基于纠缠交换的量子信息签名方案

温晓军　　刘　云　　张振江
(北京交通大学电子信息工程学院　北京　100044)

摘　要：该文提出了一种利用纠缠粒子对交换的量子信息签名方案。在该签名方案中，Alice 根据消息的编码对自己的纠缠粒子对作一局域操作，在与系统管理员及 Bob 进行粒子对交换后测量的结果即为消息的签名，Bob 根据三方测量结果可以验证签名。该方案具有绝对的安全性，可以应用在量子通信网络中，同时还具有量子身份认证的功能，并且在现有技术条件上完全能够实现。

关键词：量子信息签名，纠缠交换，签名方案
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2005)05-0811-03

Signature Scheme Based on Qantum Entanglement Swapping

Wen Xiao-jun　　Liu Yun　　Zhang Zhen-jiang
(*School of Electronic Information Engineering*, *Beijing Jiaotong University*, *Beijing* 100044, *China*)

Abstract　In this paper, an quantum signature scheme is presented which based on the entanglement swapping. In this scheme, Alice performs a local unitary operation on her two qubits according to message code, after swapping qubits with administrator and Bob, Alice gets the signature by measure her qubits, Bob can verify signature via the measurement outcomes of three sides. This scheme is secure absolutely, it can be applied in a quantum communication network, as well as quantum identification, and it is easy to realize by the present-day technologies.

Key words　Quantum signature,　Entanglement swapping,　Signature scheme

1　引言

自 Bennett 和 Brassard 提出 BB84 协议以来，量子密钥分配被证明是安全的并且在实验上取得了成功[1]，量子计算机也进入了实验阶段[2]，这标志着不久量子计算机将代替电子计算机。基于计算复杂度的传统密码学也将被量子密码术所替代，保密通信与密码学将进入一个崭新的领域。

量子密钥分配技术(Quantum Key Distribution，QKD)被证明是绝对安全的，但如何保证量子信息的安全、真实性是目前量子密码学界的热点问题，量子秘密共享(Quantum Secret Sharing，QSS)[3]，量子安全直接通信(Quantum Secure Direct Communication，QSDC)[4]是目前较为成熟的方案。与经典密码学一样，量子保密通信也一定会涉及量子信息签名问题，正如在现实生活中，签名是一件非常重要的事情。文献[5]首次研究了基于 GHZ(Greenberger-Horne-Zeilinger)三重态粒子的量子信息签名方案，然而 GHZ 三重态粒子的制备、存储、测量技术在当前实现起来有很大的难度，本文提出了一种基于纠缠粒子对交换(Entanglement Swapping)[6]和 Bell 基测量的量子信息签名方案，1998 年第一个纠缠交换得到实验实现[2]。因此，就目前的技术而言本文提出的量子信息签名方案是不难实现的。

经典的数字签名包括两类：真实签名(True signature)和仲裁签名(Arbitrated signature)。在真实签名中，实现过程不依赖于仲裁，只在有争议的时候才需要。而在仲裁签名中，实现过程需要仲裁的参与。本文提出的基于纠缠粒子对交换的方案属于仲裁签名，它需要一个可信当局 TA(Trusted Authority，相当于通信网络中的系统管理员)参与签名过程。

2　基本原理

定义 4 个 Bell 态：

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

2004-10-08 收到，2005-01-21 改回

对处于 4 个 Bell 态中的量子位 1 进行如下 4 种局域操作

$$\left.\begin{aligned}\sigma_{00}=I=\begin{bmatrix}1&0\\0&1\end{bmatrix},\quad \sigma_{01}=\sigma_x=\begin{bmatrix}0&1\\1&0\end{bmatrix}\\ \sigma_{01}=i\sigma_y=\begin{bmatrix}0&1\\-1&0\end{bmatrix},\quad \sigma_{11}=\sigma_z=\begin{bmatrix}1&1\\0&-1\end{bmatrix}\end{aligned}\right\} \tag{2}$$

对$\left|\psi^-\right\rangle$态我们进行 4 种局域操作的结果如下：

$$\left.\begin{aligned}\sigma_{00}\left|\Psi^-\right\rangle=\left|\Psi^-\right\rangle,\quad \sigma_{01}\left|\Psi^-\right\rangle=\left|\Phi^-\right\rangle\\ \sigma_{10}\left|\Psi^-\right\rangle=\left|\Phi^+\right\rangle,\quad \sigma_{11}\left|\Psi^-\right\rangle=\left|\Psi^+\right\rangle\end{aligned}\right\} \tag{3}$$

这 4 种局域操作可以编码为 $\sigma_{00}\leftrightarrow$ ‘00’，$\sigma_{01}\leftrightarrow$ ‘01’，$\sigma_{10}\leftrightarrow$ ‘10’，$\sigma_{11}\leftrightarrow$ ‘11’。

假设 AB 为一对纠缠粒子，CD 为另一对纠缠粒子，它们均处与$\left|\Psi^-\right\rangle$态，如果先将 AB 进行局域操作后再与 CD 交换测量，这一过程的表达式如下[7]：

$$\left(\sigma_{00}\left|\Psi_{AB}^-\right\rangle\right)\otimes\left|\Psi_{CD}^-\right\rangle=\left|\Psi_{AB}^-\right\rangle\otimes\left|\Psi_{CD}^-\right\rangle$$
$$=\frac{1}{2}\left(\left|\Psi_{AC}^-\right\rangle\left|\Psi_{BD}^-\right\rangle-\left|\Phi_{AC}^-\right\rangle\left|\Phi_{BD}^+\right\rangle-\left|\Psi_{AC}^+\right\rangle\left|\Psi_{BD}^+\right\rangle+\left|\Phi_{AC}^-\right\rangle\left|\Phi_{BD}^-\right\rangle\right) \tag{4}$$

$$\left(\sigma_{01}\left|\Psi_{AB}^-\right\rangle\right)\otimes\left|\Psi_{CD}^-\right\rangle=\left|\Phi_{AB}^-\right\rangle\otimes\left|\Psi_{CD}^-\right\rangle$$
$$=\frac{1}{2}\left(\left|\Phi_{AC}^+\right\rangle\left|\Psi_{BD}^+\right\rangle+\left|\Phi_{AC}^+\right\rangle\left|\Psi_{BD}^-\right\rangle-\left|\Psi_{AC}^+\right\rangle\left|\Phi_{BD}^+\right\rangle-\left|\Psi_{AC}^-\right\rangle\left|\Phi_{BD}^-\right\rangle\right) \tag{5}$$

$$\left(\sigma_{10}\left|\Psi_{AB}^-\right\rangle\right)\otimes\left|\Psi_{CD}^-\right\rangle=\left|\Phi_{AB}^-\right\rangle\otimes\left|\Psi_{CD}^-\right\rangle$$
$$=\frac{1}{2}\left(\left|\Phi_{AC}^+\right\rangle\left|\Psi_{BD}^+\right\rangle-\left|\Psi_{AC}^+\right\rangle\left|\Phi_{BD}^-\right\rangle-\left|\Psi_{AC}^-\right\rangle\left|\Phi_{BD}^+\right\rangle+\left|\Psi_{AC}^-\right\rangle\left|\Phi_{BD}^-\right\rangle\right) \tag{6}$$

$$\left(\sigma_{11}\left|\Psi_{AB}^-\right\rangle\right)\otimes\left|\Psi_{CD}^-\right\rangle=\left|\Psi_{AB}^+\right\rangle\otimes\left|\Psi_{CD}^-\right\rangle$$
$$=\frac{1}{2}\left(\left|\Psi_{AC}^+\right\rangle\left|\Psi_{BD}^+\right\rangle-\left|\Psi_{AC}^-\right\rangle\left|\Psi_{BD}^+\right\rangle-\left|\Phi_{AC}^+\right\rangle\left|\Phi_{BD}^-\right\rangle+\left|\Phi_{AC}^-\right\rangle\left|\Phi_{BD}^+\right\rangle\right) \tag{7}$$

通信三方（Alice, Bob, Charlie）粒子交换过程如下：假设 Alice, Bob, Charlie 各自准备两纠缠态粒子并处于同一 Bell 态，分别表示为 $\left|\Psi^-\right\rangle$，$\left|\Psi_{CD}^-\right\rangle$，$\left|\Psi_{EF}^-\right\rangle$，然后他们各自把第 1 个粒子留给自己，把第 2 个粒子按照顺序 Alice→ Bob→ Charlie→Alice 发送给下一个人，使得 3 个人最后粒子为 Alice(A, F), Bob(B, C)，Charlie(D, E)。

Alice 根据编码对自己粒子(A, F)作一局域操作，然后用 Bell 基测量，并宣布其结果。例如$\left|\Psi_{AF}^+\right\rangle$，根据式(4) – (7)，光有这一结果还无法推断 Alice 采用了哪一种局域操作。Bob 和 Charlie 也分别用 Bell 基测量各自的粒子(B, C)和(D, E)，Bob 和 Charlie 通过合并他们的结果能够推断出 Alice 使用了哪一种局域操作，从而翻译出 Alice 需要传递的信息编码。例如：假设 Bob 测量结果为$\left|\Psi_{BC}^-\right\rangle$ 和 Charlie$\left|\Phi_{DE}^+\right\rangle$，根据式(6)可知在 Alice 对($A$, F)做 Bell 基测量后，粒子(B, E)的结果为$\left|\Phi_{BE}^+\right\rangle$，再结合 Alice 局域操作后的测量结果$\left|\Psi_{AF}^+\right\rangle$，根据式(5)可以知道 Alice 进行了 σ_{01} 变换，从而翻译出 Alice 要传递的信息为 ‘01’。

3 签名算法描述

3.1 初始化

(1) Alice 和 Bob 各自向系统管理员 TA 申请密钥 K_a ,K_b, K_a 和 K_b 可以通过量子密钥分配的方法来获得，如著名的 BB84 协议就是被证明具有无条件安全性并且简单而易实现。

(2) Alice，Bob 和 TA 各制备 N 对处于同一 Bell 态Ψ^- 的纠缠粒子对，记为 $\left\{\Psi(1)_{AB}^-,\Psi(1)_{CD}^-,\Psi(1)_{EF}^-\right\}$，$\left\{\Psi(2)_{AB}^-,\Psi(2)_{CD}^-,\Psi(2)_{EF}^-\right\},\cdots,\left\{\Psi(N)_{AB}^-,\Psi(N)_{CD}^-,\Psi(N)_{EF}^-\right\}$。

(3) Alice 将要发送的消息 M 转化为量子比特串 $\{M(1),M(2),\cdots,M(N)\}$，其中每一 $M(i)$ 对应 2 个量子比特，根据局域操作的编码规则，每一 $M(i)$ 对应一个局域操作 $\sigma(i)$，例如“011011”对应操作 $\sigma_{01}\sigma_{10}\sigma_{11}$。

3.2 签名过程

(1) Alice 根据 $M(i)$ 的局域操作编码对$\Psi(i)_{AB}^-$ 实施 $\sigma(i)$ 操作；

(2) 三方按照规则交换粒子，交换后结果为 Alice 粒子为(A, F)，Bob 粒子为(B, C)，TA 粒子为(D, E)；

(3) Alice 对(A, F)粒子用 Bell 基测量，将测量结果记为 $R(i)_{AF}$；

(4) Alice 获得签名。用 K_a 加密 $R(i)_{AF}$ 得到 $S_a(i)=K_a(R(i)_{AF})$，$S_a(i)$ 即为量子消息 $M(i)$ 的签名；

(5) Alice 将($M(i)$，$S_a(i)$)发送给 TA。

3.3 验签过程

验签过程需要管理员 TA 的参与，以下步骤实现验签过程。

(1) TA 收到 Alice 发送过来的签名 $S_a(i)$ 后，用 K_a 解密出 $R(i)_{AF}$；

(2) TA 对自己的粒子对(D, E)用 Bell 基测量，将测量结果记为 $R(i)_{DE}$；

(3) TA 用 K_b 加密 $R(i)_{AF}$ 及 $R(i)_{DE}$，记为 $y_{TA}=K_b(R(i)_{AF},R(i)_{DE})$，再将 y_{TA} 发送给 Bob；

(4) Bob 收到 y_{TA} 后，用 K_b 解密 y_{TA} 得到 $R(i)_{AF}$ 及 $R(i)_{DE}$；

(5) Bob 对自己的粒子对(B, C)用 Bell 基测量，测量结果记为 $R(i)_{BC}$；

(6) Bob 根据 $R(i)_{AF}$， $R(i)_{DE}$ 及 $R(i)_{BC}$ 可以推断出 Alice 实行的局域操作 $\sigma(i)$，再根据编码规则编译出 $M(i)$；

(7) 重复以上步骤，合并编译出的量子比特 $M'=\{M(1),M(2),\cdots,M(N)\}$, 若 $M'=M$, 则确认 $S_a=\{S_a(1),S_a(2),\cdots,S_a(N)\}$ 为消息 M 的有效签名。

4　安全性分析

对签名方案的攻击包括经典攻击策略与量子攻击策略。我们首先从信息签名应具有的特性来分析本方案的抵制经典攻击的安全性，然后再从量子特性来分析本方案对付量子攻击的安全性。

4.1　经典安全性

(1) 签名是可信的，任何人都可以验证签名的有效性。Bob 根据三方测量自己粒子对的结果就可以推断出签名是否有效。

(2) 签名是不可伪造的，除了合法的签名者之外，任何其他人伪造签名是困难的。在本方案中，签名者 Alice 必须拥有向系统管理员 TA 申请的密钥 K_a 才能发送签名，所以对手 Eve 是不能伪造签名的。

(3) 签名是不能复制和被篡改的，不能复制是指对一个消息的签名不能通过复制变为另一个消息的签名。

Eve 的攻击方案中有一种截获/重发方案，他将包含签名的信息截获后复制一份或者修改后发送给 TA，留下一份供自己分析。但 Eve 没有 Alice 与 TA 的共享密钥 K_a，因此 Eve 的截获/重发方案是不可能成功的。而且在本方案中签名的发送、接收以及纠缠粒子对的测量都是通信三方根据协议同步进行的，被复制的签名在其他的通信过程中是无效的。

(4) 签名是不可抵赖的，签名者事后不能否认自己的签名。

Alice 不可能抵赖，因为签名 S_a 中包含了她的密钥，而且 Bob 收到签名通过了系统管理员 TA 的帮助，有了系统管理员，不仅 Alice 不能否认自己的签名，Bob 也不能否认收到了签名。

4.2　量子安全性

量子的不可克隆原理保证了量子信息是不能被复制的，如果 Eve 采取截获/重发方案，他对 Alice 的粒子进行克隆，但这势必对签名信息产生扰动，签名信息将被拒绝，同时系统将检测到窃听者的存在。

还可以用以下方法来检查量子信道的安全性，下面步骤以 Alice ↔ Bob 的通信信道为例，Alice ↔ TA，TA↔ Bob 的量子信道的安全性检测方法相同。

(1) Alice 随机选择两套测量基，$\chi_z=\{|1\rangle,|0\rangle\}$ 和 $\chi_x=\{|+\rangle,|-\rangle\}$ 来测量粒子 1；

(2) Alice 公开宣布她的测量基和测量结果；

(3) Bob 采用与 Alice 相同的测量基测量粒子 2，如果没有 Eve 的存在，两者的测量结果正好相反。例如 Alice 的测量结果为 $|1\rangle$ 则 Bob 的结果为 $|0\rangle$，若测量结果为 $|+\rangle$ 则 Bob 的结果为 $|-\rangle$；

(4) 如果测量结果没有相干性，则量子信道中可能存在窃听。通信各方测量 n 对 EPR 粒子，如果没有相干性的粒子对数为 m，当 $c=m/n$ 超过一定的阈值则放弃本次通信。

5　结束语

本文提出了利用纠缠粒子对交换的量子信息签名方案。本签名方案需要系统管理员参与，发送方 Alice 根据消息 M 的编码对自己的纠缠粒子对作一局域操作，然后再与系统管理员 TA 及接收方 Bob 进行粒子对交换，交换粒子后 Alice 的测量结果即为消息 M 的签名，TA 与 Bob 根据自己的粒子的测量结果可以验证签名。

像量子密钥分配(QKD)一样，量子签名具有经典数字签名所无法比拟的安全性。该方案可以应用在量子通信网络中，同时还具有量子身份认证的功能，并且在现有技术条件上完全能够实现。

参 考 文 献

[1] Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 2000, 85(7): 441 – 444 .

[2] 张镇九. 量子计算机进入实验阶段. 计算机工程, 1999, 25(1): 3 – 8.

[3] Hillery M, Buzek V, Berthiaume A. Quantum secret sharing. *Phys. Rev. A*, 1999, 59(3): 1829 – 1834.

[4] Beige A, *et al*.. Secure communication with a publicly known key. http://arxiv.org/abs/quant-ph/0111106 2001-11-20.

[5] 曾贵华, 马文平, 王新梅, 诸鸿文. 基于量子密码的签名方案. 电子学报, 2001, 29(8): 1098 – 1100.

[6] Zukowski M, *et al*.. Event-ready-detectors Bell experiment via entanglement swapping[J]. *Phys. Rev. Lett.*, 1993, 71(26): 4287 – 4290.

[7] Man Zhongxiao, Zhang Zhanjun. Multiparty quantum secret sharing based on entanglement swapping and local operation. http://arxiv.org/abs/quant-ph/0406103 2004-6-23.

温晓军：　男，1971 年生，博士生，主要研究方向为信息网络技术与信息安全.

刘　云：　女，1955 年生，教授，主要研究方向为计算机网络.

张振江：　男，1973 年生，博士生，主要研究方向为 IP 网多媒体.