文章编号:1000－2367(2017)04－0111－07 DOI:10.16366/j.cnki.1000－2367.2017.04.018

一种新型弱仲裁量子签名方案

辛向军[1],黄守佳[1],张阳[1],化小林[1],李发根[2]

(1. 郑州轻工业学院 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)

摘 要:弱仲裁量子签名的安全性依赖于量子力学的一些基本原理,其不仅比传统的数字签名具有更好的安全性,而且比仲裁量子签名计算效率较高.为此,给出了一种新型弱仲裁量子签名,该签名具有以下特点:(1)仲裁者并不参与签名的产生和验证过程,只在发生纠纷时,仲裁者才参与纠纷的解决;(2)通过利用签名者身份信息以及与密钥绑定的旋转算子对签名进行认证,可以抵抗伪造攻击,并具有不可否认性;(3)该签名方案具有基于身份的数字签名方案的优点,即用户的身份信息直接用作公钥,无须量子公钥证书,这将给用户提供更多的方便.

关键词:量子签名;仲裁;不可伪造;安全

中图分类号:TP309 **文献标志码**:A

数字签名是公钥密码学的一种重要原语,可以验证签名的发起者,保证消息的完整性,可验证性和不可否认性.目前,传统的数字签名理论和技术已经得到广泛研究,并在电子商务、移动通信等领域中有着很多应用.然而,传统的数字签名是基于某些尚未得到严格证明的数学困难假设(如,大数分解困难假设和离散对数求解困难假设)构造的.尽管这些数学困难假设还没有得到严格证明,但人们已经将这些数字签名系统广泛地用于电子商务等各种领域.

然而,随着量子信息与量子计算研究成果的不断涌现,这些基于传统数学困难假设的数字签名系统的安全性受到严峻的挑战.Shor 的量子方法的出现[1],使得人们对数字签名的乐观态度有所改变.为探索具有更高安全性的签名方案,很多研究人员付出很大努力来探索具有无条件安全特性的量子签名,以取代安全性受到挑战的传统数字签名.事实上,利用量子力学的一些基本原理和反常属性[2－3],可以构造不同类型的量子签名.同传统基于数学困难问题的数字签名相比,量子签名不仅具有经典签名的一些属性(如信息的完整性保护、可验证性、不可否认性等),更重要的是,理论上量子签名具有无条件安全性,这使得量子签名的研究受到了很大的重视.文献[4]利用量子单向函数,给出第一个量子签名方案.此后,众多学者在量子签名的研究方面做出了不懈的努力,并取得了大量的研究成果[5－17].例如,利用仲裁者,文献[5]给出两个具有消息恢复功能的量子签名方案.在 2002 年,基于 Greenberger-Horne-Zeilinger(GHZ)态,文献[10]提出了仲裁量子签名.然而,文献[11]指出文献[10]中的量子签名协议并不完善.类似文献[10]的做法,文献[12]利用纠缠 Bell 态给出了一种仲裁量子签名.然而,文献[10,12]中的方案并不安全,文献[18]指出文献[10,12]所提出的方案中签名接收者可以伪造签名.为此,文献[18]给出了一个改进方案.文献[19]深刻地指出文献[10,12,18]方案中加密算法使用了可交换的 Pauli 算子,故签名验证者可以通过 Pauli 算子作用到合法签名上,从而可伪造出任意消息的签名.为此,文献[20]尝试避免 Pauli 算子攻击,给出了改进的仲裁量子签名方案.但是,遗憾的是,文献[21]的签名方案并不能抵抗优化的伪造攻击.2013 年,文献[22]利用 Hash 函数给出了一个可以对任意长度的经典消息进行签名的仲裁量子签名.然而,文献[23]发现,在 Li 等人的量子签名方案中,由于验证者和仲裁者之间的量子信道缺乏认证,所以签名可以被篡改并通过验证,从而签名者可以否认自己的签名.

收稿日期:2016-11-04;**修回日期**:2017-05-03.

基金项目:国家自然科学基金(61272525);河南省基础与前沿技术研究项目(152300410129);河南省高等学校重点科研项目(16A520096).

作者简介(通信作者):辛向军(1974－),男,河南淇县人,郑州轻工业学院副教授,博士,主要从事信息安全方面的研究,E-mail:xin_xiang_jun@126.com.

为提高仲裁量子签名的安全性和计算效率,并对仲裁者的依赖进行弱化,文献[24]提出具有非可信仲裁者的量子签名.它的可行性主要依赖于参与者之间的密钥共享,特别是签名者和验证者所共享的密钥对于仲裁者而言是不可见的.主要创新在于在量子签名方案中使用的是非可信仲裁者.并且,在不同的会话时期,签名者 Alice 和验证者 Bob 共享密钥在随机更新.即使在某个时期 Alice 和 Bob 之间的共享的密钥 Ks 泄露,也不会影响其他会话时期签名的安全性.然而,这种签名方案并不安全.文献[25]指出在文献[24]的仲裁量子签名方案中,签名者可以否认自己的签名,签名的验证者可以伪造签名.并且,这种非可信仲裁者量子签名方案要求所有的用户两两之间必须共享一个密钥.为此,文献[25]给出了一种改进的非可信仲裁者量子签名方案.然而,文献[25]的方案的安全性在一定程度上依赖于对经典信道的安全假设.

从上面的分析可以看出,在多数的仲裁量子签名方案中,存在着一些安全隐患.为此,文献[26-27]给出了安全的仲裁量子签名存在性分析,指出以前所给出的基于加密的量子签名的安全漏洞,并给出了安全仲裁量子签名的框架和构造措施,例如,利用钥控量子一次一密代替优化的量子一次一密.并且,在实践中,仲裁量子签名的产生或验证过程需要仲裁者参与,这无疑会大大降低签名方案的效率.并且,仲裁者可能会成为一个通信瓶颈.另外,仲裁量子签名的产生或验证方式是利用了对称加密和解密的原理,需要仲裁者、签名者和验证者之间共享多个密钥,导致仲裁量子签名方案需要多次重复执行量子密钥分配协议用于共享密钥.所有这些因素都无疑会大大影响仲裁量子签名的效率.

2012 年,文献[28]利用量子单向函数[4,29-32]、量子比特和未知状态比较算法[33]提出一种具有弱仲裁者的量子签名.这种签名克服了以前具有仲裁者量子签名的缺点,具有很好的计算效率,并具有公开验证性,这实际上是一种非对称密码技术.在这种签名方案中,所有参与者两两之间无须利用量子密钥分配协议分配共享密钥,仲裁者无须参与签名的生成.而单量子比特比多粒子纠缠态更容易制备、分发和实现.并且,仲裁者只有在发生纠纷时才参与协议.然而,该方案存在着安全缺陷.文献[34-35]指出该方案无法完成对签名者公钥与身份信息的对应,且不能抵抗伪造签名攻击,同时,文献[36]也指出该方案不能抵抗中间人攻击.为此,文献[36]给出了改进方案,然而,并未改进文献[28]中方案的基本算法.因此,文献[36]的方案仍然不能抵抗文献[34-35]所述的伪造签名攻击.2015 年,文献[37]利用单量子比特旋转算子给出了一种量子签名方案,但这种方案仍然是仲裁量子签名,签名的产生和验证需要签名者、验证者、仲裁者之间大量的在线通信,从而影响了签名方案的效率.

从上面的分析可知,弱仲裁量子签名有很好的性质,特别是在计算效率方面,其效率高于仲裁量子签名.然而,目前关于弱仲裁量子签名的研究成果并不多.并且,由前面的分析可知,已有的弱仲裁量子签名并不安全.为此,本文通过利用量子密码单向函数和密钥生成中心实现量子密钥的生成和分配,并利用新型量子认证协议实现对签名者公钥和身份的认证.在此基础上,进一步实现新型弱仲裁量子签名的构造,给出弱仲裁量子签名的安全证明,弱化仲裁者的作用,提高量子签名的计算效率.

1 新型弱仲裁量子签名方案

弱仲裁量子签名包括 5 个算法:初始化算法、密钥生成算法、签名的生成算法、签名的验证算法、仲裁算法.在方案中,需要用到一个量子单向函数[28].令酉矩阵 $U_t=\mathrm{e}^{\mathrm{i}tH}$,其中,$H$ 为某一 Hermite 矩阵.参数 $t\in R$ 和 H 可以作为秘密信息保存.由于 U_t 具有连续性,则对于随机选取的 $t_1,t_2\in R$,U_{t_1} 和 U_{t_2} 是不可区分的.另外,在方案中,始终假设签名者的身份为 $I_A\in\{0,1\}^*$,验证者的身份为 $I_B\in\{0,1\}^*$.

(a)初始化算法.

在初始化算法中,需要用到一个密钥生成中心(KGC).假定 KGC 是可信的,比如,政府机构,公安机关等权威机构可以作为 KGC.KGC 根据用户的身份信息为每个用户产生自己的量子私钥.令 N 和 L 为安全参数($N\gg1,L\gg1$).在算法中,需要用到 3 个输出分布均匀的 Hash 函数:

$$H_1:\{0,1\}^*\to\{0,1\}^L,H_2:\{0,1\}^*\to Z_{2^N}^L,H_3:\{0,1\}^*\to Z_{2^N}^L.$$

KGC 随机选取矢量 $\vec{t}=(t_1,t_2,\cdots,t_L)\in Z_{2^N}^L/2^N$,并秘密选取 Hermite 矩阵矢量 $\vec{H}=(H_1,H_2,\cdots,H_L)$.其中每个 $H_i(i=1,2,\cdots,L)$ 都是一个 Hermite 矩阵.比如,$H_i(i=1,2,\cdots,L)$ 可以在 Pauli 矩阵$\{\sigma_x,\sigma_y,\sigma_z\}$ 中

随机选取. KGC 秘密保存$(\hat{t},\vec{H})$作为自己的主密钥. 令$\vec{U}=(U_1,U_2,\cdots,U_L)$,其中$U_i=e^{ii_iH_i}$,下标$i=0,1,\cdots,L$.

(b)密钥生成算法.

在密钥生成算法中,KGC 为每个用户产生自己的量子私钥. 假定用户的经典身份信息为$I\in\{0,1\}^*$. KGC 通过以下步骤为每个用户产生自己的量子私钥.

步骤 1　KGC 利用量子密钥分配协议(如,BB84 协议[2])和用户 I 共享一个二进制密钥串k_I.

步骤 2　KGC 计算$H_1(I)=(d_1,d_2,\cdots,d_L)\in\{0,1\}^L$和$|K_I\rangle=\bigotimes_{i=1}^{L}U_i|d_i\rangle$.

步骤 3　KGC 利用量子信道将$|K_I\rangle$发送给用户 I. 为保证量子比特传递的安全性,可在量子比特串中$|K_I\rangle$不同的位置随机插入诱骗比特(decoy photon),通过窃听检测来保证量子信道的安全性.

步骤 4　当用户 I 接收到$|K_I\rangle$后,其将$|K_I\rangle$作为自己的私钥秘密保存,而将个人身份信息 I(或者$|H_1(I)\rangle=\bigotimes_{i=1}^{L}|d_i\rangle$)作为自己的公钥.

(c)签名的生成算法.

假定签名者为用户 I_A. I_A 和 KGC 共享的二进制密钥串为k_{I_A}. 记$H_1(I_A)=(d_1^A,d_2^A,\cdots,d_L^A)$. I_A 从 KGC 处获得的私钥为$|K_{I_A}\rangle=\bigotimes_{i=1}^{L}U_i|d_i^A\rangle$. 假定待签名的消息为$M\in\{0,1\}^L$. 不妨设$M=m_1m_2\cdots m_L$,其中$m_i\in\{0,1\}(i=1,2,\cdots,L)$. 其对应于$|M\rangle=\bigotimes_{i=1}^{L}|m_i\rangle$. 为对 M 进行签名,I_A 执行以下步骤.

步骤 1　I_A 利用自己和 KGC 共享的密钥k_{I_A}计算

$$H_1(M\|K_{I_A})=(n_1^A,n_2^A,\cdots,n_L^A),$$

其中,$n_i^A\in Z_{2^N}$,$i=0,1,\cdots,L$.

步骤 2　I_A 对$|K_{I_A}\rangle$进行旋转操作$R(\theta_i^A)$,得到$|W\rangle=\bigotimes_{i=1}^{L}R(\theta_i^A)U_i|d_i^A\rangle$,其中

$$\theta_i^A=2n_i^A\pi/2^N,R(\theta_i^A)=e^{-i\theta_i^A\sigma_y/2}=\cos\frac{\theta_i^A}{2}I-i\sin\frac{\theta_i^A}{2}\sigma_y,$$

这里的$I\equiv|0\rangle\langle0|+|1\rangle\langle1|$,$\sigma_y\equiv i(|1\rangle\langle0|-|0\rangle\langle1|)$. 记$|w_i\rangle=R(\theta_i^A)U_i|d_i^A\rangle$,则$|W\rangle=\bigotimes_{i=1}^{L}|w_i\rangle$.

步骤 3　以$|W\rangle$中的各个量子比特为控制比特,以$|M\rangle$相应位置的各个量子比特为目标比特进行C_{NOT}操作,从而得到$|S\rangle=\bigotimes_{i=1}^{L}C_{NOT}(|w_i\rangle\otimes|m_i\rangle)$.

步骤 4　签名者 I_A 将自己的签名$(|S\rangle,|M\rangle,I_A)$发送给验证者.

需要注意的是,对于同一消息 M,签名者 I_A 需要制备多份签名$(|S\rangle,|M\rangle,I_A)$发送给验证者,其中一份用于验证签名的有效性,一份用于出现纠纷时进行仲裁,其他的留作备用.

(d)签名的验证算法.

假定验证者为身份为 I_B 的用户. 类似于 I_A,用户 I_B 和 KGC 共享的二进制密钥串为k_{I_B}. 记$H_1(I_B)=(d_1^B,d_2^B,\cdots,d_L^B)$. I_B 从 KGC 处获得的私钥为$|K_{I_B}\rangle=\bigotimes_{i=1}^{L}U_i|d_i^B\rangle$. 当验证者收到签名者发送的多份签名$(|S\rangle,|M\rangle,I_A)$后,验证者首先利用量子态比较算法 SWAP[33] 比较这些签名是否相同. 若不同,则拒绝签名;若相同,则验证者拿出其中一份用于签名的验证,一份专门用于出现纠纷时进行仲裁,而将其他的留作备用. 为验证签名$(|S\rangle,|M\rangle,I_A)$,用户 I_B 执行以下步骤.

步骤 1　对签名$|S\rangle$进行相应的C_{NOT}操作,从而得到$\bigotimes_{i=1}^{L}(|w_i\rangle\otimes|m_i\rangle)$. 对于每个$|w_i\rangle\otimes|m_i\rangle$,$I_B$ 用$|0\rangle$和$|1\rangle$基对第二比特执行正交测量,从而恢复出消息$M=m_1m_2\cdots m_L$和$|M\rangle$,其中$m_i\in\{0,1\}(i=1,2,\cdots,L)$. 并且,用户 I_B 获得$|w_i\rangle(i=1,2,\cdots,L)$.

用户 I_B 对$H_1(I_B)$和$H_2(I_A)$对应位置的比特进行比较,记下比特相同的位置. 例如,假定$H_1(I_A)=101101$,$H_1(I_B)=001011$,易知$H_1(I_B)$和$H_1(I_A)$对应的第 2 比特、第 3 比特、第 6 比特相同,则用户 I_B 将存储这些具有相同比特的位置信息. 对于$H_1(I_B)$和$H_1(I_A)$,假定它们对应的第$i_1,i_2,\cdots,i_r$个位置的比特相同(由于H_1的输出是随机均匀分布的,故大约有$L/2$个位置相同,即$r\approx L/2$).

用户 I_B 计算$H_3(M\|I_A\|I_B\|k_{I_B})=(n_1^B,n_2^B,\cdots,n_L^B)$. 并根据$i_1,i_2,\cdots,i_r$,用户 I_B 计算$\theta_{i_j}^B=2n_{i_j}^B\pi/2^N(j=1,\cdots,r)$. 针对每个$|w_{i_j}\rangle(j=1,\cdots,r)$,用户 I_B 进行旋转操作$R(\theta_{i_j}^B)$,从而得到$|\alpha_{i_j}\rangle=R(\theta_{i_j}^B)|w_{i_j}\rangle$. 并且,用户 I_B 对自己的私钥$|K_{I_B}\rangle=\bigotimes_{i=1}^{L}U_i|d_i^B\rangle$中处于$i_1,i_2,\cdots,i_r$位置的量子比特做相同的旋转操作$R(\theta_{i_j}^B)$,从而得到$|\beta_{i_j}^1\rangle=R(\theta_{i_j}^B)u_{i_j}|d_{i_j}^B\rangle(j=1,\cdots,r)$. 用户 I_B 将$\bigotimes_{j=1}^{r}|\alpha_{i_j}\rangle$和$\bigotimes_{j=1}^{r}|\beta_{i_j}^1\rangle$发送给用

户 I_A,并在公告栏中公布(M,I_A,I_B).

步骤 2 在接收到 $\otimes_{j-1}^{r}|\alpha_{i_j}\rangle$ 和 $\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{I}}\rangle$ 后,签名者查看公告栏,若验证者已经公布(M,I_A,I_B)后,则 I_A 利用自己的密钥串 k_{I_A},根据公告栏中公布的(M,I_A,I_B) 计算 $H_2(M\|k_{I_A})=(n_1^A,n_2^A,\cdots,n_L^A),\theta_i^A=2n_i^A\pi/2^N$,然后对 $|\alpha_{i_j}\rangle(j=1,\cdots,r)$ 进行逆向旋转操作得到 $|\beta_{i_j}^{\mathrm{II}}\rangle=R(-\theta_{i_j}^A)|\alpha_{i_j}\rangle(j=1,\cdots,r)$. 然后签名者对于 $\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{I}}\rangle$ 和 $\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{II}}\rangle$ 的第 $l(l=1,2,\cdots,r)$ 比特投掷均匀的硬币:若投掷结果为 0,则不交换 $|\beta_{i_j}^{\mathrm{I}}\rangle$ 和 $|\beta_{i_j}^{\mathrm{II}}\rangle$ 的位置;若投掷结果为 1,则交换 $|\beta_{i_j}^{\mathrm{I}}\rangle$ 和 $|\beta_{i_j}^{\mathrm{II}}\rangle$ 的位置. 从而,签名者由 $\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{I}}\rangle$ 和 $\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{II}}\rangle$ 分别得到 $\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{III}}\rangle$ 和 $\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{IV}}\rangle$. 显然,若 $\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{I}}\rangle=\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{II}}\rangle$,则 $\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{III}}\rangle=\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{IV}}\rangle$. 最后,签名者 I_A 将 $\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{III}}\rangle$ 发送给验证者 I_B,而自己保留 $\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{IV}}\rangle$.

步骤 3 当验证者 I_B 收到 $\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{III}}\rangle$ 后,其计算为

$$H_3(M\|I_A\|I_B\|k_{I_B})=(n_1^B,n_2^B,\cdots,n_L^B),\theta_{i_j}^B=2n_{i_j}^B\pi/2^N(j=1,\cdots,r).$$

并对自己的私钥 $|K_{I_B}\rangle=\otimes_{i=1}^{L}U_i|d_i^B\rangle$ 中处于第 $i_j(j=1,\cdots,r)$ 个位置的量子比特做旋转操作 $R(\theta_{i_j}^B)$,即其计算 $|\beta_{i_j}\rangle=R(\theta_{i_j}^B)U_{i_j}|d_{i_j}^B\rangle(j=1,\cdots,r)$. 最后,用户 I_B 利用未知量子比特状态比较算法 SWAP[33],对 $|\beta_{i_j}\rangle$ 和 $|\beta_{i_j}^{\mathrm{III}}\rangle(j=1,\cdots,r)$ 进行比较. 若这些量子态相同,则接受签名$(|S\rangle,|M\rangle,I_A)$;否则,用户 I_B 拒绝该签名.

(e)仲裁算法.

由于 KGC 是可信的,因此,当签名者和验证者发生纠纷时,KGC 可以作为仲裁者解决纠纷. 在上述的签名方案中,签名者需要制备多份签名 $(|S\rangle,|M\rangle,I_A)$ 发送给验证者,其中一份用于验证签名的有效性,一份用于出现纠纷时进行仲裁,其他的签名留作备用. 由于签名者的身份信息 I_A 用作公钥,所以验证者可以根据签名者的身份信息验证签名的有效性.

若用户 I_A 否认自己的签名时,则验证者将自己的身份信息 I_B,用作仲裁的签名$(|S\rangle,|M\rangle,I_A)$ 发送给 KGC. 则仲裁者 KGC 根据主密钥$(\vec{t},\vec{H})$、同用户 I_A 共享的密钥串 k_{I_A}、公告栏中公布的(M,I_A,I_B) 以及签名消息 M,计算出用户 I_A 的量子密钥 $|K_{I_A}\rangle$ 以及对 M 执行的秘密旋转操作 $R(\theta_{i_j}^A)$. 从而,仲裁者 KGC 可以和验证者可执行签名验证算法,验证签名的有效性,防止 I_A 否认自己的有效签名.

若用户 I_B 否认自己参与了对签名的验证过程,则签名者可以向仲裁者提供(M,I_A,I_B) 和 $\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{IV}}\rangle$ 作为证据. 这样,仲裁者可以根据(M,I_A,I_B) 和 k_{I_B} 计算出 $\otimes_{j-1}^{r}R(\theta_{i_j}^B)U_{i_j}|d_{i_j}^B\rangle$. 若签名者和验证者确实有效执行了签名验证过程,可知 $\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{IV}}\rangle=\otimes_{j-1}^{r}R(\theta_{i_j}^B)U_{i_j}|d_{i_j}^B\rangle$. 这样,由于只有 I_B 可以根据 k_{I_B} 和 M 获得旋转操作 $R(\theta_{i_j}^B)$,并进一步得到 $\otimes_{j-1}^{r}R(\theta_{i_j}^B)U_{i_j}|d_{i_j}^B\rangle$,使得仲裁者能够利用未知态比较算法 SWAP 比较 $|\beta_{i_j}^{\mathrm{IV}}\rangle$ 与 $R(\theta_{i_j}^B)U_{i_j}|d_{i_j}^B\rangle(j=1,\cdots,r)$ 是否相等,从而证明 $\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{IV}}\rangle$ 确实来自于 I_B,从而确认 I_B 对签名验证的参与. 并且,$|\beta_{i_j}^{\mathrm{IV}}\rangle$ 与 $R(\theta_{i_j}^B)U_{i_j}|d_{i_j}^B\rangle(j=1,\cdots,r)$ 相等进一步说明了签名的有效性,即验证者 I_B 无法否认所验证签名的有效性.

2 可行性与安全分析

2.1 正确性分析

在签名的验证阶段可知,验证者通过正交测量易得 M 和 $|w_i\rangle(i=1,2,\cdots,L)$.

$$|\alpha_{i_j}\rangle=R(\theta_{i_j}^B)|w_{i_j}\rangle=R(\theta_{i_j}^B)R(\theta_{i_j}^A)U_{i_j}|d_{i_j}^A\rangle,j=0,1,\cdots,r.$$

$$|\beta_{i_j}^{\mathrm{II}}\rangle=R(-\theta_{i_j}^A)|\alpha_{i_j}\rangle=R(-\theta_{i_j}^A)R(\theta_{i_j}^B)R(\theta_{i_j}^A)U_{i_j}|d_{i_j}^A\rangle=R(\theta_{i_j}^B)U_{i_j}|d_{i_j}^A\rangle. \tag{1}$$

因此,注意到 $H_1(I_B)$ 和 $H_1(I_A)$ 的第 $i_1,i_2,\cdots,i_r$ 个位置的比特相同,可知

$$|\beta_{i_j}^{\mathrm{II}}\rangle=|\beta_{i_j}^{\mathrm{I}}\rangle=R(\theta_{i_j}^B)U_{i_j}|d_{i_j}^A\rangle=R(\theta_{i_j}^B)U_{i_j}|d_{i_j}^B\rangle,j=0,1,\cdots,r.$$

在上式成立的基础上,签名者随机交换 $\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{I}}\rangle$ 和 $\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{II}}\rangle$ 中部分量子比特,所得到新量子比特串满足 $\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{III}}\rangle=\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{IV}}\rangle(=\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{I}}\rangle=\otimes_{j-1}^{r}|\beta_{i_j}^{\mathrm{II}}\rangle$. 由于

$$|\beta_{i_j}\rangle=R(\theta_{i_j}^B)U_{i_j}|d_{i_j}^B\rangle,j=0,1,\cdots,r.$$

显然成立 $|\beta_{i_j}\rangle=|\beta_{i_j}^{\mathrm{III}}\rangle,j=1,\cdots,r$.

事实上,由于在(1)式中,只有签名者才能根据消息 M 和自己的密钥串 k_{I_A} 来执行逆向旋转操作 $R(-\theta_{i_j}^A)$ 得到 $|\beta_{i_j}^{\mathrm{II}}\rangle(j=1,\cdots,r)$,并进一步得到 $|\beta_{i_j}^{\mathrm{III}}\rangle(j=1,\cdots,r)$. 在签名为真的情况下,必然满足 $|\beta_{i_j}\rangle=$

$|\beta_{i_j}^{\mathrm{III}}\rangle, j=1,\cdots,r$. 因此,验证者可以在签名的验证阶段步骤 3 通过比较 $|\beta_{i_j}\rangle$ 和 $|\beta_{i_j}^{\mathrm{III}}\rangle (j=1,\cdots,r)$ 完成对签名的验证.

类似地,可以验证仲裁算法的正确性.

2.2　密钥的安全性

在本方案中,需要用到酉矩阵 $U_t=\mathrm{e}^{\mathrm{i}tH}$. 由于 U_t 具有连续性,则对于随机选取的 $t_1,t_2\in R, U_{t_1}$ 和 U_{t_2} 是不可区分的. 在初始化算法中,KGC 秘密保存 $(\vec{t},\vec{H})$ 作为自己的主密钥. 对于任意的用户 I,其签名密钥为 $|K_I\rangle=\otimes_{i=1}^{L}U_i|d_i\rangle$,其中 $U_i=\mathrm{e}^{\mathrm{i}t_iH_i}$, $\vec{t}=(t_1,t_2,\cdots,t_L)\in Z_{2^N}^{L}/2^N$ 为 KGC 随机选取的向量,$\vec{H}=(H_1,H_2,\cdots,H_L)$ 也由 KGC 秘密选取. 因此,给定 $|K_I\rangle=\otimes_{i=1}^{L}U_i|d_i\rangle$,由 U_t 的不可区分性很难推出 $\vec{t}=(t_1,t_2,\cdots,t_L)$ 和 $\vec{H}=(H_1,H_2,\cdots,H_L)$. 因此,KGC 的主密钥是安全的.

在方案中的密钥生成阶段,用户的身份信息 $I\in\{0,1\}^*$ 作为自己公钥. 在不知道主密钥的情况下,任何人很难生成用户的签名密钥 $|K_I\rangle=\otimes_{i=1}^{L}U_i|d_i\rangle$. 对于任何两个不同的用户 I_A 和 I_B,由于 H_1 是分布均匀的,所以会导致 $H_1(I_A)$ 和 $H_1(I_B)$ 对应位置约有 $L/2$ 个比特不同,从而导致量子比特串 $|K_{I_A}\rangle$ 和 $|K_{I_B}\rangle$ 中对应位置约有 $L/2$ 个量子比特不同. 在这里安全参数 $L\gg 1$. 从而,用户 I_A 很难推出用户 I_B 的签名密钥.

在方案中,每个用户需要利用量子密钥分配协议(如,BB84 协议[2])和 KGC 共享一个二进制密钥串 k_I. 比如,可以采用 BB84 协议实现密钥共享. 而 Shor 和 Preskill[3] 已经证明了 BB84 协议的无条件安全性. 因此,用户和 KGC 所共享的密钥串 k_I 是安全的.

2.3　签名的不可伪造性和不可否认性

对于敌手而言,若要直接伪造用户 I_A 的签名,则由签名生成算法可知,敌手需要获得 I_A 的签名密钥和共享密钥串 k_{I_A}. 然而,由上面的分析可知,用户 I_A 的签名密钥和密钥串 k_{I_A} 是安全的. 因此,敌手直接伪造 I_A 的签名是困难的.

对于给定的签名 $(|S\rangle,|M\rangle,I_A)$,对其测量可以获得 $\otimes_{i=1}^{L}(|w_i\rangle\otimes|m_i\rangle)$. 敌手若将 $|M\rangle$ 和 I_A 篡改为 $|M'\rangle$ 和 $I_{A'}$,则在签名验证过程中,就会导致 $\otimes_{i=1}^{L}|w_i\rangle$ 中蕴含的旋转操作 $R(\theta_i^A)(i=1,2,\cdots,L)$ 无法与 $|M'\rangle$ 和 $I_{A'}$ 匹配,从而导致 $|\beta_{i_j}^{\mathrm{I}}\rangle,|\beta_{i_j}^{\mathrm{II}}\rangle,|\beta_{i_j}^{\mathrm{III}}\rangle,|\beta_{i_j}^{\mathrm{IV}}\rangle,|\beta_{i_j}\rangle (j=1,\cdots,r)$ 两两互不相同,从而导致签名无法通过验证. 若敌手企图通过篡改 $\otimes_{i=1}^{L}|w_i\rangle$ 为 $\otimes_{i=1}^{L}|w'_i\rangle$,使得 $\otimes_{i=1}^{L}|w'_i\rangle$ 与 $|M'\rangle$ 和 $I_{A'}$ 保持一致,则敌手需要获得对应的旋转操作,因此其需要计算 $H_2(M'\|k_{I_{A'}})$,但其不知道 $k_{I_{A'}}$,因此其无法获得旋转操作 $R(\theta_i^{A'})(i=1,\cdots,L)$,从而导致敌手所篡改的 $\otimes_{i=1}^{L}|w'_i\rangle$ 无法与 $|M'\rangle$ 和 $k_{I_{A'}}$ 匹配,因此敌手伪造签名失败.

给定签名者身份 I_A 和验证者身份 I_B,则 $i_1,i_2,\cdots,i_r$ 确定. 假定敌手的身份 I_E 恰好满足:$H_1(I_E)$ 和 $H_1(I_A)$ 也恰好在第 $i_1,i_2,\cdots,i_r$ 位置的比特相同,则敌手对消息 M 伪造用户 I_A 签名可以通过验证者 I_B 的验证. 然而,这个事件发生的概率是可以忽略的. 事实上,给定 I_A 和 I_B,假定

$$H_1(I_A)=(d_1^A,d_2^A,\cdots,d_L^A)\in\{0,1\}^L, H_1(I_B)=(d_1^B,d_2^B,\cdots,d_L^B)\in\{0,1\}^L.$$

敌手计算 $H_1(I_E)=(d_1^E,d_2^E,\cdots,d_L^E)\in\{0,1\}^L$. 在 $H_1(I_A)$ 和 $H_1(I_B)$ 第 $i_1,i_2,\cdots,i_r$ 位置的比特相同条件下,

$$p(d_{i_1}^E=d_{i_1}^A,d_{i_2}^E=d_{i_2}^A,\cdots,d_{i_r}^E=d_{i_r}^A\mid d_{i_1}^A=d_{i_1}^B,d_{i_2}^A=d_{i_2}^B,\cdots,d_{i_r}^A=d_{i_r}^B)=2^{-r}.$$

由于 H_1 的输出是分布均匀的,因此 $r\approx L/2$. 例如,当 $L=256$ 时,这个概率约为 2^{-128},这是一个可以忽略的概率.

下面,分析方案在文献[19]给出的伪造攻击下的不可伪造性. 即任意攻击者截获签名生成算法中生成的签名 $(|S\rangle,|M\rangle,I_A)$ 后,若对 $|S\rangle$ 和 $|M\rangle$ 执行相同的酉操作,签名的验证将会失败. 假定攻击者对 $|M\rangle$ 进行 U^* 操作,使得

$$U^*|M\rangle=|M^*\rangle=\otimes_{i=1}^{L}|m_i^*\rangle,$$

另设有辅助酉操作 $V^*,V_i^*(i=1,2,\cdots,L)$,使得

$$(V^*\otimes U^*)|S\rangle=(V^*\otimes U^*)\otimes_{i=1}^{L}C_{NOT}(|w_i\rangle\otimes|m_i\rangle)=\otimes_{i=1}^{L}C_{NOT}(V_i^*|w_i\rangle\otimes|m_i^*\rangle)=\otimes_{i=1}^{L}C_{NOT}(V_i^*R(\theta_i^A)U_i|d_i^A\rangle\otimes|m_i^*\rangle).$$

设 $V_i^*R(\theta_i^A)=R(\theta_i^*)(i=1,2,\cdots,L)$,且 $\theta_i^*=2n_i^*\pi/2^N(i=1,2,\cdots,L)$,其中 $n_i^*\in Z_{2^N}, i=0,1,\cdots,L$. 若 $H_2(M^*\|k_{I_A})=(n_1^*,n_2^*,\cdots,n_L^*)$ 恰好成立,则伪造签名成功. 然而,由于攻击者不知道 I_A 的密钥 k_{I_A},因

此其对消息摘要 $H_2(M^* \| k_{I_A})$ 一无所知. 因此,对于敌手而言,

$$H_2(M^* \| k_{I_A}) = (n_1^*, n_2^*, \cdots, n_L^*)$$

能否恰好成立依赖于 Hash 函数 H_2 的随机碰撞. 也就是说,攻击者伪造签名成功的概率依赖于 Hash 函数 H_2 的成功碰撞概率,而这个概率是可以忽略的. 因此,本方案可以抵抗文献[19]所提出的伪造攻击.

由于所构造的量子签名具有不可伪造性,并且仲裁者能够有效地解决纠纷,因此签名者和验证者都无法否认一个有效的签名.

3 结束语

多数已有的量子签名为仲裁量子签名,其签名的产生或验证过程需要仲裁者参与,并且仲裁者容易成为一个瓶颈,从而大大影响了签名方案的效率. 本文研究的是弱仲裁量子签名方案,仲裁者并不参与签名的产生和验证过程. 只有在发生纠纷时,仲裁者才参与纠纷的解决. 因此,本文所给出的量子签名方案具有较高的效率. 并且,已有的弱仲裁量子签名方案不能抵抗伪造攻击. 本文通过利用量子密钥对消息进行签名,利用签名者身份信息以及与密钥绑定的旋转算子对签名进行认证,可以抵抗伪造攻击,并具有不可否认性. 在本文的方案中,其具有传统的基于身份的签名方案的优点,即用户的身份直接用作签名者的公钥,无须量子公钥证书,无需其他设施对公钥和公钥证书进行复杂的管理,从而大大方便了用户.

参 考 文 献

[1] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer [J]. SIAM J Comput,1997,26(5):1484-1509.

[2] Bennett C H,Brassard G. An update on quantum cryptography. Proceedings of the IEEE International Conference on Computers[C] // Systems and Signal Processing 1984. New York:IEEE Press,1984:175-179.

[3] Shor P W,Preskill J. Simple proof of security of the BB84 quantum key distribution protocol [J]. Phys Rev Lett,2000,85(2):441-444.

[4] Gottesman D,Chuang I L. Quantum digital signatures [EB/OL]. (2001-11-15)[2016-10-13]. https://arxiv.org/pdf/quant-ph/0105032.pdf,2001.

[5] Lee H,Hong C,Kim H,et al. Arbitrated quantum signature scheme with message recovery [J]. Phys Lett A,2004,321:295-300.

[6] Wen X J,Niu X M,Ji L P,et al. A weak blind signature scheme based on quantum cryptography [J]. Opt Commun,2009,282:666-669.

[7] Wen X J,Liu Y,Zhou N R. Realizable quantum broadcasting multi-signature scheme [J]. Int J Mod Phys B,2008,22(24):4251-4259.

[8] Yang Y G,Wen Q Y. Quantum threshold group signature [J]. Sci China Ser G,2008,51(10):1505 -1514.

[9] Yang Y G,Wen Q Y. Threshold proxy quantum signature scheme with threshold shared verification [J]. Sci China Ser G,2008,51(8):1079-1088.

[10] Zeng G H,Keitel C H. Arbitrated quantum-signature scheme [J]. Phys Rev A,2002,65:042312.

[11] Curty M,Lutkenhaus N. Comment on "Arbitrated quantum-signature scheme" [J]. Phys Rev A,2008,77:046301.

[12] Li Q,Chan W H,Long D Y. Arbitrated quantum signature scheme using Bell states [J]. Phys Rev A,2009,79:054307.

[13] Zeng G H. Reply to Comment on "Arbitrated quantum-signature scheme" [J]. Phys Rev A,2008,78:016301.

[14] Zeng G H,Lee M H,Guo Y,et al. Continuous variable quantum signature algorithm [J]. Int J Quantum Inf,2007,5(4):553-573.

[15] Lv X,Feng D G. An arbitrated quantum message signature scheme [C]// Proceeding of 1st International Symposium on Computational and Information Science,CIS 2004,LNCS 3314. Berlin:Spring-Verlag,2004:1054-1060.

[16] Wang J,Zhang Q,Tang C J. Quantum signature scheme with single photons [EB/OL]. (2005-11-23)[2016-10-13]. https://arxiv.org/pdf/quant-ph/0511224v1.pdf,2005.

[17] Cao Z J,Markowitch O. A note on an arbitrated signature scheme [J]. Int J Quantum Inf,2009,7(6):1205-1029.

[18] Zou X,Qiu D W. Security analysis and improvements of arbitrated quantum signature schemes [J]. Phys Rev A,2010,82:042325.

[19] Gao F,Qin S J,Guo F Z,et al. Cryptanalysis of the arbitrated quantum signature protocols [J]. Phys Rev A,2011,84:022344.

[20] Choi J W,Chang K Y,Hong D. Security problem on arbitrated quantum signature schemes [J]. Phys Rev A,2011,84:062330.

[21] Zhang K J,Zhang W W,Li D. Improving the security of arbitrated quantum signature against the forgery attack [J]. Quantum Inf Process,2013,12:2655-2669.

[22] Li Q,Li C,Long D,et al. Efficient arbitrated quantum signature and its proof of security [J]. Quantum Inf Process,2013,12:2427-2439.

[23] Liu F,Zhang K,Cao T. Security weaknesses in arbitrated quantum signature protocols [J]. Int J Theor Phys,2014,53:277-288.

[24] Yang Y G,Zhou Z,Teng Y W,et al. Arbitrated quantum signature with untrusted arbitrator [J]. Eur Phys J D,2011,61:773-778.

[25] Zou X,Qiu D,Mateus P. Security analyses and improvement of arbitrated quantum signature with an untrusted arbitrator [J]. Int J Theor Phys,2013,52:3259-3305.
[26] Li Q,Chan W H,Wu C. On the existence of quantum signature for quantum [J]. Int J Theor Phys,2013,52:4335-4341.
[27] Zhang K J,Qin S J,Sun Y,et al. Reexamination of arbitrated quantum signature:the impossible and possible [J]. Quantum Inf Process,2013,12:3127-3141.
[28] Luo M X,Chen X B,Yun D,et al. Quantum signature scheme with weak arbitrator [J]. Int J Theor Phys,2012,51:2135-2142.
[29] Crépeau C,LégaréF,Salvail L. How to convert the flavor of a quantum bit commitment [C]// Advances in Cryptology-EUROCRYPT 2001,LNCS 2045. Berlin:Spring-Verlag,2001:60-77.
[30] Kashe E,Kerenidis I. Statistical zero knowledge and quantum one-way functions [J]. Theor Comput Sci,2007,378:101-116.
[31] Kawachi A,Kobayashi H,Koshiba T,et al. Universal test for quantum one-way permutations [J]. Theor Comput Sci,2005,345:370-385.
[32] Dumais P,Mayers D,Salvail L. Perfectly concealing quantum bit commitment from any quantum one-way permutation [C]// Advances in Cryptology-Eurocrypt 2000,LNCS 1807. Berlin:Spring-Verlag,2000:300-315.
[33] Buhrman H,Cleve R,Watrous J,et al. Quantum fingerprinting [J]. Phys Rev Lett,2001,87:167902.
[34] Kang M S,Hong C H,Heo J. Comment on "quantum signature scheme with weak arbitrator" [J]. Int J Theor Phys,2014,53:1862-1866.
[35] Zou X,Qiu D,Yu F,et al. Security problems in the quantum signature scheme with a weak arbitrator [J]. Int J Theor Phys,2014,53:603-611.
[36] Su Q,Li W M. Improved quantum signature scheme with weak arbitrator [J]. Int J Theor Phys,2013,52:3343-3352.
[37] Kang M S,Hong C H,Heo J,et al. Quantum signature scheme using a single qubit rotation operator [J]. Int J Theor,Phys,2015,54:614-629.

New Quantum Signature Scheme with Weak Arbitrator

Xin Xiangjun[1], Huang Shoujia[1], Zhang Yang[1], Hua Xiaolin[1], Li Fagen[2]

(1. School of Mathematics and Information Sciences, 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)

Abstract:Quantum signatures with weak arbitrator, whose security is based on some fundamental properties of quantum mechanics, are believed to be more secure than the traditional digital signatures. They are more efficient than the quantum signatures with arbitrator. Then, a new quantum signature with weak arbitrator is proposed. Our scheme has the properties as follows. (1) The arbitrator doesn't involve the signing or verifying phase unless the disavowals occur. (2) The signature is verified by using the identity information of the signer and the rotation operator combined with secret key, and it can resist against forgery attack and has the property of undeniablilty. (3) Our scheme has the virtues of the identity-based signature. That is, the signer's identity information is used as the public key. It does not need any quantum public-key certificate, so it can provide more convenience for the users.

Keywords:quantum signature; arbitrator;unforgeability; security

[责任编辑　陈留院]