doi:10.11959/j.issn.1000-436x.2016028

# 基于量子纠缠的盲签名方案

梁建武，王晓慧，郭迎，程资
（中南大学信息科学与工程学院，湖南 长沙 410083）

**摘 要：**基于量子纠缠交换的原理，提出了一种基于量子纠缠的盲签名方案。制备后的 EPR 纠缠粒子通过 EPR 纠缠交换，变化为全新的纠缠态。对新量子态的测量可以作为签名者和测量者的签名、测量依据，实现了量子通信、盲签及验证。不同于基于数学求解困难性的经典盲签名，本方案保证了消息对签名者的匿名性和方案的无条件安全性。

**关键词：**量子信息；量子签名；盲签名；量子纠缠
**中图分类号：**TN918.1 **文献标识码：**A

# Blind signature scheme based on entangled quantum

LIANG Jian-wu, WANG Xiao-hui, GUO Ying, CHENG Zi
(Institute of Information Science and Engineering, Central South Uni ersity, Changsha 410083,China)

**Abstract:** Based on the principle of quantum entanglement swapping, a blind signature scheme based on quantum entanglement was proposed. Through being entangled and exchanged, particles prepared before could transform into entangled state. The measurements of new entangled particles complete signature and verification and realize the quantum communication, blind signature and verification. Different from the classical blind signatures which based on the mathematics difficulty, the scheme could guarantee not only the anonymity but also the unconditionally security.

**Key words:** quantum information, quantum signature, blind signature, entangled quantum

## 1 引言

1983 年，Chaum 第一次提出了盲签名的概念。盲签名指签名者并不知道所签文件或消息的具体内容，而文件或消息的拥有者可以得到签名者的签名[1,2]。由于消息对签名者来说是未知的，盲签名技术在电子选举、电子现金等要求保护用户匿名性的场合得到广泛应用[3]。

在量子计算机出现以后，基于数学复杂性的盲签名将会被轻易攻破。而基于量子物理特性的量子签名方案具有无条件安全性，随着量子信息安全技术在实验上不断取得成功，对量子签名方案的研究引起了人们的浓厚兴趣。2001 年，Gottesman 和 Chuang[4]提出了基于量子单向函数的签名方案。同年，曾贵华等[5]提出了 GHZ 三粒子态相干特性的仲裁量子签名方案。上述 2 个方案签名和验证的过程都需要借助可信任的第三方才可以实现。随后，温晓军等[6]利用 EPR 粒子的纠缠特性和隐形传态的特点提出 2 个不需要仲裁的量子签名协议，以及基于纠缠交换的量子有序多重签名方案[7]。2009 年，温晓军等[8]提出了一个基于量子密码术的弱盲签名。2010 年，温晓军等[9]一种基于秘密共享的量子强盲签名协议。2011 年，陈永志等[10]在此基础上提出了一个基于可控形态的代理弱盲签名方案。本文考虑到盲签名的广泛用途，基于量子纠缠交换原理设计了一个签名方案，可以用于保护用户匿名性的系统。

## 2 基本原理

纠缠光子对的研究取得了一定的成果，并可以

**收稿日期：**2015-02-03；**修回日期：**2015-08-25
**基金项目：**国家自然科学基金资助项目（No.11379153）
**Foundation Item:** The National Natural Science Foundation of China (No.11379153)

在实验中实现。已知 Bell 的 4 个态由式(1)~式(4)给出。

$$|F^{+}\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle) \tag{1}$$

$$|F^{-}\rangle=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle) \tag{2}$$

$$|j^{+}\rangle=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle) \tag{3}$$

$$|j^{-}\rangle=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle) \tag{4}$$

对$|j^{-}\rangle$的第一个量子比特进行 4 种局域操作，可以得到表 1 中所述的关系。

**表 1　　逻辑操作及状态变化**

| 初始态 | 量子门 | 逻辑作用 | 新的态 |
|---|---|---|---|
| $\|j^{-}\rangle$ | $I$ | $I\|0\rangle=\|0\rangle; I\|1\rangle=\|1\rangle$ | $\|j^{-}\rangle$ |
| $\|j^{-}\rangle$ | $X$ | $X\|0\rangle=\|1\rangle; X\|1\rangle=\|0\rangle$ | $\|F^{-}\rangle$ |
| $\|j^{-}\rangle$ | $Z$ | $Z\|0\rangle=\|0\rangle; Z\|1\rangle=-\|1\rangle$ | $\|F^{+}\rangle$ |
| $\|j^{-}\rangle$ | $Y$ | $Y\|0\rangle=-\|1\rangle; Y\|1\rangle=\|0\rangle$ | $\|j^{+}\rangle$ |

假设 AB 为一对 EPR 纠缠光子对，CD 为另一对 EPR 纠缠光子对，分别表示如下

$$|j^{-}_{AB}\rangle=\frac{1}{\sqrt{2}}(|01\rangle_{AB}-|10\rangle_{AB}) \tag{5}$$

$$|j^{-}_{CD}\rangle=\frac{1}{\sqrt{2}}(|01\rangle_{CD}-|10\rangle_{CD}) \tag{6}$$

对 AB 纠缠光子对的第一个量子比特进行上述 4 种局域操作中的某一种逻辑操作后可能得到$|j^{-}_{AB}\rangle$、$|F^{-}_{AB}\rangle$、$|F^{+}_{AB}\rangle$、$|j^{+}_{AB}\rangle$中某一态，之后新得到的态再与 CD 纠缠光子对交换测量，那么交换过程的表达式如下

$$|j^{-}_{AB}\rangle\otimes|j^{-}_{CD}\rangle=\frac{1}{2}(|j^{-}_{AC}\rangle|j^{-}_{BD}\rangle-|F^{+}_{AC}\rangle|F^{+}_{BD}\rangle-|j^{+}_{AC}\rangle|j^{+}_{BD}\rangle+|F^{-}_{AC}\rangle|F^{-}_{BD}\rangle) \tag{7}$$

$$|F^{-}_{AB}\rangle\otimes|j^{-}_{CD}\rangle=\frac{1}{2}(|j^{-}_{AC}\rangle|F^{-}_{BD}\rangle-|j^{+}_{AC}\rangle|F^{+}_{BD}\rangle+|F^{+}_{AC}\rangle|j^{+}_{BD}\rangle+|F^{-}_{AC}\rangle|j^{-}_{BD}\rangle) \tag{8}$$

$$|F^{+}_{AB}\rangle\otimes|j^{-}_{CD}\rangle=\frac{1}{2}(|F^{-}_{AC}\rangle|j^{+}_{BD}\rangle-|j^{+}_{AC}\rangle|F^{+}_{BD}\rangle-|j^{+}_{AC}\rangle|F^{+}_{BD}\rangle+|F^{+}_{AC}\rangle|j^{-}_{BD}\rangle) \tag{9}$$

$$|j^{+}_{AB}\rangle\otimes|j^{-}_{CD}\rangle=\frac{1}{2}(|j^{+}_{AC}\rangle|j^{-}_{BD}\rangle-|F^{+}_{AC}\rangle|F^{-}_{BD}\rangle-|j^{-}_{AC}\rangle|j^{+}_{BD}\rangle+|F^{-}_{AC}\rangle|F^{+}_{BD}\rangle) \tag{10}$$

假设 Alice、Bob 和 Charlie 是参与通信的三方，Alice、Bob 和 Charlie 各自拥有处于纠缠态$|j^{-}\rangle$的光子对，其中，Alice 拥有光子 A、B，Bob 拥有光子 C、D，而 Charlie 拥有光子 E、F。Alice 在采取某种逻辑操作后，将纠缠光子中的一个粒子保留，剩下的一个光子发送给 Bob。Bob 和 Charlie 也重复同样的动作，保留一个粒子，将剩下的一个粒子发送给 Charlie 和 Alice。最后使 Alice 手中持有光子 A、F，Bob 持有光子 B、C，而 Charlie 持有光子 D、E。具体交换过程如图 1 所示，交换结果如图 2 所示。

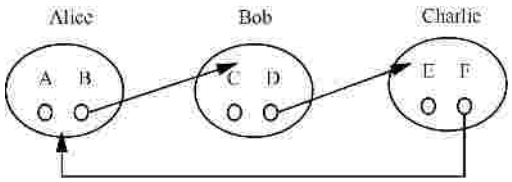


图 1　纠缠光子交换示意

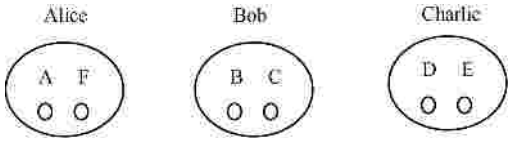


图 2　纠缠光子交换结果

交换之后，Alice 用 Bell 基测量自己手上的光子 A、F。根据量子纠缠交换原理，Alice 的测量将产生响应的普分解和塌缩，光子 B、E 将瞬间塌缩成为某一个 Bell 态。过程表示为

$$Bell_{AB}\otimes Bell_{EF}\rightarrow Bell_{AF}\otimes Bell_{BE} \tag{11}$$

接着 Bob 和 Charlie 也分别用 Bell 基测量自己手上的光子。过程表示为

$$Bell_{BE}\otimes Bell_{CD}\rightarrow Bell_{BC}\otimes Bell_{DE} \tag{12}$$

将 Bob 和 Charlie 得到的测量结果，合并 Alice 的测量结果，可以推导出 Alice 经过逻辑操作后的量子态。

由于 Alice、Bob、Charlie 间的测量不公开，单方面的测量无法得知 Alice 最先做的逻辑操作究竟是哪一个，基于上述的原理，将在下节方案中对原始消息进行盲签名。

## 3　量子盲签名方案

在本方案中，设消息 $m$ 的所有者为 Alice，Bob 为签名验证人，而 Charlie 则在不知道消息的具体内容下进行盲签名。

### 3.1 初始化阶段

1)**消息变换**：Alice **将她的消息转换为二进制序列，记为** $m=\{m(1),m(2),m(3),\cdots,m(i),\cdots,m(n)\}$。

2)**密钥分配**：Alice **与** Bob **共享密钥** $K_{ab}$，Bob **与** Charlie **共享密钥** $K_{bc}$，**这些密钥的分配可以通过** BB84 **协议实现。**

3)**量子纠缠态的制备**：Alice、Bob **和** Charlie **各自制备** $N$ **对处于** $|j^-\rangle$ **态的纠缠光子对，记为**

$$\{j(1)^-_{AB},j(2)^-_{AB},j(3)^-_{AB},\cdots,j(i)^-_{AB},\cdots j(n)^-_{AB}\}$$

$$\{j(1)^-_{CD},j(2)^-_{CD},j(3)^-_{CD},\cdots,j(i)^-_{CD},\cdots,j(n)^-_{CD}\}$$

$$\{j(1)^-_{EF},j(2)^-_{EF},j(3)^-_{EF},\cdots,j(i)^-_{EF},\cdots,j(n)^-_{EF}\}$$

### 3.2 签名阶段

1) **对** $j(i)^-_{AB}$ **局域操作**：Alice **根据要发送的消息** $m(i)$**按表** 2 **对** $j(i)^-_{AB}$ **实施操作。**

**表 2 编码及状态变化**

| 编码 | 进行的变换 | 新的态 |
|---|---|---|
| 00 | $(I\otimes I)\|j^-\rangle$ | $\|j^-\rangle$ |
| 01 | $(X\otimes I)\|j^-\rangle$ | $\|F^-\rangle$ |
| 10 | $(Y\otimes I)\|j^-\rangle$ | $\|F^+\rangle$ |
| 11 | $(Z\otimes I)\|j^-\rangle$ | $\|j^+\rangle$ |

**例如，消息** $m$=011011，**则经过对应的局域操作后，**Alice **的纠缠态变为** $\{|F^-\rangle,|F^+\rangle,|j^+\rangle\}$。

2)**粒子的分发**：Alice、Bob **和** Charlie **按照图** 2 **所示交换粒子，交换后** Alice **持有粒子** A、F，Bob **持有粒子** B、C， Charlie **持有粒子** D、E。

3)Alice **用** Bell **基测量手上的光子对,测量结果记为** $R(i)_a$，**然后用** $K_{ab}$ **加密** $R(i)_a$ **得到** $E_{K_{ab}}(R(i)_a)$，**将** $E_{K_{ab}}(R(i)_a)$ **发送给** Charlie。**同时** Alice **用一个与** Bob **商量好的杂凑函数** $H$，**得到** $T(i)=H(m(i))$，**用** $K_{ab}$ **加密** $T(i)$ **得到** $E_{K_{ab}}(T(i))$ **发送给** Bob。

4) **获得盲签名**：Charlie **用** Bell **基测量手上的光子对，测量结果记为** $R(i)_c$，**然后将从** Alice **处收到的** $E_{K_{ab}}(R(i)_a)$ **联合** $R(i)_c$ **用** $K_{bc}$ **加密得到** $S=E_{K_{bc}}(R(i)_c,E_{K_{ab}}(R(i)_a))$。

5) **发送盲签名**：Charlie **将** $S$ **发送给** Bob。

### 3.3 验签阶段

1) Bob **收到** $S$ **后，用** $K_{bc}$ **解密得到** $R(i)_c$、$E_{K_{ab}}(R(i)_a)$，**再用** $K_{ab}$ **解密得到** $R(i)_a$。

2) Bob **用** Bell **基测量手上的光子对，测量结果记为** $R(i)_b$。

3) Bob **根据表** 3 **可以推断出** Alice **经过局域操作后的** $Bell_{AB}$，**再根据表** 2 **的编码规则译出** $m'(i)$。Bob **用** $H$ **进行，得到** $T'(i)=H(m'(i))$。**比较** $T'$ **与** $T$，**如果** $T'=T$，**则确认** $S$ **有效。**

**表 3 $R_a$、$R_b$、$R_c$ 及 $Bell_{AB}$ 的对应关系**

| $R_b$ | $R_c$ | $R_a$ | $Bell_{AB}$ | $R_b$ | $R_c$ | $R_a$ | $Bell_{AB}$ |
|---|---|---|---|---|---|---|---|
| $\|j^-\rangle$ | $\|j^-\rangle$ | $\|j^-\rangle$ | $\|j^-\rangle$ | $\|F^-\rangle$ | $\|j^+\rangle$ | $\|F^+\rangle$ | $\|j^-\rangle$ |
| $\|j^-\rangle$ | $\|j^-\rangle$ | $\|j^-\rangle$ | $\|F^-\rangle$ | $\|F^-\rangle$ | $\|j^+\rangle$ | $\|j^+\rangle$ | $\|F^-\rangle$ |
| $\|j^-\rangle$ | $\|j^-\rangle$ | $\|F^+\rangle$ | $\|F^+\rangle$ | $\|F^-\rangle$ | $\|j^+\rangle$ | $\|F^-\rangle$ | $\|j^+\rangle$ |
| $\|j^-\rangle$ | $\|j^-\rangle$ | $\|j^+\rangle$ | $\|j^+\rangle$ | $\|F^-\rangle$ | $\|j^+\rangle$ | $\|j^-\rangle$ | $\|F^+\rangle$ |
| $\|F^+\rangle$ | $\|F^+\rangle$ | $\|j^-\rangle$ | $\|j^-\rangle$ | $\|j^+\rangle$ | $\|F^-\rangle$ | $\|F^+\rangle$ | $\|j^-\rangle$ |
| $\|F^+\rangle$ | $\|F^+\rangle$ | $\|F^-\rangle$ | $\|F^-\rangle$ | $\|j^+\rangle$ | $\|F^-\rangle$ | $\|j^+\rangle$ | $\|F^-\rangle$ |
| $\|F^+\rangle$ | $\|F^+\rangle$ | $\|F^+\rangle$ | $\|F^+\rangle$ | $\|j^+\rangle$ | $\|F^-\rangle$ | $\|F^-\rangle$ | $\|j^+\rangle$ |
| $\|F^+\rangle$ | $\|F^+\rangle$ | $\|j^+\rangle$ | $\|j^+\rangle$ | $\|j^+\rangle$ | $\|F^-\rangle$ | $\|j^-\rangle$ | $\|F^+\rangle$ |
| $\|F^-\rangle$ | $\|F^-\rangle$ | $\|j^-\rangle$ | $\|j^-\rangle$ | $\|j^-\rangle$ | $\|F^+\rangle$ | $\|F^+\rangle$ | $\|j^-\rangle$ |
| $\|F^-\rangle$ | $\|F^-\rangle$ | $\|F^-\rangle$ | $\|F^-\rangle$ | $\|j^-\rangle$ | $\|F^+\rangle$ | $\|j^+\rangle$ | $\|F^-\rangle$ |
| $\|F^-\rangle$ | $\|F^-\rangle$ | $\|F^+\rangle$ | $\|F^+\rangle$ | $\|j^-\rangle$ | $\|F^+\rangle$ | $\|F^-\rangle$ | $\|j^+\rangle$ |
| $\|F^-\rangle$ | $\|F^-\rangle$ | $\|j^+\rangle$ | $\|j^+\rangle$ | $\|j^-\rangle$ | $\|F^+\rangle$ | $\|j^-\rangle$ | $\|F^+\rangle$ |
| $\|j^+\rangle$ | $\|j^+\rangle$ | $\|j^-\rangle$ | $\|j^-\rangle$ | $\|F^+\rangle$ | $\|j^-\rangle$ | $\|F^+\rangle$ | $\|j^-\rangle$ |
| $\|j^+\rangle$ | $\|j^+\rangle$ | $\|F^-\rangle$ | $\|F^-\rangle$ | $\|F^+\rangle$ | $\|j^-\rangle$ | $\|j^+\rangle$ | $\|F^-\rangle$ |
| $\|j^+\rangle$ | $\|j^+\rangle$ | $\|F^+\rangle$ | $\|F^+\rangle$ | $\|F^+\rangle$ | $\|j^-\rangle$ | $\|F^-\rangle$ | $\|j^+\rangle$ |
| $\|j^+\rangle$ | $\|j^+\rangle$ | $\|j^+\rangle$ | $\|j^+\rangle$ | $\|F^+\rangle$ | $\|j^-\rangle$ | $\|j^-\rangle$ | $\|F^+\rangle$ |
| $\|F^+\rangle$ | $\|j^+\rangle$ | $\|F^-\rangle$ | $\|j^-\rangle$ | $\|j^+\rangle$ | $\|j^-\rangle$ | $\|j^+\rangle$ | $\|j^-\rangle$ |
| $\|F^+\rangle$ | $\|j^+\rangle$ | $\|j^-\rangle$ | $\|F^-\rangle$ | $\|j^+\rangle$ | $\|j^-\rangle$ | $\|F^+\rangle$ | $\|F^-\rangle$ |
| $\|F^+\rangle$ | $\|j^+\rangle$ | $\|j^+\rangle$ | $\|F^+\rangle$ | $\|j^+\rangle$ | $\|j^-\rangle$ | $\|F^-\rangle$ | $\|F^+\rangle$ |
| $\|F^+\rangle$ | $\|j^+\rangle$ | $\|F^+\rangle$ | $\|j^+\rangle$ | $\|j^+\rangle$ | $\|j^-\rangle$ | $\|j^-\rangle$ | $\|j^+\rangle$ |
| $\|F^-\rangle$ | $\|j^-\rangle$ | $\|F^-\rangle$ | $\|j^-\rangle$ | $\|j^-\rangle$ | $\|j^+\rangle$ | $\|j^+\rangle$ | $\|j^-\rangle$ |
| $\|F^-\rangle$ | $\|j^-\rangle$ | $\|j^-\rangle$ | $\|F^-\rangle$ | $\|j^-\rangle$ | $\|j^+\rangle$ | $\|F^+\rangle$ | $\|F^-\rangle$ |
| $\|F^-\rangle$ | $\|j^-\rangle$ | $\|j^+\rangle$ | $\|F^+\rangle$ | $\|j^-\rangle$ | $\|j^+\rangle$ | $\|F^-\rangle$ | $\|F^+\rangle$ |
| $\|F^-\rangle$ | $\|j^-\rangle$ | $\|F^+\rangle$ | $\|j^+\rangle$ | $\|j^-\rangle$ | $\|j^+\rangle$ | $\|j^-\rangle$ | $\|j^+\rangle$ |
| $\|j^+\rangle$ | $\|F^+\rangle$ | $\|F^-\rangle$ | $\|j^-\rangle$ | $\|F^+\rangle$ | $\|F^-\rangle$ | $\|j^+\rangle$ | $\|j^-\rangle$ |
| $\|j^+\rangle$ | $\|F^+\rangle$ | $\|j^-\rangle$ | $\|F^-\rangle$ | $\|F^+\rangle$ | $\|F^-\rangle$ | $\|F^+\rangle$ | $\|F^-\rangle$ |
| $\|j^+\rangle$ | $\|F^+\rangle$ | $\|j^+\rangle$ | $\|F^+\rangle$ | $\|F^+\rangle$ | $\|F^-\rangle$ | $\|F^-\rangle$ | $\|F^+\rangle$ |
| $\|j^+\rangle$ | $\|F^+\rangle$ | $\|F^+\rangle$ | $\|j^+\rangle$ | $\|F^+\rangle$ | $\|F^-\rangle$ | $\|j^-\rangle$ | $\|j^+\rangle$ |
| $\|j^-\rangle$ | $\|F^-\rangle$ | $\|F^-\rangle$ | $\|j^-\rangle$ | $\|F^-\rangle$ | $\|F^-\rangle$ | $\|j^+\rangle$ | $\|j^-\rangle$ |
| $\|j^-\rangle$ | $\|F^-\rangle$ | $\|j^-\rangle$ | $\|F^-\rangle$ | $\|F^-\rangle$ | $\|F^+\rangle$ | $\|F^+\rangle$ | $\|F^-\rangle$ |
| $\|j^-\rangle$ | $\|F^-\rangle$ | $\|j^+\rangle$ | $\|F^+\rangle$ | $\|F^-\rangle$ | $\|F^+\rangle$ | $\|F^-\rangle$ | $\|F^+\rangle$ |
| $\|j^-\rangle$ | $\|F^-\rangle$ | $\|F^+\rangle$ | $\|j^+\rangle$ | $\|F^-\rangle$ | $\|F^+\rangle$ | $\|j^-\rangle$ | $\|j^+\rangle$ |

## 4 方案分析

### 4.1 正确性分析

**为了说明方案的正确性，给出下列实例。假如**

$\{0,1,\perp\}$，那么按照表 2，Alice 按照 $H$ 函数得到 $H(m)$，之后 Alice 对自己的纠缠光子对作对应的局域操作后，将变成 $\{|F^-\rangle,\perp\}$。交换光子后，假设测量后的 $R_a=\{|j^+\rangle,\perp\}$，$R_b=\{|j^-\rangle,\perp\}$，$R_c=\{|F^+\rangle,\perp\}$。即 $Bell_{AF}(1)=|j^+\rangle$，$Bell_{BC}(1)=|j^-\rangle$，$Bell_{DE}(1)=|F^+\rangle$。由式(12)可知，在 $Bell_{BC}$ 和 $Bell_{DE}$ 已知的情况下，可以推出 $Bell_{BE}=|F^+\rangle$，即 B、E 光子瞬间塌缩为 $|F^+\rangle$。同理，由式(11)可知，在 $Bell_{BE}$ 和 $Bell_{AF}$ 已知的情况下，可以推出 $Bell_{AB}=|F^-\rangle$，也可根据表 3 可得 $Bell_{AB}=|F^-\rangle$。据表 2 的编码规则 Bob 可以翻译出信息为 $m'=\{0,1,\perp\}$，对比 $H(m')$ 和 $H(m)$，必有 $H(m')=H(m)$，这就说明了方案的正确性。

### 4.2　安全性分析

对签名的攻击包括经典攻击策略和量子攻击策略。

1) 经典安全性

Charlie 对信息的签名是盲的。只有在 $R_a$、$R_b$、$R_c$ 都公布的情况下，才能推测出 $Bell_{AB}$ 的状态。Charlie 不可能根据自己手上的 $R_c$ 推测出 Alice 的态，进而推测出 Alice 发送的消息内容。虽然 Charlie 不知道 Alice 发送的消息内容，但是他对 D、E 光子的测量操作完成了盲签名的过程。

如果 Charlie 为了谋取自己的某种利益伪造消息及签名，但这样是困难的。首先，签名 $S$ 中包含了 $E_{K_{AB}}(R(i)_a)$，$K_{AB}$ 是 Alice 与 Bob 共享密钥，Charlie 无法知悉 $R(i)_a$ 的具体内容。其次，伪造签名也是困难的，仍旧以 4.1 节分析中的实例作为分析对象。在经过一系列操作测量后，得到测量结果为 $R_a=\{|j^+\rangle,\perp\}$，$R_b=\{|j^-\rangle,\perp\}$，$R_c=\{|F^+\rangle,\perp\}$。假设此时 Charlie 为了谋取自己的某种利益伪造测量结果，$R_a'=\{|j^+\rangle,\perp\}$。Bob 在接收 $S$ 后，根据 $R_b$、$R_c$ 推出 $Bell_{BE}=|j^+\rangle$，$Bell_{AB}=|j^-\rangle$。根据表 2 的编码规则，Bob 可以翻译出信息为 $m'=\{0,0,\perp\}$。比较 $H(m'(i))$ 和 $H(m(i))$，有 $H(m'(i))\neq H(m(i))$，Bob 拒绝签名。

如果 Bob 为了谋取自己的某种利益伪造消息及签名，这样是困难的。由于 Bob 知道 $H$ 函数及表 2 的编码规则，人们可能担心 Bob 的权限过大，进而肆无忌惮地伪造消息及签名为自己谋利。其实，在经过量子局域操作、通信三方在交换粒子、Alice 与 Charlie 分别测量自己的粒子对后，Bob 的粒子对状态已经确定。Bob 一旦与 Alice 发生冲突，只要 Charlie 介入，查看自己的测量记录，Bob 就无法继续自己的阴谋。

杂凑函数 $H$ 使信息 $m$ 间接提供给 Bob 和 Charlie，增加了保密性。Charlie 的签名对象是根据 $H$ 函数压缩后的信息，Charlie 根本不知道 Alice 的真实消息内容。

由于签名 $S$ 中包含了密钥 $K_{AB}$ 和 $K_{BC}$，而 Alice 与 Bob 共享密钥 $K_{AB}$，Bob 与 Charlie 共享密钥 $K_{BC}$。因此，Alice 不能否认自己的请求签名，Charlie 不能抵赖签名的事实，而 Bob 同样不能否认自己收到签名。

对手 Eve 同样无法进行截获重发攻击。假设 Eve 截获了 Alice 发给 Charlie 的信息，但在本方案中 Eve 由于没有密钥 $K_{AC}$，无法获取消息内容。同样，假设 Eve 截获了 Charlie 发给 Bob 的信息，但在本方案中 Eve 由于没有密钥 $K_{BC}$，无法伪造签名。而且，签名的发送、接收以及纠缠光子对的测量都是 Alice、Bob 和 Charlie 根据协议同步进行的。

2) 量子安全性

本方案采用的是 BB84 进行密钥分配协议。由 QKD 协议的无条件安全性保证，若对手 Eve 采用中间人攻击，冒充 Alice、Bob 或者 Charlie 篡改消息或签名是不可能的。

若对手 Eve 进行截获重发攻击，由量子不可克隆性保证了量子信息是不可被复制的。Eve 对 Alice 光子的检测克隆势必破坏粒子对的纠缠特性，对签名信息产生扰动。Charlie 将拒绝签名，同时，Bob 也将注意到窃听者的存在。

一般情况下，可以用以下途径在实现签名前，检测量子信道是否由攻击者存在。在本方案中，以 Alice 和 Bob 的量子通信信道为例。Alice 制备完 EPR 纠缠粒子对，将光子 A 留在自己手上，将光子 B 发送给遥远的 Bob。Alice 和 Bob 各自采用随机的测量基测量各自手中的光子。然后 Alice 和 Bob 各自公布采用的测量基，并选取测量基相同的位公布测量结果。考虑量子信道为理想无噪声信道，如果没有对手 Eve 的存在，那么在本方案中，测量结果应该正好相反。在现实情况中，信道总不可能是理想无噪声的，可以设置阈值门限判别是否有对手 Eve 的存在。假设 Alice 依次发送了 $n$ 个光子给 Bob，各自采用随机的测量基测量各自手中的光子，公布测量基相同位上的测量结果。假设 A、B 光子测量

结果中有不是正好相反的光子对，统计没有相关性的光子对数为 $m$。当 $c\left(c=\frac{m}{n}\right)$ 大于可以容忍的常数时，则认为这条量子信道上存在对手干扰，Alice 和 Bob 将放弃本次通信。同理，Alice 和 Charlie、Bob 和 Charlie 都可以在开始签名前运用这个方法来检测信道的安全性。

## 5 结束语

本文提出了基于纠缠光子对交换的量子盲签名协议。该方案不同于温晓军提出的弱盲签及强盲签，在消息拥有者调制信息阶段就盲化信息，而是签名者直接对信息盲签。温晓军提出的量子盲签名基于 EPR 纠缠对、GHZ 三光子的随机测量实现信息的盲化。前者基于 EPR 纠缠对的盲签名在验证阶段，由于取密钥奇数位参与验证，有 50%的信息是不确定的，浪费了带宽；后者基于 GHZ 三光子的盲签名在制备、存储和测量等技术上较本法案更难于实现，验签阶段签名更容易判断。早在 1998 年，潘建伟等就用实验验证了量子纠缠交换。因此，在当前技术下，实现本文介绍的量子签名方案是完全可行的。

此外，本方案还非常便于在原来的基础上扩展，信息的签名者可以根据实际需要增加，实现多重有序签名。参与签名方只要制备好 EPR 纠缠对，参与粒子的纠缠交换，测量自己手上的新纠缠态即可完成自己的签名。

## 参考文献：


[1] CHUAM D. Blind signature for untraceable payment[C]//Advances in Cryptology-Cypto'82. Berlin, c1983:199-203.

[2] **杨义先，孙伟，钮心忻. 现代密码新理论**[M]. **北京: 科学出版社**, 2002: 134-135.
YANG Y X, SUN W, NIU X X. The new theory of modern cryptography[M]. Beijing: Science Press, 2002:134-145.

[3] **温晓军，陈永志. 量子签名及应用**[M]. **北京: 航空工业出版社**, 2012:121.
WEN X J, CHEN Y Z. Quantum signature and application[M]. Beijing: Aviation Industry Press, 2012:121.

[4] GOTTESMAN D, CHUANG I. Quantum digital signatures[EB/OL]. http://arxiv.org/abs/quant-ph/ 0105032.

[5] **曾贵华，马文平，王新梅，等. 基于量子密码的签名方案**[J]. **电子学报**. 2001, 29(8): 1098-1100.
ZENG G H, MA W P, WANG X M, et al. Signature scheme based on quantum cryptography[J]. Acta Electronica Sinaca, 2001, 29(8): 1098-1100.

[6] WEN X J, LIU Y, ZHANG P Y. Information signature protocols using Einstein-Podolsky-Rosen pairs[J]. Journal of Dalian University of Technology, 2007, 47(3): 424-428.

[7] **温晓军，刘云. 一种可实现的量子有序多重数字签名方案**[J]. **电子学报**, 2007, 35(6):1079-1083.
WEN X J, LIU Y. A realizable quantum sequential muti-signature scheme[J]. Acta Electronica Sinica, 2007, 35 (6): 1079-1083.

[8] WEN X J, NIU X M, JI L P, et al. A weak blind signature scheme based on quantum cryptography[J]. Optics Communications, 2009, 282: 666-669.

[9] **温晓军,田原,牛夏牧. 一种基于秘密共享的量子强盲签名协议**[J]. **电子学报**, 2010, 38(3): 720-724.
WEN X J, TIAN Y, NIU Z M. A strong blind quantum signature protocol based on secret saring[J]. Acta Electronica Sinica, 2010, 2010, 38(3): 720-724.

[10] **陈永志，刘云，温晓军. 一个量子代理弱盲签名方案**[J]. **量子电子学报**, 2011, 28(3): 341-349.
CHEN Y Z, LIU Y, WEN X J. A quantum proxy weak blind s gnature scheme[J]. Chinese Journal of Quantum Electronics, 2011, 28(3): 341-349.


**作者简介：**


**梁建武**（1964-），男，湖南长沙人，中南大学副教授，主要研究方向为量子通信和无线通信。

**王晓慧**（1990-），女，上海人，中南大学硕士生，主要研究方向为量子安全保密通信和无线通信。

**郭迎**（1975-），男，山东临沂人，中南大学教授，主要研究方向为量子安全保密通信和无线通信。

**程资**（1990-），女，河北晋州人，中南大学硕士生，主要研究方向为量子安全保密通信和无线通信。