激光与光电子学进展

基于两粒子和三粒子最大纠缠态的量子盲签名协议

王俊辉[1]，李云霞[1***]，蒙文[1**]，魏家华[1*]，唐杰[1]，武天雄[1]
空军工程大学信息与导航学院，陕西 西安 710077

摘要 量子盲签名作为量子密码学的重要组成部分，近年来受到了越来越多的关注。提出了一个基于两粒子和三粒子最大纠缠态的量子盲签名方案，利用量子纠缠特性实现了消息盲化，并借助量子相干性原理进行了消息恢复。所提方案利用量子逻辑门对量子态进行操作，实现了两比特经典信息的量子态表示。最后证明了该方案满足不可否认性、不可伪造性和盲性。基于量子密钥分发和一次一密技术，所提方案的无条件安全性得到了保证，且与现有其他方案对比，该方案有较高的签名效率。

关键词 量子光学；量子通信；量子盲签名；最大纠缠态；安全性分析
中图分类号 O431.2 **文献标志码** A **doi**：10.3788/LOP202158.0727002

Protocol of Quantum Blind Signature Based on Two-Qubit and Three-Qubit Maximally Entangled States

Wang Junhui[1], Li Yunxia[1***], Meng Wen[1**], Wei Jiahua[1*], Tang Jie[1], Wu Tianxiong[1]
Information and Navigation College, Air Force Engineering University, Xi'an, Shaanxi 710077, *China*

Abstract As an important part of quantum cryptography, quantum blind signature has attracted more and more attentions in recent years. A protocol of quantum blind signature based on two-qubit and three-qubit maximally entangled states is proposed. By using the special characteristics of quantum entanglement, the blindness of a message is realized, and the recovery of this message is conducted by the help of the quantum coherence principle. In the proposed protocol, the operation on qubits via quantum logic gates is used for the realization of the quantum state expression of two-bit classical information. Finally the proposed protocal is confirmed to satisfy the properties of undeniability, unforgeability and blindness. Based on the quantum key distribution and one-time pad technology, the absolute security of the proposed protocol is guaranteed. Moreover, the proposed protocol is more efficient than other existing protocols.

Key words quantum optics; quantum communication; quantum blind signature; maximally entangled states; security analysis
OCIS codes 270.5565; 270.5568; 270.5585

1 引 言

数字签名可用于验证数字消息的真实性、完整性和不可否认性，并实现通信双方的消息认证，是信息安全的核心技术之一[1]。经典数字签名大多基于复杂问题的计算，但随着具有并行计算优势的量

收稿日期：2020-08-24；**修回日期**：2020-08-30；**录用日期**：2020-09-14
基金项目：国家自然科学基金(61971436,61803382)、陕西省自然科学基础研究计划(2018JQ6020)
*E-mail：weijiahua@126.com；**E-mail：mengwen_mw@126.com；***E-mail：yunxial@foxmail.com

子计算机的快速发展，经典签名受到了巨大的挑战。Shor算法[2]提供了在多项式时间解决大数分解问题的方法。如何保证签名的真实性、完整性和不可否认性是值得进一步研究的问题。量子签名基于量子特性，签名协议的无条件安全性得到保证，从而得到了越来越多的关注。

量子签名依据其使用的密码体制可分为两大类[3]，即基于非对称密码体制的一般量子签名[4]和基于对称密码体制的仲裁量子签名[5]；按照用途可分为一般量子签名、量子盲签名（Quantum Blind Signature，QBS）、量子群签名和量子门限签名等。其中一般量子签名可与量子身份认证技术相互转换[1]。近些年，量子密钥分发（Quantum Key Distribution，QKD）技术飞速发展，实用化量子签名协议[6-7]的提出和不同环境下QKD技术的发展[8-10]对量子签名技术研究有着重要意义，同时实验方面[11-12]也有很大进展。

与经典盲签名类似，量子盲签名允许签名者在不知道消息具体内容的情况下完成签名。2009年，Wen等[13]首次提出了基于EPR纠缠粒子的量子弱盲签名方案。2010年，基于双态向量（Time-state Vector Form，TSVF）的性质，Su等[14]提出了一种新的盲签名方案。2013年，利用三体纠缠态GHZ的相干性，Wang等[15]提出了一种盲签名方案。2014年，Khodambashi等[16]提出了基于会话的量子盲签名方案，签名者选择一个随机的二进制序列作为会话签名，然后根据会话签名生成盲签名。Tian等[17]提出了广播多重量子盲签名方案，Zhang等[18]针对其可能遭受的签名伪造行为，进行了协议优化。2019年，Chen等[19]利用非正交单光子，提出了一个不需要纠缠的量子盲签名协议。Liang等[20]和Liu等[21]分别基于四粒子纠缠态和五粒子纠缠态，各自提出了盲代理签名协议。Zhang等[22]和Yang等[23]分别基于六粒子纠缠态和七粒子纠缠态，提出了盲代理签名的改进协议。2020年，Li等[24]基于量子行走实现了量子隐形传态，从而提出了新的量子盲签名协议。Niu等[25]基于量子密集编码原理，提出了一种量子代理盲签名协议。

量子盲签名主要包含盲化、签名和验证三个部分。盲化阶段主要基于量子特性，如只有当量子制备基和测量基一致时[19]，才能实现有效测量；或者采用单向函数或者量子傅里叶变换（Quantum Fourier Transmission，QFT），对量子态进行加密以实现盲化[26]。签名和验证部分主要基于量子相干性。量子盲签方案分为初始化阶段、签名阶段和验证阶段，其中初始化用于量子比特分发，签名阶段包含盲化和签名两部分。利用两粒子和三粒子的最大纠缠态，本文提出了一种可签名两比特经典信息的量子盲签名方案，与现有方案相比较，本方案具有较高效率。

2　基本原理

2.1　量子纠缠态

本文用到的量子纠缠态包含两体纠缠态和三体纠缠态，且均为最大纠缠态。其中两体纠缠态为Bell态，即

$$\begin{cases}\left|\phi^{\pm}\right\rangle_{AB}=\dfrac{1}{\sqrt{2}}\left(\left|00\right\rangle>\pm\left|11\right\rangle\right)_{AB}\\ \left|\psi^{\pm}\right\rangle_{AB}=\dfrac{1}{\sqrt{2}}\left(\left|01\right\rangle\pm\left|10\right\rangle\right)_{AB}\end{cases},\tag{1}$$

式中：A、B为两体中的粒子。

其中三体纠缠态包含

$$\begin{cases}\left|\zeta_1\right\rangle_{CDE}=\dfrac{1}{\sqrt{2}}\left(\left|000\right\rangle+\left|111\right\rangle\right)_{CDE}\\ \left|\zeta_2\right\rangle_{CDE}=\dfrac{1}{\sqrt{2}}\left(\left|001\right\rangle+\left|110\right\rangle\right)_{CDE}\end{cases},\tag{2}$$

式中：C、D、E为三体中的粒子。

假设Alice拥有$\left|\phi^{+}\right\rangle_{AB}$，Bob拥有$\left|\zeta_1\right\rangle_{CDE}$，首先让$\left|\phi^{+}\right\rangle_{AB}$和$\left|\zeta_1\right\rangle_{CDE}$构成一个复合系统，再分别对粒子B、C和粒子D、E进行联合Bell测量，则五粒子系统状态为

$$\begin{aligned}&\left|\varphi\right\rangle_{ABCDE}=\left|\varphi^{+}\right\rangle_{AB}\otimes\left|\zeta_1\right\rangle_{CDE}=\\&\frac{1}{\sqrt{2}}\left(\left|00\right\rangle+\left|11\right\rangle\right)_{AB}\otimes\frac{1}{\sqrt{2}}\left(\left|000\right\rangle+\left|110\right\rangle\right)_{CDE}=\\&\frac{1}{4}\left[\left(\left|0\right\rangle+\left|1\right\rangle\right)_A\left|\phi^{+}\right\rangle_{BC}+\left(\left|0\right\rangle-\left|1\right\rangle\right)_A\left|\phi^{-}\right\rangle_{BC}\right]\otimes\left|\phi^{+}\right\rangle_{DE}+\\&\left[\left(\left|0\right\rangle+\left|1\right\rangle\right)_A\left|\psi^{+}\right\rangle_{BC}+\left(\left|0\right\rangle-\left|1\right\rangle\right)_A\left|\psi^{-}\right\rangle_{BC}\right]\otimes\left|\phi^{+}\right\rangle_{DE}+\\&\left[\left(\left|0\right\rangle-\left|1\right\rangle\right)_A\left|\phi^{+}\right\rangle_{BC}+\left(\left|0\right\rangle+\left|1\right\rangle\right)_A\left|\phi^{-}\right\rangle_{BC}\right]\otimes\left|\phi^{-}\right\rangle_{DE}-\\&\left[\left(\left|0\right\rangle-\left|1\right\rangle\right)_A\left|\psi^{+}\right\rangle_{BC}-\left(\left|0\right\rangle+\left|1\right\rangle\right)_A\left|\psi^{-}\right\rangle_{BC}\right]\otimes\left|\phi^{-}\right\rangle_{DE}=\\&\frac{1}{2\sqrt{2}}\left(\left|+\right\rangle_A\left|\phi^{+}\right\rangle_{BC}+\left|-\right\rangle_A\left|\phi^{-}\right\rangle_{BC}\right)\otimes\left|\phi^{+}\right\rangle_{DE}+\\&\left(\left|+\right\rangle_A\left|\psi^{+}\right\rangle_{BC}+\left|-\right\rangle_A\left|\psi^{-}\right\rangle_{BC}\right)\otimes\left|\phi^{+}\right\rangle_{DE}+\\&\left(\left|-\right\rangle_A\left|\phi^{+}\right\rangle_{BC}+\left|+\right\rangle_A\left|\phi^{-}\right\rangle_{BC}\right)\otimes\left|\phi^{+}\right\rangle_{DE}-\\&\left(\left|-\right\rangle_A\left|\psi^{+}\right\rangle_{BC}-\left|+\right\rangle_A\left|\psi^{-}\right\rangle_{BC}\right)\otimes\left|\phi^{-}\right\rangle_{DE},\end{aligned}\tag{3}$$

式中：$|+\rangle_A=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_A$；$|-\rangle_A=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)_A$。

2.2 量子逻辑门

量子信息处理的本质就是对量子态进行一系列幺正操作，其中最基本的操作称为量子逻辑门。Pauli门是常见的逻辑门，包含以下四种：

$$\begin{cases}\boldsymbol{I}=|0\rangle\langle 0|+|1\rangle\langle 1|=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\\ \boldsymbol{\sigma}_X=|0\rangle\langle 1|+|1\rangle\langle 0|=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\\ \boldsymbol{\sigma}_Z=|0\rangle\langle 0|-|1\rangle\langle 1|=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\\ \boldsymbol{\sigma}_Y=-\mathrm{i}|0\rangle\langle 1|+\mathrm{i}|1\rangle\langle 0|=\begin{pmatrix}0 & -\mathrm{i}\\ \mathrm{i} & 0\end{pmatrix}\end{cases}。\tag{4}$$

将这四种 Pauli 门分别作用于处于纠缠态$|\phi^+\rangle_{AB}$的粒子 A 上，使其量子态发生改变。对应操作和操作后的量子态如表 1 所示。

表 1　量子逻辑门与对应的量子态

Table 1　Quantum logic gates and corresponding quantum states

Operation on particle A	Primitive quantum state	Post-operation quantum state
$\boldsymbol{I}$	$\|\phi^+\rangle_{AB}$	$\|\phi^+\rangle_{AB}$
$\boldsymbol{\sigma}_X$	$\|\phi^+\rangle_{AB}$	$\|\psi^+\rangle_{AB}$
$\boldsymbol{\sigma}_Z$	$\|\phi^+\rangle_{AB}$	$\|\phi^-\rangle_{AB}$
$\mathrm{i}\boldsymbol{\sigma}_Y$	$\|\phi^+\rangle_{AB}$	$\|\psi^-\rangle_{AB}$

3　量子盲签名方案

量子签名包含三方：签名发送和盲化者 Alice，签名接收和验证者 Charlie，签名者 Bob。与现有签名方案架构一致，本方案分为初始化阶段、签名阶段和验证阶段。

3.1 初始化阶段

1）消息变换：Alice 将待签名消息转化为二进制序列 $M=\{m_1, m_2, \cdots, m_i, \cdots, m_n\}$，其中 m_i 为二进制消息比特，$m_i\in\{0,1\}$，i 为二进制消息序列的序号，$i=1,2,\cdots,n$，n 为二进制消息序列的长度 。

2）密钥共享：通过 QKD 技术，使 Alice 和 Charlie 共享密钥 K_{AC}，Bob 和 Charlie 共享密钥 K_{BC}。QKD 的特性保证了密钥分发过程的绝对安全。

3）粒子制备与分发：Alice 依据消息 M 的奇数位，制备量子态$|\zeta\rangle_{CDE}$，即

$$|\zeta\rangle_{CDE}^{j}=\begin{cases}|\zeta_1\rangle_{CDE}^{j}, & m_{2j-1}=0\\ |\zeta_2\rangle_{CDE}^{j}, & m_{2j-1}=1\end{cases},\tag{5}$$

式中：$|\zeta\rangle_{CDE}^{j}$ 为 Alice 制备的第 j 个三体 GHZ 态；m_{2j-1} 为第 $2j-1$ 个二进制消息比特；$j=1,2,\ldots,m$，其中 $m=\left\lceil\frac{n}{2}\right\rceil$。Alice 将粒子 C 发送给 Bob，将粒子 D、E 发送给 Charlie。Bob 制备 m 个纠缠态$\left\{|\phi'\rangle_{AB}^{1},|\phi'\rangle_{AB}^{2},\ldots,|\phi'\rangle_{AB}^{i},\ldots,|\phi'\rangle_{AB}^{m}\right\}$，其中第 i 个纠缠态所处的量子态$|\phi'\rangle_{AB}^{i}=|\phi^+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$。Bob 将粒子 A 发送给 Alice，具体分发过程如图 1 所示，图 1(a)表示量子的分发，图 1(b)表示分发完成后 Alice、Bob 和 Charlie 三方所拥有的粒子。

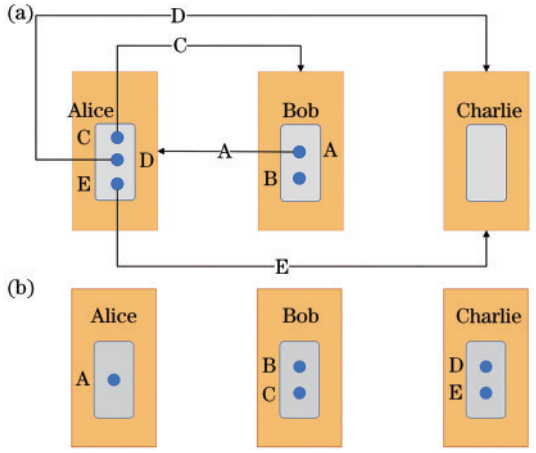

图 1　量子分发示意图。(a)初始状态；(b)分发完成状态

Fig. 1　Schematic of quantum distribution. (a) Initial state; (b) states after distribution

随后 Bob 将$|\phi'\rangle_{AB}^{i}$和$|\zeta\rangle_{CDE}^{i}$组成复合系统，复合系统表示为

$$|\phi\rangle_{ABCDE}^{i}=|\phi'\rangle_{AB}^{i}\otimes|\zeta\rangle_{CDE}^{i}。\tag{6}$$

3.2 签名阶段

1）量子态制备：Alice 用 t 表示消息 M 长度 n 的奇偶，当 n 为偶数时，令 $t=1$；当 n 为奇数时，令 $t=0$，并在消息 M 后加一个 0。随后得到重组消息 $M'=\{l_1, l_2, \cdots, l_i, \cdots, l_m\}$，其中 l_i 为两个经典比特。Alice 根据表 1 执行相应操作，得到对应的四个态$|\phi^+\rangle$，$|\phi^-\rangle$，$|\psi^+\rangle$ 和 $|\psi^-\rangle$ 分别对应经典消息 $l_i=00,01,10,11$。

2) Alice 用 X 基 $\{|+\rangle,|-\rangle\}$ 测量 A 粒子，得测量结果 β_A。

3) Alice 将经密钥 K_{AC} 加密后的消息 $S_A=E_{K_{AC}}(\beta_A,t,T)$ 发送给 Charlie，其中 $T=H(M)$ 为仅由 Alice 和 Charlie 共享的单向函数，$E_{K_{AC}}$ 为 Alice 利用密钥 K_{AC} 对信息进行量子一次一密加密操作。

4) Bob 使用 Bell 基测量粒子 B、C，得结果 β_B。结果 β_B 经密钥 K_{BC} 加密后，Bob 将盲化消息 $S_B=E_{K_{BC}}(\beta_B)$ 发送给 Charlie，其中 $E_{K_{BC}}$ 为 Bob 利用密钥 K_{BC} 对信息进行量子一次一密加密操作。

3.3　验证阶段

1) Charlie 利用 K_{AC} 对收到的 S_A 进行解密，得到 β_A，t 和 T。利用 K_{BC} 对 S_B 进行解密，得到 β_B。

2) Charlie 使用 Bell 基测量粒子 D、E，得结果 β_C，并根据表 2 和 t 恢复出消息 l_i'，组合成 $M''=\{l_1',l_2',\cdots,l_i',\cdots,l_m'\}$，计算 $T'=H(M'')$。若 $T'=T$，则接受签名消息对 (S_B,M)，否则拒绝签名。

为了更好地理解消息的恢复过程，现举例说明。假设 Alice 将消息转化为二进制后的结果为 $M=\{0,0,1,0,0\}$，则重组消息 $M'=\{l_1,l_2,l_3\}$，$t=0$，其中 $l_1=00$，$l_2=10$，$l_3=00$。则 Alice 制备的三粒子最大纠缠态和 Bob 制备的两粒子最大纠缠态经过图 1 所示的量子分发过程，并完成签名阶段的量子态制备后，总系统表示为 $|\phi^+\rangle\otimes|\zeta_1\rangle$，$|\psi^+\rangle\otimes|\zeta_2\rangle$，$|\phi^+\rangle\otimes|\zeta_1\rangle$。对于复合系统 $|\phi^+\rangle\otimes|\zeta_1\rangle$ 而言，Alice 测量粒子 A 得到结果 β_A，Bob 测量粒子 B、C 得到结果 β_B，Charlie 测量粒子 D、E 得到结果 β_C，则 β_A、β_B 和 β_C 满足(3)式；对于复合系统 $|\psi^+\rangle\otimes|\zeta_2\rangle$ 而言，测量结果 β_A、β_B 和 β_C 满足

表 2　验证规则

Table 2　Validation rules

β_C	β_B	β_A	Operation on particle A	l'	β_C	β_B	β_A	Operation on particle A	l'
$\|\phi^+\rangle$	$\|\phi^+\rangle$	$\|+\rangle$	$\boldsymbol{I}$	00	$\|\phi^-\rangle$	$\|\phi^+\rangle$	$\|+\rangle$	$\boldsymbol{\sigma}_Z$	01
$\|\phi^+\rangle$	$\|\phi^+\rangle$	$\|-\rangle$	$\boldsymbol{\sigma}_Z$	01	$\|\phi^-\rangle$	$\|\phi^+\rangle$	$\|-\rangle$	$\boldsymbol{I}$	00
$\|\phi^+\rangle$	$\|\phi^-\rangle$	$\|+\rangle$	$\boldsymbol{\sigma}_Z$	01	$\|\phi^-\rangle$	$\|\phi^-\rangle$	$\|+\rangle$	$\boldsymbol{I}$	00
$\|\phi^+\rangle$	$\|\phi^-\rangle$	$\|-\rangle$	$\boldsymbol{I}$	00	$\|\phi^-\rangle$	$\|\phi^-\rangle$	$\|-\rangle$	$\boldsymbol{\sigma}_Z$	01
$\|\phi^+\rangle$	$\|\psi^+\rangle$	$\|+\rangle$	$\boldsymbol{I}$	00	$\|\phi^-\rangle$	$\|\psi^+\rangle$	$\|+\rangle$	$\boldsymbol{\sigma}_Z$	01
$\|\phi^+\rangle$	$\|\psi^+\rangle$	$\|-\rangle$	$\boldsymbol{\sigma}_Z$	01	$\|\phi^-\rangle$	$\|\psi^+\rangle$	$\|-\rangle$	$\boldsymbol{I}$	00
$\|\phi^+\rangle$	$\|\psi^-\rangle$	$\|+\rangle$	$\boldsymbol{\sigma}_Z$	01	$\|\phi^-\rangle$	$\|\psi^-\rangle$	$\|+\rangle$	$\boldsymbol{I}$	00
$\|\phi^+\rangle$	$\|\psi^-\rangle$	$\|-\rangle$	$\boldsymbol{I}$	00	$\|\phi^-\rangle$	$\|\psi^-\rangle$	$\|-\rangle$	$\boldsymbol{\sigma}_Z$	01
$\|\psi^+\rangle$	$\|\phi^+\rangle$	$\|+\rangle$	$\mathrm{i}\boldsymbol{\sigma}_Y$	10	$\|\psi^-\rangle$	$\|\phi^+\rangle$	$\|+\rangle$	$\boldsymbol{\sigma}_X$	11
$\|\psi^+\rangle$	$\|\phi^+\rangle$	$\|-\rangle$	$\boldsymbol{\sigma}_X$	11	$\|\psi^-\rangle$	$\|\phi^+\rangle$	$\|-\rangle$	$\mathrm{i}\boldsymbol{\sigma}_Y$	10
$\|\psi^+\rangle$	$\|\phi^-\rangle$	$\|+\rangle$	$\boldsymbol{\sigma}_X$	11	$\|\psi^-\rangle$	$\|\phi^-\rangle$	$\|+\rangle$	$\mathrm{i}\boldsymbol{\sigma}_Y$	10
$\|\psi^+\rangle$	$\|\phi^-\rangle$	$\|-\rangle$	$\mathrm{i}\boldsymbol{\sigma}_Y$	10	$\|\psi^-\rangle$	$\|\phi^-\rangle$	$\|-\rangle$	$\boldsymbol{\sigma}_X$	11
$\|\psi^+\rangle$	$\|\psi^+\rangle$	$\|+\rangle$	$\mathrm{i}\boldsymbol{\sigma}_Y$	10	$\|\psi^-\rangle$	$\|\psi^+\rangle$	$\|+\rangle$	$\boldsymbol{\sigma}_X$	11
$\|\psi^+\rangle$	$\|\psi^+\rangle$	$\|-\rangle$	$\boldsymbol{\sigma}_X$	11	$\|\psi^-\rangle$	$\|\psi^+\rangle$	$\|-\rangle$	$\mathrm{i}\boldsymbol{\sigma}_Y$	10
$\|\psi^+\rangle$	$\|\psi^-\rangle$	$\|+\rangle$	$\boldsymbol{\sigma}_X$	11	$\|\psi^-\rangle$	$\|\psi^-\rangle$	$\|+\rangle$	$\mathrm{i}\boldsymbol{\sigma}_Y$	10
$\|\psi^+\rangle$	$\|\psi^-\rangle$	$\|-\rangle$	$\mathrm{i}\boldsymbol{\sigma}_Y$	10	$\|\psi^-\rangle$	$\|\psi^-\rangle$	$\|-\rangle$	$\boldsymbol{\sigma}_X$	11

$$
\begin{aligned}
&|\varphi\rangle_{ABCDE}=|\psi^+\rangle_{AB}\otimes|\zeta_2\rangle_{CDE}=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)_{AB}\otimes\frac{1}{\sqrt{2}}(|001\rangle+|110\rangle)_{CDE}=\\
&\frac{1}{4}\Big[(|0\rangle+|1\rangle)_A|\phi^+\rangle_{BC}-(|0\rangle-|1\rangle)_A|\phi^-\rangle_{BC}\Big]\otimes|\psi^+\rangle_{DE}+\Big[(|0\rangle+|1\rangle)_A|\psi^+\rangle_{BC}-(|0\rangle-|1\rangle)_A|\psi^-\rangle_{BC}\Big]\otimes|\psi^+\rangle_{DE}+\\
&\Big[-(|0\rangle-|1\rangle)_A|\phi^+\rangle_{BC}+(|0\rangle+|1\rangle)_A|\phi^-\rangle_{BC}\Big]\otimes|\psi^-\rangle_{DE}+\Big[(|0\rangle-|1\rangle)_A|\psi^+\rangle_{BC}-(|0\rangle+|1\rangle)_A|\psi^-\rangle_{BC}\Big]\otimes|\psi^-\rangle_{DE}=\\
&\frac{1}{2\sqrt{2}}\Big(|+\rangle_A|\phi^+\rangle_{BC}-|-\rangle_A|\phi^-\rangle_{BC}\Big)\otimes|\psi^+\rangle_{DE}+\Big(|+\rangle_A|\psi^+\rangle_{BC}-|-\rangle_A|\psi^-\rangle_{BC}\Big)\otimes|\psi^+\rangle_{DE}+\\
&\Big(|-\rangle_A|\phi^+\rangle_{BC}+|+\rangle_A|\phi^-\rangle_{BC}\Big)\otimes|\psi^-\rangle_{DE}+\Big(|-\rangle_A|\psi^+\rangle_{BC}-|+\rangle_A|\psi^-\rangle_{BC}\Big)\otimes|\psi^-\rangle_{DE}。
\end{aligned}
\tag{7}
$$

假设测量结果β_A、β_B和β_C已知，则依据(3)式和(7)式恢复的经典比特如表3所示。Charlie根据Alice发来的消息$S_A=E_{K_{AC}}(\beta_A,t,T)$，利用密钥$K_{AC}$得到$t$值，当$t=0$时，删去恢复比特序列最后一位，即恢复的比特序列为{0,0,1,0,0}。当$t=1$时，保留恢复的消息比特序列。

表3　测量结果及恢复的比特

Table 3　Measurement results and recovery bits

β_A	β_B	β_C	t'
$\|+\rangle$	$\|\phi^+\rangle$	$\|\phi^+\rangle$	00
$\|-\rangle$	$\|\phi^+\rangle$	$\|\psi^-\rangle$	10
$\|+\rangle$	$\|\phi^-\rangle$	$\|\phi^-\rangle$	00

由前述可知，系统共存在的状态有4种，分别是$|\phi^+\rangle\otimes|\zeta_1\rangle$，$|\phi^-\rangle\otimes|\zeta_1\rangle$，$|\psi^+\rangle\otimes|\zeta_2\rangle$和$|\psi^-\rangle\otimes|\zeta_2\rangle$。每种复合状态有8种可能的测量结果，因此验证规则对32种可能的测量结果进行消息比特恢复。

4　性能分析

4.1　安全性分析

量子盲签名的安全性是基于QKD和一次一密，从信息论角度严格证明其安全性，则需要证明QKD的安全性和一次一密的安全性。QKD的信息论安全性证明已由文献[27]给出。在任何攻击条件下都具有无条件安全性的密码系统唯有“一次一密”密码系统[28]。量子一次一密加密算法是经典一次一密加密算法在量子信息领域的推广。与经典一次一密加密算法相同，量子一次一密加密算法中密钥的长度和被加密信息的长度一致。通常通信双方利用已经被证明的具有无条件安全性的量子密钥分发协议共享密钥，然后传输方根据该密钥的值选择对应的西操作算子对量子态信息进行酉变换，以达到对初始量子态加密的目的。因此，我们认为该系统是安全的。签名的安全性分析主要包含两个方面：不可伪造性和不可抵赖性。量子盲签名还应保证盲性，下面我们将详细分析该协议的安全性能。

4.1.1　不可伪造性

在该协议中，Alice与Charlie，Bob与Charlie共享的密钥都是通过量子密钥分发技术实现的。量子密钥分发技术结合一次一密(one-time pad，OTP)在理论和实践上都已被证明是无条件安全的，因此密钥K_{AC}和K_{BC}都是安全的。

若攻击者Eve采取截断-重发攻击，即Eve在Alice的签名阶段步骤3)处发起攻击。该阶段有安全密钥K_{AC}或K_{BC}加密，可保证传输的安全。即使Eve拥有足够的技术手段，获取了信息T和β_A，β_B，但由于单向函数$H(x)$仅由Alice和Charlie共享，因此Eve不能获取消息M。即使Eve得到T和β_A，β_B，Charlie在验证时，依据表2可得，Charlie仍能以3/4的概率发现窃听，从而重新传输消息。消息M的伪造成功概率为

$$P_{\text{forge}}(n)=4^{-\left\lceil\frac{n}{2}\right\rceil}\times 100\%。\tag{8}$$

当n足够大时，伪造成功的概率可忽略不计。

4.1.2　不可抵赖性

根据协议的描述，Alice加密消息所使用的密钥为Alice和Charlie秘密共享的K_{AC}，Bob加密使用的密钥为Bob和Charlie秘密共享的K_{BC}。该协议的不可抵赖性由密钥K_{AC}和K_{BC}保证。

4.1.3　盲性

Alice将处于纠缠态$|\zeta\rangle_{CDE}$的粒子C发送给Bob。Bob在复合系统$|\varphi\rangle_{ABCDE}$中用Bell基测量粒子B、C，得到β_B，进而得盲化签名$S_B=E_{K_{BC}}\beta_B$。根据表2对应关系，Bob从β_B中不能得到任何关于M的信息。因此，该签名方案具有盲性。

4.2　效率分析

分析本方案的效率，一是要考虑到量子信道中传输的比特数和实际签名的比特数，二是要考虑到实现签名的复杂度。我们定义签名效率(Signature efficiency)为

$$\eta=\frac{N_s}{N_q}\times 100\%,\tag{9}$$

式中：N_q为所需的量子总数；N_s为实际签名的比特数。

本方案的效率为$\eta=\frac{N_s}{N_q}\times 100\%=\frac{n}{\frac{5(n-1)+t+1}{2}}\times 100\%$。当$n$足够大时，效率$\eta$约为40%。将本文方案与文献[17]和文献[16]进行了对比，如表4所示，可以看出，本文方案有较高的签名效率。

表 4 方案对比

Table 4 Comparison of protocols

Parameter	Protocol in Ref. [17]	Protocol in Ref. [16]	Proposed protocol
Quantum resource	n five-qubit entangled states	$3n$ hybrid entangled states	$\left\lceil\frac{n}{2}\right\rceil$ Bell states and $\left\lceil\frac{n}{2}\right\rceil$ GHz states
Measurement basis	GHz basis and Bell basis	Hybrid entangled basis	Bell basis and single photon basis
Verification method	Two-level comparison	One-level comparison	One-level comparison
Signature efficiency	20%	33.3%	40%

5 结 论

提出了一个基于两粒子和三粒子最大纠缠态的量子盲签名协议。该协议采用一次一密和量子密钥分发技术实现无条件安全性。相比于传统签名方案和其他量子签名方案，所提方案实现了一次签名过程的两比特信息签名，具有较高的签名效率；在外部攻击者采取截断-重发攻击的情况下，当消息长度 n 足够大时，攻击成功的概率可忽略不计，所提方案满足不可伪造性、不可抵赖性和盲性；所提方案基于 Bell 态和三粒子纠缠态，在当前技术和实验条件下有实现的可能。因此，所提方案具有进一步研究和发展的价值。

参 考 文 献

[1] Wen X J, Chen Y Z. Quantum signature and applications[M]. Beijing: Aviation Industry Press, 2012: 50-63.
温晓军, 陈永志. 量子签名及应用[M]. 北京: 航空工业出版社, 2012: 50-63.

[2] Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring[C]//Proceedings 35th Annual Symposium on Foundations of Computer Science, November 20-22, 1994, Santa Fe, NM, USA. New York: IEEE, 1994: 124-134.

[3] Wen K. Security analysis and improvement of arbitration quantum signature protocol[D]. Beijing: Beijing University of Posts and Telecommunications, 2019:1-5
闻楷. 仲裁量子签名协议的安全性分析与改进[D]. 北京:北京邮电大学,20019:1-5.

[4] Chuang I L, Gottesman D. Quantum digital signatures [EB/OL]. (2001-11-15)[2020-07-15]. https://arxiv.org/abs/quant-ph/0105032.

[5] Zeng G H, Keitel C H. Arbitrated quantum-signature scheme[J]. Physical Review A, 2002, 65(4): 042312.

[6] Amiri R, Wallden P, Kent A, et al. Secure quantum signatures using insecure quantum channels [J]. Physical Review A, 2016, 93(3): 032325.

[7] Puthoor I V, Amiri R, Wallden P, et al. Measurement-device-independent quantum digital signatures[J]. Physical Review A, 2016, 94(2): 022328.

[8] Zhu Z D, Zhao S H, Gu W Y, et al. Orbital-angular-momentum-encoded measurement-device-independent quantum key distributions under atmospheric turbulence [J]. Acta Optica Sinica, 2018, 38(12): 1227002.
朱卓丹, 赵尚弘, 谷文苑, 等. 大气湍流下的轨道角动量编码测量设备无关量子密钥分发[J]. 光学学报, 2018, 38(12): 1227002.

[9] Zhang X Z, Xu X, Liu B Y. Influence of fog on performance of free-space quantum communication [J]. Acta Optica Sinica, 2020, 40(7): 0727001.
张秀再, 徐茜, 刘邦宇. 雾对自由空间量子通信性能的影响[J]. 光学学报, 2020, 40(7): 0727001.

[10] He Y F, Wang D, Yang H J, et al. Quantum key distribution based on heralded single photon sources and quantum memory [J]. Chinese Journal of Lasers, 2019, 46(4): 0412001.
何业锋, 王登, 杨红娟, 等. 基于指示单光子源和量子存储的量子密钥分配[J]. 中国激光, 2019, 46(4): 0412001.

[11] Roberts G L, Lucamarini M, Yuan Z L, et al. Experimental measurement-device-independent quantum digital signatures [J]. Nature Communications, 2017, 8(1): 1098.

[12] An X B, Zhang H, Zhang C M, et al. Practical quantum digital signature with a gigahertz BB84 quantum key distribution system[J]. Optics Letters, 2019, 44(1): 139-142.

[13] 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(4):666-669.

[14] Su Q, Huang Z, Wen Q Y, et al. Quantum blind signature based on two-state vector formalism [J]. Optics Communications, 2010, 283(21): 4408-4410.

[15] Wang M M, Chen X B, Yang Y X. A blind quantum signature protocol using the GHZ states [J]. Science China Physics, Mechanics and Astronomy, 2013, 56(9): 1636-1641.

[16] Khodambashi S, Zakerolhosseini A. A sessional blind signature based on quantum cryptography[J]. Quantum Information Processing, 2014, 13(1): 121-130.

[17] Tian Y, Chen H, Ji S F, et al. A broadcasting multiple blind signature scheme based on quantum teleportation[J]. Optical and Quantum Electronics, 2014, 46(6): 769-777.

[18] Zhang W, Qiu D W, Zou X F, et al. Analyses and improvement of a broadcasting multiple blind signature scheme based on quantum GHZ entanglement [J]. Quantum Information Processing, 2017, 16(6): 1-23.

[19] Chen F L, Wang Z H, Hu Y M. A new quantum blind signature scheme with BB84-state[J]. Entropy, 2019, 21(4): 336.

[20] Liang X Q, Wu Y L, Zhang Y H, et al. Quantum multi-proxy blind signature scheme based on four-qubit cluster states [J]. International Journal of Theoretical Physics, 2019, 58(1): 31-39.

[21] Liu G, Ma W P, Cao H, et al. A novel quantum group proxy blind signature scheme based on five-qubit entangled state [J]. International Journal of Theoretical Physics, 2019, 58(6): 1999-2008.

[22] Zhang J L, Zhang J Z, Xie S C. Improvement of a quantum proxy blind signature scheme[J]. International Journal of Theoretical Physics, 2018, 57(6): 1612-1621.

[23] Yang Y Y, Xie S C, Zhang J Z. An improved quantum proxy blind signature scheme based on genuine seven-qubit entangled state [J]. International Journal of Theoretical Physics, 2017, 56(7): 2293-2302.

[24] Li X Y, Chang Y, Zhang S B, et al. Quantum blind signature scheme based on quantum walk [J]. International Journal of Theoretical Physics, 2020, 59(7): 2059-2073.

[25] Niu X F, Ma W P, Chen B Q, et al. A quantum proxy blind signature scheme based on superdense coding [J]. International Journal of Theoretical Physics, 2020, 59(4): 1121-1128.

[26] Lou X P, Tang W S, Long H, et al. A quantum blind signature scheme based on block encryption and quantum Fourier transfer[J]. International Journal of Theoretical Physics, 2019, 58(10): 3192-3202.

[27] Renner R. Security of quantum key distribution[J]. International Journal of Quantum Information, 2008, 6(1): 1-127.

[28] Shannon C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4): 656-715.