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

基于量子游走的仲裁量子签名方案

冯艳艳 施荣华 石金晶 郭迎

Arbitrated quantum signature scheme based on quantum walks

Feng Yan-Yan Shi Rong-Hua Shi Jin-Jing Guo Ying

引用信息 Citation: Acta Physica Sinica, 68, 120302 (2019) DOI: 10.7498/aps.68.20190274
在线阅读 View online: https://doi.org/10.7498/aps.68.20190274
当期内容 View table of contents: http://wulixb.iphy.ac.cn

基于量子游走的仲裁量子签名方案*

冯艳艳 施荣华 石金晶† 郭迎

(中南大学计算机学院, 长沙 410083)

(2019 年 2 月 27 日收到; 2019 年 4 月 15 日收到修改稿)

基于量子游走的量子隐形传输模型, 提出了一种仲裁量子签名方案. 发送者编码要签名的信息在硬币态上, 并应用硬币态和位置态之间的条件相移算符产生用于量子隐形传输必需的纠缠态. 对生成的纠缠态测量可作为签名设计和信息恢复依据. 然后, 接收者依据来自发送者的测量结果测量其量子态, 进而验证签名的有效性和信息的真实性、完整性. 由于量子游走的应用, 本签名方案的初始化阶段不需要提前制备必须的纠缠态. 安全性分析表明方案满足不可抵赖、不可伪造和不可否认特性, 讨论和比较展示了键控链式受控非加密算法和随机数的使用可以抵抗已有方案中的抵赖和存在性伪造攻击. 此外, 量子游走已经被证明可以在多种不同的物理系统中和实验上实现, 因此本签名方案未来也许是可实现的.

关键词: 量子密码, 仲裁量子签名, 量子游走隐形传输, 键控链式受控非操作

PACS: 03.67.Dd, 03.67.–a, 03.65.Ud, 03.65.Aa **DOI:** 10.7498/aps.68.20190274

1 引 言

量子签名是数字签名的量子相对物. 类似于经典数字签名, 依照仲裁的参与度, 量子签名区分为真实量子签名 (true quantum signature, TQS) 和仲裁量子签名 (arbitrated quantum signature, AQS). 在 TQS 算法中, 签名算法是隐秘的, 验证算法是暴露的. 只有在产生纠纷或者分歧的时候, 仲裁才被需求. 在 AQS 算法中, 签名和验证算法均为秘密的. 仲裁作为可信任的第三方参与算法的设计和实现过程. 尽管 TQS 是有利的, AQS 被证明在电子投票和电子支付场景是更加实用的[1,2]. 因此, 本文重点关注 AQS.

随着未来量子计算机[3]的出现, 依据不可证明计算假设和许多难解数学难题的签名算法将被攻破. 而依据物理特性的量子密码签名算法是信息安全的, 加之量子保密通信技术在理论和实验上的不断发展[4–8], 许多学者们对 AQS 方案的研究一直密切关注. 2002 年, Zeng 和 Keitel[2] 首次基于 Greenberger-Horne-Zeilinger (GHZ) 态提出 AQS 方案. 2008 年, Curty 和 Lütkenhaus[9] 对文献 [2] 方案的描述和操作给出了评论. 同年, Zeng[10] 对文献 [2] 给出了一个详细的证明并对文献 [9] 给出了回应. 2009 年, Li 等[11] 使用 Bell 态代替 GHZ 态提出了相对应的 AQS 方案, 并展示了其在传输效率和实现具有低复杂度的优势. 之后, 研究者对 AQS 的安全性进行了深入研究. 2010 年, Zou 和 Qiu[12] 宣称已有的 AQS 方案不能保证来自接收者的抵赖, 并设计了可以抵抗接收者抵赖的 AQS 算法. 2011 年, Gao 等[13] 指出基于量子一次一密 (quantum one time pad, QOTP) 的 AQS 方案中存在签名的抵赖攻击和接收者的伪造攻击, 并给出了相应的改进方法. 同年, Choi 等[14]

* 国家自然科学基金 (批准号: 61871407, 61572529, 61872390)、中南大学中央高校基本科研业务费专项基金 (批准号: 2018zzts179) 和湖南省自然科学基金(批准号: 2017JJ3415)资助的课题.

† 通信作者. E-mail: shijinjing@csu.edu.cn

强调已有 AQS 协议中存在一种通过修改传输消息和签名的伪造攻击, 并提出了抵御这种攻击的方法. 2013 年, 张骏和吴吉义 [15] 建议了一种能够抵抗验证者已知明文攻击的 AQS 协议. 2015 年, Li 和 Shi[16] 使用链式受控非操作代替 QOTP 提出了 AQS 方案. 2016 年, Yang 等 [17] 设计了基于簇态的 AQS 协议, 其效率可以达到 1. 2017 年, Zhang 等 [18] 设计了基于键控链式受控非 (key-controlled chained CNOT, KCCC) 操作的改进的 AQS 方案. 2018 年, Zhang 和 Zeng[19] 提出一个改进的基于 Bell 态 AQS 方案. 以上这些方案都是基于离散变量的 AQS 方案. 在连续变量 AQS 协议方面, 我们分别提出了基于相干态 [20] 和压缩真空态 [21] 的 AQS 方案.

依据信息副本从签名者到接收者被传输的方式, 以上所提到的 AQS 协议可以分为两类: 1) 基于纠缠态的隐形传输方式, 例如 GHZ[2]、Bell[11]、连续 Einstein-Podolsky-Rosen (EPR)[20, 21]; 2) 简单的量子加密方式, 例如 QOTP[12]、链式受控非操作 [16]、KCCC 操作 [18]. 第二种 AQS 协议又可以分为可以抵抗存在性伪造攻击和不可以抵抗存在性伪造攻击的协议. 其中在基于 QOTP 的 AQS[12–16] 中, 由于其一个比特对应一个比特的加密方式, 签名者能够执行抵赖攻击且接收者在已知信息环境下可以执行存在性伪造攻击, 基于 KCCC 算法的改进的 AQS 协议 [18] 可以较优地抵抗这两类攻击. 相比于第二种信息传输方式, 基于纠缠的量子隐形传输方式具有如下特性: 第一, 在传输过程中具有防窃听功能, 即一旦有窃听者想要窃听信息, 测量引起的扰动会被诚实的参与者发现; 第二, 可以避免传输载体本身, 只是转移粒子所处的量子状态; 第三, 不受物理距离的限制, 普通的加密方式仅限在地区性的网络上. 因此, 应用基于量子游走的隐形传输转移信息副本和 KCCC 算法执行中间过程的加密传输, 本文提出一种新型的 AQS 协议.

量子游走是经典游走的量子对应. 1993 年, Aharonov 等 [22] 初次提出量子游走模型. 量子游走在多个方面展示了有意义的应用 (详见综述文献 [23, 24]), 其中量子游走在通信协议方面的应用 [25–27] 也开始暂露头角. 例如, 近两年, Wang 等 [25] 和 Shang 等 [26] 提出了量子游走的不同模型在隐形传输的成功应用, 文中指出必要的纠缠态无需提前制备, 它们可以在量子游走的第一步之后被制备 (相对于纠缠态的难以制备, 这是一种很大的改进). 而且, 作者给出了一维量子游走的实现线路图. 由于量子游走已经被证明可以在多种不同的物理系统和实验上实现 [28–30], 将其应用在量子通信协议中是有益的.

因此, 本文通过将基于量子游走的隐形传输方式应用在 AQS 方案中传输信息副本, 提出了基于量子游走的 AQS 方案. 提出的方案具有以下优势: 1) 纠缠态不必提前制备, 量子游走的第一步会产生信息传输必需的纠缠态; 2) KCCC 操作和随机数的应用可以抵抗已有 AQS 方案中的抵赖和存在性伪造攻击, 本方案满足不可抵赖、不可伪造和不可否认特性; 3) 由于量子游走已经被证明可以通过现有的光学元素实现, 提出的 AQS 方案实验上也许是可实现的.

本文的结构如下: 第 2 节描述基于图的量子游走; 第 3 节提出基于量子游走的 AQS 算法; 第 4 节对提出的 AQS 算法给出安全性分析、讨论以及比较; 第 5 节为结论.

2 基于图的量子游走

图上基于硬币的量子游走模型的定义由 Aharonov 等 [31] 给出. 已知 $G=(V, E)$ 为一个图, V 代表 G 的顶点集, E 代表 G 的边集. 对于规则图形, 图中的每个顶点具有相同的邻居, 其希尔伯特 (Hilbert) 空间可以表述为位置空间和硬币空间的张量积, 即

$$\mathcal{H}=\mathcal{H}_v\otimes\mathcal{H}_c, \tag{1}$$

其中 $\mathcal{H}_v$ 是顶点态 $|v\rangle$ 张成的 Hilbert 位置空间, 其中 $v\in V$. 在每一个顶点 j, 有 d 条有向边连接到其他的顶点, $\mathcal{H}_c$ 是边态 $|c\rangle$ 张成的 Hilbert 硬币空间, 其中 $c\in\{0,\cdots,d-1\}$, 它们用来标记有向边. 位置空间 $\mathcal{H}_v$ 和硬币空间 $\mathcal{H}_c$ 之间的条件移算符可以表示为

$$T=\sum\nolimits_{j,c}|k\rangle\langle j|\otimes|c\rangle\langle c|, \tag{2}$$

其中标签 c 指示游走者从顶点 j 游走到顶点 k.

考虑一个包含 l ($l=4$) 个顶点的图 (环), 如图 1 所示, 顶点标记为 0, 1, 2, 3, 构成量子游走的位置空间为 $\mathcal{H}_v=\{|0\rangle,|1\rangle,|2\rangle,|3\rangle\}$. 在每个顶点有两条边, 它们的标记分别为 0 和 1, 构成量子游走的硬

币空间为$\mathcal{H}_c=\{|0\rangle,|1\rangle\}$. 其条件移算符为

$$T_{\text{circle}}=\sum_{k=0}^{l-1}[|(k+1)\bmod l\rangle\langle k|\otimes|0\rangle\langle 0|]+\sum_{k=0}^{l-1}[|(k-1)\bmod l\rangle\langle k|\otimes|1\rangle\langle 1|], \quad (3)$$

其中 k 代表环中的顶点. 环上的相移规则见图 1.

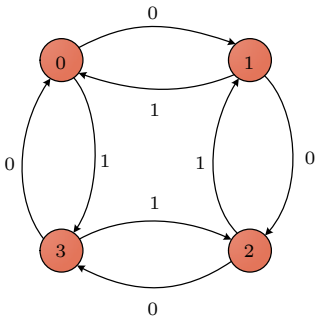

图 1 具有四个顶点的环及其相移规则

Fig. 1. Shift regulations on a cycle with four vertexes.

3 基于量子游走的量子签名算法

本 AQS 算法中, Alice 是信息的发送者和签名者, Bob 是签名后信息的接收者和验证者, Charlie 是值得 Alice 和 Bob 信任的第三方仲裁. 对于一个安全量子签名算法[2], 它应该遵循 Alice 对签名后的信息和签名的不可抵赖、任何人对 Alice 签名的不可伪造和 Bob 对接收到的签名信息或文件的不可否认特性.

3.1 初始化阶段

1) 密钥制备和分发: Alice 和 Charlie 制备共享密钥 K_a, Bob 和 Charlie 制备共享密钥 K_b, K_a 和 K_b 分别记为

$$K_a=\{K_a^1,K_a^2,\cdots,K_a^i,\cdots,K_a^n\}, \quad (4)$$

$$K_b=\{K_b^1,K_b^2,\cdots,K_b^i,\cdots,K_b^n\}, \quad (5)$$

其中 K_a^i 和 K_b^i $(i=1,2,\cdots,n)$ 是密钥序列 K_a 和 K_b 中第 i 个密钥. 它们的制备和分发可以通过量子密钥分发系统[4,5]完成.

2) 系统配置: 当 Alice 和 Bob 需要通信时, Alice 或 Bob 向 Charlie 申请通信.

3.2 签名阶段

1) Alice 准备量子比特信息序列$|\varphi\rangle$, 它承载着要签名的消息. 假设 n 个量子比特被包含在$|\varphi\rangle$中, 因此$|\varphi\rangle$可描述为

$$|\varphi\rangle=\{|\varphi_1\rangle,|\varphi_2\rangle,\cdots,|\varphi_i\rangle,\cdots|\varphi_n\rangle\}, \quad (6)$$

其中$|\varphi_i\rangle(i=1,2,\cdots,n)$代表一个单量子比特, 记为

$$|\varphi_i\rangle=a_i|0\rangle+b_i|1\rangle, \quad (7)$$

其中 a_i 和 b_i 是复数且满足$|a_i|^2+|b_i|^2=1$.

2) Alice 选择一个随机数 r, 并用其变换$|\varphi\rangle$为秘密的信息序列$|\varphi'\rangle$, 可记为

$$|\varphi'\rangle=E_r|\varphi\rangle=\{|\varphi_1'\rangle,|\varphi_2'\rangle,\cdots,|\varphi_i'\rangle,\cdots|\varphi_n'\rangle\}, \quad (8)$$

其中$|\varphi_i'\rangle=a_i'|0\rangle+b_i'|1\rangle$.

3) 应用 Zhang 等[18]提出的 KCCC 算法, Alice 使用密钥 K_a 生成量子态$|S_a\rangle$, 记为

$$|S_a\rangle=E'_{K_a}E_{K_a}(|\varphi'\rangle). \quad (9)$$

其中 E_K 代表改进的链式受控非加密操作, 包含两步操作: 第一步使用受控非操作加密$|\varphi'\rangle$, 第二步使用二进制密钥控制的 Hadamard H 门执行操作, 当二进制密钥为 0, H 门执行单位矩阵 I 操作, 反之, 执行 H 门操作. E'_K 代表 KCCC 加密操作, 关键点是引进了受控的转换操作, 用以重组签名态中的量子比特位置, 来规避 QOTP 中一个比特对应一个比特的加密方式引起的可能的抵赖和存在性伪造攻击[13,18]. 这个 KCCC 算法在文献 [18] 中已详细介绍, 这里将不再赘述.

4) 为了继续签名过程, 考虑四个顶点的环上的基于两个硬币的量子游走模型, 其线路原理图如图 2 所示. 作用在位置和硬币空间的条件相移算符 T_{circle} 重写如下:

$$T_{\text{circle}}=\sum_{k=0}^{2}|k+1\rangle\langle k|\otimes|0\rangle\langle 0|+\sum_{k=1}^{3}|k-1\rangle\langle k|\otimes|1\rangle\langle 1|+|0\rangle\langle 3|\otimes|0\rangle\langle 0|+|3\rangle\langle 0|\otimes|1\rangle\langle 1|, \quad (10)$$

Alice 持有两个粒子 A1 和 A2, 硬币 1 的态编码在 A1, 位置态编码在 A2. Bob 拥有一个粒子 B, 硬币 2 的态编码在 B. A1, A2 和 B 的初始态分别为$|\varphi_i'\rangle$, $|0\rangle$和$|+\rangle$, 则游走系统的总初始态为

$$|\phi\rangle^0=|0\rangle\otimes(a_i'|0\rangle+b_i'|1\rangle)\otimes|+\rangle, \quad (11)$$

其中$|+\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$.

量子游走第一步的幺正演化操作符为

$$W_1=E_1\cdot(I_p\otimes C_1\otimes I_2), \quad (12)$$

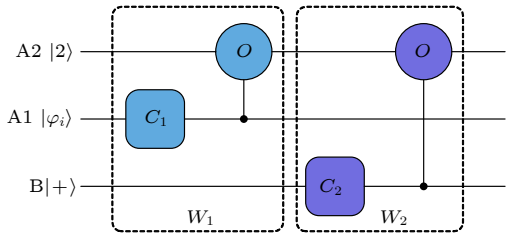

图 2 两个硬币的环上的量子游走线路原理图

Fig. 2. Circuit diagram of quantum walks on cycles with two coins.

其中$E_1=O\otimes|0\rangle_1\langle 0|\otimes I_2+O^\dagger\otimes|1\rangle_1\langle 1|\otimes I_2$且$E_1=T_{\text{circle}}\otimes I_2$, C_1是作用在硬币 1 的硬币算符, $O=\sum\limits_k|k+1\rangle\langle k|$为作用在位置空间的相移算符, $O^\dagger$为O的厄米共轭算符. 令$C_1=I$, 基于条件相移规则系统的初始量子态动态演变为

$$|\phi\rangle^1=\frac{1}{\sqrt{2}}(a_i'|1\rangle|0\rangle|0\rangle+b_i'|3\rangle|1\rangle|1\rangle). \tag{13}$$

这一步使得位置空间和硬币空间产生了纠缠, 即 Alice 和 Bob 之间有了纠缠. 量子游走第二步演化算符为

$$W_2=E_2\cdot(I_p\otimes I_1\otimes C_2), \tag{14}$$

其中$E_2=O\otimes I_1\otimes|0\rangle_2\langle 0|+O^\dagger\otimes I_1\otimes|1\rangle_2\langle 1|$且$E_2=T_{\text{circle}}\otimes I_1$, C_2是作用在硬币 2 的硬币算符. 令$C_2=I$, 同样基于相移规则得到系统的终态为

$$\begin{aligned}|\phi\rangle^2=&|0\rangle\otimes(a_i'|01\rangle+b_i'|10\rangle)/\sqrt{2}+|2\rangle\\&\otimes(a_i'|00\rangle+b_i'|11\rangle)/\sqrt{2}.\end{aligned} \tag{15}$$

有必要提到的是对于本文系统量子态的表达, 其所有的粒子是按照 A2, A1 与 B 粒子的顺序书写.

5) Alice 应用测量基$\{|0\rangle,|1\rangle,|2\rangle,|3\rangle\}$在粒子 A2 且应用测量基$\{|+\rangle,|-\rangle\}$在粒子 A1. 测量 A2 之后可获取 A1 和 B 所处的纠缠状态, 测量 A1 使得 A1 的信息塌陷到 B. Alice 的测量基可表示为

$$|M_a\rangle=\{|M_a^1\rangle,|M_a^2\rangle,\cdots,|M_a^i\rangle,\cdots,|M_a^n\rangle\}, \tag{16}$$

其中$|M_a^i\rangle$包含分别作用在 A2 和 A1 的两种测量基, 前者可以是$|0\rangle$与$|2\rangle$中的一个, 后者是$|+\rangle$与$|-\rangle$中的一个.

6) Alice 发送$|S\rangle=(|M_a\rangle,|S_a\rangle)$以及信息$|\varphi'\rangle$的一个副本给 Bob.

3.3 验证阶段

1) Bob 通过 KCCC 加密算法应用密钥K_b加密$|S_a\rangle$和$|\varphi'\rangle$, 得到$|Y_b\rangle$,

$$|Y_b\rangle=E'_{K_b}E_{K_b}(|S_a\rangle,|\varphi'\rangle), \tag{17}$$

然后 Bob 传输$|Y_b\rangle$给 Charlie.

2) Charlie 使用密钥K_b解密接收到的$|Y_b\rangle$, 得到$|S_a\rangle$和$|\varphi'\rangle$. 接着 Charlie 用密钥K_a加密$|\varphi'\rangle$, 获得$|S_c\rangle$. 为了判断$|S_a\rangle$和$|S_c\rangle$是否连续, Charlie 设计了验证参数 t,

$$t=\begin{cases}1, & \text{if } |S_a\rangle=|S_c\rangle=E'_{K_a}E_{K_a}|\varphi'\rangle,\\0, & \text{if } |S_a\rangle\neq|S_c\rangle=E'_{K_a}E_{K_a}|\varphi'\rangle,\end{cases} \tag{18}$$

其中$|S_c\rangle$和$|S_a\rangle$分别从$|\varphi'\rangle$和$|Y_b\rangle$得到. 接着 Charlie 应用 KCCC 加密算法使用密钥K_b加密$|S_a\rangle$, $|\varphi'\rangle$和 t, 生成$|Y_{cb}\rangle$,

$$|Y_{cb}\rangle=E'_{K_b}E_{K_b}(|S_a\rangle,|\varphi'\rangle,t), \tag{19}$$

将其传输给 Bob.

3) Bob 使用密钥K_b解密接收到的$|Y_{cb}\rangle$, 得到$|S_a\rangle$, $|\varphi'\rangle$和 t. 基于 t的值, Bob 进行第一轮验证: 如果$t=0$, 签名也许被伪造, Bob 立即拒绝来自 Alice 的信息$|\varphi\rangle$; 如果$t=1$, 它仅仅说明量子态$|S_a\rangle$是连续的, 需要进行第二轮的验证.

4) 在$t=1$的情况下, 首先 Bob 需要恢复出密文信息序列, 然后与原密文信息序列$|\varphi'\rangle$进行比较. 由于量子游走的第一步之后使得位置空间和硬币空间之间具有纠缠, Alice 对位置和硬币 1 的测量使得传输的信息坍塌在 Bob 的硬币 2 上. 基于 Alice 的 A1 和 A2 的测量结果M_a, Bob 执行相应的泡利操作在硬币 2, 如表 1 所列. Bob 的测量基表示为

$$|M_b\rangle=\{|M_b^1\rangle,|M_b^2\rangle,\cdots,|M_b^i\rangle,\cdots,|M_b^n\rangle\}, \tag{20}$$

其中$|M_b^i\rangle$可以是$\{I,Z,X,ZX\}$中的一种操作. 恢复的密文信息序列为$|\varphi'^{\text{out}}\rangle$, 即

$$|\varphi'^{\text{out}}\rangle=\{|\varphi'^{\text{out}}_1\rangle,|\varphi'^{\text{out}}_2\rangle,\cdots|\varphi'^{\text{out}}_i\rangle,\cdots,|\varphi'^{\text{out}}_n\rangle\}. \tag{21}$$

如果$|\varphi'\rangle\neq|\varphi'^{\text{out}}\rangle$, Bob 拒绝$|\varphi'\rangle$并放弃这次通信. 否则, Bob 发布一个请求 Alice 公布随机数 r的通知.

根据表 1, 例如, 基于 Alice 的位置和硬币 1 的测量结果 M_a, Bob 可以得到$|\varphi'^{\text{out}}\rangle$. 其相应的变换规则为: 测量结果 0 与 2 分别对应于 A2 的$|0\rangle$与$|2\rangle$, 测量结果 1 与–1 分别对应于 A1 的$|+\rangle$与$|-\rangle$. 假设 Alice 应用测量基$|2\rangle$在粒子 A2, 并得到测量结果为 2, A1 和 B 之间的纠缠态为

$$|\phi\rangle_{\text{A1,B}}=(a_i'|00\rangle+b_i'|11\rangle)/\sqrt{2}. \tag{22}$$

然后当 Alice 对粒子 A1 选择测量基$|+\rangle$, 即测量结

果对应为 1, 可以看到 Bob 应用单位矩阵 I 在硬币 2 得到 $|\varphi'^{\text{out}}\rangle$ 为 $a'_i|0\rangle + b'_i|1\rangle$, 即 $|\varphi'^{\text{out}}\rangle = |\varphi'\rangle$. 然而当 Alice 对 A1 应用测量基 $|-\rangle$, Bob 得到 $|\varphi'^{\text{out}}\rangle$ 为 $a'_i|0\rangle - b'_i|1\rangle$, 根据表 1, Bob 应用泡利 Z 操作在 $a'_i|0\rangle - b'_i|1\rangle$, 得到变换后结果为 $a'_i|0\rangle + b'_i|1\rangle$, 即 $Z|\varphi'^{\text{out}}\rangle = |\varphi'\rangle$. 其他两种情况可以类似的得到验证. 因此, 倘若密文信息序列 $|\varphi'\rangle$ 中的 n 个量子比特都可以得到验证, 那么确定 Alice 执行的签名是有效的, 密文信息 $|\varphi'\rangle$ 是完整且真实的.

表 1 测量结果与对应的恢复操作

Table 1. Measurement outcomes and the corresponding recovery operations.

A2和A1的测量结果	幺正操作
2, 1	I
2, –1	Z
0, 1	X
0, –1	ZX

5) Alice 通过公共板公布 r.

6) Bob 使用 r 从 $|\varphi'\rangle$ 恢复 $|\varphi\rangle$ 并确认 $(|S_a\rangle, r)$ 为 Alice 的信息序列 $|\varphi\rangle$ 的签名. 本 AQS 算法的方案原理图如图 3 所示.

4 安全性分析

首先, 我们重述仲裁 Charlie 在所提出的签名算法中所起的作用. 在初始化阶段, Charlie 和 Alice (Bob) 通过量子密钥分发系统制作准备并分配了秘密钥 K_a (K_b); 在验证阶段, Charlie 创造了验证参数 t, 用以判断量子态 $|S_a\rangle$ 和 $|S_c\rangle$ 的连续性, 这一步骤有效地辅助 Bob 完成两轮的验证, 如步骤 3) 和 4). 然后, 基于一个签名算法的安全性规则, 我们对提出的签名算法从不可抵赖、不可伪造与不可否认三个方面给出相应的安全性分析、讨论以及与已有典型 AQS 协议的比较. 在这个过程中, 我们说 Charlie 是绝对安全且值得信任的.

4.1 不可抵赖性

Alice 不可抵赖自己完成的签名. 从 (9) 式可以看到, 量子态 $|S_a\rangle$ 是通过 K_a 加密 $|\varphi'\rangle$ 得到, 即 $|S_a\rangle = E'_{K_a} E_{K_a}(|\varphi'\rangle)$, 其中 K_a 是 Alice 和 Charlie 通过无条件安全的量子密钥分发系统制备. 如果 Alice 抵赖了 $|S_a\rangle$ 并因此与 Bob 陷入了纠纷, 此时通过传输 $|S_a\rangle$ 给 Charlie. 如果 Charlie 判定接收到的 $|S_a\rangle$ 中有 K_a, 则 $|S_a\rangle$ 一定由 Alice 创造; 否则, 它也许被叛变的 Bob 或外部攻击者伪造.

而且, Alice 抵赖 $|S_a\rangle$ 的概率可以被量化. Alice 对 $|S_a\rangle$ 有抵赖或接受两种可能, 因此 Alice 抵赖和接受的概率分别是 1/2, 将抵赖和接受看作二分变量. 假设 $|S_a\rangle$ 中的 n 个量子比特有 m 个被抵赖, 那么 Alice 抵赖签名的概率为

$$P_{\text{disavowal}}(m) = \begin{pmatrix} n \\ m \end{pmatrix} \left(\frac{1}{2}\right)^m \left(\frac{1}{2}\right)^{n-m}, \tag{23}$$

其中

$$\begin{pmatrix} n \\ m \end{pmatrix} = \frac{n!}{m!(n-m)!}. \tag{24}$$

如图 4 所示, 图中呈现了 $n = 50, 100, 150$ 三种情况, 横轴表示被抵赖的量子比特数 m, 纵轴为 Alice 抵

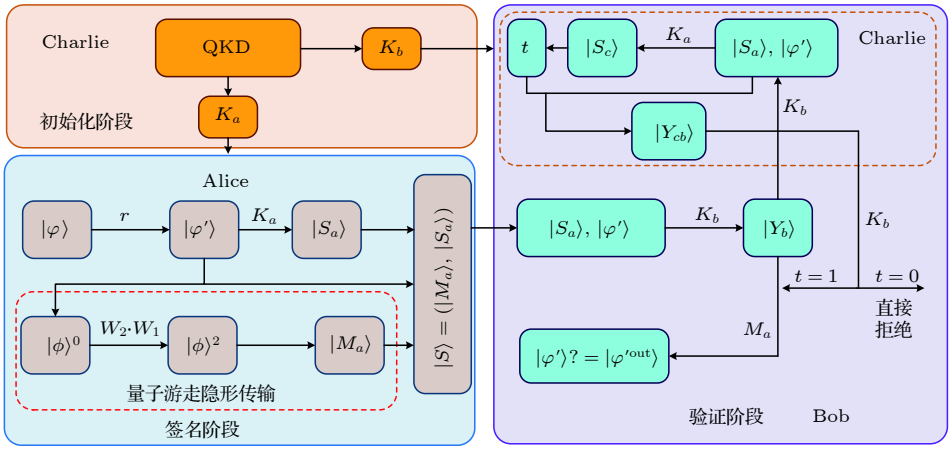

图 3 签名方案原理图 (QKD 代表量子密钥分发)

Fig. 3. Schematic of the suggested arbitrated quantum signature scheme. QKD is short for quantum key distribution.

赖 m 个量子比特的概率 $P_{\text{disavowal}}(m)$, 可以发现随着 n 值变大, 抵赖概率的最大值在变小, 可以推断当 n 非常大时, Alice 抵赖的概率可以非常小或接近 0. 这时假定抵赖概率阈值为 $P_{\text{threshold}}$, 我们规定如果 $P_{\text{disavowal}}(m)$ 小于 $P_{\text{threshold}}$, 认为不存在抵赖行为, 否则认为有抵赖行为存在. 当 n 是确定的, 抵赖概率阈值可以选择为抵赖概率的平均值, 即 $P_{\text{threshold}} = \sum_m P_{\text{disavowal}}(m)/n$.

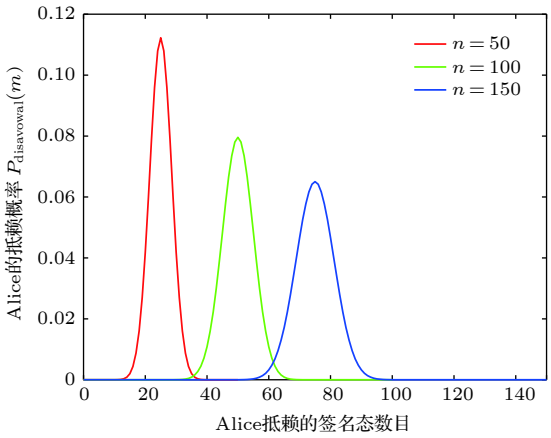

图 4 $n = 50$, 100, 150 三种情况下 Alice 成功抵赖签名的概率 $P_{\text{disavowal}}(m)$

Fig. 4. Alice's disavowal probability $P_{\text{disavowal}}(m)$ as a function of the amount m of the disavowed qubit in the signature state $|S_a\rangle$ for the respective $n = 50$, $n = 100$ and $n = 150$.

4.2 不可伪造性

任何人无法伪造 Alice 的签名量子态 $|S_a\rangle$. 如果 Bob 是一个叛徒, 他想要伪造 $|S_a\rangle$. 假设 Bob 成功伪造了 $|S_a\rangle$, 那他一定知道了生成 $|S_a\rangle$ 的元素 K_a 和 $|\varphi'\rangle$. 然而, 获取这些元素对于 Bob 来说是不可能的. 原因是 K_a 是 Alice 和 Charlie 通过量子密钥分发系统制备和分配的, 它具有无条件安全性, Bob 无法获取 K_a, 则 Bob 也就无法成功伪造正确的 $|S_a\rangle$. 不正确的 $|S_a\rangle$ 在验证阶段将被 Charlie 检测得到 $t = 0$. 因此, 在 Charlie 的辅助验证下, Bob 无法伪造正确的 $|S_a\rangle$.

任何外部的攻击者也一定是不可能成功伪造签名 $|S_a\rangle$ 的. 对于外部攻击者来说, 在本算法中暴露的参数是 $|S\rangle$, $|S_a\rangle$, $|Y_b\rangle$ 和 $|Y_{cb}\rangle$, 它们均通过 KCCC[18] 加密得到, 具有很高的安全性. 前面我们已经分析内部参与者 Bob 是不可能伪造出正确的 $|S_a\rangle$, 且推断外部的攻击者也一定是不可能的, 也就是说, 无条件安全的量子密钥分发以及高安全性的加密算法确保了本方案的安全性. 因此内部参与者和外部潜在的攻击者都不能成功变造 Alice 的签名 $|S_a\rangle$.

4.3 不可否认性

在提出的 AQS 算法中, Bob 无法否认收到 Alice 的签名 $|S_a\rangle$ 以及信息 $|\varphi\rangle$, 即包含 Alice 签名的信息或文件. Charlie 的存在使得 Bob 的否认攻击策略是不可能的, 这种情况和 Alice 不可抵赖的情况是类似的. 即使通过签名方案减少对 Charlie 的依赖, 这个特性仍然是满足的. 在验证阶段的第一步, Bob 传输 $|Y_b\rangle$ 给 Alice 而不是 Charlie. 然后 Alice 实现新的签名 $|S'\rangle$, 即

$$|S'\rangle = (|M_a\rangle, |Y_b\rangle, |\varphi'\rangle, |S_a\rangle), \tag{25}$$

随后将 $|S'\rangle$ 传送给 Charlie. 在验证阶段的第二步 Charlie 制备新的 $|Y_{cb}\rangle$, 即

$$|Y'_{cb}\rangle = E'_{K_b} E_{K_b}(|M_a\rangle, |\varphi'\rangle, |S'\rangle, |t\rangle), \tag{26}$$

这时可以看到 $|S'\rangle$ 包含 Alice 的密钥 K_a 和 Bob 的密钥 K_b. 一旦 Bob 想要否认, Charlie 如果检测到 $|S'\rangle$ 中包含 K_b, 则 Bob 一定接收到了包含 Alice 签名的文件或信息. 因此 Bob 是不可能成功否认接收到的 Alice 的文件或消息.

4.4 讨 论

根据 Gao 等 [13] 对 AQS 算法的密码学分析, 讨论本方案是否可抵抗 Alice 的抵赖攻击以及 Bob 的存在性伪造攻击. 例如在验证阶段的第二步, 在 Charlie 完成判断之后, Charlie 传输 $|Y_{cb}\rangle = E'_{K_b} E_{K_b}(|S_a\rangle, |\varphi'\rangle, t)$ 给 Bob. 此时, Alice 有时机去修改签名态 $|S_a\rangle$ 产生 $|\tilde{S}_a\rangle$, 使得它不再是信息序列 $|\varphi\rangle$ 的有效签名. 由于所使用的 KCCC 算法的特点, 这种修改是无法成功的, Alice 不再像 QOTP 算法中一样可以准确获取签名量子态中量子比特的位置和顺序. 因此, KCCC 算法在 AQS 中的使用可以规避此类攻击.

此外, Bob 也是无法成功实现已知有效的签名信息对下的存在性伪造攻击. 这种攻击是假如 Bob 拥有一个有效的信息签名对 $(|\varphi\rangle, |S_a\rangle)$, 他执行 n 次泡利操作 (I, X, Y, Z) 在 $|\varphi\rangle$ 中的量子比特, 同时相同的操作执行在 $|S_a\rangle$ 的后 n 个量子比特, 得到的新的信息签名对 $(|\varphi''\rangle, |S''_a\rangle)$ 称为是一个成功

的伪造, 其中每一个泡利操作是四个泡利操作I, X, Y, Z之一, Bob 至少可以实现$4^n - 1$种伪造, 他可以选择对自己利益最大化的信息声称是 Alice 签的. 这时 Charlie 总会站在 Bob 这边. 然而由于 KCCC 加密算法的应用, 这种攻击是不可能的. 首先需要明确的是在 Bob 接收 Alice 的签名之前是不可能的, 原因是信息序列是以密文$|\varphi'\rangle$的形式存在, 在完成验证之后, Bob 才可以通过公布的随机数获取原始信息序列$|\varphi\rangle$. 在验证阶段之后, 仍然是不可能的, 因为 Bob 无法准确获取签名态中量子比特的准确位置和顺序, 则 Bob 无法执行等效的操作在有效的信息签名对, 无法成功获取签名$|S_a\rangle$的伪造.

4.5 比 较

基于量子游走隐形传输模型、KCCC 操作、随机数以及公共板的应用, 本文提出了一种目前较好的一种 AQS 方案. 我们将其与已存在的几种典型的 AQS 协议进行比较, 如表 2 所列: 根据所使用的量子资源、信息副本的传输方式、加解密操作、Alice 的抵赖攻击是否成功以及 Bob 的存在性伪造攻击是否成功进行对比. 可以看到信息副本的传输方式分为三种: 基于纠缠态的隐形传输[2,11,14,16], 普通量子加密方式[12] 以及本协议的基于量子游走不需要提前准备纠缠态的隐形传输方式. 对于采用 QOTP 算法或者改进的 QOTP 的 AQS 协议, 均不能抵抗 Alice 的抵赖攻击和 Bob 的存在性伪造攻击, 这个现象在文献 [13] 中已做了分析, 他们展示抵赖或伪造攻击成功的原因是 QOTP 加密的方式是一个比特对应一个比特, 量子比特的位置和顺序在基于 QOTP 的 AQS 协议中是确定的, 攻击者可以找到相应的量子比特位置并执行泡利操作对其修改. 文献 [16] 中提出的采用受控非代替 QOTP, 仍然不能抵抗 Bob 的伪造攻击[18], 幸运的是受控非修改了量子签名中的量子比特使其之间互相关联, 可以有效防止 Alice 的抵赖攻击. 本方案使用 Zhang 等[18] 提出的 KCCC 操作作为中间量子态传输的加解密方法, 使用量子游走隐形传输模型[25,26] 传输信息副本, 本协议具有文献 [18] 的所有优势. 此外, 相比于普通的量子加密方式, 基于量子游走的隐形传输具有如下优势: 第一, 不需要传输载体粒子本身, 传输的是粒子所处的量子状态; 第二, 没有物理限制, 便于扩展传输距离, 量子加密仅限在地区性的网络上, 量子中继器还不存在; 第三, 由于纠缠的存在在传输过程中具有防窃听功能, 即一旦有窃听者想要窃听信息, 测量引起的扰动会被诚实的参与者发现. 相比于普通的量子隐形传输, 基于量子游走的隐形传输不需要提前制备纠缠态, 必要的纠缠态可以在量子游走的第一步自动产生. 此外, 从通信效率来说, 相比于典型的文献 [2] 和文献 [11], 本方案的验证阶段的第一步不需要传输测量基M_b, 所以本方案的通信效率更高, 通信负担更小. 因此, 本 AQS 方案目前来讲是较优的.

表 2 协议比较

Table 2. Protocols comparison.

协议	量子资源	信息副本传输方式	加解密算法	Alice的抵赖攻击是否成功	Bob的存在性伪造攻击是否成功
文献[2]	GHZ态	基于GHZ态的隐形传输	QOTP	是	是
文献[11]	Bell态	基于Bell态的隐形传输	QOTP	是	是
文献[12]	单比特态	量子加密	QOTP	是	是
文献[14]	GHZ态	基于GHZ态的隐形传输	改进的QOTP	是	是
文献[16]	Bell态	基于Bell态的隐形传输	链式受控非	否	是
文献[18]	单比特态	量子加密	KCCC	否	否
本协议	单比特态	量子游走的隐形传输	KCCC	否	否

5 结 论

本文设计了基于环上两个硬币的量子游走的 AQS 算法. 不同于已有的 AQS 协议, 在初始化阶段不需要制备纠缠态, 而是在签名阶段量子游走的第一步产生 Alice 和 Bob 之间的纠缠态. 基于量子游走的量子隐形传输模型, 两步游走之后, Alice 应用测量基$|0\rangle$, $|2\rangle$和$|+\rangle$, $|-\rangle$在自己的量子态, 由于 Alice 和 Bob 之间纠缠的存在, Alice 的测量使得

传输信息塌陷在 Bob 的量子态. Bob 执行相应的泡利操作恢复信息, 进而验证签名的有效性以及信息的完整性和真实性. 由于 KCCC 算法的使用, 本算法满足签名方案的安全性规则. 目前, Xue 等[32]在实验上已成功证实了量子游走可以应用于量子通信, 且量子游走在一维空间已经做到 20 步以上. 所以, 基于当前的技术, 实现本文提出的 AQS 协议是切实可行的.

参考文献

[1] Meijer H, Akl S 1981 *ACM SIGCOMM Comp. Com.* **11** 37
[2] Zeng G, Keitel C H 2002 *Phys. Rev. A* **65** 042312
[3] Nielsen M A, Chuang I, Grover L K 2002 *Am. J. Phys.* **70** 558
[4] Guo Y, Xie C L, Liao Q, Zhao W, Zeng G H, Huang D 2017 *Phys. Rev. A* **96** 022320
[5] Guo Y, Liao Q, Wang Y, Wang Y J, Huang D, Huang P, Zeng G H 2017 *Phys. Rev. A* **95** 032304
[6] Xu G, Chen X B, Dou Z, Yang Y X, Li Z 2015 *Quantum Inf. Process.* **14** 2959
[7] Chen X B, Sun Y R, Xu G, Jia H Y, Qu Z, Yang Y X 2017 *Quantum Inf. Process.* **16** 244
[8] Chen X B, Tang X, Xu G, Dou Z, Chen Y L, Yang Y X 2018 *Quantum Inf. Process.* **17** 225
[9] Curty M, Lütkenhaus N 2008 *Phys. Rev. A* **77** 046301
[10] Zeng G 2008 *Phys. Rev. A* **78** 016301
[11] Li Q, Chan W H, Long D Y 2009 *Phys. Rev. A* **79** 054307
[12] Zou X, Qiu D 2010 *Phys. Rev. A* **82** 042325
[13] Gao F, Qin S J, Guo F Z, Wen Q Y 2011 *Phys. Rev. A* **84** 022344
[14] Choi J W, Chang K Y, Hong D 2011 *Phys. Rev. A* **84** 062330
[15] Zhang J, Wu J Y 2013 *J. Beijing Univ. Posts Telecommun.* **36** 113 (in Chinese) [张骏, 吴吉义 2013 北京邮电大学学报 **36** 113]
[16] Li F G, Shi J H 2015 *Quantum Inf. Process.* **14** 2171
[17] Yang Y G, Lei H, Liu Z C, Zhou Y H, Shi W M 2016 *Quantum Inf. Process.* **15** 2487
[18] Zhang L, Sun H W, Zhang K J, Jia H Y 2017 *Quantum Inf. Process.* **16** 70
[19] Zhang Y, Zeng J 2018 *Int. J. Theor. Phys.* **57** 994
[20] Guo Y, Feng Y Y, Huang D Z, Shi J J 2016 *Int. J. Theor. Phys.* **55** 2290
[21] Feng Y Y, Shi R H, Guo Y 2018 *Chin. Phys. B* **27** 020302
[22] Aharonov Y, Davidovich L, Zagury N 1993 *Phys. Rev. A* **48** 1687
[23] Venegas-Andraca S E 2012 *Quantum Inf. Process.* **11** 1015
[24] Kempe J 2003 *Contemp. Phys.* **44** 307
[25] Wang Y, Shang Y, Xue P 2017 *Quantum Inf. Process.* **16** 221
[26] Shang Y, Wang Y, Li M, Lu R Q 2019 *EPL- Europhys. Lett.* **124** 60009
[27] Chen X B, Wang Y L, Xu G, Yang Y X 2019 *IEEE Access* **7** 13634
[28] Zou X, Dong Y, Guo G 2006 *New J. Phys.* **8** 81
[29] Bian Z H, Li J, Zhan X, Twamley J, Xue P 2017 *Phys. Rev. A* **95** 052338
[30] Tang H, Lin X F, Feng Z, Chen J Y, Gao J, Sun K, Wang C Y, Lai P C, Xu X Y, Wang Y, Qiao L F, Yang A L, Jin X M 2018 *Sci. Adv.* **4** eaat3174
[31] Aharonov D, Ambainis A, Kempe J, Vazirani U 2001 *Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing* New York, USA, 2001 p50
[32] Xue P, Zhang R, Qin H, Zhan X, Bian Z H, Li J, Sanders Barry C 2015 *Phys. Rev. Lett.* **114** 140502

Arbitrated quantum signature scheme based on quantum walks*

Feng Yan-Yan Shi Rong-Hua Shi Jin-Jing † Guo Ying

(*School of Computer Science and Engineering, Central South University, Changsha* 410083, *China*)

(Received 27 February 2019; revised manuscript received 15 April 2019)

Abstract

Quantum signature is quantum counterpart of classical digital signature, which has been widely applied to modern communication, such as electronic payment, electronic voting and electronic medical, owing to its great implication in ensuring the authenticity and the integrity of the message and the non-repudiation. Arbitrated quantum signature (AQS) is an important and practical type of quantum signature. The AQS algorithm is a symmetric key cryptography-based quantum signature algorithm, and its implementation requires the trusted arbitrator to be directly involved. In this paper, employing the key-controlled chained CNOT (KCCC) operation as the appropriate encryption (decryption) algorithm, we suggest an AQS scheme based on teleportation of quantum walks with two coins on a four-vertex cycle, which is used to transfer the message copy from the sender to the receiver. In light of the model of teleportation of quantum walks, the sender encodes the message to be signed into her or his coin state, and the necessary entangled states can be created as a result of the conditional shift between the coin state and the position state. The measurements performed on the generated entangled states are the bases of signature production and message recovery. Then according to the classical measurement results from the sender, the receiver performs the appropriate local unitary operations (i.e., Pauli operations) on his own coin state to recover the original message and further verifies the validity of the completed signature by using the appropriate verification algorithms under the aid of the trustworthy arbitrator.

The suggested AQS scheme makes the following contributions: 1) the necessary entangled states for quantum teleportation of message copy do not need preparing in advance, and they can be produced automatically by the first step of quantum walks; 2) the scheme satisfies the features of non-repudiation, unforgeability and non-disavowal due to the use of the KCCC operation; 3) the scheme may be achieved by linear optical elements such as beam splitters, wave plates, etc., because quantum walks have proven to be realizable in different physical systems and experiments.

Analysis and discussion show that the proposed AQS scheme possesses the impossibility of disavowals by the signer and the receiver and impossibility of forgeries by anyone. Comparisons reveal that the designed AQS protocol is favorable. Furthermore, it provides an idea by employing the quantum computing model into quantum communication protocols with a possible improvement with respect to its favorable properties, for example, the automatic generation of entangled states via the first step of quantum walks on different models. In the near future, we will further investigate the production of entanglement by quantum walks and its applications with some improvements in designing the quantum communication protocols.

Keywords: quantum cryptography, arbitrated quantum signature, quantum walk-based teleportation, key-controlled chained CNOT operation

PACS: 03.67.Dd, 03.67.–a, 03.65.Ud, 03.65.Aa **DOI:** 10.7498/aps.68.20190274

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61871407, 61572529, 61872390), the Fundamental Research Funds for the Central Universities of Central South University, China (Grant No. 2018zzts179), and the Natural Science Foundation of Hunan Province, China (Grant No. 2017JJ3415).

† Corresponding author. E-mail: shijinjing@csu.edu.cn