基于纠缠交换的仲裁量子签名方案*

李 伟† 范明钰 王光卫

(电子科技大学计算机科学与工程学院,成都 610054)

(2010 年 10 月 17 日收到;2010 年 12 月 27 日收到修改稿)

提出了一种基于量子纠缠交换的仲裁签名协议. 以 Bell 态为基础,首先将待签消息利用幺正算符序列进行编码,通过算符序列对 Bell 态进行调制,再通过对量子信息加密产生签名. 验证者将签名信息与仲裁者通过纠缠交换所产生的关联态相结合,通过 Bell 测量来对签名的真实性进行验证. 算法利用量子加密保障了真实签名的不可伪造性,同时通过仲裁的参与结合量子密钥有效解决了双方的抵赖问题,方案还能够有效实现对通信双方隐私信息的保护.

关键词: 量子密码, 量子签名, 纠缠交换

PACS: 03.67.Dd, 03.67.Hk

1. 引 言

量子信息学是量子物理学与信息科学相结合而产生的新兴交叉学科. 量子信息学中发展速度最快的分支学科是量子密码,它是以经典密码学和量子力学为基础,利用量子效应实现无条件安全的信息交互的一种新型密码体制[1]. 自 Bennett 等[2]提出第一个量子密钥分发(QKD)方案 BB84 以来,量子密码学的发展十分迅速,研究内容也在逐步扩展. 目前量子密码学的研究主要包括 QKD[3—10]、量子数据加密[11,12]、量子秘密共享[13—16]、量子身份认证[17,18]、量子数字签名[19—26]以及量子安全直接通信等领域. 虽然 QKD 被证明是绝对安全的,但如何保证量子信息的真实性是量子密码学目前面临的一个重要问题,因此与经典密码学一样,量子保密通信也一定会涉及量子签名问题.

曾贵华等[19]研究了量子签名问题,提出了一个利用 Greenberger-Horne-Zeilinger(GHZ)三重态的相干特性实现对量子比特串的签名方案. 同年,Gottesman 和 Chuang[20]提出了一种原理性的量子签名协议,该协议利用量子单向函数产生公钥,并采用量子交换来验证签名. 文献[21]提出了一种基于 GHZ 三重态的仲裁签名方案,可以同时实现对已知和未知量子比特的签名,Li 等[22]对文献[21]中的签名方案进行了改进,提出了基于 Bell 态的量子签名方案. 文献[23]提出了两个带消息恢复的仲裁签名协议. 受经典密码学单向函数在数字签名中作用的启发,Lu 等[24]提出了一个基于量子单向函数的量子签名方案. 温晓军等[25,26]对量子签名进行了深入的研究,提出了诸如量子多重签名、量子盲签名等一些新型的量子签名方案. 另外,文献[27,28]以量子纠错码为基础构造了量子公钥算法来实现量子签名和认证.

本文提出了一种基于量子纠缠交换的仲裁签名协议. 它以 Bell 态为基础,首先将待签名信息利用幺正算符序列进行编码,通过算符序列对 Bell 态进行调制,再通过对量子信息加密产生签名. 验证者将签名信息与仲裁者通过纠缠交换所产生的关联态相结合,通过 Bell 测量来对签名的真实性进行验证. 算法利用量子加密保障了真实签名的不可伪造性,同时通过仲裁的参与结合量子密钥有效预防了双方的抵赖问题,方案还能够有效实现对通信双方隐私信息的保护.

2. 基本原理

2.1. Bell 态

由 A 和 B 两粒子序列组成的量子纠缠系统可

* 国家高技术研究发展计划(批准号: 2009AA01Z403,2009AA01Z435)资助的课题.

† E-mail: 7imei@163.com

以由以下的 4 个 Bell 态描述:

$$\begin{aligned}
|\Phi^+\rangle_{AB} &= \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}),\\
|\Phi^-\rangle_{AB} &= \frac{1}{\sqrt{2}}(|00\rangle_{AB} - |11\rangle_{AB}),\\
|\Psi^+\rangle_{AB} &= \frac{1}{\sqrt{2}}(|01\rangle_{AB} + |10\rangle_{AB}),\\
|\Psi^-\rangle_{AB} &= \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB}).
\end{aligned} \tag{1}$$

这 4 个 Bell 态可通过算符 $\boldsymbol{\sigma}_{00},\boldsymbol{\sigma}_{01},\boldsymbol{\sigma}_{10},\boldsymbol{\sigma}_{11}$ 进行局部操作相互转换. 算符 $\boldsymbol{\sigma}_{ij}(i,j\in\{0,1\})$ 以 Pauli 矩阵为基础进行构造,由以下 4 个矩阵来描述:

$$\begin{aligned}
\boldsymbol{\sigma}_{00} &= \boldsymbol{I} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\\
\boldsymbol{\sigma}_{01} &= \boldsymbol{\sigma}_x = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix},\\
\boldsymbol{\sigma}_{10} &= \mathrm{i}\boldsymbol{\sigma}_y = \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix},\\
\boldsymbol{\sigma}_{11} &= \boldsymbol{\sigma}_z = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}.
\end{aligned} \tag{2}$$

以 $|\Phi^+\rangle_{AB}$ 为例,容易验证以下关系成立:

$$\begin{aligned}
\boldsymbol{\sigma}_{00}|\Phi^+\rangle_{AB} &= |\Phi^+\rangle_{AB},\\
\boldsymbol{\sigma}_{01}|\Phi^+\rangle_{AB} &= |\Psi^+\rangle_{AB},\\
\boldsymbol{\sigma}_{10}|\Phi^+\rangle_{AB} &= |\Phi^-\rangle_{AB},\\
\boldsymbol{\sigma}_{11}|\Phi^+\rangle_{AB} &= |\Psi^-\rangle_{AB}.
\end{aligned} \tag{3}$$

2.2. 纠缠交换

纠缠交换在量子信息中起着非常重要的作用,其基本思想是将两个本来不纠缠的量子系统变成纠缠态. 下面给出量子纠缠交换的基本原理.

假设有光子 1 和光子 2 处于纠缠态 $|\Phi^+\rangle_{12}$,光子 3 和光子 4 处于纠缠态 $|\Phi^+\rangle_{34}$ 此时两对光子之间没有任何纠缠关系. 假设光子 1 和光子 3 在 Alice 手中而光子 2 和光子 4 在 Bob 手中,于是整个系统的初态为[25]

$$\begin{aligned}
|\Phi\rangle_{1234} &= |\Phi^+\rangle_{12}\otimes|\Phi^+\rangle_{34}\\
&= \frac{1}{\sqrt{2}}(|00\rangle_{34} + |11\rangle_{34})\\
&\quad\otimes\frac{1}{\sqrt{2}}(|00\rangle_{12} + |11\rangle_{12}).
\end{aligned} \tag{4}$$

如果 Alice 对手中的光子 1 和光子 3 做 Bell 基测量,那么这一测量将产生相应的谱分解和塌陷,这一过程用 4 个 Bell 态表示如下[29]:

$$\begin{aligned}
|\Phi\rangle_{1234} &= |\Phi^+\rangle_{12}\otimes|\Phi^+\rangle_{34}\\
&= \frac{1}{2}(|\Phi^+\rangle_{13}|\Phi^+\rangle_{24} + |\Phi^-\rangle_{13}|\Phi^-\rangle_{24}\\
&\quad + |\Psi^+\rangle_{13}|\Psi^+\rangle_{24} + |\Psi^-\rangle_{13}|\Psi^-\rangle_{24}),
\end{aligned} \tag{5}$$

系统将以 0.25 的概率随机塌陷到四项中的一项. 例如,在某单次测量中 Alice 的测量结果为 $|\Psi^-\rangle_{13}$,当她将这一结果告诉 Bob 时,Bob 就知道他手中的光子 2 和光子 4 已经通过关联塌陷而纠缠起来,处于 $|\Psi^-\rangle_{24}$ 态.

在上述例子中,光子 2 和光子 4 之间并没有直接的相互作用,而是 Alice 对光子 1 和光子 3 作 Bell 基测量,通过光子 1 和光子 3 的相互作用,以间接相互作用的方式纠缠起来. 如果选择 4 个 Bell 态中的任意两个作为初态,则通过纠缠交换后将得到不同的纠缠组合,如表 1[25] 所列.

3. 量子签名方案

该签名方案有三个参与方,分别是签名者 Alice、签名验证者 Bob 以及仲裁者 T. 通信双方分别与仲裁者共享一个经典密钥(因为量子存储技术在目前还不成熟),密钥由通信终端保存可长期使用. 方案由初始化、签名和验证三个过程组成.

3.1. 初 始 化

本方案假设仲裁者 T 与 Alice 共享秘密密钥 K_A,与 Bob 共享秘密密钥 K_B,秘密密钥可以通过相应的 QKD 协议(如 BB84 等)来实现. 仲裁者 T 制备两个 Bell 态序列

$$|\Phi\rangle_{AT1} = (|\Phi^+\rangle_{AT1}, |\Phi^+\rangle_{AT2},\cdots, |\Phi^+\rangle_{ATn}), \tag{6}$$

$$|\Phi\rangle_{BT2} = (|\Phi^+\rangle_{BT1}, |\Phi^+\rangle_{BT2},\cdots, |\Phi^+\rangle_{BTn}), \tag{7}$$

其中

$$\begin{aligned}
|\Phi\rangle_{ATi} &= \frac{1}{\sqrt{2}}(|00\rangle_{AT} + |11\rangle_{AT}),\\
|\Phi^+\rangle_{BTi} &= \frac{1}{\sqrt{2}}(|00\rangle_{BT} + |11\rangle_{BT}).
\end{aligned} \tag{8}$$

然后 T 将下标为 A 的粒子序列 $|A\rangle = (|A_1\rangle, |A_2\rangle,\cdots, |A_n\rangle)$ 以及下标为 B 的粒子序列 $|B\rangle = (|B_1\rangle, |B_2\rangle,\cdots, |B_n\rangle)$ 分别发送给 Alice 和 Bob,而保留下标为 T 的两个粒子序列 T_1(与 Alice 的序列 $|A\rangle$ 纠缠)和 T_2(与 Bob 的序列 $|B\rangle$ 纠缠). 仲裁者 T 制备 Bell 态序列

$$|\Phi\rangle_{A'B'} = (|\Phi^+\rangle_{AB1}, |\Phi^+\rangle_{AB2},\cdots, |\Phi^+\rangle_{ABn}), \tag{9}$$

表 1 纠缠交换塌陷态组合

初 始 态	交换后纠缠态组合
$\|\Phi^+\rangle_{12}\otimes\|\Phi^+\rangle_{34}$	$\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Phi^+\rangle_{24}+\|\Phi^-\rangle_{13}\|\Phi^-\rangle_{24}+\|\Psi^+\rangle_{13}\|\Psi^+\rangle_{24}+\|\Psi^-\rangle_{13}\|\Psi^-\rangle_{24})$
$\|\Phi^+\rangle_{12}\otimes\|\Phi^-\rangle_{34}$	$\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Phi^-\rangle_{24}+\|\Phi^-\rangle_{13}\|\Phi^+\rangle_{24}-\|\Psi^+\rangle_{13}\|\Psi^-\rangle_{24}-\|\Psi^-\rangle_{13}\|\Psi^+\rangle_{24})$
$\|\Phi^+\rangle_{12}\otimes\|\Psi^+\rangle_{34}$	$\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Psi^+\rangle_{24}+\|\Phi^-\rangle_{13}\|\Psi^-\rangle_{24}+\|\Psi^+\rangle_{13}\|\Phi^+\rangle_{24}+\|\Psi^-\rangle_{13}\|\Phi^-\rangle_{24})$
$\|\Phi^+\rangle_{12}\otimes\|\Psi^-\rangle_{34}$	$\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Psi^-\rangle_{24}+\|\Phi^-\rangle_{13}\|\Psi^+\rangle_{24}-\|\Psi^+\rangle_{13}\|\Phi^-\rangle_{24}-\|\Psi^-\rangle_{13}\|\Phi^-\rangle_{24})$
$\|\Phi^-\rangle_{12}\otimes\|\Phi^+\rangle_{34}$	$\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Phi^-\rangle_{24}+\|\Phi^-\rangle_{13}\|\Phi^+\rangle_{24}+\|\Psi^+\rangle_{13}\|\Psi^-\rangle_{24}+\|\Psi^-\rangle_{13}\|\Psi^+\rangle_{24})$
$\|\Phi^-\rangle_{12}\otimes\|\Phi^-\rangle_{34}$	$\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Phi^+\rangle_{24}+\|\Phi^-\rangle_{13}\|\Phi^-\rangle_{24}-\|\Psi^+\rangle_{13}\|\Psi^+\rangle_{24}-\|\Psi^-\rangle_{13}\|\Psi^-\rangle_{24})$
$\|\Phi^-\rangle_{12}\otimes\|\Psi^+\rangle_{34}$	$\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Psi^-\rangle_{24}+\|\Phi^-\rangle_{13}\|\Psi^+\rangle_{24}+\|\Psi^+\rangle_{13}\|\Phi^-\rangle_{24}+\|\Psi^-\rangle_{13}\|\Phi^+\rangle_{24})$
$\|\Phi^-\rangle_{12}\otimes\|\Psi^-\rangle_{34}$	$\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Psi^+\rangle_{24}+\|\Phi^-\rangle_{13}\|\Psi^-\rangle_{24}-\|\Psi^+\rangle_{13}\|\Phi^+\rangle_{24}-\|\Psi^-\rangle_{13}\|\Phi^-\rangle_{24})$
$\|\Psi^+\rangle_{12}\otimes\|\Phi^+\rangle_{34}$	$\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Psi^+\rangle_{24}-\|\Phi^-\rangle_{13}\|\Psi^-\rangle_{24}+\|\Psi^+\rangle_{13}\|\Phi^-\rangle_{24}-\|\Psi^-\rangle_{13}\|\Phi^-\rangle_{24})$
$\|\Psi^+\rangle_{12}\otimes\|\Phi^-\rangle_{34}$	$\frac{1}{2}(-\|\Phi^+\rangle_{13}\|\Psi^-\rangle_{24}+\|\Phi^-\rangle_{13}\|\Psi^+\rangle_{24}+\|\Psi^+\rangle_{13}\|\Phi^-\rangle_{24}-\|\Psi^-\rangle_{13}\|\Psi^-\rangle_{24})$
$\|\Psi^+\rangle_{12}\otimes\|\Psi^+\rangle_{34}$	$\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Phi^+\rangle_{24}-\|\Phi^-\rangle_{13}\|\Phi^-\rangle_{24}+\|\Psi^+\rangle_{13}\|\Psi^+\rangle_{24}-\|\Psi^-\rangle_{13}\|\Psi^-\rangle_{24})$
$\|\Psi^+\rangle_{12}\otimes\|\Psi^-\rangle_{34}$	$\frac{1}{2}(-\|\Phi^+\rangle_{13}\|\Phi^-\rangle_{24}+\|\Phi^-\rangle_{13}\|\Phi^+\rangle_{24}+\|\Psi^+\rangle_{13}\|\Psi^-\rangle_{24}-\|\Psi^-\rangle_{13}\|\Psi^+\rangle_{24})$
$\|\Psi^-\rangle_{12}\otimes\|\Phi^+\rangle_{34}$	$\frac{1}{2}(-\|\Phi^+\rangle_{13}\|\Psi^-\rangle_{24}+\|\Phi^-\rangle_{13}\|\Psi^+\rangle_{24}-\|\Psi^+\rangle_{13}\|\Phi^-\rangle_{24}+\|\Psi^-\rangle_{13}\|\Phi^+\rangle_{24})$
$\|\Psi^-\rangle_{12}\otimes\|\Phi^-\rangle_{34}$	$\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Psi^+\rangle_{24}-\|\Phi^-\rangle_{13}\|\Psi^-\rangle_{24}-\|\Psi^+\rangle_{13}\|\Phi^+\rangle_{24}+\|\Psi^-\rangle_{13}\|\Phi^-\rangle_{24})$
$\|\Psi^-\rangle_{12}\otimes\|\Psi^+\rangle_{34}$	$\frac{1}{2}(-\|\Phi^+\rangle_{13}\|\Phi^-\rangle_{24}+\|\Phi^-\rangle_{13}\|\Phi^+\rangle_{24}-\|\Psi^+\rangle_{13}\|\Psi^+\rangle_{24}+\|\Psi^-\rangle_{13}\|\Psi^-\rangle_{24})$
$\|\Psi^-\rangle_{12}\otimes\|\Psi^-\rangle_{34}$	$\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Phi^+\rangle_{24}-\|\Phi^-\rangle_{13}\|\Phi^-\rangle_{24}-\|\Psi^+\rangle_{13}\|\Psi^+\rangle_{24}+\|\Psi^-\rangle_{13}\|\Psi^-\rangle_{24})$

分别将 $|A'\rangle$ 和 $|B'\rangle$ 分发给 Alice 和 Bob,参与方共享一个安全的单向函数 $h:\{0,1\}^*\rightarrow\{0,1\}^{2n}$,其中上标 $2n$ 代表所生成消息摘要的长度,星号代表任意长度的二进制消息串.

在粒子分发过程中仲裁者用双方共享密钥选择调制算符对粒子进行调制,可让 0 对应算符 I 门,1 对应算符 H 门. 例如,当密钥为 10011 时选择的算符序列为(H, I, I, H, H),因为 $H^2=I^2=I$. 所以,接收端只需根据密钥选择与发送端相同的操作即可.

3.2. 签　　名

设 Alice 要签名的消息是 M,则她的签名过程由 5 个步骤组成.

步骤 1 Alice 首先计算 $h(M)$ 得到一个比特长度为 $2n$ bit 的消息串 m,然后根据 m 生成算符序列 $\Omega=(\sigma_1,\sigma_2,\cdots,\sigma_n)$,其中 $\sigma_i\in\{\sigma_{00},\sigma_{01},\sigma_{10},\sigma_{11}\}$,对应关系如下:$00\rightarrow\sigma_{00}$,$01\rightarrow\sigma_{01}$,$10\rightarrow\sigma_{10}$,$11\rightarrow\sigma_{11}$. Alice 根据 Ω 对 $|\Phi\rangle_{\mathrm{ATI}}$ 进行局域操作,将 Ω 与粒子序列 $|A\rangle$ 作用后可得

$$|A_\Omega\rangle=\Omega|A\rangle=(\sigma_1|A_1\rangle,\sigma_2|A_2\rangle,\cdots,\sigma_n|\rangle). \tag{10}$$

步骤 2 Alice 根据自己和仲裁者的共享密钥 K_{A} 对 $|A_\Omega\rangle$ 进行作用. 具体过程如下:首先根据 K_{A} 生成调制算符序列

$$U_{K_{\mathrm{A}}}=(U_1,U_2,\ldots,U_n), \tag{11}$$

当 $K_{\mathrm{A}i}=0$ 时,$U_i=\sigma_{01}$;当 $K_{\mathrm{A}i}=1$ 时 $U_i=\sigma_{11}$. 然后 Alice 利用 $U_{K_{\mathrm{A}}}$ 对 $|A_\Omega\rangle$ 进行调制后可得

$$|R_{\mathrm{A}}\rangle=U_{K_{\mathrm{A}}}|A_\Omega\rangle. \tag{12}$$

步骤 3 Alice 根据 m 选择操作算符序列对与 Bob 共享的 Bell 态序列 $|\Phi\rangle_{A'B'}$ 中自己的粒子序列 $|A'\rangle$ 进行操作. 具体过程如下:首先根据与步骤 1 相同的方法对 m 进行编码,然后用生成的算符序列选择相应的量子逻辑门对她的粒子进行操作. 这时 Alice 与 Bob 纠缠的粒子序列变为

$$|A'_\Omega\rangle=\Omega|A'\rangle=(|A'_{\Omega1}\rangle,|A'_{\Omega2}\rangle,\cdots,|A'_{\Omega n}\rangle), \tag{13}$$

其中

$$|A'_{\Omega i}\rangle=\sigma_i|A'_i\rangle.$$

步骤 4 Alice 生成签名 $|S\rangle=E_{K_{\mathrm{A}}}(|R_{\mathrm{A}}\rangle,$

$|A'_\Omega\rangle$)),这里 E_{K_A} 代表用 Alice 和仲裁者的共享密钥 K_A 加密,加密可以采用任意安全的量子加密算法.

步骤 5 Alice 将 M 量子化为 $|M\rangle$,然后将 $|M\rangle$,$|A_\Omega\rangle$ 以及 $|S\rangle$ 发送给 Bob. 目前有很多方案可以实现经典信息与量子信息的相互转换,如文献[12]中提出的方案. 如果系统中有经典辅助信道,则可以通过辅助信道将 M 直接发送给 Bob 而不用对其进行量子化操作.

3.3. 验 证

当 Bob 收到 Alice 发送过来的消息之后,他必须借助仲裁者对其真实性进行验证,验证过程由 6 个步骤组成.

步骤 1 Bob 将 $|A_\Omega\rangle$ 以及 $|S\rangle$ 用他和仲裁者的共享密钥 K_B 进行加密得到 $|Y_B\rangle = E_{K_B}(|S\rangle, |A_\Omega\rangle)$,将 $|Y_B\rangle$ 发送给仲裁者 T.

步骤 2 仲裁者 T 解密得到 $|A_\Omega\rangle$,$|R_A\rangle$ 以及 $|A'_\Omega\rangle$,然后根据 K_A 利用与签名过程中步骤 2 相同的方法对 $|A_\Omega\rangle$ 进行操作得到 $|R'_A\rangle$,比较 $|R_A\rangle$ 和 $|R'_A\rangle$ 是否相同(量子态比较可参见文献[22]的方案),如果相同则置参数 $r=1$,否则置 $r=0$.

步骤 3 仲裁者对自己与 Alice(这时 Alice 与 T 的纠缠序列为 $|A_\Omega\rangle$)和 Bob 纠缠的粒子序列 T_1 和 T_2 进行 Bell 测量. 这一测量操作将导致系统原先的纠缠关系发生相应的谱分解和塌陷,使得 $|T_1\rangle$ 和 $|T_2\rangle$ 成为 Bell 纠缠序列,而 $|A_\Omega\rangle$ 和 $|B\rangle$ 成为 Bell 纠缠序列. 这一过程可以用下式表示:

$$|\Phi_1\rangle_{AT1} \otimes |\Phi_2\rangle_{BT2} = |\Phi_3\rangle_{AB} \otimes |\Phi_4\rangle_{(T1)(T2)}, \tag{14}$$

其中 $|\Phi_i\rangle$($i=1,2,3,4$)的取值从 4 个 Bell 态中选取,$|\Phi_1\rangle_{AT1}$ 是经过签名操作后 Alice 与仲裁者 T 的 Bell 纠缠序列,它由 m 的值决定,$|\Phi_2\rangle_{BT2} = |\Phi\rangle_{BT2}$,$|\Phi_4\rangle_{(T1)(T2)}$ 是仲裁者的测量结果,$|\Phi_3\rangle_{AB}$ 是因仲裁者对 $|T_1\rangle$ 和 $|T_2\rangle$ 的测量操作通过关联塌陷而生成的纠缠序列. (14)式应满足表 1 中的对应关系.

步骤 4 仲裁者生成 $|Y_{TB}\rangle = E_{K_B}(|S\rangle, |A_\Omega\rangle, |A'_\Omega\rangle, |\Phi_4\rangle_{(T1)(T2)}, r)$,将 $|Y_{TB}\rangle$ 发送给 Bob.

步骤 5 Bob 解密 $|Y_{TB}\rangle$ 得到 $|S\rangle$,$|A_\Omega\rangle$,$|A'_\Omega\rangle$,$|\Phi_4\rangle_{(T1)(T2)}$ 以及 r 并验证 r 的值. 若 $r=0$,则 Bob 拒绝接受签名,协议终止;若 $r=1$,则进行下一步.

步骤 6 Bob 对 $|A'_\Omega\rangle$ 和 $|B'\rangle$ 进行 Bell 测量,根据测量结果可得 m,若 $m=h(M)$,则 Bob 继续对 $|A_\Omega\rangle$ 和 $|B\rangle$ 进行 Bell 测量得到 $|\Phi_3\rangle_{AB}$,根据 m 可以确定 $|\Phi_1\rangle_{AT1}$. 然后 Bob 结合 $|\Phi_2\rangle_{BT2}$ 以及 $|\Phi_4\rangle_{(T1)(T2)}$ 根据表 1 中的对应关系可以确定签名的真实性,如果满足表 1 中的逻辑关系则接受签名,否则拒绝接受签名.

4. 安全性与性能分析

4.1. 安全性分析

本文方案满足真实签名的不可伪造性、不可抵赖性以及信息传输的安全性等通用安全指标,同时还能够实现对通信双方隐私信息的保护.

4.1.1. 不可伪造性

首先讨论方案的不可伪造性. 假设攻击者 Eve 想伪造 Alice 的签名来欺骗 Bob,由以上所述可知,合法签名的形式为 $|S\rangle = E_{K_A}(|R_A\rangle, |A'_\Omega\rangle)$,因此 Eve 要想伪造成功她必须知道 Alice 的密钥 K_A,然而密钥是采用无条件安全的 QKD 协议(如 BB84 等)来实现的,因此 Eve 不可能通过窃听信道来获得密钥.

即使 Eve 能够获取 E_{K_A}(如 Alice 因管理漏洞导致密钥泄露),她仍然不能伪造合法签名,因为根据 $|S\rangle = E_{K_A}(|R_A\rangle, |A'_\Omega\rangle)$,签名除了需要 K_A 之外还需要 $|R_A\rangle$ 以及 $|A'_\Omega\rangle$. 根据(10)和(12)式可知,$|R_A\rangle$ 的计算需要 Alice 与仲裁者共享的 Bell 态序列 $|A\rangle$;而根据(13)式可知,计算 $|A'_\Omega\rangle$ 需要 Alice 和 Bob 共享的纠缠态序列 $|A'\rangle$. 如果粒子序列已经分发完成,那么 Eve 就不能得到量子态的任何有用信息,而她随机伪造的量子序列不可能与仲裁者存储的序列构成纠缠态,所以将在验证阶段的步骤 2 中被检测出来,且伪造的量子态序列不可能通过 Bell 测量而产生纠缠交换,因此(14)式也不能满足. Eve 唯一能获得这一粒子序列的方式就是在初始化阶段对 Alice 和仲裁者的量子信道进行窃听,但仲裁者在初始化阶段对粒子序列进行的调制操作使得各量子态之间呈现非正交态,所以 Eve 的窃听行为不能获取任何有用信息,而且 Alice 和仲裁者通过量子信道完整性检测很容易挫败 Eve 的窃听行为.

消息接收者 Bob 虽然能够通过对 $|B'\rangle$ 进行

Bell 测量来获得 $|A'\rangle$ 的信息,但对于 $|A'_\Omega\rangle$ 他所面临的情况和 Eve 一样,因此 Bob 也不能伪造 Alice 的合法签名.

4.1.2. 不可抵赖性

本文提出的方案具有不可抵赖性,即 Alice 不能否认她对消息 M 的签名,同样 Bob 不能否认他曾经收到 Alice 的签名. 如果 Alice 否认签名,则 Bob 可向仲裁者出示 $(M, |S\rangle)$. 下面给出仲裁者执行的操作步骤.

步骤 1 利用 K_A 来解密 $|S\rangle$ 而得到 $|R_A\rangle$ 和 $|A'_\Omega\rangle$.

步骤 2 根据 Bob 所提供的消息以及与 Alice 的共享密钥 K_A 利用与签名过程步骤 1 和步骤 2 相同的方法计算 $|R_A\rangle$.

步骤 3 根据 M 利用(13)式计算 $|A'_\Omega\rangle$.

如果步骤 2 和步骤 3 中所得到的 $|R_A\rangle$ 和 $|A'_\Omega\rangle$ 与解密 $|S\rangle$ 得到的相同,则 Alice 不能否认她的签名,因为 $|A'_\Omega\rangle$ 与消息 M 相关联,而 $|R_A\rangle$ 的计算需要 K_A 以及 M,另外签名的生成也需要 Alice 的密钥信息. 同样,仲裁者可以通过 $(M, |S\rangle, |Y_B\rangle)$ 来证明 Bob 确实收到了签名,因为根据验证过程的步骤 1 可知只有同时拥有 $|S\rangle$ 和 K_B 才能够计算 $|Y_B\rangle$.

4.1.3. 信息传输的安全性

协议执行过程中在信道上传输的信息有 $|S\rangle, |M\rangle, |A_\Omega\rangle, |Y_B\rangle$ 以及 $|Y_{TB}\rangle$, 因为 $|S\rangle, |Y_B\rangle$ 和 $|Y_{TB}\rangle$ 是加密形式,攻击者不能从中得到任何关于密钥和签名的信息,而 $|A_\Omega\rangle$ 与消息摘要 m 有关,任何对它的篡改行为将导致验证过程的步骤 2 不能通过. 签名过程的步骤 3 以及验证过程的步骤 3 所生成的消息 $|A'_\Omega\rangle$ 和 $|\Phi_4\rangle_{(T1)(T2)}$ 均是在终端生成,且分别包含在 $|S\rangle$ 和 $|Y_{TB}\rangle$ 中以加密形式传输. 因此,方案可以有效地抵御量子态纠缠攻击和特洛伊木马攻击.

4.1.4. 隐私信息的保护

以往的仲裁量子签名方案中仲裁者可以读取消息发送者的信息,这样通信双方的隐私得不到保护. 在本方案中仲裁者虽然像其他的仲裁签名方案一样参与了辅助验证过程,但是却不能得到 Alice 所发送的消息 M 的内容. 在验证过程中,仲裁者能够获得 $|A_\Omega\rangle, |R_A\rangle$ 以及 $|A'_\Omega\rangle$. 根据(10)和(13)式知, $|A_\Omega\rangle$ 和 $|A'_\Omega\rangle$ 是通过消息摘要生成的,而从消息摘要不可能推断出消息 M 的任何信息. $|R_A\rangle$ 是用于比较的参考信息,由(11)和(12)式知, $|R_A\rangle$ 是根据密钥和消息摘要生成的,从中也不能获得 M 的任何信息. Alice 和 Bob 通过量子信道完整性检测技术很容易检测出窃听行为,因此该签名方案能够有效地保护通信双方的隐私信息.

4.2. 性能分析

分析量子签名协议的性能时,一方面要考虑对比特消息签名时需要传输的量子比特数和经典比特数,另一方面还需考虑签名和验证过程中的复杂度,包括量子态的制备、量子态的测量以及量子态的比较等操作.

Wang 等[30]在研究量子签名方案的性能时提出了如下计算量子签名效率 η 的度量公式:

$$\eta = \frac{|M|}{Q_t + C_t}, \tag{15}$$

其中 $|M|$ 表示签名消息的长度, Q_t 表示协议中传输的量子比特数, C_t 表示协议中传输的经典比特数, $Q_t + C_t$ 就是为了传输长度为 $|M|$ 的签名信息所需传输的总比特数. (15)式的本质就是计算签名信息在传输的总信息中所占的比例.

下面对 $|M|$ bit 长度的消息进行签名时所需要传输的量子比特数和经典比特数为指标来比较现有的几种量子签名方案的效率. 根据(15)式可计算出文献[19,23,24]中签名方案的效率分别是 9%, 11%, 11%, 文献[29]在上述基础上将签名效率进一步提高到 16%, 而文献[20]方案的签名效率为

$$\eta = \frac{|M|}{|M| + N|M|},$$

其中 N 是每对一个比特签名所需验证的公钥数,可见该方案的效率也不是很高(最高不会超过 50%). 本文提出的方案一个重要特点就是所需共享的密钥长度是固定值而与待签名消息的长度无关,因此可以显著提高效率. 下面对本文签名方案的效率进行分析.

在本文的方案中,对 $|M|$ bit 长度的消息进行签名所需传输的信息如下:签名过程的信息包括 $|A_\Omega\rangle$ (长度为 $2n$ bit)、$|S\rangle$ (长度为 $4n$ bit)以及 $|M|$ bit 的签名消息 $|M\rangle$ (或者经典信息 M);验证过程的信息包括给仲裁者所发送的信息 $|Y_B\rangle = E_{K_B}(|S\rangle, |A_\Omega\rangle)$ (长度为 $6n$ bit)、仲裁者回复的信息 $|Y_{TB}\rangle = E_{K_B}(|S\rangle, |A_\Omega\rangle, |A'_\Omega\rangle, |\Phi_4\rangle_{(T1)(T2)}, r)$ (长度为 $(10n+1)$ bit).

根据(15)式,可以计算出本文签名方案的效

率为

$$\eta = \frac{|M|}{|M| + 22n + 1},$$

其中 n 与所选定的 Hash 函数(输出值固定为 $2n$ bit)有关,如选用 MD5 算法对待签名信息进行摘要计算时 $n=64$,而选用 SHA-1 算法时得到 $n=80$. 一般而言,相对于签名消息的长度 $|M|$,n 是一个很小的值. 例如,我们对 512 bit 的消息(在实际应用中属于很短的消息)进行签名,假设 $n=80$,那么本文方案的效率为 22.5%,而对 1 kbit 的消息和 2 kbit 的消息进行签名则签名效率分别提高到 36.8% 和 53.8%,签名效率随着待签名消息的长度增加而提高. 由此可知,与其他方案相比本文方案在一般情况下具有较高的效率.

影响量子密码方案性能的还有量子测量、量子比较及量子态制备等因素. 文献[19,21,23]都使用了 GHZ 态,相对与 Bell 态,GHZ 态制备的复杂度较高[31,32]. 另外,文献[19]方案共需要 4 次量子测量和 1 次量子态比较,文献[22]的方案在签名过程中签名方对 GHZ 粒子执行 1 次测量,在验证过程中仲裁和验证方同样各自进行了 1 次 GHZ 粒子的测量和 1 次量子态比较,共需要 3 次测量和 1 次比较操作. 文献[22]提出的针对文献[21]的改进方案虽然不需要 GHZ 三重态,但是仍然需要 3 次量子测量(签名过程 1 次,验证过程 2 次)和 1 次量子态比较(在验证过程执行). 相比较而言,本文方案在签名过程中不需要进行量子态测量,只需在验证过程的步骤 3 和步骤 6 中各进行 1 次量子态测量,在步骤 2 中进行 1 次量子态比较,因此共需进行 2 次量子测量和 1 次量子态比较操作,因而在方案的复杂度方面有所降低.

5. 结 论

传统的仲裁签名方案在验证过程中仲裁者容易得到通信双方的信息,因此通信双方的隐私得不到有效保护,针对这一情况本文以 Bell 态为基础结合量子纠缠交换的思想提出了一种仲裁量子签名方案. 本文方案利用幺正算符序列对消息进行编码,通过算符序列对 Bell 态进行调制,再通过对量子信息加密产生签名. 验证者将签名信息与仲裁者通过纠缠交换所产生的关联态相结合,通过 Bell 测量来对签名的真实性进行验证. 算法利用量子加密保障了真实签名的不可伪造性,同时通过仲裁者的参与结合量子密钥有效预防了双方的抵赖问题. 方案还能够有效实现对通信双方隐私信息的保护.

[1] Gisin N, Ribordy G, Tittel W, Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[2] Bennett C H, Braasard G 1984 *Proc. IEEE Int. Conf. Comp. Sys. Sig. Proc.* (New York: IEEE Press) p175

[3] Bennett C H, Brassard G, Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[4] Lin Q Q, Wang F Q, Mi J R, Liang R S, Liu S H 2007 *Acta Phys. Sin.* **56** 5796 (in Chinese)[林青群、王发强、米景隆、梁瑞生、刘颂豪 2007 物理学报 **56** 5796]

[5] Deng F G, Long G L 2003 *Phys. Rev.* A **68** 042315

[6] Ma H Q, Li Y L, Zhao H, Wu L A 2005 *Acta Phys. Sin.* **54** 5014 (in Chinese)[马海强、李亚玲、赵 环、吴令安 2005 物理学报 **54** 5014]

[7] Yang L, Wu L A, Liu S H 2002 *Acta Phys. Sin.* **51** 2446 (in Chinese)[杨 理、吴令安、刘颂豪 2002 物理学报 **51** 2446]

[8] Zhou R N, Wang L J, Ding J, Gong L H, Zuo X W 2010 *Int. J. Theory Phys.* **49** 2035

[9] Gao T, Yah F L, Wang Z X 2005 *Chin. Phys.* **14** 893

[10] Chen X B, Wen Q Y, Sun Z X, Shangguan L Y, Yang Y X 2010 *Chin. Phys.* B **19** 010303

[11] Waks E, Inoue K, Santori C 2002 *Nature* **420** 762

[12] Zeng G H 2004 *Chin. J. Electron.* **13** 651

[13] Yang Y G, Wen Q Y, Zhu F C 2007 *Sci. China* G **50** 331

[14] Sun Y, Du J Z, Qin S J, Wen Q Y, Zhu F C 2008 *Acta Phys. Sin.* **57** 4689 (in Chinese)[孙 莹、杜建忠、秦素娟、温巧燕、朱甫臣 2008 物理学报 **57** 4689]

[15] Liu Y, Zhang B B 2010 *Chin. Phys.* B **19** 010312

[16] Yang Y G, Cao W F, Wen Q Y 2010 *Chin. Phys.* B **19** 050306

[17] Yang Y G, Wen Q Y, Zhang X 2008 *Sci. China* G **51** 321

[18] He G Q, Zeng G H 2005 *Chin. Phys.* **14** 371

[19] Zeng G H, Ma W P, Wang X M 2001 *Acta Electron. Sin.* **29** 1098 (in Chinese)[曾贵华、马文平、王新梅 2001 电子学报 **29** 1098]

[20] Gottesman D, Chuang I 2001 *J. ACM* **48** 351

[21] Zeng G, Christoph K 2002 *Phys. Rev.* A **65** 042312

[22] Li Q, Chan W H, Long D Y 2009 *Phys. Rev.* A **79** 054307

[23] Lee H, Hong C, Kim H 2004 *Phys. Lett.* A **321** 295

[24] Lu X, Feng D G 2004 *LNCS* **3314** 1054

[25] Wen X J, Liu Y 2007 *Acta Electron. Sin.* **35** 1079 (in Chinese)[温晓军、刘 云 2007 电子学报 **35** 1079]

[26] Wen X J, Tian Y, Niu X M 2010 *Acta Electron. Sin.* **38** 720 (in Chinese)[温晓军、田 原、牛夏牧 2010 电子学报 **38** 720]

[27] Li Z, Xing L J 2007 *Acta Phys. Sin.* **56** 5602 (in Chinese)[李卓、邢莉娟 2007 物理学报 **56** 5602]
[28] Li Z, Xing L J 2008 *Acta Phys. Sin.* **57** 28 (in Chinese)[李卓、邢莉娟 2008 物理学报 **57** 28]
[29] Horodecki R, Horodecki P, Horodecki M, Horodecki K 2009 *Rev. Mod. Phys.* **81** 865
[30] Wang J, Zhang Q, Tang C J 2006 *Optoelectron. Lett.* **2** 209
[31] Chen X D, Gu Y J, Liang H H, Ni B B, Liu X M 2010 *Chin. Phys.* B **19** 040310
[32] Hu X Y, Gu Y, Gong Q H, Guo G C 2010 *Chin. Phys.* B **19** 050305

Arbitrated quantum signature scheme based on entanglement swapping*

Li Wei† Fan Ming-Yu Wang Guang-Wei
(*School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu* 610054, *China*)
(Received 17 October 2010; revised manuscript received 27 December 2010)

Abstract

An arbitrated quantum signature scheme based on entanglement swapping is proposed in this paper. On the foundation of Bell states, the message to be signed is coded with a unitary sequence, and consequently the unitary sequence is used to calibrate the Bell states between the signer and the arbitrator, finally the signature is generated through quantum cryptography. Using the correlation states generated through entanglement swapping on the arbitrator's side, the receiver can verify the signature through Bell measurement on his own side. In this scheme, anyone except the authentic signer cannot forge a legal signature and the true receiver cannot deny his recipient because the security of underling quantum cryptography and the participants' privacy are effectively protected in this scheme.

Keywords: quantum cryptography, quantum signature, entanglement swapping
PACS: 03.67.Dd, 03.67.Hk

* Project supported by the National High Technology Research and Development Program of China (Grant Nos. 2009AA01Z403, 2009AA01Z435).
† E-mail: 7imei@163.com