不依赖于第三方的动态量子身份认证方案

曾贵华
(上海交通大学电子工程系,上海 200030)

摘 要: 提出了一个量子身份认证方案,该方案仅在注册时需要认证中心,以后不再依赖于任何第三方. 在方案的实施过程中采用一种动态方式,即合法通信者之间每次可动态获得一个新的认证密钥. 所提方案具有可证明安全性,安全性由量子不可克隆性和方案本身的动态特性保证.

关键词: 身份认证; 量子密码; 密码学
中图分类号: TN918.1 **文献标识码**: A **文章编号**: 0372-2112 (2004) 07-1148-04

Quantum Identity Authentication Without Trusted-Party

ZENG Gui-hua
(Electronic Engineering Department of Shanghai Jiaotong University, Shanghai 200030, China)

Abstract: A quantum identity authentication scheme which is independent on trusted-party is proposed. The main characteristic in the proposal is that the authentication key can be obtained dynamically. The security is guaranteed by the no-cloning theory and the dynamical feature of the proposed scheme.

Key words: identity authentication; quantum cryptography; cryptography

1 引言

自从第一个量子密钥分发协议 —BB84 协议[1]提出以来,量子密钥分发经过多年的努力取得了丰富的成果[2]. 但是,人们对量子认证的认识还刚刚开始. 文献[3]首次研究了量子密钥的验证问题,在此基础上,人们进一步探讨了量子身份认证[4,5]、量子签名[6,7]和量子消息确认[8]. 不过,量子认证方面还有很多问题有待进一步的研究.

本文研究量子身份认证,并设计了一个量子身份认证方案. 所提出的方案不仅可以实现量子通信中用户间的身份认证,而且可以实现文献[3]中的功能,即方案不但能分发量子密钥而且能验证所获得的密钥的可靠性. 所设计的方案采用量子逻辑门实现,因为单比特量子逻辑门技术已经成熟,因此本方案是一个可实现的有很好应用前景的方案. 另外,本方案还利用了量子比特的不可克隆性,以提高方案的整体安全性.

2 协议描述

设任意两个合法用户 A 和 B 已经向认证中心 CA 注册,注册信息分别为 I_a 和 I_b(I_a 和 I_b 可以是量子信息也可以是经典信息). 若 A 与 B 之间希望建立通信,他们首先向 CA 申请,CA 验证他们的身份后执行下面的过程.

2.1 初始阶段

设一个算子集合可表示为如下形式,

$$\sigma = \{\sigma_1, \sigma_2, \cdots, \sigma_r\} \tag{1}$$

该算子集合中的每一个算子表示一种可能的对量子比特的操作. 一般地,用户如 A 可以采用 r 种可能的操作对所选取的量子比特进行测量或做其它操作. 由于量子力学中测量算子是厄米算子,式(1)中的每一个算子都存在本征态,即

$$\sigma_i|\psi_{ij}\rangle = \lambda_{ij}|\psi_{ij}\rangle \tag{2}$$

其中 $i = 1, 2, \cdots, r$; j 表示 σ_i 的维数,$|\cdots\rangle$ 为 Dirac 符号,表示一个状态矢量,即一个量子比特;$|\psi_{ij}\rangle$ 表示状态为 ψ_{ij} 的量子比特. 于是,式(1)中算子对应的本征态矢的集合为

$$|\Psi\rangle = \{\{|\psi_{11}\rangle, |\psi_{12}\rangle, \cdots, |\psi_{1k}\rangle\}, \{|\psi_{21}\rangle, |\psi_{22}\rangle, \cdots, |\psi_{2k}\rangle\}, \cdots, \{|\psi_{r1}\rangle, |\psi_{r2}\rangle, \cdots, |\psi_{rk}\rangle\}\} \tag{3}$$

k 表示算子的维数. 考虑二维 Hilbert 空间中的算子,这时上式中 j 的取值为 $j = 1, 2$,上式可简化为,

$$|\Psi\rangle = \{\{|\psi_{11}\rangle, |\psi_{12}\rangle\}, \{|\psi_{21}\rangle, |\psi_{22}\rangle\}, \cdots, \{|\psi_{r1}\rangle, |\psi_{r2}\rangle\}\} \tag{4}$$

为方便起见,以下只考虑二维算子对应的情况.

若用户 A 希望与用户 B 建立通信,A 从 σ 中随机选取 n 个测量算子构成她的测量基序列(这里 n 可以大于、等于或小于 r),该序列所表示的集合可表示为如下形式,

$$m_a = \{m_a^1, m_a^2, \cdots, m_a^n\} \tag{5}$$

其中,$m_a^i \in \sigma (i = 1, 2, \cdots, n)$. 然后 A 生成一个随机量子比特串,

$$S_a^0 = \{|\psi_1^0\rangle, |\psi_2^0\rangle, \cdots, |\psi_n^0\rangle\} \tag{6}$$

用式(5)中对应的算子作用于式(6)中的每一个量子比特得到

收稿日期:2002-11-15;修回日期:2003-05-12
基金项目:国家自然科学基金项目(No. 60102001);国家自然科学基金重大研究计划(No. 90104005);国家 863 项目(No. 2002AA145091)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

一个新的量子比特,

$$m_a^i|\psi_i^0\rangle \rightarrow |\psi_a^i\rangle, \quad i=1,2,\cdots,n \tag{7}$$

由此得到一个新的量子比特串,

$$S_a=\{|\psi_a^1\rangle,|\psi_a^2\rangle,\cdots,|\psi_a^n\rangle\} \tag{8}$$

式(8)实际上是将随机生成的量子比特投影到相应的测量基的本征态矢上,因此,$|\psi_a^i\rangle$是 m_a^i 的本征态集合中的一个. $|\psi_a^i\rangle$可以一般地表示为,

$$|\psi_a^i\rangle=a_i|0\rangle+b_i|1\rangle, \quad i=1,2,\cdots,n \tag{9}$$

其中系数 a_i 和 b_i 为复数,且 $\|a_i\|^2+\|b_i\|^2=1$,$|0\rangle$和$|1\rangle$为二维 Hilbert 空间中的基矢,在实际系统中 a_i 和 b_i 是一个具体的值. 一般地,$|\psi_a^i\rangle$可以从 A 的测量算子的本征态集合中随机选取,如式(8)所示.

设表示用户 A 的身份信息的量子比特串为 I_a. 量子比特串 S_a 中有 n 个量子比特,这些量子比特对应 n 个量子(如光子、电子、光子偏振、光子相位等),用 P_a 表示这些量子的集合. 用户 A 将$\{P_a, I_a\}$发送给认证中心,根据用户 A 提供的信息 I_a,认证中心 CA 对用户 A 做身份认证. 若 A 的身份正确,CA 将$\{P_a, I_b\}$发送给用户 B,其中 I_b 为 CA 与 B 间的量子身份信息. 若 I_b 正确或 B 对 CA 的验证成功,B 接受 S_a,否则拒绝. 为描述方便,记 B 收到的量子比特串为 S_b. 在 CA 转发 S_a 的过程中,基于安全性的考虑不允许 CA 对 S_a 做任何操作,理由将在后面叙述. 上面的描述过程如图 1 所示,在 A 到 CA 和 CA 到 B 之间的通信中需要分别验证用户 A 的身份和 CA 的身份,这个过程可以采用经典的方法实现,也可以采用量子方法实现.

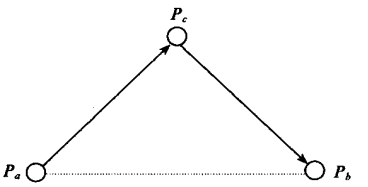

图 1　量子比特在用户 A,认证中心 CA 和用户 B 之间的分发模型

收到 S_b 后,用户 B 从式(1)表示的算子集合 σ 中随机选取 n 个构成测量基序列,

$$m_b=\{m_b^1, m_b^2, \cdots, m_b^n\} \tag{10}$$

按照式(10)所选的测量基序列,B 用 m_b 中每一个测量算子分别测量 S_b 中的相应的量子比特$|\psi_a^i\rangle$,测量后得到一个测量结果$|\psi_b^i\rangle$,即

$$|\psi_b^i\rangle=m_b^i|\psi_a^i\rangle, \quad i=1,2,\cdots,n \tag{11}$$

$|\psi_a^i\rangle$和$|\psi_b^i\rangle$可能相等也可能不相等,具体结果由 m_a^i 和 m_b^i 决定.

A 和 B 公布他们的随机测量基序列 m_a^i 和 m_b^i,保留测量基相同的测量结果,放弃测量基不同的测量结果. 例如,若 $m_a^i=m_b^i$ 则保留相应的测量结果$|\psi_a^i\rangle$和$|\psi_b^i\rangle$,因为这种情况下 A 和 B 相互知道各自的测量结果;若 $m_a^i\neq m_b^i$ 则放弃相应的测量结果,因为这种情况下 A 和 B 无法知道对方的测量结果.

在理想条件下,即信道无噪音和窃听等干扰的情况下,通过上面的操作后,A 和 B 所得到的量子比特串相同,即 $S_a=S_b$. 但是,由于噪音和窃听等因素的影响,S_a 和 S_b 中存在一定的差异. 这个差异可以通过经典保密加强和密钥协商等经典方法解决,也可以采用纯量子它方法实现.

通过上面的操作,A 和 B 最终获得共享密钥 K_a 和 K_b,且 $K_a=K_b=K$. K由 n 个量子比特构成,即

$$K_a=K_a=K=\{|k_1\rangle,|k_2\rangle,\cdots,|k_n\rangle\} \tag{12}$$

其中任意一个元素$|k_i\rangle=\alpha_i|0\rangle+\beta_i|1\rangle$,且 $\|\alpha_i\|^2+\|\beta_i\|^2=1$.

2.2　认证阶段

当 A 和 B 需要建立通信并验证他们的身份时,他们执行下面的步骤,第一步,建立量子信道. 用户 A 随机产生一个量子比特串,并将该量子比特串发送给用户 B,收到该量子比特串后,剔除传输和接收测量中所产生的错误,设所获得的最终量子比特串为

$$S=\{|\phi_1\rangle,|\phi_2\rangle,\cdots,|\phi_m\rangle\} \tag{13}$$

这里 $m>n$,$|\phi_i\rangle$可表示为$|\phi_i\rangle=\omega_1|0\rangle+\omega_2|1\rangle$.

将上面的量子比特串 S 分为两部分:S_1 和 S_2,其中 S_1 的长度为 n,由 S 中前面 n 个量子比特构成,

$$S_1=\{|\phi_1\rangle,|\phi_2\rangle,\cdots,|\phi_n\rangle\} \tag{14}$$

该量子比特串用于验证 A 和 B 的身份. S_2 的长度为 $m-n$,由 S 中后面 $m-n$ 个量子比特构成,

$$S_2=\{|\phi_{n+1}\rangle,|\phi_{n+2}\rangle,\cdots,|\phi_m\rangle\} \tag{15}$$

该量子比特串用于获取新的认证密钥.

第二步,验证身份. 根据上面所获得的 S_1 和初始阶段分配的共享密钥 K可实现对通信用户 A 和用户 B 的身份验证,具体做法如下:首先,在认证密钥 K_b 的控制下,B 利用量子 Vernam 密码算法[9]对 S_1 加密,从而得到,

$$S_1'=US_1=\{u^{\beta_1}|\phi_1\rangle,u^{\beta_2}|\phi_2\rangle,\cdots,u^{\beta_n}|\phi_n\rangle\} \tag{16}$$

其中,β_i 是$|k_i\rangle=\alpha_i|0\rangle+\beta_i|1\rangle$($i=1,2,\cdots,n$)中 β_i 的取值. 为方便起见,假设 β_i 有四个可能的取值,于是 u^{β_i}也有四个可能的取值,即

$$u^{\beta_i}\in\{u^0,u^{1/2},u^{-1/2},u^1\} \tag{17}$$

用单位矩阵 I 代替 u^0,Pauli 矩阵的 x 分量代替 $u^{1/2}$,Hadaman 矩阵 H 代替 $u^{-1/2}$,Pauli 矩阵的 z 分量代替 u^1,则 u^{β_i}作用在$|\phi_i\rangle$产生四种可能的结果,

$$u^{\beta_i}|\phi_i\rangle=\begin{cases}u^0|\phi_i\rangle\rightarrow I|\phi_i\rangle=|\phi_i\rangle\\ u^{1/2}|\phi_i\rangle\rightarrow X|\phi_i\rangle=\omega_2|0\rangle+\omega_1|1\rangle\\ u^{-1/2}|\phi_i\rangle\rightarrow H|\phi_i\rangle=\dfrac{\omega_2+\omega_1}{\sqrt{2}}|0\rangle+\dfrac{\omega_2-\omega_1}{\sqrt{2}}|1\rangle\\ u^1|\phi_i\rangle\rightarrow Z|\phi_i\rangle=\omega_1|0\rangle-\omega_2|1\rangle\end{cases} \tag{18}$$

完成上面的操作后,B 将 S_1' 发送给 A. A 对收到的量子比特串 S_1' 做逆操作,也就是说,采用算子$(u^{\beta_i})^{-1}$作用于 S_1' 上,根据获得的结果判定 B 的身份是否真实.

上述身份认证过程可用图 2 所示的模型表示. 图中实线表示一个量子信道,该量子信道反映出量子比特在单比特量子逻辑门 G 的作用下的转化过程. 具体来说,量子比特$|\phi_i\rangle$在单量子比特逻辑门 G 的作用下成为一个新的量子比特$|c_i\rangle$,然后$|c_i\rangle$在

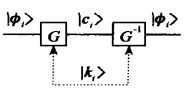

图 2　身份认证过程的信道模型

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

单比特量子逻辑门 G^{-1}的作用下又被编码成$|\phi_i\rangle$. 当然,单比特量子门 G和 G^{-1}受到密钥 K_a和 K_b的控制. 除了上面提到的量子信道,这里还涉及到一个经典信道,即密钥信道,图中用虚线表示.

第三步,获取新的量子认证密钥:A和 B以量子比特串 S_2为基本量子比特串获得新的共享密钥,其实现和操作过程可采用类似于 BB84 协议的有关操作方式. 即首先对 S_2做随机测量,然后比较各自采取的测量基,最后,利用保密加强等手段获取最后的认证密钥. 由于这里采用一般性量子比特串,方案在理论上具有更好的通用性,但是,在具体操作时需要考虑多个测量基的使用与操作,因此比 BB84 协议略微复杂.

3 安全性分析

为了比较全面地考察本文提出的协议是否安全,下面从量子攻击和经典攻击两个方面着手讨论本文方案的安全性问题. 本文方案的安全性包括两个阶段的安全性:初始阶段和认证阶段. 为了统一描述方案的安全性,用$|S\rangle$统一表示用户 A发送的量子比特串 S_a(初始阶段)和 S(认证阶段).

首先考察协议受到量子攻击的情况. 为了获取用户 A和 B间的共享信息,即认证密钥,攻击者可以采取三种量子方式进行攻击:第一种为个体攻击,这种攻击方式是对用户 A和 B间传送的量子比特串中每一个量子比特做单个处理,并获取信息;第二种是集体攻击,这种攻击方式将通信用户 A和 B间传送的量子比特串作为一个统一体,采用量子系统的处理方法进行攻击. 第三种方式是前面两种攻击方式的结合. 从本质上来说,只要前面两种方式不能成功,则第三种方式必然不能成功. 因此,下面主要分析第一种和第二种攻击方式.

第一种策略的具体攻击方式有:1) 复制量子比特串$|S\rangle$; 2) 采用截取/重发攻击. 首先研究复制量子比特$|S\rangle$的攻击方法. 攻击者要获取 A和 B间的共享信息,必须能够精确地复制量子比特串$|S\rangle$,即要求攻击者者有一种特殊的量子机器,这种机器能够克隆未知量子比特. 但是,由于组成量子比特串$|S\rangle$中的量子比特是不正交的,量子不可克隆定理表明,攻击者不可能获得$|S\rangle$的翻版,即精确复制$|S\rangle$. 因此,攻击者的操作将不可避免地引入错误,根据量子力学中的测不准原理,合法用户根据结果中产生的错误可以识别出是否有攻击者的存在与否,不诚实的攻击者不能获得 A和 B间的共享信息. 实际上,在这种情况下,即便是认证中心 CA 也是不可能获取 A和 B间的共享信息,其中理由与上面一样,这就是为什么不允许 CA 对 S_a做任何操作的原因. 当然,这是建立在不诚实 CA 只能进行被动攻击而不能进行主动攻击的前提下的(这是量子密码中通常采用的假定条件). 需要强调的是,对于有主动攻击能力的 CA,则本文的方案要求 CA 是可信赖的,因为一个不可信赖的 CA 可以采用中间人攻击的方式使自己与 A和 B共享消息 m_{ac}和 m_{bc},从而可以获取用户 A和 B之间的有效信息. 当然,在量子保密通信中,用户 A和 B之间需要建立两个信道:一个经典信道和一个量子信道. 在实际通信中,攻击者同时获取两种信道上的消息是很难的,因此,在量子密码中上面的攻击通常认为不可能. 除了中间人攻击外,已有研究表明,任何其它的攻击都是不可能的.

若攻击者采用截取/重发攻击方法,则攻击者将试图获取 A发出的量子比特串$|S\rangle$,这里$|S\rangle$可以是 S_a也可以是 S,其中 S_a为初始阶段 A发出的量子比特串,而 S为认证阶段发出的量子比特串. 为便于讨论,下面用$|S\rangle$统一表示 S_a和 S,设$|S\rangle$中的任意元素为$|S\rangle$,它可表示为如下形式,

$$|S_i\rangle = a_{i1}|A_i^1\rangle + a_{i2}|A_i^2\rangle, \quad i = 1,2,\cdots,n \tag{19}$$

其中$|A_i^1|$和$|A_i^2|$为 A的测量算子 m_a^i的本征态. 在这种攻击方法中攻击者试图获取 A发出的量子比特串 S_a或 S,然后通过各种量子方法从中获取有效信息. 其中,最有效的方法是对所获取的量子比特串做幺正操作,用 n_e表示这个幺正操作. 攻击者要想获得有效信息,只能以它的本征态为测量基矢进行测量. 设攻击者的单位测量基矢为$|E_i^j\rangle$, $j = 1,2$,且

$$n_e^i|A_i^1\rangle = e_{i1}^1|E_i^1\rangle + e_{i1}^2|E_i^2\rangle,\ n_e^i|A_i^2\rangle = e_{i2}^1|E_i^1\rangle + e_{i2}^2|E_i^2\rangle,$$

则
$$n_e^i|S_i\rangle = a_{i1}n_e^i|A_i^1\rangle + a_{i2}n_e^i|A_i^2\rangle = \delta_{i1}|E_i^1\rangle + \delta_{i2}|E_i^2\rangle \tag{20}$$

式中:$\delta_{i1} = a_{i1}e_{i1}^1 + a_{i2}e_{i1}^2$; $\delta_{i2} = a_{i1}e_{i2}^1 + a_{i2}e_{i2}^2$;

$e_{ij}^k = \langle E_i^k|\, n_e^i|\, A_i^j\rangle$, $k, j = 1,2$;

最后一项中出现的符号$\langle E_i^k|$为$|E_i^k\rangle$的复数共轭,即$\langle E_i^k| = (|E_i^k\rangle)^*$. 在此基础上,$B$测量的是攻击者发送的量子比特 $n_e^i|S_i\rangle$. B测量攻击者发来的量子比特就是将这个量子比特投影到 B的测量基上,设 $m_b^i|E_i^1\rangle = b_{i1}^1|B_i^1\rangle + b_{i1}^2|B_{i1}^2\rangle$,, $m_b^i|E_i^2\rangle = b_{i2}^1|B_i^1\rangle + b_{i2}^2|B_{i2}^2\rangle$,于是容易得到下面的结果,

$$m_b^i n_e^i|S_i\rangle = \varepsilon_{i1}|B_i^1\rangle + \varepsilon_{i2}|B_i^2\rangle \tag{21}$$

其中:$\varepsilon_{i1} = \delta_{i1}b_{i1}^1 + \delta_{i2}b_{i2}^1$, $\varepsilon_{i1} = \delta_{i1}b_{i1}^2 + \delta_{i2}b_{i2}^2$, $b_{ij}^k = \langle B_i^k|\, m_b^i|\, E_i^j\rangle$, $k, j = 1,2$.

由于 A和 B的测量基矢是随机的,攻击者不能精确选取与 B相同的测量基,因而攻击者的测量将引起一定的错误(例如在 BB84 协议中的错误率为 25 %),于是在随后的处理中可以检测出来从而保证方案的安全性. 这种方式与 BB84 协议是一致的.

第二种攻击的具体表现方式为纠缠攻击. 在这种攻击中,攻击者用一个她知道的辅助比特$|F\rangle$纠缠 A发出的量子比特,使它的量子比特与 A发出的量子比特成为纠缠比特. 产生这种结果的典型方式可以通过量子 SWAP 实现,也可采用量子逻辑门来实现两个量子比特间的纠缠. 本文不考虑纠缠的过程,只关心作用后的结果. 通过纠缠后所获得的纠缠量子比特可表示为如下形式,

$$|S_i\rangle \otimes |F\rangle = a_{i1}|A_i^1\rangle \otimes |F\rangle + a_{i2}|A_i^2\rangle \otimes |F\rangle \tag{22}$$

将$|F\rangle$用攻击者的本征态表示:$|F\rangle = e_1^f|E_1\rangle + e_2^f|E_2\rangle$,则上式可表示为

$$\begin{aligned}|S_i\rangle \otimes |F\rangle &= a_{i1}e_1^f|A_i^1E_1\rangle + a_{i1}e_2^f|A_i^1E_2\rangle \\ &\quad + a_{i2}e_1^f|A_i^2E_1\rangle + a_{i2}e_2^f|A_i^2E_2\rangle \\ &= \left(a_{i1}e_1^f|A_i^1\rangle + a_{i2}e_1^f|A_i^2\rangle\right)|E_1\rangle \\ &\quad + \left(a_{i1}e_2^f|A_i^1\rangle + a_{i2}e_2^f|A_i^2\rangle\right)|E_2\rangle\end{aligned} \tag{23}$$

上式表明攻击者不能获取 A发出的量子比特串,因为攻击者的每一个本征态前的系数部分包括两种可能情况,即 A发出的量子比特可能处在$|A_1^1\rangle$态也可能处在$|A_i^2\rangle$态,它们的

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

概率分别为

$$\| a_{i1} e_1^f \|^2 \text{ 和 } \| a_{i2} e_1^f \|^2 \text{ 或者 } \| a_{i1} e_2^f \|^2 \text{ 和 } \| a_{i2} e_2^f \|^2.$$

若采用经典攻击策略,则攻击者可从两个方面获取信息,第一,攻击者可采用中间人攻击的方式对量子信道进行攻击;第二,攻击者对合法通信者间的经典过程(如秘密协商、保密加强等)进行攻击,从而获得所谓的边信息. 对于第一种攻击方式,涉及到量子密码的一个基本假定,即攻击者不能同时获得量子信道和经典信道上的信息,在这种假定下,研究表明量子密码是无条件安全的. 对于第二种攻击,人们已经给出了比较详细的研究,结果表明,攻击者所获得的边信息无法威胁方案的安全性.

综上所述,本方案与所提出的量子密码其它方案一样具有可证明的安全性. 不论攻击者采用个体攻击还是联合攻击方式,都不能获取有效信息. 即便是初始阶段中的认证中心也不能获取通信者间的有效信息.

4　实现与应用

本文方案中使用到量子信道和单比特量子逻辑门,量子信道可用空气和普通光纤实现,按照目前的技术,量子比特在光纤中可传输 80km 左右,而在空气中也可传输 48km,理论上则可通过量子中继在任意长的距离范围内传输. 对于量子逻辑门,按照目前的技术可非常容易地实现单比特量子逻辑门,例如通过量子比特旋转,在一定的角度控制下可容易地实现 X 门、Y 门、Z 门等单比特量子逻辑门. 因此,本方案是一个技术上容易实现的具有良好应用前景的方案. 该方案可应用于身份认证、量子网络身份验证、量子密钥的可靠性验证等几个方面.

5　结论

本文研究了单用户量子身份认证技术,提出了一个量子身份认证协议. 除了初始阶段,该协议不需要可信赖第三方. 同时,虽然在初始阶段需要 CA,但是不会影响系统的安全性,因为 CA 不可能获取有效信息. 另外,该协议具有动态效果,这种效果在协议的安全性方面具有很好的作用.

参考文献:

[1] Bennett C H, Brassard G. An update on quantum cryptography[A]. Advances in Cryptology: Proceedings of Crypto 84 [C]. USA: ACPC, Springer-Verlag, 1984. 475.

[2] 曾贵华. 量子信息安全系统[J]. 物理, 2000, 29(4): 623 - 625.

[3] Zeng Guihua, Zhang Weiping. Identity verification in quantum cryptography[J]. Phys Rev A, 2000, 61(2): 022303/1 - 5.

[4] 曾贵华, 王新梅, 诸鸿文. 可完全脱离信赖第三方的认证系统[J]. 通信学报, 2001, 22(8): 41 - 46.

[5] Dusek M, Haderka O, Hendrych M, Myski R. Quantum identification system [J]. Physics Review A, 1999, 60(1): 149.

[6] Zeng Guihua, Keitel Christoph H. An arbitrated quantum signature algorithm [J]. Physics Review A, 2002, 65(4): 042312.

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

[8] Barnum H, Crepeau C, et al. Authentication of quantum messages [J]. Physics Review A, 2002, 66(1): 021037/1 - 6.

[9] Leung D W. Quantum Vernam algorithm, Quantum information and computation [J], 2001, 2(3): 37 - 45.

作者简介:

曾贵华　男,1966 年生于湖南. 上海交通大学教授,博士生导师. 主要从事密码学、网络与通信安全、多媒体检索等方面的研究. 承担了国家和省部级科研项目 14 项,发表学术论文 70 余篇.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net