量子多重代理盲签名协议

姚洪迪 邹 海
(安徽大学计算机科学与技术学院 合肥 230601)

摘 要 多数情况下,原始签名人只需委托一个代理人对文件进行签名,但是为了分散代理签名人的权利,使得多人对文件进行代理签名,提出了一种量子多重代理盲签名协议。该协议利用了Bell态和Bell测量之间的关联特性,使得原始签名人可以委托多人对文件进行签名,而且签名人数可以根据实际的需求进行变化,提高了方案的灵活性。安全性分析表明,该协议能够抵制内部攻击和外部攻击,是一个安全可实现的协议。

关键词 量子签名,多重代理签名,Bell态,Bell测量

中图法分类号 TN918 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.07.019

Quantum Multi-proxy Blind Signature Protocol

YAO Hong-di ZOU Hai
(School of Computer Science and Technology, Anhui University, Hefei 230601, China)

Abstract In most cases, the original signer only needs to entrust one proxy to sign the file. But in order to decentralize the proxy signer's rights, more proxies are invited to make a proxy signature on the file. Based on this situation, a quantum multi-proxy blind signature protocol was proposed. The protocol, which makes use of the link between Bell state and Bell measurement, can make the original signer entrust more proxies to have a signature on the file, but also the number of signers can be changed according to actual needs, which increasingly improves the flexibility of the scheme. The security analysis shows that the protocol can resist both internal attacks and external attacks, and it is a safe and achievable protocol.

Keywords Quantum signature, Multi-proxy signature, Bell state, Bell measurement

1 引言

当前是信息时代,信息安全也就自然成为了大家关注的焦点。传统的信息安全是基于计算复杂度来实现的,然而,伴随着计算机计算能力的不断提高,尤其是量子计算机逐步成为现实,经典密码的安全性受到了挑战。信息签名[1-2]是信息安全的重要部分,也是电子商务发展所依赖的重要领域,为了保证信息的绝对无条件安全,越来越多的人开始研究量子密码学。

量子密码学是基于量子的物理特性来保证其无条件安全,主要包括量子密钥分配[3-4]、量子安全通信[5]、量子认证[6]和量子秘密共享[7]等。自从Bennett和Brassard提出第一个量子密钥分发协议以来,量子密码学得到迅速的发展。2001年,曾贵华等人提出了一个基于对称密码体制的量子签名方案[8];2005年,温晓军等[9]提出了基于纠缠交换的量子信息签名方案,该方案利用纠缠粒子对交换实现量子信息签名;2009年,Li等[10]提出了使用Bell态的仲裁量子签名方案;2012年,王郁武[11]提出了Cluster态的量子签名方案,方案中使用Cluster态作为量子信道,保证其安全性;2015年,陈晓峰[12]提出了基于单粒子的仲裁量子签名方案。

本文利用了Shi等人[13]提出的量子秘密共享的基本原理,设计了一种量子多重代理盲签名协议,协议有一个可信任的仲裁Trent,一个消息的拥有者Alice,一个原始签名人Bob,m个代理签名人U_i,一个验证者Charlie。当原始签名人Bob不能亲自对文件进行签名时,可委托若干个代理人进行签名。本协议的特点在于代理签名的人数可以根据实际需求进行变化,增加了方案的灵活性。

2 基础知识

首先介绍Bell态和Bell测量之间的关联特性。本文主要使用了4个Bell态,分别定义如下:

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

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

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

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

到稿日期:2016-05-12 返修日期:2016-09-30 本文受国家自然科学基金项目(61374128)资助。

姚洪迪(1992—),男,硕士生,主要研究方向为量子密码学,E-mail:751558479@qq.com;邹 海(1969—),男,博士,副教授,主要研究方向为信息安全。

(1)如果把 Bell 态$|\phi^+\rangle$编码为 00，$|\phi^-\rangle$编码为 01，$|\psi^+\rangle$编码为 10，$|\psi^-\rangle$编码为 11，此时，从中任意选出两个 Bell 态，对其 1,3 粒子和 2,4 粒子分别进行 Bell 基测量，有如下几种可能情况：

$$|\phi^+\rangle_{12}|\phi^+\rangle_{34}=\frac{1}{2}(|\phi^+\rangle_{13}|\phi^+\rangle_{24}+|\phi^-\rangle_{13}|\phi^-\rangle_{24}+|\psi^+\rangle_{13}|\psi^+\rangle_{24}+|\psi^-\rangle_{13}|\psi^-\rangle_{24}) \quad (5)$$

$$|\phi^+\rangle_{12}|\phi^-\rangle_{34}=\frac{1}{2}(|\phi^+\rangle_{13}|\phi^-\rangle_{24}-|\phi^+\rangle_{13}|\psi^-\rangle_{24}+|\phi^-\rangle_{13}|\phi^+\rangle_{24}-|\psi^-\rangle_{13}|\psi^+\rangle_{24}) \quad (6)$$

$$|\phi^+\rangle_{12}|\psi^+\rangle_{34}=\frac{1}{2}(|\phi^+\rangle_{13}|\psi^+\rangle_{24}+|\psi^+\rangle_{13}|\phi^+\rangle_{24}+|\phi^-\rangle_{13}|\psi^-\rangle_{24}+|\psi^-\rangle_{13}|\phi^-\rangle_{24}) \quad (7)$$

$$|\phi^+\rangle_{12}|\psi^-\rangle_{34}=\frac{1}{2}(|\phi^+\rangle_{13}|\psi^-\rangle_{24}+|\phi^-\rangle_{13}|\psi^+\rangle_{24}-|\psi^+\rangle_{13}|\phi^-\rangle_{24}-|\psi^-\rangle_{13}|\phi^+\rangle_{24}) \quad (8)$$

$$|\phi^-\rangle_{12}|\phi^-\rangle_{34}=\frac{1}{2}(|\phi^+\rangle_{13}|\phi^+\rangle_{24}+|\phi^-\rangle_{13}|\phi^-\rangle_{24}-|\psi^+\rangle_{13}|\psi^+\rangle_{24}-|\psi^-\rangle_{13}|\psi^-\rangle_{24}) \quad (9)$$

$$|\phi^-\rangle_{12}|\psi^+\rangle_{34}=\frac{1}{2}(|\phi^+\rangle_{13}|\psi^-\rangle_{24}+|\phi^-\rangle_{13}|\psi^+\rangle_{24}+|\psi^+\rangle_{13}|\phi^-\rangle_{24}+|\psi^-\rangle_{13}|\phi^+\rangle_{24}) \quad (10)$$

$$|\phi^-\rangle_{12}|\psi^-\rangle_{34}=\frac{1}{2}(|\phi^+\rangle_{13}|\psi^+\rangle_{24}+|\phi^-\rangle_{13}|\psi^-\rangle_{24}-|\psi^+\rangle_{13}|\phi^+\rangle_{24}-|\psi^-\rangle_{13}|\phi^-\rangle_{24}) \quad (11)$$

$$|\psi^+\rangle_{12}|\psi^+\rangle_{34}=\frac{1}{2}(|\phi^+\rangle_{13}|\phi^+\rangle_{24}-|\phi^-\rangle_{13}|\phi^-\rangle_{24}+|\psi^+\rangle_{13}|\psi^+\rangle_{24}-|\psi^-\rangle_{13}|\psi^-\rangle_{24}) \quad (12)$$

$$|\psi^+\rangle_{12}|\psi^-\rangle_{34}=\frac{1}{2}(-|\phi^+\rangle_{13}|\phi^-\rangle_{24}+|\phi^-\rangle_{13}|\phi^+\rangle_{24}+|\psi^+\rangle_{13}|\psi^-\rangle_{24}-|\psi^-\rangle_{13}|\psi^+\rangle_{24}) \quad (13)$$

$$|\psi^-\rangle_{12}|\psi^-\rangle_{34}=\frac{1}{2}(|\phi^+\rangle_{13}|\phi^+\rangle_{24}-|\phi^-\rangle_{13}|\phi^-\rangle_{24}-|\psi^+\rangle_{13}|\psi^+\rangle_{24}+|\psi^-\rangle_{13}|\psi^-\rangle_{24}) \quad (14)$$

通过上式的计算可以得到如下关系：

$$R_{12}\oplus R_{34}=M_{13}\oplus M_{24} \quad (15)$$

其中，R_{12}，R_{34}表示原始 Bell 态编码后的结果，M_{13}，M_{24}表示测量后的 Bell 态编码后的结果。以式(7)为例，$R_{12}\oplus R_{34}=00\oplus 10=10$，那么其可能的测量结果$M_{13}\oplus M_{24}$也都为 10。

(2)此时，如果从 4 个 Bell 态中任意选出 3 个，以$|\phi^+\rangle_{12}$，$|\phi^-\rangle_{34}$，$|\psi^+\rangle_{56}$为例，对其 1,6 粒子，2,3 粒子，4,5 粒子进行 Bell 基测量，可能的测量结果如下：

$$\begin{aligned}&|\phi^+\rangle_{12}|\phi^-\rangle_{34}|\psi^+\rangle_{56}\\&=\frac{1}{\sqrt{2}}(|00\rangle_{12}+|11\rangle_{12})\otimes\frac{1}{\sqrt{2}}(|00\rangle_{34}-|11\rangle_{34})\otimes\frac{1}{\sqrt{2}}(|01\rangle_{56}+|10\rangle_{56})\\&=\frac{1}{4}(|\psi^+\rangle_{16}|\phi^+\rangle_{23}|\phi^-\rangle_{45}+|\psi^+\rangle_{16}|\phi^-\rangle_{23}|\phi^+\rangle_{45}+|\psi^-\rangle_{16}|\phi^+\rangle_{23}|\phi^+\rangle_{45}+|\psi^-\rangle_{16}|\phi^-\rangle_{23}|\phi^-\rangle_{45}+|\phi^+\rangle_{16}|\phi^+\rangle_{23}|\psi^-\rangle_{45}+|\phi^+\rangle_{16}|\phi^-\rangle_{23}|\phi^+\rangle_{45}+|\phi^-\rangle_{16}|\phi^+\rangle_{23}|\phi^+\rangle_{45}+|\phi^-\rangle_{16}|\phi^-\rangle_{23}|\psi^+\rangle_{45}+|\psi^+\rangle_{16}|\psi^-\rangle_{23}|\psi^-\rangle_{45}+|\phi^+\rangle_{16}|\phi^+\rangle_{23}|\phi^-\rangle_{45}-|\phi^+\rangle_{16}|\psi^-\rangle_{23}|\phi^+\rangle_{45}-|\phi^-\rangle_{16}|\phi^+\rangle_{23}|\phi^+\rangle_{45}+|\phi^-\rangle_{16}|\psi^-\rangle_{23}|\phi^-\rangle_{45})\end{aligned} \quad (16)$$

通过式(16)的计算，可以得到原始 Bell 态和可能的测量结果之间满足：

$$R_{12}\oplus R_{34}\oplus R_{56}=M_{16}\oplus M_{23}\oplus M_{45} \quad (17)$$

其中，R_{12}，R_{34}，R_{56}表示原始 Bell 态编码后的结果，M_{16}，M_{23}，M_{45}表示测量后的 Bell 态编码后的结果。

通过类比可以得出，任意从 4 个 Bell 态中选出 3 个，按照上式的方式进行测量，都满足式(17)之间的关系。

(3)由此，可以推出，如果从 4 个 Bell 态中任意选出 n 个，按照如上的关系进行 Bell 基测量，那么原始 Bell 态和可能的测量结果之间将满足如下特性：

$$R_{12}\oplus R_{34}\oplus\cdots\oplus R_{(2n-1)2n}=M_{1(2n)}\oplus M_{23}\oplus M_{45}\oplus\cdots\oplus M_{(2n-2)(2n-1)} \quad (18)$$

3　协议描述

本协议涉及的参与人员可以描述为：消息的拥有者Alice，原始签名人 Bob，代理签名人U_1，U_2，…，U_m，验证者 Charlie 以及一个可信任中心 Trent。协议包括 4 个阶段：协议初始化阶段、代理授权阶段、代理签名阶段、验证阶段。

3.1　协议初始化阶段

步骤 1　Alice 将待签名的消息转化为二进制序列 $m=\{m(1),m(2),\cdots,m(i),\cdots,m(2n)\}$。

步骤 2　Alice 和 Trent 共享 $2n$ 位的密钥 K_{AT}，Bob 和 Trent 共享 $2n$ 位的密钥 K_{BT}，第一位代理签名人 U_1 与 Trent 共享 $2n$ 位的密钥 K_{U_1T}，代理签名人 U_i 与 U_{i+1} 之间共享密钥 $K_{U_iU_{i+1}}$ $(1\leqslant i\leqslant m-1)$，同时，Charlie 与 Trent 共享 $2n$ 位的密钥 K_{CT}，并与最后一个代理签名人 U_m 共享密钥 K_{U_mC}。这些密钥的分发全部使用 BB84 协议或 B92 协议，确保密钥的无条件安全。

步骤 3　Trent 使用本文中提到的方案，随机从 4 个 Bell 态中选择 n 组 $m+3$ 对 Bell 态。这些 Bell 态被分成 n 组，每组 $m+3$ 对。其每组量子分发的示意图如图 1 所示。

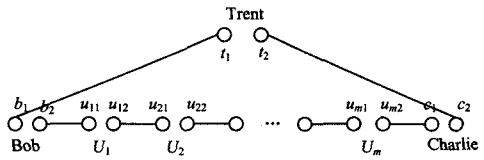

图 1　量子分发示意图

其中，Trent 所拥有的两个粒子序列记为 $S_{t_1}=[P_1(t_1),P_2(t_1),\cdots,P_n(t_1)]$，$S_{t_2}=[P_1(t_2),P_2(t_2),\cdots,P_n(t_2)]$，Bob 的记为 $S_{b_1}=[P_1(b_1),P_2(b_1),\cdots,P_n(b_1)]$，$S_{b_2}=[P_1(b_2),P_2(b_2),\cdots,P_n(b_2)]$，$U_i$ 的记为 $S_{u_{i1}}=[P_1(u_{i1}),P_2(u_{i1}),\cdots,P_n(u_{i1})]$ $(1\leqslant i\leqslant m)$，$S_{u_{i2}}=[P_1(u_{i2}),P_2(u_{i2}),\cdots,P_n(u_{i2})]$ $(1\leqslant i\leqslant m)$，Charlie 的记为 $S_{c_1}=[P_1(c_1),P_2(c_1),\cdots,P_n(c_1)]$，$S_{c_2}=[P_1(c_2),P_2(c_2),\cdots,P_n(c_2)]$。在 Trent 为 Bob，$U_i$，Charlie 分发粒子序列之前，需要在每一个序列中插入一定数量的诱导粒子$\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$，来进行窃听检测。Bob，$U_i$，Charlie 在收到序列后，根据 Trent 公布的诱导粒子的位

置和状态与自己的粒子进行比较，如果错误率高于所规定的阈值，则取消此次协议，重新生成序列进行发送，否则说明不存在窃听，然后去掉诱导粒子，恢复成初始序列。

步骤 4 Trent 对原始的 $m+3$ 个 n 组 Bell 态分别进行编码（$|\phi^+\rangle$ 编码为 00，$|\phi^-\rangle$ 编码为 01，$|\psi^+\rangle$ 编码为 10，$|\psi^-\rangle$ 编码为 11），即对 $(P_i(t_1),P_i(b_1))(1\leqslant i\leqslant n)$，$(P_i(b_2),P_i(u_{11}))(1\leqslant i\leqslant n)$，$(P_i(u_{12}),P_i(u_{21}))(1\leqslant i\leqslant n)$，…，$(P_i(u_{m2}),P_i(c_1))(1\leqslant i\leqslant n)$，$(P_i(c_2),P_i(t_2))(1\leqslant i\leqslant n)$ 分别进行编码，将最终编码后的比特串分别记为 p_t，p_b，$p_{u_i}(1\leqslant i\leqslant m)$ 和 p_c，并做如下计算：

$$p_1=p_t\oplus p_b\oplus p_{u_1}\oplus p_{u_2}\oplus\cdots\oplus p_{u_m}\oplus p_c \tag{19}$$

至此，整个协议的初始化完成。

3.2 代理授权阶段

步骤 1 Alice 使用密钥 K_{AT} 对消息 m 进行加密，得到密文 $E_{K_{AT}}(m)$，加密使用一次一密算法，保证其无条件安全。

步骤 2 Alice 将密文 $E_{K_{AT}}(m)$ 发送给 Trent，Trent 使用与 Bob 共享的密钥 K_{BT} 并将其加密后发送给 Bob，Bob 收到后使用 K_{BT} 将其解密，得到密文 $E_{K_{AT}}(m)$。

步骤 3 若 Bob 同意代理签名的授权，则 Bob 对自己手中的粒子序列 S_{b_1}，S_{b_2} 中的相应粒子进行 n 次 Bell 基测量，即分别对 $(P_i(b_1),P_i(b_2))(1\leqslant i\leqslant n)$ 进行 Bell 基测量。将测量后的结果转化为相应的二进制串，记为 k_b（k_b 即可作为 Bob 授权的凭证）。Bob 使用与 Trent 共享的密钥 K_{BT} 加密 $E_{K_{AT}}(m)$ 和 k_b，即 $E_{K_{BT}}(E_{K_{AT}}(m),k_b)$，然后将其发送给 Trent。Trent 使用 K_{BT} 将其解密，然后用 K_{U_1T} 加密，得到密文 $E_{K_{U_1T}}(E_{K_{AT}}(m),k_b)$，发送给代理签名人 U_1，U_1 解密后得到密文 $E_{K_{AT}}(m)$ 和授权凭证 k_b。至此，完成整个代理授权的过程。

3.3 代理签名阶段

步骤 1 U_1 对自己手中的粒子序列 $S_{u_{11}}$，$S_{u_{12}}$ 中的相应粒子进行 n 次 Bell 基测量，即分别对 $(P_i(u_{11}),P_i(u_{12}))(1\leqslant i\leqslant n)$ 进行 Bell 基测量。将测量后的结果转化为相应的二进制串，记为 k_{u_1}。

步骤 2 U_1 使用 k_{u_1} 与解密后得到的 k_b 进行异或操作，并将其作为自己对密文 $E_{K_{AT}}(m)$ 的签名操作，然后使用与 U_2 共享的密钥 $K_{U_1U_2}$ 进行加密，得到 $E_{K_{U_1U_2}}(E_{K_{AT}}(m),k_b\oplus k_{u_1})$，再将其发送给 U_2。

步骤 3 U_2 将其解密后，重复上述操作，直到最后一名代理签名人 U_m 完成其签名过程。此时，U_m 使用密钥 K_{U_mC} 对密文和签名后的结果进行加密，即 $E_{K_{U_mC}}(E_{K_{AT}}(m),k_b\oplus k_{u_1}\oplus k_{u_2}\oplus\cdots\oplus k_{u_m})$，然后将加密后的结果发送给验证者 Charlie。

3.4 验证阶段

步骤 1 Charlie 使用 K_{U_mC} 对密文进行解密得到 $E_{K_{AT}}(m)$ 和 $k_b\oplus k_{u_1}\oplus k_{u_2}\oplus\cdots\oplus k_{u_m}$，并通过经典信道通知 Trent 进行辅助验证。

步骤 2 Trent 对其手中的粒子序列 S_{t_1}，S_{t_2} 进行 Bell 基测量，即分别对 $(P_i(t_1),P_i(t_2))(1\leqslant i\leqslant n)$ 进行 Bell 基测量。将测量后的结果转化为相应的二进制串，记为 k_t。

步骤 3 Trent 用与验证者 Charlie 共享的密钥 K_{CT} 加密 k_t 和 $p_1(p_1=p_t\oplus p_b\oplus p_{u_1}\oplus p_{u_2}\oplus\cdots\oplus p_{u_m}\oplus p_c)$，即 $E_{K_{CT}}(k_t,p_1)$，将加密后的结果发送给验证者 Charlie。

步骤 4 Charlie 使用密钥 K_{CT} 解密得到 k_t 和 p_1。然后对自己手中的粒子序列 S_{c_1}，S_{c_2} 进行 Bell 基测量，即分别对 $(P_i(c_1),P_i(c_2))(1\leqslant i\leqslant n)$ 进行 Bell 基测量。将测量后的结果转化为相应的二进制串，记为 k_c。按照第 2 节中提及的方法，如果前面的步骤中没有窃听者或者发生任何错误，那么此时 k_t，$k_b\oplus k_{u_1}\oplus k_{u_2}\oplus\cdots\oplus k_{u_m}$，$k_c$ 和 p_1 之间应该满足：

$$p_1=k_t\oplus k_b\oplus k_{u_1}\oplus k_{u_2}\oplus\cdots\oplus k_{u_m}\oplus k_c \tag{20}$$

即 $p_t\oplus p_b\oplus p_{u_1}\oplus p_{u_2}\oplus\cdots\oplus p_{u_m}\oplus p_c=k_t\oplus k_b\oplus k_{u_1}\oplus k_{u_2}\oplus\cdots\oplus k_{u_m}\oplus k_c$。

如果 Charlie 的计算结果满足式(20)，则说明签名有效，此时，Charlie 要求 Alice 公布密钥 K_{AT}，然后解密得到原始消息 m；否则拒绝签名。

至此，整个协议完成。

4 安全性分析

4.1 外部攻击

(1)假设攻击者 Eve 在 Trent 给各个参与方发送粒子时采用截获重发攻击，但是，由于 Eve 并不知道粒子序列中哪些位置插入了诱导粒子{$|0\rangle$，$|1\rangle$，$|+\rangle$，$|-\rangle$}，因此 Eve 进行随机猜测而不被检测到的概率为 $(\frac{1}{4})^m$，其中，m 为诱导粒子的数量，当 m 的数量足够大时，不被检测到的概率趋于 0。

(2)假如 Eve 试图伪造签名，也是不可能成功的。其一，Bob 在未对自己的粒子进行测量之前，U_i 所拥有的粒子状态是不确定的，U_i 所拥有的签名信息 k_{u_i} 也是未知的。其二，每一个代理签名者 U_i 都必须使用与 U_{i+1} 共享的密钥 $K_{U_iU_{i+1}}$ 加密后才能发送信息，而密钥 $K_{U_iU_{i+1}}$ 是由 BB84 协议或 B92 协议进行分发，确保其无条件安全。

4.2 内部攻击

(1)原始签名人 Bob 试图伪造代理签名也是不可能成功的。量子序列的分发使得 Bob 只能测量自己的量子序列，在测量后，代理签名者 U_i 手中的粒子塌缩后的状态 Bob 是未知的。这一特性决定了 Bob 不可能伪造代理签名。同理，第一个代理签名者 U_1 并不知道其他签名者手中的信息，不可能伪造签名，而后续的代理签名者 $U_i(2\leqslant i\leqslant m)$ 拿到的是 k_b 与 $k_{u_{i-1}}(2\leqslant i\leqslant m)$ 异或后的结果，仅凭异或后的结果是不能推出签名信息 k_{u_i} 的，因此任意一个代理签名者都不能伪造签名。同样，作为验证者的 Charlie，他得到的是 k_b 与 $k_{u_i}(1\leqslant i\leqslant m)$ 异或后的结果，因此 Charlie 也不能伪造签名。

(2)代理签名者 U_i 试图抵赖签名也是不可能成功的。假如有一个签名者没有进行签名，那么此时式(20)是不成立的，Charlie 的验证过程是不可能通过的。而签名者 U_i 的签名信息 k_{u_i} 对其他人来说都是未知的，因此验证一旦通过，说明 U_i 一定对其进行了签名。

同样，Bob 试图抵赖其委托代理签名也是不可能成功的。Bob 的授权凭证 k_b 是使用密钥 K_{BT} 进行传递的，而且授权凭证 k_b 也需要满足式(20)，因此 Bob 不能抵赖其委托代理签名。

(下转第 127 页)

nics (ICEOE). IEEE,2011:V4-308-V4-311.

[13] YEO C S,BUYYA R. Integrated risk analysis for a commercial computing service[C]// Proceedings of the 2007 IEEE International Parallel and Distributed Processing Symposium (IPDPS 2007). IEEE,2007:1-10.

[14] XU X,YU H,PEI X. A Novel Resource Scheduling Approach in Container Based Clouds[C]// Proceedings of the 2014 IEEE 17th International Conference on Computational Science and Engineering (CSE). IEEE,2014:257-264.

[15] DEJUN J,PIERRE G,CHI C H. EC2 performance analysis for resource provisioning of service-oriented applications[C]// Proceedings of the 2010 International Conference on Service-oriented Computing. Springer-Verlag,2010:197-207.

[16] YU L,XIE Y,CHEN B H,et al. Towards Runtime Dynamic Provision of Virtual Resources using Feedforward and Feedback Control[J]. Journal of Computer Research and Development, 2015(4):889-897.

[17] ADUFU T,CHOI J,KIM Y. Is container-based technology a winner for high performance scientific applications? [C]// Proceedings of the 2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS). IEEE,2015:507-510.

[18] CAI K Y,WANG X Y. Towards a control-theoretical approach to software fault-tolerance[C]// Proceedings of the 2004 Fourth International Conference on Quality Software (QSIC 2004). IEEE,2004:198-205.

[19] LIN R,CHEN B,XIE Y,et al. Learning-Based Multi-controller Coordination for Self-Optimization[C]// Proceedings of the 2012 IEEE 36th Annual Computer Software and Applications Conference Workshops (COMPSACW). IEEE,2012:164-169.

[20] YU S,WANG C,REN K,et al. Achieving secure,scalable,and fine-grained data access control in cloud computing[C]// Proceedings of the 2010 IEEE Infocom. IEEE,2010:1-9

(上接第 106 页)

(3)假设仲裁者 Trent 是不诚实的,那么他企图伪造签名也是不可能成功的。首先,U_i 所拥有的签名信息 k_{u_i} 对 Trent 来说是未知的;其次,U_i 传递的信息都是使用密钥 $K_{U_iU_{i+1}}$ 进行加密的,因此 Trent 是不能获得签名信息的,那么他仅凭随机猜测伪造的签名是不能够通过最后的验证的。即使 Trent 与第三方的攻击者 Eve 进行合谋,也不能得到 k_{u_i} 的信息,进而不能够伪造签名。

结束语　本文提出了一个量子多重代理盲签名协议,首先介绍了 Bell 态和 Bell 测量之间的关联特性,然后利用关联特性构造密钥之间的联系,使得原始签名人的密钥与多个代理签名人密钥异或的结果构成关联,进而满足了多个人代理一个人签名的要求,而且代理签名的人数可以根据实际的需求而定,增加了协议的灵活性和应用性。最后的安全性分析表明了本协议是一个安全可实现的量子多重代理盲签名协议。

参 考 文 献

[1] STALLINGS W. Cryptography and Network Security Principles and Practices[J]. Printice Hill Publishing Pp,2005,11(7):655-660.

[2] CAO Z J,LIU M L. Classification of signature-only signature models[J]. Science in China Series F: Information Sciences,2008,51(8):1083-1095.

[3] SHOR P W,PRESKILL J. Simple proof of security of the BB84 quantum key distribution protocol[J]. Physical Review Letters,2000,85(2):441.

[4] HUGHES R J,MORGAN G L,PETERSON C G. Quantum key distribution over a 48km optical fibre network[J]. Journal of Modern Optics,2000,47(2/3):533-547.

[5] BOSTROM K,FELBINGER T. Deterministic secure direct communication using entanglement[J]. Physical Review Letters,2002,89(18):187902.

[6] ZENG G,ZHANG W. Identity verification in quantum key distribution [J]. Physical Review A,2000,61(2):22301-22303.

[7] HILLERY M,BUZEK V,BERTHIAUME A. Quantum secret sharing[J]. Physical Review A,1999,59(3):1829-1834.

[8] ZENG G H,MA W P,WANG X M,et al. Signature scheme based on quantum cryptography[J]. Acta Electronica Sinica,2001,29(8):1098-1100. (in Chinese)
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.

[9] WEN X J,LIU Y,ZHANG Z J. Signature Scheme Based on Quantum Entanglement Swapping[J]. Journal of Electronics & Information Technology,2005,27(5):811-813. (in Chinese)
温晓军,刘云,张振江. 基于纠缠交换的量子信息签名方案[J]. 电子与信息学报,2005,27(5):811-813.

[10] LI Q,CHAN W H,LONG D Y. Arbitrated quantum signature scheme using Bell states[J]. Physical Review A,2009,79(5):1744-1747.

[11] WANG Y W. Cluster state quantum entangled signature scheme [J]. Computer Engineering and Applications,2012,48(5):93-95. (in Chinese)
王郁武. Cluster 态的量子签名方案[J]. 计算机工程与应用,2012,48(5):93-95.

[12] Cheng Xiao-feng. Arbitrated quantum signature with single particle[J]. Chinese Journal of Quantum Electronics,2015,32(1):77-82. (in Chinese)
陈晓峰. 基于单粒子的仲裁量子签名方案[J]. 量子电子学报,2015,32(1):77-82.

[13] SHI R H,HUANG L S,YANG W,et al. Multiparty quantum secret sharing with Bell states and Bell measurements[J]. Optics Communications,2010,283(11):2476-2480.

[14] BUHRMAN H,CLEVE R,WATROUS J,et al. Quantum fingerprinting[J]. Physical Review Letters,2001,87(16):167902-167904.

[15] TIAN J H,ZHANG J Z,LI Y P. A Quantum Multi-proxy Blind Signature Scheme Based on Genuine Four-Qubit Entangled State [J]. International Journal of Theoretical Physics,2016,55(2):809-816.