



具有强安全性的指定验证者量子签名方案

荣民希 辛向军 李发根

Quantum signature for designated verifier with strong security

Rong Min-Xi Xin Xiang-Jun Li Fa-Gen

引用信息 Citation: *Acta Physica Sinica*, 69, 190302 (2020) DOI: 10.7498/aps.69.20200244

在线阅读 View online: <https://doi.org/10.7498/aps.69.20200244>

当期内容 View table of contents: <http://wulixb.iphy.ac.cn>

您可能感兴趣的其他文章

Articles you may be interested in

基于量子游走的仲裁量子签名方案

Arbitrated quantum signature scheme based on quantum walks

物理学报. 2019, 68(12): 120302 <https://doi.org/10.7498/aps.68.20190274>

基于Bell态粒子和单光子混合的量子安全直接通信方案的信息泄露问题

Information leakage problem in quantum secure direct communication protocol based on the mixture of Bell state particles and single photons

物理学报. 2017, 66(13): 130304 <https://doi.org/10.7498/aps.66.130304>

一个基于三粒子部分纠缠态的量子广播多重盲签名协议

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

物理学报. 2019, 68(7): 070301 <https://doi.org/10.7498/aps.68.20182044>

基于cluster态的信道容量可控的可控量子安全直接通信方案

Cluster state based controlled quantum secure direct communication protocol with controllable channel capacity

物理学报. 2017, 66(18): 180303 <https://doi.org/10.7498/aps.66.180303>

基于Cayley图上量子漫步的匿名通信方案

Anonymous communication scheme based on quantum walk on Cayley graph

物理学报. 2020, 69(16): 160301 <https://doi.org/10.7498/aps.69.20200333>

基于量子隐形传态的量子保密通信方案

Quantum communication scheme based on quantum teleportation

物理学报. 2017, 66(23): 230303 <https://doi.org/10.7498/aps.66.230303>

具有强安全性的指定验证者量子签名方案

荣民希¹⁾ 辛向军^{1)†} 李发根²⁾

1) (郑州轻工业大学数学与信息科学学院, 郑州 450002)

2) (电子科技大学计算机科学与工程学院, 成都 611731)

(2020 年 2 月 19 日收到; 2020 年 5 月 19 日收到修改稿)

多数传统的指定验证者签名方案无法抵抗量子计算机的攻击. 本文给出一种具有强安全性的指定验证者量子签名方案. 在方案中, 参与方利用量子密钥分配协议和量子直接通信协议共享密钥. 密钥生成中心制备 Bell 态序列并将其分配给签名者和指定验证者. 签名者利用其密钥和受控量子态对消息进行签名. 同时, 指定的验证者可以利用对称的签名步骤对量子签名进行仿真. 而验证者仿真的量子签名与签名者产生的量子签名完全一样. 这使得量子签名具有不可传递的属性. 本文所给出的签名方案可以抵抗伪造攻击, 截获重放攻击和木马攻击. 并且, 其理论上的信息安全属性可以得到证明. 同时, 密钥生成中心无需完全可信. 方案无需使用量子单向函数. 当产生量子签名时, 签名者无需制备纠缠态序列. 当验证签名时, 验证者无需执行量子态比较算法. 方案的量子比特效率达到 100%. 因此, 与类似方案相比, 本文所给方案具有较好的安全性和效率.

关键词: 量子签名, 安全, Bell 态, 不可传递性

PACS: 03.67.Dd

DOI: 10.7498/aps.69.20200244

1 引言

1976 年, Diffie 与 Hellmann^[1] 引入了数字签名的概念. 在公钥密码系统中, 数字签名具有公开验证的属性. 也就是说, 给定一个签名, 任何人都可以验证它的有效性. 这就意味着任何人都可通过数字签名验证所收到消息的完整性以及其原始的消息来源.

然而, 在某些情况下, 这种可公开验证性并不适用. 有时候, 签名者希望只有指定的签名接收者才能验证签名的有效性. 例如, 在项目投标过程中, 为保护投标者的经济利益, 一些投标者希望只有那些可信的机构才能验证投标者对文件的签名^[2]. 在一些投票系统中, 投票者希望只有可信的机构才能验证投票者的实名签名投票^[3,4]. 研究发现, 指定验证者签名也适用于可否认系统的应用^[5,6]. 因此, 基

于这种指定验证的属性, 研究者提出很多指定验证者签名方案 (SDVS)^[2,7–9]. 一般而言, SDVS 应满足如下属性^[8,9]:

1) 正确性. 利用签名算法所产生的签名, 必然能够通过验证算法来证实其有效性. 一旦签名通过验证, 指定的签名验证者 (DV) 应该接受该签名为有效签名.

2) 不可传递性. DV 不能向任何第三方证明所接收的签名的真实来源.

3) 信源隐蔽性. 给定一个签名, 即使签名者和 DV 公开他们的密钥, 任何人无法判断该签名是由签名者产生, 还是由 DV 仿真产生.

4) 不可伪造性. 任何外部敌手都无法有效伪造签名者的签名.

尽管人们提出了许多 SDVS, 但多数 SDVS 是传统的数字签名^[2,7–11]. 它们的安全性依赖于一些尚未得到证明的数学困难假设, 如离散对数问题和

† 通信作者. E-mail: xin_xiang_jun@126.com

大数分解问题. 研究发现, 这些数学困难问题并不能抵抗量子敌手的攻击^[12]. 为应对量子敌手对数字签名的安全威胁, Gottesman 和 Chuang^[13] 引入了量子签名的概念. 量子签名不同于传统的数字签名, 其具有物理的安全属性. 即量子签名的安全性主要依赖于一些基本量子力学原理, 如非正交量子态的不可区分性, 未知量子态的不可克隆性等. 量子签名的这种安全属性引起了研究者的浓厚兴趣, 人们提出了大量的量子签名方案^[14–24]. 按照构造方式, 量子签名方案可分为基于离散变量的量子签名方案^[14–22] 和基于连续变量相干态的量子签名方案^[23,24].

为使得 SDVS 可以抵抗量子敌手, Shi 等^[25,26] 提出两类指定验证者量子签名 (QSDV). Shi 等的 QSDV 方案具有传统的 SDVS 的属性. 需要注意的是, QSDV 方案本身是一种量子加密方案. 而安全的量子加密方案应在理论上具备信息安全属性 (information-theoretical security)—量子密文不可区分性^[27–29]. 然而, 文献^[25,26] 的量子密文的不可区分性并不能从理论上得到有效证明. 另外, 在文献^[25,26] 中, 需要使用量子单向函数, 验证者需要进行量子态比较算法来比较两个量子态是否相同. 需要注意的是, 量子态比较算法的输出具有一定的错误率. 因此, 需要进行执行大量的量子态比较测试才能验证两个量子态是否相同. 因此, 这将会影响文献^[25,26] 的执行和计算效率. 最近, 利用基于身份的密码系统的优点, Xin 等^[30] 提出了一个基于身份的 QSDV. 文献^[30] 的方案可以简化签名系统的密钥管理. 然而, 类似于文献^[25,26], 文献^[30] 的量子密文不可区分性也没有从理论上得到证明. 并且, 在文献^[30] 中, 量子签名是一个加密的 Bell 态序列. 而在实践中, Bell 态的制备相对于非纠缠态单光子来说较为麻烦.

本文提出一个新的 QSDV. 在本文的 QSDV 方案中, 签名者无需执行量子态比较算法. 在签名算法的步骤中, 签名者无需制备纠缠态或发送纠缠态粒子给 DV. 并且, 新方案的量子比特效率可达到 100%. 新方案不仅具备传统的指定验证属性, 而且具有较强的安全属性, 即其理论上的量子密文不可区分性可以得到证明. 该方案可以抵抗重放攻击, 冒充攻击和木马攻击. 并且, 与类似方案相比, 本文方案中的密钥生成中心不必完全可信. 因此, 与类似方案相比, 新方案相对具有较好的安全属性

和效率.

本文安排如下, 第 2 节简要回顾一次一密加密算法 (OTP); 第 3 节给出新的 QSDV; 第 4 节给出 QSDV 的安全分析; 第 5 节对类似的方案进行安全和效率比较; 最后, 给出本文的结论.

2 OTP 简要回顾

OTP 是一种对称加密算法. 其具有无条件安全性^[31]. 在该算法中, 消息发送者 Amy 和消息接收者 Jack 共享随机的密码本 r (长度为 n 的比特串). 为将长度为 n 的消息比特串 α 秘密发送给 Jack, Amy 利用 r 将 α 加密为 $\beta = \alpha \oplus r$. 这里的“ \oplus ”代表 XOR 操作. 一旦 Jack 收到 β , 其只需计算 $\alpha = \beta \oplus r$ 便可得到相应的消息 α .

3 新的具有强安全属性的 QSDV

在方案中, Amy 为签名者, 而 Jack 和 TC 分别为 DV 和密钥生成中心. 方案包括四个算法: 初始化算法, 密钥生成算法, QSDV 生成算法和验证算法.

3.1 初始化

步骤 1 通过执行量子密钥分配协议 (QK-DP)^[32,33], TC 与 Amy 共享二进制密钥比特串 $x = (x_1, x_2, \dots, x_n)$. 并且, TC 与 Jack 共享二进制密钥比特串 $y = (y_1, y_2, \dots, y_n)$. 类似地, 通过执行 QK-DP^[32,33], Amy 和 Jack 共享密钥 $c^1 = (c_1^1, c_2^1, \dots, c_n^1) \in \{0, 1\}^n$ 和 $c^2 = (c_1^2, c_2^2, \dots, c_n^2) \in \{0, 1\}^n$. 然后, TC 随机选取 $r = (r_1, r_2, \dots, r_n) \in \{0, 1\}^n$ 并计算 $u = (u_1, u_2, \dots, u_n)$ 和 $v = (v_1, v_2, \dots, v_n)$, 其中

$$u_i = y_i \oplus r_i, v_i = x_i \oplus r_i, i = 1, 2, \dots, n. \quad (1)$$

利用确定性量子直接通信^[34–36], TC 与 Amy 秘密地共享 u . 类似地, 利用确定性量子直接通信^[34–36], TC 与 Jack 秘密地共享 v .

步骤 2 TC 制备 n 个 Bell 态 $\{|\phi_1\rangle, |\phi_2\rangle, \dots, |\phi_n\rangle\}$, 其中

$$|\phi_i\rangle = \frac{1}{\sqrt{2}} (|0_{a_i} 0_{b_i}\rangle + |1_{a_i} 1_{b_i}\rangle), i = 1, 2, \dots, n. \quad (2)$$

根据 $\{|\phi_1\rangle, |\phi_2\rangle, \dots, |\phi_n\rangle\}$, TC 构建两个粒子序列 $\phi_a = \{\phi_{a_1}, \phi_{a_2}, \dots, \phi_{a_n}\}$ 和 $\phi_b = \{\phi_{b_1}, \phi_{b_2}, \dots, \phi_{b_n}\}$. 其中, ϕ_{a_i} 代表 $|\phi_i\rangle$ 的第一个粒子, 而 ϕ_{b_i} 代表 $|\phi_i\rangle$ 的

第二个粒子, $i = 1, 2, \dots, n$. 最后, TC 分别将序列 ϕ_a 和 ϕ_b 发送给 Amy 和 Jack. 为防止敌手对量子态序列 ϕ_a 和 ϕ_b 的窃听和干扰, 可采用 GLLP 公式^[37]和诱骗态方法^[38–40], 根据不同强度相干态的计数率和误码率检测敌手的窃听行为.

步骤 3 为安全接收量子态序列 ϕ_a 和 ϕ_b , Amy 和 Jack 采用 GLLP 公式^[37]和诱骗态方法^[38–40]分别对量子信道进行窃听检测. 若不存在窃听行为, 则 Amy 和 Jack 分别保存好量子态序列 ϕ_a 和 ϕ_b ; 否则, 重新执行初始化算法.

3.2 QSDV 的生成

假定 $H = (|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|)/\sqrt{2}$ 为 Hadamard 算子. 令

$$\begin{aligned} Y &= |0\rangle\langle 1| - |1\rangle\langle 0|, \\ Y^+ &= |1\rangle\langle 0| - |0\rangle\langle 1|, \\ |+\rangle &= (|0\rangle + |1\rangle)/\sqrt{2}, \\ |-\rangle &= (|0\rangle - |1\rangle)/\sqrt{2}. \end{aligned}$$

定义 $H^0 = Y^0 = I$, 其中 I 为单位算子. 假定 Amy 需要对消息 $m = (m_1, m_2, \dots, m_n) \in \{0, 1\}^n$ 产生 QSDV. 步骤如下:

步骤 1 根据 u, x, c^1 和 c^2 , Amy 计算 $k = (k_1, k_2, \dots, k_n)$ 和 $w = (w_1, w_2, \dots, w_n)$, 其中

$$\begin{aligned} k_i &= x_i \oplus u_i \oplus c_i^1 \oplus m_i, \quad w_i = c_i^2 \oplus m_i \\ (i &= 1, 2, \dots, n). \end{aligned} \quad (3)$$

然后, 其对每个 $|m_i\rangle$ 执行操作 $H^{k_i} Y^{w_i}$ 而得到量子态:

$$|s_i\rangle = H^{k_i} Y^{w_i} |m_i\rangle, \quad (4)$$

令 $|s\rangle = \otimes_{i=1}^n |s_i\rangle$.

步骤 2 针对每个 $|s_i\rangle$ ($i = 1, 2, \dots, n$), Amy 利用粒子 ϕ_{a_i} 和受控 Y 操作对 $|s_i\rangle$ 进行加密, 其中, ϕ_{a_i} 为受控粒子, 而 s_i 为目标粒子. 也就是说, 若 ϕ_{a_i} 的状态为 $|0\rangle$, Amy 对 $|s_i\rangle$ 执行 I 操作; 否则, Amy 对 $|s_i\rangle$ 执行 Y 操作. 因此, $|s_i\rangle$ 被加密为 $|s'_i\rangle$, 其中含有子系统 ϕ_{a_i} , ϕ_{b_i} 和 s_i 的系统的量子态为

$$|\chi_i^{a_i, b_i, s_i}\rangle = \frac{1}{\sqrt{2}} (|0_{a_i} 0_{b_i}\rangle \otimes |s_i\rangle + |1_{a_i} 1_{b_i}\rangle \otimes Y |s_i\rangle). \quad (5)$$

Amy 将量子签名

$$|s'\rangle = \{|s'_1\rangle, |s'_2\rangle, \dots, |s'_n\rangle\}, \quad (6)$$

和消息 m 发送给 Jack.

图 1 简要给出了初始化和 QSDV 的生成过程.

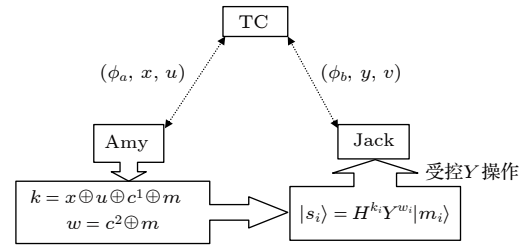


图 1 初始化和 QSDV 的生成过程
Fig. 1. Initialization and QSDV generation.

3.3 QSDV 的验证

步骤 1 当收到消息 m 和相应的量子签名 $|s'\rangle = \{|s'_1\rangle, |s'_2\rangle, \dots, |s'_n\rangle\}$ 后, Jack 针对每个 $|s'_i\rangle$ 执行受控 Y^+ 操作. 其中, ϕ_{b_i} 用作受控粒子, 而 s'_i 用作目标粒子. 也就是说, 若 ϕ_{b_i} 的状态为 $|0\rangle$, 则 Jack 针对 $|s'_i\rangle$ 执行 I 操作; 否则, Jack 针对 $|s'_i\rangle$ 执行 Y^+ 操作. 这样, Jack 解密 $|s'_i\rangle$ 而得到 $|s_i\rangle$. 则 Jack 得到序列 $|s\rangle = \otimes_{i=1}^n |s_i\rangle$.

步骤 2 根据 m, v, y, c^1 和 c^2 , Jack 计算 $k = (k_1, k_2, \dots, k_n)$ 和 $w = (w_1, w_2, \dots, w_n)$, 其中

$$\begin{aligned} k_i &= y_i \oplus v_i \oplus c_i^1 \oplus m_i, \quad w_i = c_i^2 \oplus m_i \\ (i &= 1, 2, \dots, n). \end{aligned} \quad (7)$$

然后, 针对每个 $|s_i\rangle$, Jack 对 $|s_i\rangle$ 执行操作 $(Y^+)^{w_i} H^{k_i}$ 而得到量子态:

$$|m'_i\rangle = (Y^+)^{w_i} H^{k_i} |s_i\rangle. \quad (8)$$

步骤 3 Jack 利用计算基 $\{|0\rangle, |1\rangle\}$ 测量每个 $|m'_i\rangle$. 若测量结果为 $|0\rangle$, 则其设 $m'_i = 0$. 否则, 其设 $m'_i = 1$. 令 $m' = (m'_1, m'_2, \dots, m'_n)$. Jack 验证是否 $m' = m$. 若相等, 则 Jack 接受 $|s'\rangle = \{|s'_1\rangle, |s'_2\rangle, \dots, |s'_n\rangle\}$ 为有效的 QSDV. 否则, Jack 拒绝该签名.

3.4 指定验证者对 QSDV 的仿真

为保证 QSDV 的不可传递性, 使得 Jack 具备仿真 Amy 的 QSDV 的能力. 也就是说, Jack 能够产生 QSDV 使得其与 Amy 产生的 QSDV 一样. 这样, 给定一个 QSDV, Jack 无法向任何第三方证明谁是真正的签名者, 这是因为 Amy 和 Jack 皆可产生同样的 QSDV. 在本节, 演示 Jack 如何仿真 Amy 的 QSDV.

步骤 1 根据 m, v, y, c^1 和 c^2 , Jack 计算 $k = (k_1, k_2, \dots, k_n)$ 和 $w = (w_1, w_2, \dots, w_n)$, 其中 $k_i = y_i \oplus v_i \oplus c_i^1 \oplus m_i$ 和 $w_i = c_i^2 \oplus m_i (i = 1, 2, \dots, n)$. Jack 对每个 $|m_i\rangle$ 执行操作 $H^{k_i}Y^{w_i}$ 得到 $|s\rangle = \otimes_{i=1}^n |s_i\rangle$, 其中 $|s_i\rangle = H^{k_i}Y^{w_i}|m_i\rangle$.

步骤 2 针对每个 $|s_i\rangle$, Jack 利用受控 Y 操作和粒子 ϕ_{b_i} 加密 $|s_i\rangle$, 其中 ϕ_{b_i} 用作受控粒子, 而 s_i 用作目标粒子. 即若 ϕ_{b_i} 的状态为 $|0\rangle$, Jack 对 $|s_i\rangle$ 执行 I 操作; 否则, Jack 对 $|s_i\rangle$ 执行 Y 操作. 因此, $|s_i\rangle$ 被加密为 $|s'_i\rangle$. 这样, 包含子系统 ϕ_{a_i}, ϕ_{b_i} 和 s_i 的系统的状态为 $|\chi_i^{a,b,s_i}\rangle$, 其满足 (5) 式. 消息 m 的 QSDV 为 $|s'\rangle = \{|s'_1\rangle, |s'_2\rangle, \dots, |s'_n\rangle\}$.

4 安全与效率分析

4.1 正确性

由 (1) 式、(3) 式、(7) 式、签名算法的步骤 1 和验证算法的步骤 2, 可知:

$$k_i = x_i \oplus y_i \oplus r_i \oplus c_i^1 \oplus m_i, i = 1, 2, \dots, n. \quad (9)$$

由 (4) 式和 (8) 式, 易知若 $|s'\rangle = \{|s'_1\rangle, |s'_2\rangle, \dots, |s'_n\rangle\}$ 为有效的 QSDV, 则 $m' = m$.

4.2 指定验证属性

方案为一个 QSDV 方案. 在方案的验证算法中, 为验证所收到的 QSDV 的有效性, 需要使用粒子序列 ϕ_b , 密钥 y, c^1, c^2 和 v . 需要注意的是, 只有 Jack 拥有 ϕ_b . 同时, 只有 Jack 具有 y, c^1, c^2 和 v . 因此, 只有 Jack 能够验证 QSDV. 虽然 TC 也具有 y 和 v , 但其不拥有 c^1, c^2 以及粒子序列 ϕ_b . 因此, 即使 TC 也无法验证 QSDV. 因此, 方案具有指定验证的属性.

4.3 不可传递性

根据 (3) 式、(7) 式和 (9) 式, 可知 Amy 和 Jack 都可计算 k 和 w . 因此, 他们都可对 $|m_i\rangle$ 执行操作 $H^{k_i}Y^{w_i}$ 而得到 $|s_i\rangle$. 同时, 根据 (2) 式, 可知 Amy 和 Jack 分别掌握 ϕ_{a_i} 和 ϕ_{b_i} . 因此, Amy 和 Jack 都可对 $|\phi_i\rangle$ 和 $|s_i\rangle$ 执行受控 Y 操作. 因此, 给定 m , Amy 和 Jack 能产生同样的 QSDV, 这使得 Jack 所仿真的 QSDV 与 Amy 所生成的 QSDV 无法相互区分. 因此, 本文所给出的 QSDV 满足不可传递性.

4.4 信源隐蔽性

在方案中, 签名者和验证者可以产生同样的 QSDV. 这使得即使密钥 x, y, c^1 和 c^2 遭到泄露, 包括 TC 在内的任何第三方都无法判断究竟 Amy 是签名者还是 Jack 为签名者. 因此, 方案具有信源隐蔽的特性.

4.5 理论上的信息安全属性-量子密文不可区分性

事实上, QSDV 是消息 m 的量子密文. 因此, 方案可视为消息 m 的量子加密方案 (QES). 而一个 QES 的理论上的信息安全属性是根据选择明文攻击下的量子密文的不可区分性来定义的 [27–29].

定义 1 [28,29] 一个 QES 方案 E 具备理论上的信息安全属性, 如果不存在量子多项式敌手 Ad 使得 Ad 能够以优势 $1/p(n)$ 有效区分量子密文 $E_{L(1^n)}(x)$ 和 $E_{L(1^n)}(y)$, 其中 n 为安全参数, x 和 y 为所有的不同的明文, $p(n)$ 为关于 n 的任意多项式, 而 L 为 E 内部的一个随机抛掷硬币算法.

由定义 1 可知, 具有理论上信息安全属性的 E 应该满足

$$\left| \Pr [Ad(E_{L(1^n)}(x)) = 1] - \Pr [Ad(E_{L(1^n)}(y)) = 1] \right| < 1/p(n). \quad (10)$$

根据 (10) 式, Yang 等 [29] 进一步证明, 理论上 QES 的信息安全属性依赖于 x 和 y 的量子密文对应的密度算子之间的迹距离. 相关结论如下.

定理 1 [29] 一个 QES 方案 E 具备理论上的信息安全属性, 如果其在选择明文攻击下密度算子 ρ_x 和 ρ_y 满足:

$$D(\rho_x, \rho_y) < 1/p(n), \quad (11)$$

其中 ρ_x 和 ρ_y 分别是量子密文 $E(x)$ 和 $E(y)$ 对应的密度算子.

关于定理 1 的详细证明, 请参考文献 [29]. 利用定理 1, 可以证明方案具备理论上的信息安全属性.

定理 2 QSDV 方案具备理论上的信息安全属性.

证明 令 $|s'\rangle$ 为消息 m 对应的 QSDV, 而 $|s'^*\rangle$ 为消息 m^* 对应的 QSDV. 由定理 1 可知, 要想证明方案的理论上的信息安全属性, 需要计算 $|s'\rangle$ 和 $|s'^*\rangle$ 对应的密度算子. 令 $\rho_{s',m}$ 和 $\rho_{s'^*,m^*}$ 分别表示 $|s'\rangle$ 和 $|s'^*\rangle$ 对应的密度算子. 由 (3)—(6) 式和 (9) 式, 可得

$$\begin{aligned}\rho_{s',m} &= \frac{1}{2^{5n}} \sum_{x,y,c^1,c^2,r \in \{0,1\}^n} \otimes_{i=1}^n (|s_i\rangle \langle s_i| + Y |s_i\rangle \langle s_i| Y^+) / 2 \\ &= \frac{1}{2^{6n}} \otimes_{i=1}^n \sum_{x_i,y_i,c_i^1,c_i^2,r_i \in \{0,1\}} \left(\begin{aligned} &H^{x_i \oplus y_i \oplus r_i \oplus c_i^1 \oplus m_i} Y^{c_i^2 \oplus m_i} |m_i\rangle \langle m_i| (Y^+)^{c_i^2 \oplus m_i} H^{x_i \oplus y_i \oplus r_i \oplus c_i^1 \oplus m_i} + \\ &Y H^{x_i \oplus y_i \oplus r_i \oplus c_i^1 \oplus m_i} Y^{c_i^2 \oplus m_i} |m_i\rangle \langle m_i| (Y^+)^{c_i^2 \oplus m_i} H^{x_i \oplus y_i \oplus r_i \oplus c_i^1 \oplus m_i} Y^+ \end{aligned} \right) = \frac{I}{2^n}.\end{aligned}$$

类似地, 可得 $\rho_{s'^*,m^*} = I/2^n$. 因此, 迹距离 $D(\rho_{s',m}, \rho_{s'^*,m^*}) = 0$. 根据定理 1, 可知 QSDV 具备理论上的信息安全属性.

4.6 不可伪造性

假定存在一个伪造者 Ad , 其目标是伪造 Amy 的一个 QSDV. 需要注意的是, 对于 Ad 而言, 为对消息 m 伪造一个有效的 QSDV, 其不得不计算 (4) 式和 (5) 式, 而在 (4) 式和 (5) 式中需要使用密钥 x, y, c^1, c^2 以及受控粒子序列 ϕ_a 或 ϕ_b . 然而, 由初始化算法可知, TC 通过执行 QKDP^[32,33] 与 Amy 和 Jack 分别共享密钥 x 和 y . 类似地, 利用 QKDP^[32,33], Amy 和 Jack 共享密钥 c^1 和 c^2 . 需要注意的, 文献 [32,33] 的 QKDP 具有无条件安全性. 因此, 密钥 x, y, c^1 和 c^2 也是无条件安全的. 因此, Ad 无法得到 x, y, c^1 和 c^2 . 需要注意的是, 在初始化阶段, TC 与 Amy 利用量子直接通信^[34–36] 秘密地共享 u . 类似地, TC 与 Jack 利用确定性量子直接通信^[34–36] 秘密地共享 v . 而文献 [34–36] 的量子直接通信协议具有无条件安全性^[41–43], 因此 Ad 无法得到 u 和 v . 另外, u (或 v) 为 y (或 x) 的 OTP 密文. 即使 Ad 能够获得 u (或 v), 根据 OTP 的无条件安全性^[31], 可知 Ad 仍无法由 u (或 v) 获得密钥 y (或 x). 根据 (3) 式和 (7) 式, 可知在不知道 x, y, u, v 和 c^1 的情况下, Ad 无法计算秘密参数 k . 更进一步, 若不知 k 和 c^2 , Ad 无法生成量子态 $|s\rangle = H^k Y^{c^2 \oplus m} |m\rangle$. 而且, 在不具备粒子序列 ϕ_a 或 ϕ_b 的情况下, Ad 无法实现对目标量子态 $|s\rangle$ 的加密. 因此, Ad 对消息 m 伪造一个有效的 QSDV 粒子序列 $|s'\rangle = \{|s'_1\rangle, |s'_2\rangle, \dots, |s'_n\rangle\}$ 是不可行的. 因此, Ad 无法伪造一个有效的签名. 另外, 虽然 TC 可以计算 k , 但其不知道 c^1 和 c^2 . 同时, TC 不掌握受控粒子序列 ϕ_a 和 ϕ_b . 因此, 即使 TC 也无法伪造消息 m 的 QSDV.

4.7 截获重放攻击

首先, 在方案中, TC 将序列 ϕ_a 和 ϕ_b 分别发送给 Amy 和 Jack. 敌手 Ad 可能试图截获、测量这

些序列并替换它们的状态. 需要注意的是, TC, Amy 和 Jack 采用 GLLP 公式和诱骗态方法来检测量子信道上敌手的窃听行为. TC, Amy 和 Jack 可根据不同强度相干态的计数率和误码率检测出敌手的窃听行为. 因此, 在初始化算法步骤 3 中, Ad 对序列的截获重放攻击将会被 Amy 和 Jack 通过窃听检测发现.

其次, 在验证 QSDV 的时候, 敌手 Ad 可能会截获量子签名 $|s'\rangle = \{|s'_1\rangle, |s'_2\rangle, \dots, |s'_n\rangle\}$ 并将其替换为另外一个序列 $|s^*\rangle = \{|s_1^*\rangle, |s_2^*\rangle, \dots, |s_n^*\rangle\}$, 并企图使得 $|s^*\rangle$ 能通过 DV 的验证. 然而, 由 4.6 节的不可伪造分析可知, Ad 伪造 QSDV 签名 $|s^*\rangle$ 使得其通过验证是不可行的. 因此, Ad 的这种截获重放攻击是不可行的.

最后, 根据 (4) 式和 (5) 式, Ad 可得到 $|s'_i\rangle$ 具备状态 $\rho_{s'_i} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$. 而且, 由定理 2 可知, QSDV 具备理论上的信息安全属性. 因此, QSDV $|s'\rangle = \{|s'_1\rangle, |s'_2\rangle, \dots, |s'_n\rangle\}$ 对于敌手来说具备量子密文不可区分性. 这意味着敌手 Ad (包括 TC) 无法从 $|s'\rangle$ 中得到任何有用信息.

4.8 木马攻击

在初始化算法步骤 2 中, 一个恶意的 TC 可能会在每个 $|\phi_i\rangle$ 中插入不可见光子以便窃听 Amy 和 Jack 所共享的密钥 c^1 和 c^2 .

TC 制备不可见光子序列 $D_T = \{|0\rangle_i^T\}$ ($1 \leq i \leq n$) 并通过受控非门操作使其与序列 $\{|\phi_1\rangle, |\phi_2\rangle, \dots, |\phi_n\rangle\}$ 中的粒子纠缠而得到一个新的序列 $\{|\phi_1^T\rangle, |\phi_2^T\rangle, \dots, |\phi_n^T\rangle\}$, 其中

$$\begin{aligned}|\phi_i^T\rangle &= \frac{1}{\sqrt{2}} (|0_{a_i}\rangle |0_i^T\rangle |0_{b_i}\rangle + |1_{a_i}\rangle |1_i^T\rangle |1_{b_i}\rangle), \\ i &= 1, 2, \dots, n.\end{aligned}\quad (12)$$

根据 $\{|\phi_1^T\rangle, |\phi_2^T\rangle, \dots, |\phi_n^T\rangle\}$, 在初始化算法步骤 2 和步骤 3 中, TC 将粒子序列 $\phi_a^T = \{\phi_{a_1}^T, \phi_{a_2}^T, \dots, \phi_{a_n}^T\}$ 发送给 Amy. 则在签名算法的步骤 1 中, Amy 产生的序列 $|s\rangle$ 将和不可见光子序列 D_T 相关. 这导致量子签名 $|s'_i\rangle$ 的状态满足:

$$|\chi_i^{a,b,s_i}\rangle = \frac{1}{\sqrt{2}} (|0_{a_i} 0_{b_i}^T\rangle \otimes |s_i\rangle + |1_{a_i} 1_{b_i}^T\rangle \otimes Y|s_i\rangle). \quad (13)$$

TC 截获 Amy 发送给 Jack 的量子签名 $|s'_i\rangle$ 并用测量基 $\{|0\rangle_i^T, |1\rangle_i^T\}$ 对不可见光子序列进行测量. 这样, TC 可得到序列 $|s\rangle = \otimes_{i=1}^n |s_i\rangle$, 其中 $|s_i\rangle = H^{x_i \oplus y_i \oplus r_i \oplus c_i^1 \oplus m_i} Y^{c_i^2 \oplus m_i} |m_i\rangle$. 需要注意的是, TC 掌握着 x_i, y_i, r_i 和 m_i . 因此, 通过对 $|s_i\rangle$ 执行操作 $H^{x_i \oplus y_i \oplus r_i}$, TC 可得到:

$$|s''_i\rangle = H^{c_i^1 \oplus m_i} Y^{c_i^2 \oplus m_i} |m_i\rangle, \quad i = 1, 2, \dots, n. \quad (14)$$

于是, TC 可得 $|s''\rangle = \otimes_{i=1}^n |s''_i\rangle$. 下面, 证明 $|s''\rangle$ 具备理论上的信息安全属性, 从而 TC 无法从 $|s''\rangle$ 中获得关于密钥 c^1 和 c^2 的任何有用信息.

定理 3 量子密文 $|s''\rangle$ 具备理论上的信息安全属性.

证明 假定 $|s''\rangle$ 和 $|s''^*\rangle$ 分别是消息 m 和 m^* 的量子密文. 根据 (14) 式, 可计算 $|s''\rangle$ 的密度算子如下:

$$\begin{aligned} \rho_{s'',m} &= \frac{1}{2^{2n}} \sum_{c^1, c^2 \in \{0,1\}^n} \otimes_{i=1}^n |s''_i\rangle \langle s''_i| \\ &= \frac{1}{2^{2n}} \sum_{c^1, c^2 \in \{0,1\}^n} \otimes_{i=1}^n H^{c_i^1 \oplus m_i} Y^{c_i^2 \oplus m_i} |m_i\rangle \\ &\quad \times \langle m_i| (Y^+)^{c_i^2 \oplus m_i} H^{c_i^1 \oplus m_i} \\ &= \frac{1}{2^{2n}} \otimes_{i=1}^n \sum_{c_i^1, c_i^2 \in \{0,1\}} H^{c_i^1 \oplus m_i} Y^{c_i^2 \oplus m_i} |m_i\rangle \\ &\quad \times \langle m_i| (Y^+)^{c_i^2 \oplus m_i} H^{c_i^1 \oplus m_i} \\ &= I/2^n. \end{aligned}$$

类似地, 可得 $|s''^*\rangle$ 的密度算子 $\rho_{s'',m^*} = I/2^n$. 因此, 迹距离 $D(\rho_{s'',m}, \rho_{s'',m^*}) = 0$. 由定理 1 可知, 量子密文 $|s''\rangle$ 具备理论上的信息安全属性. 证毕.

由定理 3 可知, 由于 $|s''\rangle$ 具有量子密文不可区分性, 从而 TC 无法从 $|s''\rangle$ 获得关于密钥 c^1 和 c^2 的任何有用信息. 因此, QSDV 可以抵抗木马攻击.

4.9 冒充攻击

在初始化算法阶段, 签名生成阶段和签名验证阶段, 敌手 Ad 企图冒充合作伙伴.

首先, 在初始化算法阶段, Amy 和 Jack 可在步骤 3 中通过诱骗态方法检测敌手对量子信道的窃听和冒充干扰. 因此, Ad 冒充 TC 的行为是不可行的. 类似地, Ad 冒充 Amy 和 Jack 也是不可

行的.

其次, 在签名生成阶段, 敌手 Ad 企图冒充 Amy 产生有效的 QSDV. 根据 4.6 节分析, 可知 QSDV 具有不可伪造性. 因此, 敌手 Ad 企图冒充 Amy 产生有效的 QSDV 是不可行的.

最后, 在签名的验证阶段, 敌手 Ad 企图冒充 Jack 来对 QSDV 进行验证. 根据 4.2 节的分析, 可知 QSDV 具有指定验证的属性. 因此, 敌手 Ad 冒充 Jack 来验证 QSDV 的合法性是不可行的.

5 比较与探讨

首先, 分析方案的效率. 在文献 [44–46] 中, 量子比特效率 η_q 定义为 $\eta_q = \delta_1/\delta_2$, 其中 δ_2 表示量子信道所传递的量子比特总数, 而 δ_1 表示得到经典比特数目 (检测窃听攻击的量子比特和经典比特, 以及执行量子密钥分配协议所传递和共享的经典比特和量子比特忽略不计). 根据文献 [44–46] 可知, 量子协议或签名系统的初始化阶段只是为了在签名阶段和验证阶段的量子编码和信息的传递. 特别地, 对于签名系统, 系统的初始化只执行一次. 初始化阶段一旦完成, 系统在以后运行中, 仅仅执行量子签名算法和验证算法 (即系统在以后对所有不同的消息进行量子签名时, 只需执行量子签名算法和验证算法). 所以, 一般在计算量子比特效率 η_q 时, 只考虑在量子签名算法和验证算法中量子比特的使用效率. 而在本文的量子签名生成阶段, Amy 将 n 个量子比特 QSDV $|s'\rangle = \{|s'_1\rangle, |s'_2\rangle, \dots, |s'_n\rangle\}$ 发送给 Jack, 即 $\delta_2 = n$. 在量子签名的验证阶段, Jack 通过量子比特序列 $|s'\rangle$ 解码获得 n 比特的经典信息 m' , 即 $\delta_1 = n$. 也就是说, 量子比特序列 QSDV $|s'\rangle = \{|s'_1\rangle, |s'_2\rangle, \dots, |s'_n\rangle\}$ 承载了 n 比特的经典信息量. 类似于文献 [44–46] 的计算, 可得量子比特的利用效率 $\eta_q = \delta_1/\delta_2 = 100\%$. 本文主要讨论的是 QSDV 方案分析与比较. 文献 [15] 中给出一种仲裁量子签名方案, 其量子比特的利用效率也达到 100%. 然而, 文献 [15] 所研究的为普通的仲裁量子签名, 其并不具备 QSDV 方案所要求的特征 (如, 指定验证、不可传递和信源隐藏等), 安全属性和要求显然与本文的研究不同.

其次, 在本文的方案中, 合作伙伴之间无需使用量子单向函数. 而在文献 [25,26] 中, 需要使用量子单向函数, 这无疑会增加 QSDV 方案的复杂性.

表 1 安全与效率比较
Table 1. Comparisons of security and efficiency.

| 方案 | 量子签名密文理论上的信息安全属性 | TC是否可信 | 量子态比较 | 纠缠态 | 量子比特效率 η_q |
|------|------------------|--------|-------|-----|-----------------|
| [25] | 否 | 可信 | 是 | 否 | 50.0% |
| [26] | 否 | 可信 | 是 | 否 | 33.3% |
| [30] | 否 | 可信 | 否 | 是 | 33.3% |
| 新方案 | 是 | 半可信 | 否 | 否 | 100% |

第三, 在我们的 QSDV 方案中, 无需使用量子态比较算法. 而在文献 [25,26] 中, 为验证 QSDV 的有效性, DV 不得不执行量子态比较算法. 需要注意的是, 量子态比较算法的输出具有一定的错误概率. 因此, 在文献 [25,26] 中, 验证者需要进行大量的量子态比较测试才能确定 QSDV 的有效性. 这无疑会影响文献 [25,26] 方案的执行效率. 另外, 在文献 [30] 中, 为对消息签名, 签名者需要制备 Bell 态序列并将其发送给验证者. 需要注意的是, 在目前的条件下, 签名者制备非纠缠态相对更容易些.

最后, 进行类似方案的安全性比较. 需要注意的是, 所有的量子签名方案都是量子加密方案, 其应该具备理论上的信息安全属性[27–29]. 在类似 QSDV 文献 [25,26,30] 中, 主要讨论了 QSDV 的指定验证、不可传递、信源隐藏、不可伪造等安全属性. 然而, 文献 [25,26,30] 中方案的理论上的信息安全属性并未得到证实. 本文所给出的指定验证者量子签名不仅具有指定验证、不可传递、信源隐藏、不可伪造等安全属性, 而且其量子签名密文具有较强的不可区分度 (量子签名密文迹距离为零), 从而满足文献 [27–29] 所要求的理论上的信息安全属性 (见定理 1 和定理 2). 另外, 在文献 [25,26,30] 中, 要求 TC 必须是可信的 (因为他们掌握着签名者的密钥, 并具备伪造签名者签名的能力), 即假定 TC 不会冒充签名者伪造量子签名. 这是一个非常强的安全假设. 因为在虚拟的网络世界中, 完全可信的实体并不存在. 本文的方案可弱化这一安全假设. 即在本文的方案中, TC 不必完全可信. 注意到虽然 TC 可以计算 k , 但其不知道 c^1 和 c^2 . 同时, TC 不掌握受控粒子序列 ϕ_a 和 ϕ_b . 因此, 即使 TC 也无法伪造消息 m 的 QSDV. 因此, 可假设 TC 为半可信的, 其可以诚实地协助系统其他参与者完成系统的初始化, 但其并不能伪造签名者的量子签名. 因此, 相对类似方案而言, 本文所给的方案具有较强的安全性.

表 1 给出了类似的 QSDV 方案的安全和效率比较. 由以上分析和比较可知, 相对于类似方案, 本文所提出的 QSDV 方案具有较好的安全性和效率.

6 结 论

第一, 本文给出一种新的 QSDV 方案, 其可以抵抗伪造攻击、截获重发攻击、冒充攻击和木马攻击, 并具备指定验证、不可传递和信源隐藏等安全属性. 方案理论上的信息安全属性可得到证明. 可以弱化对 TC 的安全假设, 即 TC 无需完全可信. 而其他类似的 QSDV 方案不具备这样的强安全属性.

第二, 本文的方案无需使用量子单向函数, 可以简化方案的复杂性.

第三, 签名者生成 QSDV 时无需制备纠缠态序列; DV 验证签名时无需执行大量的量子态比较操作. 这些有利于提高方案的执行效率.

第四, 量子比特效率达到 100%.

因此, 与类似方案相比, 本文的方案相对而言有较好的安全性和效率.

参考文献

- [1] Diffie W, Hellmann M 1976 *IEEE IT* **22** 644
- [2] Saeednia S, Kremer S, Markowitch O 2003 *Information Security and Cryptology-ICISC* Seoul, Korea, November 27–28, 2003 p40
- [3] Ray I, Narasimhamurthi N 2001 *Proceedings of the 3rd international workshop on advanced issues of E-commerce and web-based information systems* San Juan, CA, USA, June 21–22, 2001 p188
- [4] Schoenmakers B 1999 *Advances in CRYPTO' 99* Santa Barbara, California, USA, August 15–19, 1999 p148
- [5] Huang X, Mu Y, Susilo W, Wu W 2007 *Proceedings of 1st International Conference on Pairing-Based Cryptography, Pairing 2007* Tokyo, Japan, July 2–4, 2007 p367
- [6] Wang B, Song Z 2009 *Inf. Sci.* **179** 858
- [7] Jakobsson M, Sako K, Impagliazzo R 1996 *Advances in Cryptology-Eurocrypt 1996* Santa Barbara, California, USA, August 18–22, 1996 p142
- [8] Kang B, Boyd C, Dawson E 2009 *J. Syst. Software* **82** 270

- [9] Lee J, Chang J, Lee D 2010 *Comput. Electr. Eng.* **36** 948
- [10] Hafizul I S, Biswas G P 2015 *Arab. J. Sci. Eng.* **40** 1069
- [11] Rastegari P, Susilo W, Dakhilalian M 2019 *Int. J. Theor. Phys.* **18** 619
- [12] Shor P W 1997 *SIAM J. Comput.* **26** 1484
- [13] Gottesman D, Chuang I 2001 arxiv: quant-ph/0105032 v2
- [14] Zeng G H, Keitel C H 2002 *Phys. Rev. A* **65** 042312
- [15] Yang Y G, Lei H, Liu Z C, Zhou Y H, Shi W M 2016 *Quantum Inf. Process.* **15** 2487
- [16] Yang Y G, Zhou Z, Teng Y W, Wen Q Y 2010 *Eur. Phys. J. D* **61** 773
- [17] Xin X, He Q, Wang Z, Yang Q, Li F 2019 *Optik* **189** 23
- [18] Wang M Q, Wang X, Zhan T 2018 *Quantum Inf. Process.* **17** 275
- [19] Xin X, Wang Z, Yang Q 2019 *Appl. Opt.* **58** 7346
- [20] Jiang D H, Xu Y L, Xu G B 2019 *Int. J. Theor. Phys.* **58** 1036
- [21] Ma H, Li F, Mao N, Guo Y 2017 *Int. J. Theor. Phys.* **56** 2551
- [22] Zhang J L, Zhang J Z, Xie S C 2018 *Int. J. Theor. Phys.* **57** 1612
- [23] Zeng G, Lee M, Guo Y, He G 2007 *Int. J. Quantum Inf.* **5** 553
- [24] Guo Y, Feng Y 2016 *Int. J. Quantum Inf.* **55** 2290
- [25] Shi W M, Zhou Y H, Yang Y G 2015 *Int. J. Theor. Phys.* **54** 3115
- [26] Shi W M, Wang Y M, Zhou Y H, Yang Y G, Zhang J B 2018 *Optik* **164** 753
- [27] Menezes A J, Oorschot P V, Vanstone S A 1996 *Handbook of Applied Cryptography* (Boca Raton: CRC Press) p41
- [28] Yang L, Yang B, Pan J 2012 *SPIE Photonics Europe* Belgium, April 16–19, 2012 p8440E1
- [29] Yang L, Xiang C, Li B 2013 *Chin. Commun.* **10** 19
- [30] Xin X, Wang Z, Yang Q, Li F 2020 *Int. J. Theor. Phys.* **59** 918
- [31] Shannon C E 1949 *Bell Syst. Tech. J.* **28** 656
- [32] Bennett C H, Brassard G 2014 *Theor. Comput. Sci.* **560** 7
- [33] Long G L, Liu X S 2002 *Phys. Rev. A* **65** 2302
- [34] Hu Y G 2018 *Int. J. Theor. Phys.* **57** 2831
- [35] Yan L, Sun Y, Chang Y, Zhang S, Wan G, Sheng Z 2018 *Quantum Inf. Process.* **17** 315
- [36] Deng F G, Long G L, Liu X S 2003 *Phys. Rev. A* **68** 042317
- [37] Gottesman D, Lo H K, Lütkenhaus N, Preskill J 2004 *Quantum Inf. Comput.* **4** 325
- [38] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
- [39] Lo H K, Ma X, Chen K 2005 *Phys. Rev. Lett.* **94** 230504
- [40] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
- [41] Lu H, Fung C H F, Ma X, Cai Q 2011 *Phys. Rev. A* **84** 042344
- [42] Fung C H F, Ma X, Chau H F, Cai Q 2012 *Phys. Rev. A* **85** 032308
- [43] Beaudry N J, Lucamarini M, Mancini S, Renner R 2013 *Phys. Rev. A* **88** 062302
- [44] Hwang T, Lee K C 2007 *IET Inf. Secur.* **1** 43
- [45] Shi W M, Zhou Y H, Yang U G 2015 *International Journal of Theoretical Physics volume* **54** 3115
- [46] Song Y 2019 *Acta Electr. Sin.* **47** 1443 (in Chinese) [宋云 2019 电子学报 **47** 1443]

Quantum signature for designated verifier with strong security

Rong Min-Xi¹⁾ Xin Xiang-Jun^{1)†} Li Fa-Gen²⁾

1) (*College of Mathematics and Information Science, Zhengzhou University of Light Industry, Zhengzhou 450002, China*)

2) (*School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China*)

(Received 19 February 2020; revised manuscript received 19 May 2020)

Abstract

Most of the classical designated verifier signature schemes are insecure against quantum adversary. In this paper, a quantum signature scheme for the designated verifier is proposed. In our scheme, during the initialization phase, the partners share secret keys by performing the quantum key distribution protocol. On the other hand, by performing the quantum direct communication protocol, the key generator center shares secret keys with the signer and the designated verifier, respectively. The key generator center generates a particle sequence of Bell state and distributes the particles between the signer and the designated verifier. During the signature generation phase, the signer encrypts the particle sequence by the secret keys and Hadamard operators. After that, the signer performs the controlled unitary operations on the encrypted particle sequence so as to generate the quantum signature. The designated verifier can simulate the quantum signature by performing the same symmetric signing steps as that performed by the original signer. Hence, the quantum signature signed by the true signer is the same as the one simulated by the receiver, which makes our scheme possess the designated properties. During the signature verification phase, the designated verifier performs the controlled unitary operations on the quantum signature and obtains the quantum ciphertexts. After that, the designated verifier decrypts the quantum ciphertexts by the symmetric secret keys and Hadamard operators so that the quantum signature can be verified. Our signature is secure against forgery attack, inter-resending attacks and Trojan horse attack. Because the trace distance between the density operators of different quantum signatures is zero, the information-theoretical security of our quantum signature scheme can be proved. The unconditionally secure quantum key distribution protocol and the one-time pad encryption algorithm can guarantee the security of the secret keys shared by the partners. What is more, the security assumption about the key generation center is weak. That is, it is not necessary to assume that the key generation center should be fully trusted. On the other hand, in our scheme, the quantum one-way function is not used. To generate a quantum signature, the signer need not prepare for entangled particle sequence. To verify a quantum signature, the verifier need not apply any state comparison to the received particles. The qubit efficiency is 100%. Therefore, our scheme has the advantages in the security and efficiency over the other quantum signature schemes for the designated verifier.

Keywords: quantum signature, security, Bell state, non-transferability

PACS: 03.67.Dd

DOI: 10.7498/aps.69.20200244

† Corresponding author. E-mail: xin_xiang_jun@126.com