基于正则图上量子游走的仲裁量子签名方案

施荣华 冯艳艳* 石金晶
(中南大学计算机学院 长沙 410083)

摘 要：量子游走已经被提出可以用于瞬时地传输量子比特或多维量子态。根据量子游走的隐形传输模型，该文提出一种无需提前准备纠缠源的基于正则图上量子游走的仲裁量子签名算法。在初始化阶段，密钥是由量子密钥分发系统制备；在签名阶段，基于正则图上的量子游走隐形传输模型被用于转移信息副本密文从发送者到接收者。具体地，发送者编码要签名信息的密文在硬币态上，通过两步正则图上的量子游走，可以自动地产生用于量子隐形传输必须的纠缠态。发送者和接收者对制备的纠缠态的测量为签名生成和签名验证的凭据。在验证阶段，在仲裁的辅助下，验证者依照发送者的经典结果核实签名的有效性。此外，随机数和认证的公共板被引进阻止接收方在接收真正信息序列之前的存在性伪造攻击和否认攻击。安全性分析表明设计的算法满足签名者和接收者的不可抵赖以及任何人的不可伪造。讨论表明方案不能抗击发送者的抵赖攻击，相应的建议被给出。由于实验上已经证明量子游走可以在多个不同的物理系统上实现，因此该签名方案未来是可实现的。

关键词：量子密码；仲裁量子签名；量子游走；量子隐形传输
中图分类号：TN918.2 **文献标识码**：A **文章编号**：1009-5896(2020)01-0089-09
DOI: 10.11999/JEIT190597

Arbitrated Quantum Signature Scheme with Quantum Walks on Regular Graphs

SHI Ronghua FENG Yanyan SHI Jinjing
(*School of Computer Science and Engineering, Central South University, Changsha* 410083, *China*)

Abstract: Quantum walks are raised for teleporting qubit or qudit. Based on quantum walk teleportation, an arbitrated quantum signature scheme with quantum walks on regular graphs is suggested, in which the entanglement source does not need preparing ahead. In the initial phase, the secret keys are generated via quantum key distribution system. In the signing phase, the signature for the transmitted message is created by the signer. Teleportation of quantum walks on regular graphs is applied to teleporting encrypted message copy from the signer to the verifier. Concretely, the sender encodes the ciphertext of message copy on coin state. Then two-step quantum walks are performed on the initial system state engendering the necessary entangled state for quantum teleportation, which can be the basis of signature generation and verification. In the verifying phase, the verifier verifies the validity of the completed signature under the aid of an arbitrator. Additionally, the applications of random number and public board deter the verifier's existential forgery and repudiation attacks before the verifier accepts the true message. Analyses show that the suggested arbitrated quantum signature algorithm satisfies the general two requirements, i.e., impossibility of disavowal from the signer and the verifier and impossibility of forgery from anyone. The discussions demonstrate that the scheme may not prevent disavowal attack from the signer and that the corresponding improvements are presented. The scheme may be realizable because quantum walks have experimentally proven to be implementable in different physical systems.

Key words: Quantum cryptography; Arbitrated quantum signature; Quantum walk; Quantum teleportation

收稿日期：2019-08-07；改回日期：2019-10-29；网络出版：2019-11-13
*通信作者： 冯艳艳 fengyanyanhenu@163.com
基金项目：国家自然科学基金(61871407, 61872390, 61972418)，中南大学中央高校基本科研业务费专项基金(2018zzts179)
Foundation Items: The National Natural Science Foundation of China (61871407, 61872390, 61972418), The Fundamental Research Funds for the Central Universities of Central South University (2018zzts179)

1 引言

签名是一种允许签名后的信息从一方传送给另一方，同时信息及相应的签名被确保不可抵赖或篡改，且不可伪造的一种密码通信协议。量子签名是经典签名在量子领域的推广。目前，经典签名已经遍及多种不同的领域，比如，电子商务、电子医疗以及电子支付。然而，由于大多数经典签名方案的安全性依赖于难解的数学难题，比如，大整数因式分解和离散对数。随着未来量子计算机[1]的产生，以及运行在量子计算机上的量子算法[2,3]的提出，这些基于计算复杂度的经典签名方案将不再是安全的。而此时依赖于物理特性的量子密码签名算法依然是信息安全的，且量子保密通信技术[4,5]在理论和实验上也在不断发展，量子签名是量子保密通信协议中一个非常有意义的研究方向。与经典签名类似，量子签名同样区分为真实量子签名和仲裁量子签名(Arbitrated Quantum Signature, AQS)。从实用的角度，有可信任第三方的参与AQS方案更加实用[6,7]，且Barnum等人[8]指出不存在绝对安全的两方量子签名协议。因此本文研究AQS算法。

2002年，Zeng和Keitel[7]初次建议了基于GHZ (Greenberger–Horne–Zeilinger)态的AQS算法，他们给出了AQS方案设计的基本框架。随后，大量AQS方案被研究。2009年，Li等人[9]使用Bell态设计了AQS方案，且其方案传输效率更高且容易实现。2010年，Zou和Qiu[10]指出已存在的AQS方案无法抵抗来自验证者的抵赖，于是建议了可以抵抗来自接收者抵赖攻击的不需要纠缠态的AQS算法。此后，除了提出新颖的AQS方案，AQS方案的密码分析也引起了研究者们的关注。2011年，Gao等人[11]声称量子一次一密并不适用于AQS方案，其将导致Bob通过执行泡利操作的存在性伪造攻击行为。同时期Choi等人[12]以基于GHZ态的AQS方案作为例子提出了一类抵抗存在性伪造攻击的方法。2013年，张骏和吴吉义[13]也提议了一个可以抗击验证者已知明文攻击的AQS算法。2015年，Li和Shi[14]设计了应用受控非加密操作的AQS方案。2016年，Yang等人[15]建议了一种效率可以达到1的基于簇态的AQS算法。2017年，Zhang等人[16]设计了基于键控链式受控非加密操作的AQS方案，用于抵抗量子一次一密加密操作所遭受的潜在威胁。2018年，Zhang和Zeng[17]提议了一个改进的基于Bell态的AQS算法。上面提到的这些方案都是在离散场景下设计的AQS协议。在连续变量场景，文献[18]和文献[19]分别设计了基于相干态和压缩真空态的AQS方案。最近，基于双模压缩真空态的AQS算法[20]也被提出，其中连续变量的量子密集编码技术被应用。

从信息副本由发送者到接收者转移方式的角度，以上的方案共包含两种方式：(1)基于纠缠态的量子隐形传输方式，比如GHZ态[7,12]、Bell态[8,17]，连续Einstein-Podolsky-Rosen (EPR)对[18–20]；(2)量子加密方式，比如，量子一次一密[10]，受控非加密[14]，键控链式受控非加密[16]。相比于第2种量子加密的传输方式，基于纠缠的量子隐形传输[21,22]方式具有以下特点：(1)不需要传输粒子本身，传输的是粒子所处的状态；(2)一种瞬时传输，传输时间取决于经典通信的时间；(3)传输距离不受物理限制更容易实现远距离的量子通讯；(4)由于纠缠的存在，具有反窃听功能。本文将应用量子游走的隐形传输模型，呈现一种新颖的AQS算法。

量子游走是经典游走在量子领域的对应物。1993年，Aharonov等人[23]首次提议了量子游走的概念，他们指出由于量子干涉效应，量子游走中的可实现的平均路径长度比经典随机游走允许的最大路径长度要长。依据时间演化，量子游走被分为离散时间量子游走[24]和连续时间量子游走[25]。之后，基于不同模型的量子游走形式已经被证明广泛应用在量子信息处理任务中，如空间搜索问题[26]、元素甄别问题[27]、图形同构[28]等问题。且1维量子游走成功在核磁共振[29]、离子肼[30]以及光学体系[31]等不同物理系统上被实现。近期，Shang和Wang等人[32,33]讨论了基于量子游走的不同模型可以成功应用在量子隐形传输和量子态转移，强调以下两点：(1)用于隐形传输的纠缠态不必提前制备，它们可以由量子游走一步之后自动产生，就纠缠态制备困难而言，这是一种较大的创新；(2)当传输d维量子态，基于量子游走的隐形传输具有更高的效率。因此，研究量子游走在量子通信协议中的应用是有意义的。

本文将应用基于量子游走的隐形传输到AQS方案中用于传输信息副本，设计一种新颖的基于量子游走的AQS方案。建议的方案具有如下优势：第一，基于量子游走的隐形传输无需提前制备纠缠态，它们可以在量子游走的一步之后生成；第二，应用基于d正则图的量子游走隐形传输转移d维量子态，具有$n+d$个元素的两个投影测量替代之前的d^2个元素的联合测量被应用，更容易实现；第三，随机数r和认证的公共板被雇用，可以抗击接收者接收信息序列之前的存在性伪造攻击和否认攻击。

本文的结构如下：第2节，描述图上的量子游走；第3节，呈现基于正则图上量子游走的AQS算法；第4节对提出的AQS算法给出安全性分析及讨论；第5节为结论。

2　图上的量子游走

2001年，Aharonov等人[34]首次给出了图上基于硬币的量子游走的定义。考虑图$G=(V,E)$, V和E分别代表图G的顶点集和边集。对于d正则图模型，其每一个顶点均有d个邻接点，则希尔伯特(Hilbert)空间可直接用位置空间和硬币空间的直积表示，即

$$\mathcal{H}=\mathcal{H}_p\otimes\mathcal{H}_c \tag{1}$$

其中，$\mathcal{H}_p$是由顶点态$|v\rangle$构成的Hilbert位置空间，$v\in V$，$\mathcal{H}_c$是由边态$|c\rangle$构成的Hilbert空间，$c\in\{0,1,\cdots,d-1\}$, $|c\rangle$用于指示有向边。作用于$\mathcal{H}_p$和$\mathcal{H}_c$上条件转换操作为

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

其中，$j,k\in V$, $k=(j+c)\bmod n$，标签c控制游走者从顶点j游走至k, n为d正则图中的顶点数目且$n\geq 2d-1$。

此外，上面的游走过程可以推广到多个硬币的情形。基于多个硬币的量子游走的定义由Brun等人[35]给出。假设共有M个硬币，作用在第m个硬币对应的幺正变换为

$$W_m=\left(\sum_{j=0}^{n-1}|(j+c)\ \bmod\ n\rangle\langle j|\otimes|c\rangle_m\langle c|\right)(I\otimes C_m) \tag{3}$$

其中，C_m为作用在第m个硬币上的硬币算符。则图上的多个硬币的量子游走线路原理图如图1所示。

图1中，第1行代表游走者的位置为目标态，其余行代表硬币态为控制态。C_i代表作用在第i个硬币的硬币算符，W_i为翻转第i个硬币的幺正变换算符，$i=1,2,\cdots,M$, $O=\sum_{j=0}^{d-1}|(j+c)\ \bmod\ n\rangle\langle j|$代表作用在位置态上的转换操作，$j$为游走者的顶点或位置，$c$为属于硬币空间的控制态。

3　基于d正则图上量子游走的AQS算法

AQS算法需要3个参与者和3个阶段，Alice为信息的签名者和发送者，Bob是签名的验证者和接收者，Charlie为值得Alice和Bob信任的第三方仲裁，他们共同参与并完成初始化、签名和验证3个阶段。一个安全的量子签名需要满足签名者和验证者抵赖的不可能性以及任何人伪造的不可能性[7,10]。

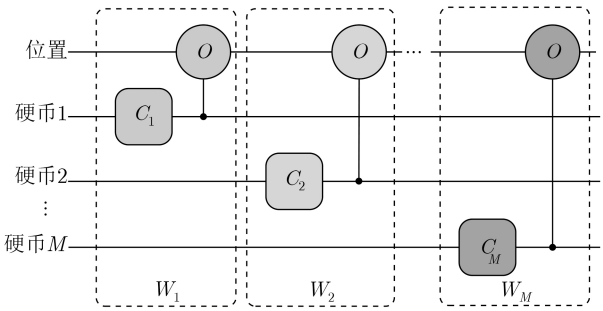

图 1 基于多个硬币的量子游走线路原理图

3.1　初始化阶段

(1) 密钥的制备和分发：Alice和Charlie制备并分配共享密钥序列$K_{\rm ac}$, Bob和Charlie制备并分配共享密钥序列$K_{\rm bc}$, $K_{\rm ac}$和$K_{\rm bc}$表示为

$$K_{\rm ac}=\{K_{\rm ac}^1,K_{\rm ac}^2,\cdots,K_{\rm ac}^i,\cdots,K_{\rm ac}^{2n}\} \tag{4}$$

$$K_{\rm bc}=\{K_{\rm bc}^1,K_{\rm bc}^2,\cdots,K_{\rm bc}^i,\cdots,K_{\rm bc}^{2n}\} \tag{5}$$

这一过程通过量子密钥分发系统完成，且已被证明是无条件安全的[4,5]。

(2) 系统配置：Alice或Bob向Charlie发出需要通信的申请。

3.2　签名阶段

(1) Alice制备含有n个d维量子态的信息序列$|\varphi\rangle$，它携带即将签名的信息，$|\varphi\rangle$可以写为

$$|\varphi\rangle=\{|\varphi_1\rangle,|\varphi_2\rangle,\cdots,|\varphi_i\rangle,\cdots,|\varphi_n\rangle\} \tag{6}$$

其中，$|\varphi_i\rangle(i=1,2,\cdots,n)$为一个$d$维量子态，写为

$$|\varphi_i\rangle=\sum_{k=0}^{d-1}a_k^i|k\rangle \tag{7}$$

其中a_k^i为复数满足$\sum_{k=0}^{d-1}|a_k^i|^2=1$。

(2) Alice随机选择一个数$r\in\{0,1,\cdots,d-1\}^{2n}$，然后编码$|\varphi\rangle$为秘密的信息序列$|\varphi'\rangle$，即

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

其中$|\varphi_i'\rangle=\sum_{k=0}^{d-1}a_k^{i'}|k\rangle$。

(3) Alice用密钥$K_{\rm ac}$加密$|\varphi'\rangle$生成$|S_a\rangle$，即

$$|S_a\rangle=E_{K_{\rm ac}}(|\varphi'\rangle) \tag{9}$$

(4) 应用第2节介绍的d正则图上量子游走模型。假设Alice占有两个粒子A1和A2, Bob有1个粒子B。A2代表游走者的位置态，A1和B均代表硬币态。Alice将每一个秘密量子态$|\varphi_i'\rangle$编码在A1上，A2和B的初始态均假设是$|0\rangle$，如图2所示，则量子游走系统的整个初始态为

$$|\psi\rangle^0=|0\rangle_{\rm A2}\otimes\left(\sum_{k=0}^{d-1}a'_k|k\rangle\right)_{\rm A1}\otimes|0\rangle_{\rm B} \tag{10}$$

在下文中系统态的表述均按照A2, A1和B的顺序，下标将被省略。应用两步量子游走，$|\varphi_i'\rangle$可以被成功传输到Bob。第1步量子游走W_1为

$$W_1=E_1\cdot(I_p\otimes C_1\otimes I_2) \tag{11}$$

其中

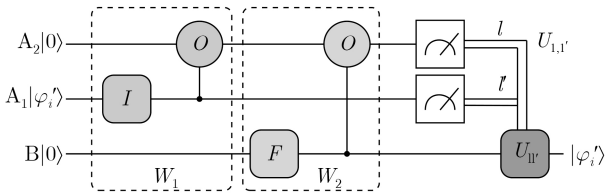

图 2 基于两个硬币量子游走的隐形传输线路原理图

$$E_1=\sum_{c=0}^{d-1}\sum_{k=0}^{n-1}|(k+c)\bmod n\rangle\langle k|\otimes|c\rangle_1\langle c|\otimes I_2 \tag{12}$$

选择$C_1=I$，得到一步量子游走W_1之后的量子态为

$$|\psi\rangle^1=\sum_{k=0}^{d-1}a'_k|k\rangle|k\rangle|0\rangle \tag{13}$$

粒子A2和A1之间的条件移操作使得它们之间有了纠缠。然后第2步量子游走W_2为

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

其中

$$E_2=\sum_{c=0}^{d-1}\sum_{k=0}^{n-1}|(k+c)\bmod n\rangle\langle k|\otimes I_1\otimes|c\rangle_2\langle c| \tag{15}$$

选择$C_2=F$，得到第2步量子游走W_2之后的量子态为

$$|\psi\rangle^2=\sum_{k=0}^{d-1}\sum_{j=0}^{d-1}a'_k|k+j\rangle|k\rangle|j\rangle\Big/\sqrt{d} \tag{16}$$

其中$F|0\rangle=\sum_{j=0}^{d-1}|j\rangle\Big/\sqrt{d}$，粒子A2和B之间的条件移操作使得它们之间有了纠缠，因此条件移操作引进了量子隐形传输必须的纠缠资源。

(5) Alice使用测量基$|l\rangle\in\{|j\rangle\pm|d+j\rangle/\sqrt{2},|d-1\rangle,\cdots,|n-1\rangle\}$测量A2，规定经典输出结果$j$，$j+d$ 和$d-1$ 分别对应态$(|j\rangle+|j+d\rangle)/\sqrt{2}$，$(|j\rangle-|j+d\rangle)/\sqrt{2}$和$|d-1\rangle$。当A2的测量输出结果为$j$，A1和B之间的态变换为

$$\sum_{k=0}^{j}a'_k|k\rangle\otimes|j-k\rangle+\sum_{k=j+1}^{d-1}a'_k|k\rangle\otimes|j+d-k\rangle \tag{17}$$

Alice使用测量基$|l'\rangle(l=0,1,\cdots,d-1)$测量粒子A1，$|l'\rangle$可描述为

$$|l'\rangle=\sum_{k=0}^{d-1}\mathrm{e}^{2\pi ilk/d}|k\rangle/\sqrt{d} \tag{18}$$

此时使用傅里叶变换的形式重写式(17)中A1的态为

$$\sum_{t'=0}^{d-1}\left(\sum_{k=0}^{j}a'_k\mathrm{e}^{-2\pi it'k/d}|t'\rangle\otimes|j-k\rangle+\sum_{k=j+1}^{d-1}a'_k\mathrm{e}^{-2\pi it'k/d}|t'\rangle\otimes|j+d-k\rangle\right) \tag{19}$$

当A1的测量结果为t', B的态变换为

$$\sum_{k=0}^{j}a'_k\mathrm{e}^{-2\pi it'k/d}|j-k\rangle+\sum_{k=j+1}^{d-1}a'_k\mathrm{e}^{-2\pi it'k/d}|j+d-k\rangle \tag{20}$$

因此，Alice的测量基可表述为

$$|M_a\rangle=\{|M_a^1\rangle,|M_a^2\rangle,\cdots,|M_a^i\rangle,\cdots,|M_a^n\rangle\} \tag{21}$$

其中$|M_a^i\rangle$包含两个部分，一个是作用在A2上的测量基$|l\rangle$，另一个是作用在A1上的测量基$|l'\rangle$。

(6) Alice发送$|S\rangle=\{|\varphi'\rangle,|S_a\rangle,|M_a\rangle\}$给Bob。

3.3 验证阶段

(1) Bob使用密钥K_{bc}加密$|\varphi'\rangle$和$|S_a\rangle$生成$|Y_b\rangle$

$$|Y_b\rangle=E_{K_{\mathrm{bc}}}(|\varphi'\rangle,|S_a\rangle) \tag{22}$$

并将其传送给Charlie。

(2) Charlie使用K_{bc}解密$|Y_b\rangle$得到$|\varphi'\rangle$和$|S_a\rangle$。接着Charlie使用K_{ac}加密$|\varphi'\rangle$获得$|S_c\rangle$。为此，Charlie使用参数K_{ac}, $|\varphi'\rangle$和$|S_a\rangle$构造验证参数χ来判断$|S_a\rangle$和$|S_c\rangle$的连续性，χ可定义为

$$\chi=\begin{cases}1, & |S_a\rangle=|S_c\rangle=E_{K_{\mathrm{ac}}}|\varphi'\rangle\\ 0, & |S_a\rangle\neq|S_c\rangle=E_{K_{\mathrm{ac}}}|\varphi'\rangle\end{cases} \tag{23}$$

其中$|S_a\rangle$和$|S_c\rangle$分别源自$|Y_b\rangle$和$|\varphi'\rangle$。当$d=2$, $|S_a\rangle$和$|S_c\rangle$连续性的判定可以采用两个未知量子态比较的技术[36]来完成，这个比较过程可以用公式描述为$(H\otimes I)(\mathrm{CSWAP})(H\otimes I)|0\rangle|S_a\rangle|S_c\rangle$，其中$H$为Hadamard门，即$H|a\rangle=\frac{1}{\sqrt{2}}(|0\rangle+(-1)^a|1\rangle)$, $a\in\{0,1\}$, I为单位算符，CSWAP为控制SWAP门，第1个量子比特为控制比特，其线路图表示如图3所示，其中第1个量子比特为辅助量子比特，追踪线路的执行，得到测量之前的终态为$\frac{1}{2}|0\rangle(|S_a\rangle|S_c\rangle+|S_c\rangle|S_a\rangle)+\frac{1}{2}|1\rangle(|S_a\rangle|S_c\rangle-|S_c\rangle|S_a\rangle)$，应用投影测量算符测量第1个量子比特为1的概率为$\frac{1}{2}-\frac{1}{2}(\langle S_a|S_c\rangle)^2$。若$|S_a\rangle=|S_c\rangle$，即$\langle S_a|S_c\rangle=1$，这个概率为0；若$\langle S_a|S_c\rangle=\delta$，这个概率至少为$\frac{1}{2}(1-\delta^2)>0$。因此测量结果为1的单边错误概率为$\frac{1}{2}(1+\delta^2)$。

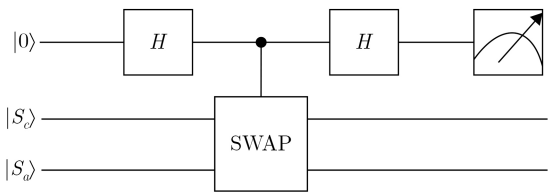

图 3 比较两个未知量子态的线路原理图

(3) Charlie使用$K_{\rm ac}$从$|S_a\rangle$或$|S_c\rangle$获取$|\varphi'\rangle$，接着用$K_{\rm bc}$加密$|\varphi'\rangle, |S_a\rangle$和$\chi$得到$|Y_{\rm cb}\rangle$

$$|Y_{\rm cb}\rangle = E_{K_{\rm bc}}(|\varphi'\rangle, |S_a\rangle, \chi) \tag{24}$$

然后，Charlie传送$|Y_{\rm cb}\rangle$给Bob。

(4) Bob从$|Y_{\rm cb}\rangle$获取$|\varphi'\rangle, |S_a\rangle$和$\chi$。如果$\chi=0$，则认为签名是无效的或签名已经被篡改，此时Bob直接拒绝这个签名，并结束此次通信。如果$\chi=1$，则说明量子态$|S_a\rangle$是正确的，为了验证签名的有效性，Bob需要完成进一步的验证。

(5) 依照接收到的经典输出结果M_a，Bob执行局域幺正操作U在粒子B(式(20))来恢复$\sum_{k=0}^{d-1} a_k^{i'}|k\rangle$。如果A2和A1的测量输出结果为$j$和$t'$, Bob执行的恢复操作为

$$\begin{aligned} U_{jt'} = &\sum_{k=0}^{j} {\rm e}^{2\pi i t'k/d}|k\rangle\langle j-k| \\ &+ \sum_{k=j+1}^{d-1} {\rm e}^{2\pi i t'k/d}|k\rangle\langle j+d-k| \end{aligned} \tag{25}$$

如果A2和A1的测量结果为$d+j$和t'，Bob执行的恢复操作为

$$\begin{aligned} U_{(d+j),t'} = &\sum_{k=0}^{j} {\rm e}^{2\pi i t'k/d}|k\rangle\langle j-k| \\ &- \sum_{k=j+1}^{d-1} {\rm e}^{2\pi i t'k/d}|k\rangle\langle j+d-k| \end{aligned} \tag{26}$$

如果A2和A1的测量结果为$d-1$和t', Bob执行的恢复操作为

$$U_{(d-1),t'} = \sum_{k=0}^{d-1} {\rm e}^{2\pi i t'k/d}|k\rangle\langle d-1-k| \tag{27}$$

因此，Bob的测量基可描述为

$$|M_b\rangle = \{|M_b^1\rangle, |M_b^2\rangle, \cdots, |M_b^i\rangle, |M_b^n\rangle\} \tag{28}$$

其中$|M_b^i\rangle$是$U_{jt'}$，$U_{(d+j),t'}$和$U_{(d-1),t'}$中的一个。Bob将恢复得到的态$|\varphi'_{\rm out}\rangle$与接收到的$|\varphi'\rangle$进行比较。如果$|\varphi'_{\rm out}\rangle \neq |\varphi'\rangle$, Bob拒绝Alice的签名并放弃此次通信；否则Bob请求Alice通过公共板公布r。这表明所有n个d维量子态都是连续的。

(6) Alice通过公共板宣告参数r。

(7) Bob使用r解密$|\varphi'\rangle$或$|\varphi'_{\rm out}\rangle$得到信息序列$|\varphi\rangle$，并确认$(|S_a\rangle, r)$为Alice对$|\varphi\rangle$执行的签名。

本AQS算法的原理图如图4所示。图4中，E和D分别代表加密和解密算法，QKD(Quantum Key Distribution)表示量子密钥分发。

4　安全性分析

一种安全的量子签名算法应该满足两个条件[7,10]：

第一，不可抵赖：签名者不能成功抵赖已经完成的签名及签过的信息，接收者不能成功抵赖接收的来自签名者的签名及签过的信息；

第二，不可伪造：没有人有能力成功伪造签名者的签名。

在分析方案的安全性之前，首先分析Charlie在本AQS算法中3个阶段的作用。在初始化阶段，Charlie分别和Alice, Bob制备了共享密钥$K_{\rm ac}$和$K_{\rm bc}$。在验证阶段，Charlie创建了验证参数χ。如果$\chi=0$, Bob认为Alice的签名已经被篡改且不需要继续下面的验证过程。因此Charlie必须是可信任的第三方。

4.1　签名者抵赖的不可能性

根据式(9)可知，构成签名的$|S_a\rangle$是Alice使用密钥$K_{\rm ac}$加密$|\varphi'\rangle$得到。如果Alice抵赖了她完成的签名并因此与Bob产生了纠纷，这时需要Charlie判断$|S_a\rangle$中是否包含Alice签名必需的$K_{\rm ac}$。如果Charlie

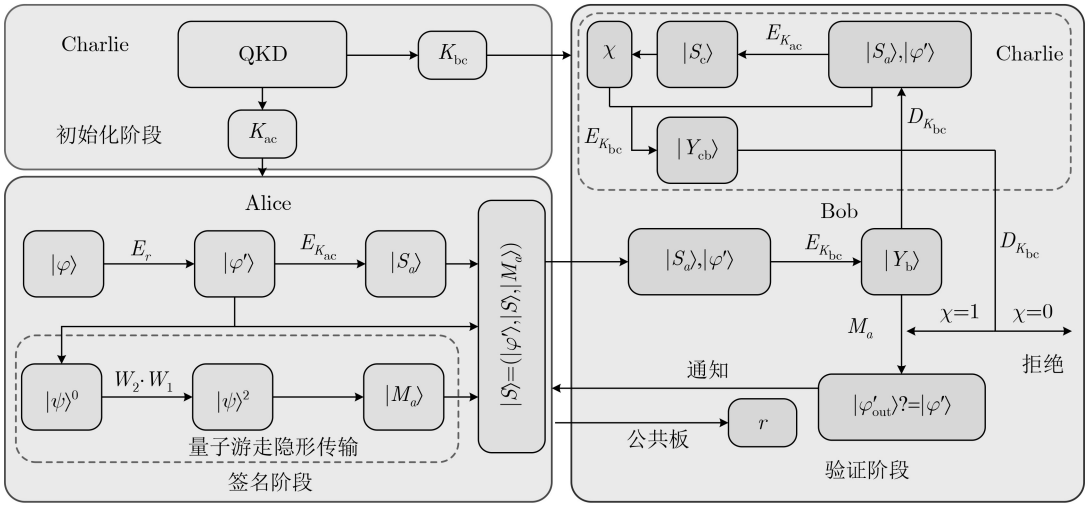

图 4 基于d正则图量子游走的AQS算法的原理图

判定$|S_a\rangle$中含有$K_{\rm ac}$，则签名肯定是Alice完成的。因此，面对可信任的Charlie, Alice无法成功地否认曾完成的签名或签名的信息。

而且，Alice抵赖签名的概率可以被量化。面对曾完成的签名，Alice分别有1/2的概率抵赖或否认它，这一事件满足二项式分布。假设在含有n个d维量子态的$|S_a\rangle$中有m个d维量子态被Alice抵赖，则Alice成功抵赖$|S_a\rangle$的概率为

$$\Pr_{\rm dis}=\left(\begin{array}{c}n\\m\end{array}\right)\left(\frac{1}{2}\right)^m\left(\frac{1}{2}\right)^{n-m} \tag{29}$$

其中，$\left(\begin{array}{c}n\\m\end{array}\right)$为二项式系数，可描述为

$$\left(\begin{array}{c}n\\m\end{array}\right)=\frac{n!}{m!(n-m)!} \tag{30}$$

在$n=50$, $n=100$和$n=150$3种不同情况下，$\Pr_{\rm dis}$作为m的函数的曲线变化，如图5所示。可以看到对于不同的n, Alice的抵赖概率$\Pr_{\rm dis}$均有一个最大值。随着n值的增加，这个最大值会减小。因而我们可以推断当n值足够大，最大的抵赖概率可以是非常小。设置Alice抵赖签名的概率阈值为$\Pr_{\rm dis}$，规定如果$\Pr_{\rm dis}<\Pr_{\rm th}$，则认为不存在抵赖，否认存在抵赖行为。值得注意的是，当n为确定值，Alice的抵赖概率阈值可以选择为抵赖概率的平均值，即$\Pr_{\rm th}=\sum\Pr_{\rm dis}/n$。

4.2 任何人否认的不可能性

为了自己的利益，Bob或外部攻击者Eve也许想试图假造Alice的签名。

假如有敌意的Bob想要伪造Alice的签名$|S_a\rangle=E_{K_{\rm ac}}(|\varphi'\rangle)$，他必须知道密钥$K_{\rm ac}$。然而，一方面从所有公开的参数$|S\rangle$, $|Y_b\rangle$和$|Y_{\rm cb}\rangle$, Bob无法获取$K_{\rm ac}$的信息；另一方面，$K_{\rm ac}$是由已被证实具有无条件安全性的量子密钥分配系统制备生成。因此，没有正确的$K_{\rm ac}$Bob无法成功伪造$|S_a\rangle$。实际上，如果Bob成功伪造了$|S_a\rangle$，他就可以修改原始的$|S_a\rangle$并对自己有益的信息创造新的签名。幸而，这种攻击

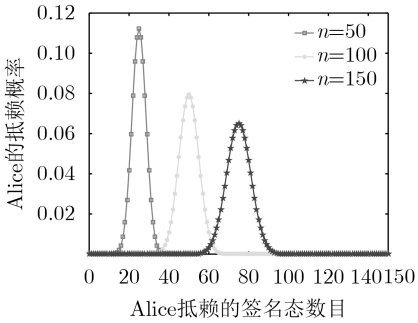

图 5 n分别取50, 100, 150 3种情况下Alice成功抵赖签名的概率$\Pr_{\rm dis}$

策略仍然可以在验证阶段被发生，Charlie将得到$\chi=0$。因此，同样面对可信任的Charlie, Bob无法成功地伪造Alice的签名。

此外，Eve也许想臆造Alice的签名。一般来说，内部参与者比外部攻击者可以获取更多的信息，上面已经分析Bob是无法成功伪造Alice的签名，可以推断Eve更不可能成功伪造Alice的签名。具体来说，量子密钥分配技术以及量子密码算法的应用保证了方案的理论安全性，且无论是量子一次一密、受控非或键控链式受控非加密算法在量子密码学不仅容易实现且具有高度的安全性。因此，Eve对Alice签名的伪造也是不可能的。

在最坏的情况下，假设Eve获得了密钥$K_{\rm ac}$和$K_{\rm bc}$，伪造仍然是不可能的，原因是Alice的完整签名包含$|S_a\rangle$和r，只有在Bob验证了信息序列的连续性成功之后，Alice才会公布参数r，而如果信息序列是连续的，那么经典测量结果M_a也一定被Eve获取。然而M_a是通过经典认证信道传输的，Eve无法获取正确的M_a，因此Eve无法知道r，也就无法获取完整且正确的签名。也就是说纠缠的存在阻止了Eve的伪造攻击。但是如果Bob得到了$K_{\rm ac}$，这种伪造也许无法避免，但是这种概率非常的小，文中假设n足够大且高维度。

4.3 接收者否认的不可能性

从一个签名方案实用性的角度，接收者Bob不能否认曾接收过Alice的签名或签名的信息。首先，与签名者Alice不能成功抵赖已完成的签名类似，在可信任的Charlie面前，Bob是不能成功否认接收过Alice的签名的。例如，在验证阶段的第1步，Bob用密钥$K_{\rm bc}$加密参数$|S_a\rangle$和$|\varphi'\rangle$获取了$|Y_b\rangle$，即$|Y_b\rangle=E_{K_{\rm bc}}(|S_a\rangle,|\varphi'\rangle)$。假如Bob抵赖接收了签名$|S_a\rangle$，这个时候Charlie只需要检测$|Y_b\rangle$中是否同时含有$K_{\rm bc}$和$K_{\rm ac}$，如果是，则Bob一定接收了$|S_a\rangle$。此外，如果整个方案是完整的，根据验证阶段的第(5)步，Bob根据Alice的测量结果，可以恢复出正确的$|\varphi'\rangle$，然后才可以请求r进而恢复信息序列$|\varphi\rangle$。如果Bob拒绝r的接收，则无法得到信息序列。而且，Bob也是无法否认签名的完整性的，例如在$|\varphi'\rangle=|\varphi'_{\rm out}\rangle$情况下是不能声称$|\varphi'\rangle\neq|\varphi'_{\rm out}\rangle$，如此他将无法得到$r$更无法接收到Alice签名的信息内容，因此Bob无法拒绝签名$|S\rangle=(|S_a\rangle,r)$的接收也无法拒绝签名的完整性。

即使减小对可信任Charlie的直接依赖，Bob仍然是不可能成功否认对Alice签名或签名信息的接收。在验证阶段的第(1)步，假设Bob传输$|Y_b\rangle$给Alice而不是Charlie。然后Alice发送新产生的

$|S'\rangle=(|M_a\rangle,|S_a\rangle,|Y_b\rangle)$给Charlie，接着Charlie转换原来的$|Y_{\rm cb}\rangle$为$|Y_{\rm cb}{}'\rangle$，即

$$|Y_{\rm cb}{}'\rangle=E_{K_{\rm bc}}(|M_a\rangle,|\chi\rangle,|S'\rangle). \tag{31}$$

在这个修改过程中，$|S'\rangle$中同时包含$K_{\rm bc}$和$K_{\rm bc}$。这时若Bob抵赖签名并因此和Alice陷入纠纷，从以上两个量子态，Charlie通过判断$K_{\rm bc}$的存在可以检测这种攻击策略。

总之，可信任第三方Charlie的存在以及通过公共板公布随机数r的方式共同保证了接收者Bob否认的不可能性。

4.4 讨论

Gao等人[11]指出虽然量子一次一密是一种信息安全的加密方式且在AQS算法中起着重要的作用，这种方式有可能引起Bob在已知信息环境下对Alice签名的存在性伪造攻击。作为Alice签名的接收者，假如Bob可以获取Alice的有效信息签名对$(|\varphi\rangle,|S_a\rangle)$满足$|S_a\rangle=E_{K_{\rm ac}}E_r|\varphi\rangle$，Bob应用$d$维泡利算符$P_i$在$|\varphi\rangle$中的每一个$d$维量子态得到$|\varphi''\rangle=\otimes_{i=1}^{n}P_i|\varphi\rangle$，同时应用相同的泡利算符在$|S_a\rangle$中相应的$d$维量子态得到$|S_a''\rangle=\otimes_{i=1}^{n}P_i|S_a\rangle$，其中泡利算符$P_i$是$\{I,\sigma_x,\sigma_y,\sigma_z\}_d$中的一种，生成的新的信息签名对$(|\varphi''\rangle,|S_a''\rangle)$也许是一种成功的伪造。由于$P_i$可以选取4种泡利算符中的1种，除了已有的那对签名信息对之外，至少还有4^n-1种可能的伪造，Bob可以从其中选择一个对自己最有益的信息签名对并宣称这个最有益的信息是Alice签的。这时，Charlie只会站在Bob的一方。然后由于在整个过程中，Bob无法获取Alice正确的签名信息，这种方式的攻击只可能发生在验证阶段之后，在通信过程中是不可能发生的。所以说本文设计的方案是可以抵抗这种存在性伪造攻击的。

此外，在Alice按照上述协议完成原始信息$|\varphi\rangle$的签署之后，发送$(|\varphi'\rangle,|S_a\rangle)$给Bob。在验证阶段Charlie发送$|Y_{\rm cb}\rangle=E_{K_{\rm bc}}(|\varphi'\rangle,|S_a\rangle,\chi)$给Bob的时候，Alice有机会修改$|S_a\rangle$得到$|S_a{}'\rangle$，使其不再是信息序列$|\varphi\rangle$的有效签名。Bob不知道密钥$K_{\rm ac}$故他不会发现Alice的修改，后续Bob需要Alice参与的时候，Alice否认这不是她曾经完成的签名。这时Charlie出来调解，并站在Alice的一方。因此，Alice可以通过上述方式抵赖成功。

基于上述可能的攻击策略，给出几种可能的改善方案：

(1) 采用其他安全的加密算法避免比特对比特的加密，使用加密集合的方式改善量子一次一密带来的缺陷，比如Li等人[14]和Zhang等人[16]等人提出的受控非和链式键控非加密方式，但是它们都是实施对量子比特的加密，对于d维量子态的加密方式还有待研究。

(2) 对于Alice实施的抵赖攻击，合适的量子认证技术可以被引进，例如Alice将签名$|S_a\rangle$传输给Bob之前，使用密钥$K_{\rm ac}$对其进行认证得到$|S_a{}'\rangle$。Charlie从Bob接收到之后确认$|S_a{}'\rangle$的完整性。同样，Charlie在发送给Bob之前也实施认证得到$|S_{\rm ab}{}'\rangle$, Bob接收到之后会确认$|S_{\rm ab}{}'\rangle$的完整性来检验是否在传输过程被Alice修改。此时，来自Alice的上述修改$|S_a\rangle$的方式实施抵赖攻击是可以被阻止的。不幸的是，目前合适的量子信息认证[37]技术还有待研究。因此就目前的研究技术而言，本文的AQS算法是较优的。

4.5 比较

使用d正则图上量子游走隐形传输模型、扩展的d维量子一次一密算法、随机数r以及公共板，本文建议了一种目前较优的用于完成d维量子态签名的AQS算法。与已有的一般的AQS方案[7,9]相比较，要签名的信息被编码在d维量子态代替单量子比特态，在一次量子通讯中，d维量子态作为信息的载体可以传输更多的信息。此外，由于随机数和公共板的应用，Bob的存在性伪造攻击和否认攻击均是无法成功的。与已有的基于量子隐形传输的AQS算法[7,9,12,18,19]相比，在初始化阶段，本文不需要在初始化阶段提前制备隐形传输必要的纠缠态。而且，当用于传输d维量子态的时候，Bennett等人[21]的方案需要执行一个包含d^2个元素的联合测量。而通过基于完全图上或正则图上的量子游走隐形传输模型只需要执行两次包含d个元素的投影算符或两次分别包含n个或d个元素组成的投影测量算符，因此这种基于量子游走的隐形传输模型不仅降低了测量的开销，即测量更加有效，而且相比于联合测量，投影测量更加容易实现，这一点在文献[32,33]中已经被提到。

5 结束语

本文建议了一种基于量子游走的AQS协议。基于d正则图量子游走的隐形传输模型被用于转移d维量子态从签名者到验证者。在初始化阶段，用于量子隐形传输的纠缠态无需事先制备，它们可在签名阶段量子游走的一步之后自动产生。两个包含d个元素的投影测量算符代替包含d^2个元素的联合测量算符被应用，在实现上更容易。随机数和公共板的应用使得整个方案中信息序列以密文的形式存在，且可以抵抗接收者在接收正确的信息序列之前的已知信息下的存在性伪造攻击。安全性分析证明了本AQS方案可以防止来自签名者和接收者的抵赖

攻击以及任何人的伪造攻击。讨论表明协议也许不能防御来自签名者的抵赖攻击，呈现了相应的改进策略。比较展示协议更加有效且容易实现。加之量子游走在实验上的可行性，本签名方案未来是实用的。目前，为了抵抗接收者的伪造攻击，受控非或链式键控受控非等加密算法代替量子一次一密已经被提出，它们用于加密量子比特，然而适用于多维量子态的相对应的加密算法还没有被研究，因此在未来的研究中，将关注多维量子态的量子密码算法以及其在量子密码协议中的应用。

参 考 文 献

[1] NIELSEN M A and CHUANG I. Quantum computation and quantum information[J]. *American Journal of Physics*, 2002, 70(5): 558–559. doi: 10.1119/1.1463744.

[2] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. *SIAM Review*, 1999, 41(2): 303–332. doi: 10.1137/S0036144598347011.

[3] GROVER L K. Quantum mechanics helps in searching for a needle in a haystack[J]. *Physical Review Letters*, 1997, 79(2): 325–328. doi: 10.1103/PhysRevLett.79.325.

[4] GUO Ying, LIAO Qin, WANG Yijun, *et al*. Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction[J]. *Physical Review A*, 2017, 95(3): 032304. doi: 10.1103/PhysRevA.95.032304.

[5] ZHANG Zhaoyuan, SHI Ronghua, ZENG Guihua, *et al*. Coherent attacking continuous-variable quantum key distribution with entanglement in the middle[J]. *Quantum Information Processing*, 2018, 17(6): 1–18. doi: 10.1007/s11128-018-1903-0.

[6] MEIJER H and AKL S. Digital signature schemes for computer communication networks[J]. *ACM SIGCOMM Computer Communication Review*, 1981, 11(4): 37–41. doi: 10.1145/1013879.802657.

[7] ZENG Guihua and KEITEL C H. Arbitrated quantum-signature scheme[J]. *Physical Review A*, 2002, 65(4): 042312. doi: 10.1103/PhysRevA.65.042312.

[8] BARNUM H, CRÉPEAU C, GOTTESMAN D, *et al*. Authentication of quantum messages[C]. The 43rd Annual IEEE Symposium on Foundations of Computer Science, Vancouver, Canada, 2002: 449–458. doi: 10.1109/SFCS.2002.1181969.

[9] LI Qin, CHAN W H, and LONG Dongyang. Arbitrated quantum signature scheme using Bell states[J]. *Physical Review A*, 2009, 79(5): 054307. doi: 10.1103/PhysRevA.79.054307.

[10] ZOU Xiangfu and QIU Daowen. Security analysis and improvements of arbitrated quantum signature schemes[J]. *Physical Review A*, 2010, 82(4): 042325. doi: 10.1103/PhysRevA.82.042325.

[11] GAO Fei, QIN Sujuan, GUO Fenzhuo, *et al*. Cryptanalysis of the arbitrated quantum signature protocols[J]. *Physical Review A*, 2011, 84(2): 022344. doi: 10.1103/PhysRevA.84.022344.

[12] CHOI J W, CHANG K Y, and HONG D. Security problem on arbitrated quantum signature schemes[J]. *Physical Review A*, 2011, 84(6): 062330. doi: 10.1103/PhysRevA.84.062330.

[13] 张骏, 吴吉义. 可证明安全高效的仲裁量子签名方案[J]. 北京邮电大学学报, 2013, 36(2): 113–116.
ZHANG Jun and WU Jiyi. Provable secure efficient arbitrated quantum signature scheme[J]. *Journal of Beijing University of Posts and Telecommunications*, 2013, 36(2): 113–116.

[14] LI Fengguang and SHI Jianhong. An arbitrated quantum signature protocol based on the chained CNOT operations encryption[J]. *Quantum Information Processing*, 2015, 14(6): 2171–2181. doi: 10.1007/s1112.

[15] YANG Yuguang, LEI He, LIU Zhichao, *et al*. Arbitrated quantum signature scheme based on cluster states[J]. *Quantum Information Processing*, 2016, 15(6): 2487–2497. doi: 10.1007/s11128-016-1293-0.

[16] ZHANG Long, SUN Hongwei, ZHANG Kejia, *et al*. An improved arbitrated quantum signature protocol based on the key-controlled chained CNOT encryption[J]. *Quantum Information Processing*, 2017, 16(3): 1–15. doi: 10.1007/s11128-017-1531-0.

[17] ZHANG Yingying and ZENG Jiwen. An improved arbitrated quantum scheme with Bell states[J]. *International Journal of Theoretical Physics*, 2018, 57(4): 994–1003. doi: 10.1007/s10773-017-3632-z.

[18] GUO Ying, FENG Yanyan, HUANG Dazu, *et al*. Arbitrated quantum signature scheme with continuous-variable coherent states[J]. *International Journal of Theoretical Physics*, 2016, 55(4): 2290–2302. doi: 10.1007/s10773-015-2867-9.

[19] FENG Yanyan, SHI Ronghua, and GUO Ying. Arbitrated quantum signature scheme with continuous-variable squeezed vacuum states[J]. *Chinese Physics B*, 2018, 27(2): 020302. doi: 10.1088/1674-1056/27/2/020302.

[20] LOU Xiaoping, LONG Hu, TANG Wensheng, *et al*. Continuous-variable arbitrated quantum signature based on dense coding and teleportation[J]. *IEEE Access*, 2019, 7: 85719–85726. doi: 10.1109/ACCESS.2019.2925635.

[21] BENNETT C H, BRASSARD G, CRÉPEAU C, *et al*. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels[J]. *Physical Review*

Letters, 1993, 70(13): 1895–1899. doi: 10.1103/PhysRevLett.70.1895.

[22] REN Lijie, HE Guangqiang, and ZENG Guihua. Universal teleportation via continuous-variable graph states[J]. *Physical Review A*, 2008, 78(4): 042302. doi: 10.1103/PhysRevA.78.042302.

[23] AHARONOV Y, DAVIDOVICH L, and ZAGURY N. Quantum random walks[J]. *Physical Review A*, 1993, 48(2): 1687–1690. doi: 10.1103/PhysRevA.48.1687.

[24] MEYER D A. From quantum cellular automata to quantum lattice gases[J]. *Journal of Statistical Physics*, 1996, 85(5/6): 551–574. doi: 10.1007/BF02199356.

[25] FARHI E and GUTMANN S. Quantum computation and decision trees[J]. *Physical Review A*, 1998, 58(2): 915–928. doi: 10.1103/PhysRevA.58.915.

[26] CHILDS A M and Goldstone J. Spatial search by quantum walk[J]. *Physical Review A*, 2004, 70(2): 022314. doi: 10.1103/PhysRevA.70.022314.

[27] AARONSON S and SHI Yaoyun. Quantum lower bounds for the collision and the element distinctness problems[J]. *Journal of the ACM*, 2004, 51(4): 595–605. doi: 10.1145/1008731.1008735.

[28] DOUGLAS B L and WANG J B. A classical approach to the graph isomorphism problem using quantum walks[J]. *Journal of Physics A*: *Mathematical and Theoretical*, 2008, 41(7): 075303. doi: 10.1088/1751-8113/41/7/075303.

[29] DU Jiangfeng, LI Hui, XU Xiaodong, *et al*. Experimental implementation of the quantum random-walk algorithm[J]. *Physical Review A*, 2003, 67(4): 042316. doi: 10.1103/PhysRevA.67.042316.

[30] SCHMITZ H, MATJESCHK R, SCHNEIDER C, *et al*. Quantum walk of a trapped ion in phase space[J]. *Physical Review Letter*, 2009, 103(9): 090504. doi: 10.1103/PhysRevLett.103.090504.

[31] PERUZZO A, LOBINO M, MATTHEWS J C F, *et al*. Quantum walks of correlated photons[J]. *Science*, 2010, 329(5998): 1500–1503. doi: 10.1126/science.1193515.

[32] WANG Yu, SHANG Yun, and XUE Peng. Generalized teleportation by quantum walks[J]. *Quantum Information Processing*, 2017, 16(9): 1–13. doi: 10.1007/s11128-017-1675-y.

[33] SHANG Yun, WANG Yu, LI Meng, *et al*. Quantum communication protocols by quantum walks with two coins[J]. *EPL* (*Europhysics Letters*), 2019, 124(6): 60009. doi: 10.1209/0295-5075/124/60009.

[34] AHARONOV D, AMBAINIS A, KEMPE J, *et al*. Quantum walks on graphs[C]. The 33rd Annual ACM Symposium on Theory of Computing, Hersonissos, Greece, 2001: 50–59. doi: 10.1145/380752.380758.

[35] BRUN T A, CARTERET H A, and AMBAINIS A. Quantum walks driven by many coins[J]. *Physical Review A*, 2003, 67(5): 052317. doi: 10.1103/PhysRevA.67.052317.

[36] BUHRMAN H, CLEVE R, WATROUS J, *et al*. Quantum fingerprinting[J]. *Physical Review Letters*, 2001, 87(16): 167902. doi: 10.1103/PhysRevLett.87.167902.

[37] PÉREZ E, CURTY M, SANTOS D J, *et al*. Quantum authentication with unitary coding sets[J]. *Journal of Modern Optics*, 2003, 50(6/7): 1035–1047. doi: 10.1080/09500340308234550.

施荣华：男，1963年生，教授，研究方向为量子密码协议、信息和网络安全.

冯艳艳：女，1991年生，博士生，研究方向为量子密码协议、量子游走及其应用.

石金晶：女，1986年生，副教授，研究方向为量子密码协议、量子神经网络及其应用.