收者等) 和任何的外部攻击者[24]. 不可抵赖指的是任何参与者都不能拒不承认他们的所有行为, 包括: 1) 消息发送者不能拒不承认发送消息的事实; 2) 每一个签名者不能拒不承认他们自己的签名; 3) 签名接收者不能拒不承认他收到签名的事实, 也不能拒不承认签名的完整性[25]. 对于量子盲签名而言还需要满足盲性和可追溯性[25]. 所谓盲性指的是签名者在签名的时候不能获取他所签名消息的具体内容, 而可追溯性是指在签名双方无法达成一致的时候, 签名者可以追溯到消息的发送者[25].

2014 年, Tian 等[26] 给出了一个基于量子隐形传态的量子广播多重盲签名协议, 该协议有望应用于网上银行系统. 然而 Zhang 等[27] 对该协议进行了安全性分析, 发现它存在一些潜在的安全漏洞, 并给出了一个改进协议. 针对 Zhang 等提出的协议中复合签名的大小随着签名者的个数呈线性增长这一问题, Xiao 和 Li[25] 基于纠缠交换给出了一个新的量子广播多重盲签名协议, 该协议的复合签名的大小是一个定值, 不会随参与者的个数呈线性增长. 在文献 [28] 中, Tian 等基于三粒子极大纠缠 GHZ 态给出了一个量子广播多重盲签名协议. 随后 Zhang 等[29] 指出了该协议潜在的安全风险并给出了一个改进方案. 本文在文献 [29] 的基础上给出了一个基于三粒子部分纠缠态的量子广播多重盲签名协议, 该协议使用的是三粒子部分纠缠态, 与基于 GHZ 态的协议相比, 它不再依赖于极大纠缠态, 降低了协议的实现条件, 节省纠缠资源的同时还可以不损失安全性, 这充分体现了在某些情况下, 多体部分纠缠可以作为一种资源实现完美的量子通信任务.

2 量子广播多重盲签名协议

首先介绍本文采用的量子一次一密加密算法 (QOTP encryption algorithm). 若量子信息 $|P\rangle = \otimes_{j=1}^{l}|P_j\rangle$, 其中 $|P_j\rangle = a_j|0\rangle + b_j|1\rangle$ 满足 $|a_j|^2 + |b_j|^2 = 1$. 该算法可以用一个酉算子 E_K 表示为

$$E_K(|P\rangle) = \otimes_{j=1}^{l}\sigma_x^{K_{4j}}\sigma_z^{K_{4j-1}}W\sigma_x^{K_{4j-2}}\sigma_z^{K_{4j-3}}|P_j\rangle, \tag{1}$$

其中

$$W = \frac{\mathrm{i}}{\sqrt{3}}(\sigma_x - \sigma_y + \sigma_z). \tag{2}$$

这是一个改进了的量子一次一密加密算法, 它是由 Kim 等首次在文献 [30] 中提出的. (1) 式中的辅助算子 W 是为了破坏泡利算子间的对易或反对易性, 以保证加密后的消息不能被攻击者修改. 更准确的描述为: 对任意的量子消息 $|P\rangle$, 不存在非单位的酉算子 U 和 V, 使得

$$E_K^* V E_K|P\rangle \equiv U|P\rangle \tag{3}$$

成立, 其中 E_K^* 为 E_K 的共轭转置算子. 假设存在两个酉算子 U 和 V 使得 (3) 式成立, 则加密消息 $|P\rangle$ 可以被攻击者修改为 $U|P\rangle$ 而不被发现. 具体过程如下: 当加密消息 $E_K|P\rangle$ 在信道中传输时, 攻击者可以截获它并作用一个酉操作 V, 此时消息变成了 $VE_K(|P\rangle)$, 当接收者采用解密算子 E_K^* 进行解密时, 消息就转换成了 $E_K^*VE_K(|P\rangle)$, 由 (3) 式可知它就变成了 $U|P\rangle$, 这样消息 $|P\rangle$ 就被攻击者确定地修改成了 $U|P\rangle$.

为了保证签名协议中签名的初始性, 也即签名不能被随意更改, 我们使用了哈希函数. 本文使用的哈希函数是一个单向函数, 定义如下[31]:

$$H(x): \{0,1\}^* \to \{0,1\}^n. \tag{4}$$

本文新设计的协议采用的是一个三粒子部分纠缠态[32]

$$|\psi\rangle = \frac{\sin\theta|000\rangle_{123} + \sin\theta|011\rangle_{123} + \cos\theta|110\rangle_{123} - \cos\theta|101\rangle_{123}}{\sqrt{2}}. \tag{5}$$

在签名协议的设计过程中, 利用了三粒子部分纠缠态 $|\psi\rangle$ 的量子相关性, 这种相关性可以描述如下:

1) 对 $|\psi\rangle$ 的第一个粒子做一个 Z-型基测量, 并记录测量结果如下:

$$a_1=\begin{cases}0, \text{当观测到的结果为}|0\rangle\\ 1, \text{当观测到的结果为}|1\rangle\end{cases}; \tag{6}$$

2) 对$|\psi\rangle$的第二个粒子随机地作用一个泡利算子I或Z, 并记录如下:

$$b_1=\begin{cases}0, \text{当作用的泡利算子为}I\\ 1, \text{当作用的泡利算子为}Z\end{cases}; \tag{7}$$

3) 之后对二三粒子做一个贝尔基测量, 并记录结果如下:

$$c_1=\begin{cases}00, \text{当观测到的结果为}|\beta_{00}\rangle\\ 01, \text{当观测到的结果为}|\beta_{01}\rangle\\ 10, \text{当观测到的结果为}|\beta_{10}\rangle\\ 11, \text{当观测到的结果为}|\beta_{11}\rangle\end{cases}. \tag{8}$$

由 (5) 式可以得到如下式子成立:

$$c_1=(b_1\oplus a_1)\,\|a_1\,, \tag{9}$$

其中$a\,\|b$表示的是字符串的联接运算.

协议包含$t+3$个签名者, 其中一个消息发送者 Alice, t个签名者$U_1,U_2,\cdots,U_t$, 一个签名收集者 Charlie 和一个签名接收者 Bob. 在整个签名过程中, Alice 先将准备好的t份消息进行盲化, 然后分别发送给t个签名者$U_1,U_2,\cdots,U_t$, 每一个签名者U_i对收到的消息进行签名, 并把各自的签名都发送给收集者 Charlie, Charlie 对收到的单个签名逐一验证并生成复合签名, 然后将复合签名发送给接收者 Bob, 最后 Bob 对收到的复合签名进行验证, 从而完成整个签名过程.

整个签名协议包含四个过程, 即初始过程、个体签名过程、单个签名验证和复合签名生成过程以及复合签名验证过程, 如图 1 所示.

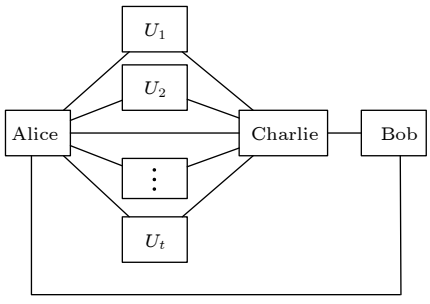

图 1 量子广播多重盲签名协议的图示

Fig. 1. The graph of quantum broadcasting multiple blind signature scheme.

下面给出协议的具体过程:

1) 初始过程:

(1) 量子密钥分配.

Alice 分别与 Bob, Charlie 以及每一个签名者U_i分享 $4n$ 比特密钥 K_{AB}, K_{AC} 和 K_{AU_i}; Charlie 与每一个签名者U_i分享 $8n$ 比特密钥 K_{CU_i}; Bob 与 Charlie 分享 $4n$ 比特密钥 K_{BC}. 为了保证协议的无条件安全性, 所有的密钥都采用量子密钥分配协议来分享密钥.

(2) 经典消息都转换成量子消息.

经典消息m转换成量子消息$|\varphi(m)\rangle$, 其中

$$|\varphi(m)\rangle=\otimes_{j=1}^{n}|\varphi(m(j))\rangle\,. \tag{10}$$

根据$|\varphi(m(j))\rangle=|0\rangle$ (或$|1\rangle$),$m(j)=0$(或1). 所有的量子消息都按照预备知识中的量子一次一密加密算法加密以后进行传输.

2) 个体签名过程:

(1) 消息盲化.

Alice 准备t份经典消息m并分别将它们盲化为

$$M_i=m\oplus K_{AB}^{(n)}\oplus K_{AU_i}^{(n)}, \tag{11}$$

其中$K_{AB}^{(n)}$和$K_{AU_i}^{(n)}$分别表示密钥K_{AB}和K_{AU_i}的前n比特. 然后将$E_{K_{AU_i}}(|\varphi(M_i)\rangle)$发送给每一个签名者$U_i$. 在此之后生成

$$T=m\oplus\left(\oplus_{i=1}^{t}M_i\right), \tag{12}$$

并将$E_{K_{AC}}(|\varphi(T)\rangle)$发给 Charlie.

(2) 纠缠分发.

Charlie 生成 n 个三粒子部分纠缠态

$$|\psi\rangle=\otimes_{j=1}^{n}|\psi(j)\rangle\,, \tag{13}$$

其中

$$|\psi(j)\rangle=\sin\theta|0\rangle_1|\beta_{00}\rangle_{23}-\cos\theta|1\rangle_1|\beta_{11}\rangle_{23}. \tag{14}$$

然后将它们的第一个粒子发送给 Alice, 第二粒子发送给签名者U_i, 保留第三粒子. 此处仅以一个签名者U_i为例来描述个体签名过程, 且所有粒子都是通过安全的量子信道来分发的, 以保证在整个签名过程中都能保持原有的量子纠缠.

(3) Alice 的测量.

Alice 对她收到的粒子做 Z-型基测量, 并生成随机字符串a_1,

$$a_1=\begin{cases}0, \text{当观测态为}|0\rangle\\ 1, \text{当观测态为}|1\rangle\end{cases}, \tag{15}$$

然后将$E_{KC}(|\psi(a_1)\rangle)$发送给 Charlie.

(4) 个体签名.

U_i 解密$E_{K_{AU_i}}(|\varphi(M_i)\rangle)$并测量得到盲化消息

M_i'(若传输过程中不出现错误, 则 $M_i'=M_i$), 然后对从 Charlie 处收到的量子态序列依次随机地选择作用一个泡利算子 I 或 Z, 生成一个随机串 $S_i^{(1)}$

$$S_i^{(1)}(j)=\begin{cases}0, \text{当}U_i\text{选择作用}I\text{算子}\\ 1, \text{当}U_i\text{选择作用}Z\text{算子}\end{cases}, \tag{16}$$

并将作用后的量子态序列依次发送给 Charlie. 同时, U_i 利用已有的密钥生成一个随机串 R_i,满足

$$R_i=K_{AU_i}\oplus K_{CU_i}^{(4n)}. \tag{17}$$

除此之外, 他还利用哈希函数生成另一个随机串 $S_i^{(2)}$

$$S_i^{(2)}=H(R_i\left\|S_i^{(1)}\right\|M'_i), \tag{18}$$

于是 U_i 生成他的个体签名

$$S_i=S_i^{(1)}\left\|S_i^{(2)}\right. . \tag{19}$$

3) 个体签名验证和复合签名生成过程.

(1) Charlie 生成 $2n$ 比特串 c_1.

Charlie 将 U_i 发送过来的量子态与手中的粒子结合, 然后做一个二粒子贝尔基测量, 依据测量结果可以生成随机串

$$c_1=\begin{cases}00, \text{当观测的量子态为}|\beta_{00}\rangle\\ 01, \text{当观测的量子态为}|\beta_{01}\rangle\\ 10, \text{当观测的量子态为}|\beta_{10}\rangle\\ 11, \text{当观测的量子态为}|\beta_{11}\rangle\end{cases}. \tag{20}$$

(2) Charlie 获取 a_1' 和 T'.

Charlie 分别解密 $E_{AC}(|\varphi(a_1)\rangle)$和 $E_{AC}(|\varphi(T)\rangle)$ 然后做 Z-型基测量得到 a_1' 和 T'.

(3) Charlie 获取 S_i' 和 M_i''.

Charlie 要求 U_i 将 $E_{K_{CU_i}}(|\psi(S_i)\rangle)$和 $E_{K_{CU_i}}(|\psi(M'_i)\rangle)$发送过来, 然后通过解密和测量得到 S_i' 和 M_i''.

(4) 个体签名验证.

首先 Charlie 依据获得的 a_1', c_1 和 S_i' 检验

$$c_1(2j-1)c_1(2j)=\left(S_i^{'(1)}(j)\oplus a'_1(j)\right)\|a'_1(j),\quad j=1,2,3,\cdots,n \tag{21}$$

是否都成立. 如果 (21) 式中的等式都成立, 则 Charlie 接受签名. 否则, 拒绝签名并终止协议.

(5) 复合签名的生成.

若 $S_1', S_2', \cdots, S_t'$ 都已经生成并通过了验证, 则 Charlie 生成复合签名

$$S=\oplus_{i=1}^{t}S_i^{'(1)}. \tag{22}$$

与此同时, Charlie 生成

$$T''=\oplus_{i=1}^{t}M_i'', \tag{23}$$

于是可以得到消息

$$m'=T''\oplus T'. \tag{24}$$

然后 Charlie 将 $E_{BC}(|\varphi(S)\rangle)$和 $E_{BC}(|\varphi(m')\rangle)$发送给 Bob.

4) 复合签名验证过程.

(1) 比对消息.

Bob 通过解密并测量 $|\varphi(m)\rangle$和 $|\varphi(m')\rangle$分别得到 m' 和 m''. 若 $m'=m''$, 则公布验证参数 $V_1=1$, 并继续后面的验证步骤; 否则, 公布 $V_1=0$ 并结束协议.

(2) 验证复合签名.

在 Bob 公布验证参数 $V_1=1$时, Alice 在公告板上公布每一个 M_i, Charlie 公布每一个 S_i'. 与此同时, 每一个签名者 U_i 都公布各自的随机串 R_i. Bob 在获取这些信息后, 通过解密 $E_{BC}(|\varphi(S)\rangle)$并测量 $|\varphi(S)\rangle$得到 S', 然后验证

$$S'=\oplus_{i=1}^{t}S_i^{'(1)}, \tag{25}$$

$$S_i^{'(2)}=H(R_i\left\|S_i^{'(1)}\right\|M_i), \tag{26}$$

$$i=1,2,\cdots\cdots,t \tag{27}$$

如果以上的等式都成立, 则 Bob 接受 S' 为消息 m' 的多重签名, 否则, Bob 拒绝签名并终止协议.

相比于文献 [29] 中提出的协议, 本文提出的协议的优势为: 用三粒子部分纠缠态取代了三粒子极大纠缠 GHZ 态, 一定程度上节省了纠缠资源, 降低了协议实现的条件, 提高了协议的可应用性.

3 安全性分析

一个安全的签名协议必须满足不可伪造和不可抵赖两个基本条件, 由于协议是一个盲签名协议, 还必须满足盲性和可追溯性. 下面就不可伪造、不可抵赖、盲性和可追溯性来一一说明.

3.1 不可伪造

3.1.1 Alice 不能伪造签名

由于签名者 U_i 是通过对其所收到的部分纠缠粒子随机地作用一个泡利算子 I 或 Z 来生成 $S_i^{(1)}$,

$S_i^{(2)}$包含U_i的密钥K_{AU_i}和K_{CU_i}以及$S_i^{(1)}$, 这些都是 Alice 所没有的信息. 因此, Alice 如果想要伪造U_i的签名S_i, 他除了去猜测U_i的密钥K_{AU_i}和K_{CU_i}以及$S_i^{(1)}$以外, 只能在S_i的传输过程中下功夫. 但是 Alice 能猜出U_i的密钥K_{AU_i}和K_{CU_i}以及$S_i^{(1)}$的概率是微乎其微的, 因此, 只有在签名的传输过程中想办法伪造U_i的签名. 但很不幸的是, 协议中所有的经典消息都已经转换成了量子消息并使用文献 [30] 中提出的改进了的量子一次一密算法. 因此, Alice 无法成功伪造U_i的个体签名. 由此可见, Alice 无法伪造复合签名.

3.1.2 Charlie 无法伪造签名

Charlie 作为签名收集者, 他可以获取所有的个体签名并生成复合签名, 被认为是最有可能伪造签名的, 下面将说明 Charlie 也是不能伪造签名的. 因为 Charlie 拥有所有的个体签名S_i, 因此, 他可以随意地更改每一个个体签名. 譬如 Charlie 将签名的前段$S_i^{(1)}$和$S_j^{(1)}$分别改为$S_i^{'(1)}$和$S_j^{'(1)}$, 但保持$S_i^{(1)} \oplus S_j^{(1)} = S_i^{'(1)} \oplus S_J^{'(1)}$, 由 (25) 式可知复合签名是保持不变的. 看似整个过程天衣无缝, 但是修改后的签名仍然是不能通过验证的. 因为在验证过程中 Bob 不但要检验复合签名, 还要对每一个个体签名进行检验. 由于 Charlie 无法提前获知生成$S_i^{(2)}$和$S_j^{(2)}$所需的签名者的密钥, 因此无法根据修改后的$S_i^{'(1)}$和$S_j^{'(1)}$去确定它们所对应的$S_i^{'(2)}$和$S_j^{'(2)}$, 使它们满足 (26) 式, 因此无法确保修改后的签名能通过验证. 由此可见 Charlie 也无法伪造签名.

3.1.3 Bob 无法伪造签名

Bob 作为签名接收者, 一个被认为是最好伪造签名的办法就是当他验证完签名S后, 再将S修改为S'并宣称S'就是他收到的签名. 但在验证阶段, 所有的信息都公布在公告板上, 任何人都可以对签名进行验证. 因此, Bob 的不诚实行为很容易就被发现了. 由此可见, Bob 也不能伪造签名.

3.1.4 外部攻击者不能伪造签名

在这一小节主要讨论几种常见的外部攻击手段, 如纠缠辅助粒子攻击, 截获-重发攻击和中间人攻击. 纠缠辅助粒子攻击是一种常见的攻击方案, 所谓纠缠辅助粒子攻击就是攻击者用一个辅助粒子与信道中所发送的量子态相结合, 然后通过 CNOT 门使得它们之间建立纠缠, 然后通过解纠缠并测量辅助粒子来获取消息[24]. 由于本协议在分发纠缠粒子的时候采用的是安全的量子信道, 外部攻击者无法将辅助粒子与信道中传输的粒子进行纠缠, 该方案是行不通的. 因此, 外部攻击者无法使用该方案来伪造签名. 对于截获-重发攻击, 由于协议中所有的消息都是先转换成量子消息, 然后经过改进后的量子一次一密加密算法加密后进行传输, 攻击者即使截获了消息也无法伪造签名. 对于中间人攻击, 由于在参与者之间事先利用量子密钥分配协议分享了安全的密钥, 由量子密钥的无条件安全性可知, 攻击者是无法获取到参与者的密钥的, 因此, 攻击者无法实行中间人攻击. 综上所述, 外部攻击者是不能伪造签名的.

3.2 不可抵赖

3.2.1 每个签名者U_i不能抵赖

由单个签名的形成过程可以知道每一个个体签名S_i都含有签名者U_i的密钥K_{AU_i}和K_{CU_i}, 在整个签名协议中只有U_i能同时拥有这两个密钥. 并且在签名验证阶段被公布在公告板上. 如果U_i拒不承认他的签名, 这时候每一个人都可以通过验证 (17) 式来戳穿他的不诚实行为.

3.2.2 接收者 Bob 不能抵赖

Bob 的抵赖包含两个层面: 1)Bob 拒不承认他收到签名这一事实; 2)Bob 拒绝签名的完整性. 首先来说明 Bob 不能拒不承认他收到了签名. 因为在验证签名的时候, Bob 需要比对消息, 如果消息一致, 则公布$V=1$, 否则, 公布$V=0$. 当他公布验证参数V时, 则表明他已经收到了消息. 在协议中 Charlie 是将消息和签名依次发送给 Bob 的. 如果 Bob 坚持声称没有收到签名, 则 Charlie 可以再发送一次或是直接公布签名. 这样 Bob 就不能不承认他已经收到签名. 接下来说明 Bob 不能拒绝签名的完整性. 所谓拒绝签名的完整性指的是 Bob 已经验证了$m=m'$成立, 但为了自身的利益, 谎称$m \neq m'$来拒绝签名. 由于该签名协议签发的都是经典消息, 且 Alice, Charlie 和 Bob 都可以得到该消息. 当 Bob 谎称$m \neq m'$来拒绝签名时, 可以要求 Alice, Charlie 和 Bob 同时公布消息m, 由

于只有 Bob 在撒谎, 因此, Alice 和 Charlie 所公布的消息一定是一致的, 此时可以根据少数服从多数的原则来判定 Bob 是在撒谎. 由此可见, Bob 也是不能拒绝签名的完整性的. 综上所述, 在协议中 Bob 是不可抵赖的.

3.3 盲性

本协议中, 消息在发送之前都通过了盲化处理, 将每一份消息 m 转换成了 $M_i = m \oplus K_{AB}^{(n)} \oplus K_{AU_i}^{(n)}$ 再发送给签名者 U_i. 由于签名者 U_i 无法获取到 Bob 的密钥 K_{AB}, 于是签名者 U_i 也无法获知消息 m. 因此, 该签名协议是一个盲签名协议, 具有盲性.

3.4 可追溯性

虽然签名者不能获取消息的内容, 但是一旦发生纠纷, 签名者可以追溯到消息的发送者. 本协议中消息在盲化处理的时候都转化成了 $M_i = m \oplus K_{AB}^{(n)} \oplus K_{AU_i}^{(n)}$, 其中含有密钥 K_{AB} 和 K_{AU_i}, 在整个协议中只有 Alice 同时拥有这两个密钥, 因此, U_i 很容易就可以确认消息来自于 Alice.

4 结 论

本文在前人已有的工作基础上, 给出了一个基于三粒子部分纠缠态的量子广播多重盲签名协议. 与文献 [29] 中基于 GHZ 态的协议相比, 该协议在安全性上并没有受到任何损失, 这是一件有意义的事情. 众所周知量子纠缠是一种重要的资源, 在量子计算和量子通信中发挥着不可替代的作用, 但是纠缠资源非常脆弱, 很容易受环境的影响而发生退相干现象. 在现有的技术条件下, 要在整个通信过程中长时间地保持极大纠缠是一件有难度的事情, 而本文的协议不再依赖极大纠缠态而使用部分纠缠态, 这不仅节约了纠缠资源, 降低了协议实现的条件, 一定程度上提高了协议的可应用性. 这也充分体现了在某些情况下, 多粒子部分纠缠也可以作为一种资源来完美地完成一些既定的通信任务. 但是本协议安全性是基于使用的哈希函数, 仍是基于计算安全的. 如何设计一个具有理论上无条件安全的基于部分纠缠的量子广播多重盲签名协议是值得考虑的.

参考文献

[1] Shor P W 1994 *Proceeding of IEEE Symposium on Foundations of Computer Science* Santa Fe NM USA, November 20—22, 1994 p124
[2] Wallden P, Dunjko V, Kent A, et al. 2014 *Phys. Rev. A* **91** 042304
[3] Amiri R, Andersson E 2015 *Entropy* **17** 5635
[4] Gottesman D, Chuang I 2001 arXiv:quant-ph/0105032v2
[5] Zeng G, Keitel C 2002 *Phys. Rev. A* **65** 042312
[6] Li Q, Chan W, Long D 2009 *Phys. Rev. A* **79** 054307
[7] Zou X, Qiu D 2010 *Phys. Rev. A* **82** 042325
[8] Yin X, Ma W, Liu W 2012 *Int. J. Quantum Inf.* **10** 1250041
[9] Wang T, Wei Z 2012 *Quantum Inf. Process.* **11** 455
[10] Yang Y 2008 *Chin. Phys. B* **17** 415
[11] Cao H, Huang J, Yu Y, et al. 2014 *Int. J. Theor. Phys.* **53** 3095
[12] Xu G 2015 *Int. J. Theor. Phys.* **54** 2605
[13] Wen X, Tian Y, Ji L, et al. 2010 *Phys. Scr.* **81** 055001
[14] Wen X 2010 *Phys. Scr.* **82** 065403
[15] Xu R, Huang L, Yang W, et al. 2011 *Opt. Commun.* **284** 3654
[16] Zhang K, Song T, Zuo H, et al. 2013 *Phys. Scr.* **87** 045012
[17] Xu G, Zhang K 2015 *Quantum Inf. Process.* **14** 2577
[18] Su Q, Huang Z, Wen Q, et al. 2010 *Opt. Commun.* **283** 4408
[19] Yin X, Ma W, Liu W 2012 *Int. J. Theor. Phys.* **51** 455
[20] Lin T, Chen Y, Chang T, et al. 2014 *Proceeding of* 2014 *IEEE 14th International Conference on Nanotechnology* Toronto Canada, August 18—21, 2014 p868
[21] Shi W, Zhang J, Zhou Y, et al. 2015 *Quantum Inf. Process.* **14** 3019
[22] Wen X, Liu Y, Sun Y 2007 *Z. Naturforsch. A* **62** 147
[23] Wen X, Liu Y, Zhou N 2008 *Int. J. Mod. Phys. B* **22** 4251
[24] Wen X, Niu X, Ji L, et al. 2009 *Opt. Commun.* **282** 666
[25] Xiao M, Li Z 2016 *Quantum Inf. Process.* **15** 3841
[26] Tian Y, Chen H, Ji S, et al. 2014 *Opt. Quant. Electron.* **46** 769
[27] Zhang W, Qiu D, Zou X 2016 *Quantum Inf. Process.* **15** 2499
[28] Tian Y, Chen H, Gao Y, et al. 2014 *Int. J. Mod. Phys.: Conf. Ser.* **33** 1460369
[29] Zhang W, Qiu D, Zou X, et al. 2017 *Quantum Inf. Process.* **16** 150
[30] Kim T, Choi J, Jho N, et al. 2015 *Phys. Scr.* **90** 025101
[31] Yu C, Guo G, Lin S 2014 *Sci. China Phys. Mech. Astron.* **57** 2079
[32] Kumar A, Adhikari S, Banerjee S, Roy S 2013 *Phys. Rev. A* **87** 022307

Quantum broadcasting multiple blind signature protocol based on three-particle partial entanglement*

Zhang Wei [1)2)†] Han Zheng-Fu [2)]

1) (*Key Laboratory of Complex Systems and Intelligent Computing, School of Mathematics and Statistics, Qiannan Normal University for Nationalities, Duyun* 558000, *China*)

2) (*CAS Key Laboratory of Quantum Information, University of Science and Technology, Hefei* 230026, *China*)

(Received 18 November 2018; revised manuscript received 18 January 2019)

Abstract

Recently, a quantum broadcasting multiple blind signature scheme based on GHZ state has been proposed, which could be used to settle the problem that a message is so important that it needs to be signed by multiple signatories, in order to guarantee the message privacy: none of signatories can acquire the content of the message they have signed. Maybe it can be applied to an E-bank system. For example, a large amount of money has to be transferred through E-bank system on the internet. The E-bank system operator submits the request to the bank after filling the application form including payment amount, bank transfer account and some other information. When the request arrives, the bank clerk signs to approve. However, it is not enough, it has to ask the manager for authority, and then it needs to be signed by the manager. In the whole process, all the signatories cannot learn what they have signed, but the application form has been recorded in the E-bank system. So, once disagreement takes place, the bank can track the message sender.

In this paper, we present a new quantum broadcasting multiple blind signature scheme which is based on a three-particle partial entanglement state. Comparing with the original scheme, the partial entanglement state is utilized in our new scheme in place of the GHZ state, and this does not bring down the security of the scheme. Particularly, using the partial entanglement state can not only save the entanglement resource to some extent, but also make the scheme much easier to be realized. As is well known, It is not easy to keep the maximum entanglement state shared among the participants in the whole quantum communication process. By using the partial entanglement in place of the maximum entanglement can improve the new scheme applicability to make it more practical. It is also indicated that multi-qubit entangled systems which are partially entangled can be efficiently used as a resource in quantum information processing with perfect performance.

Keywords: quantum broadcasting multiple blind signature scheme, three-particle partial entanglement state, hash function

PACS: 03.65.–w, 03.67.–a, 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.68.20182044

* Project supported by the National Natural Science Foundation of China (Grant Nos. 11847083, 61602532), the Natural Science Foundation of Guizhou Province, China (Grant No. Qian-Ke-He-Jichu [2019]1296), the Youth Science and Technology Talents Growth Fund of Education Department of Guizhou Province, China (Grant No. Qian Jiao He KY Zi [2018]426), the Industrial Technology Foundation of Qiannan State, China (Grant No. Qiannan Ke He Gong Zi (2017) 9 Hao), the Special Fund of Research and Innovation of Qiannan Normal University for Nationalities, China (Grant No. QNSY2018BS015), and the Scientific Research Foundation for High-level Talents of Qiannan Normal University for Nationalities, China (Grant No. QNSYRC201716).

† Corresponding author. E-mail: wzhang01@ustc.edu.cn