发明专利证书

Certificate of Invention Patent

中华人民共和国国家知识产权局

STATE INTELLECTUAL PROPERTY OFFICE OF THE PEOPLE'S REPUBLIC OF CHINA

证书号第321357号

发明专利证书

发明名称：基于偏振调制的量子身份认证系统

发 明 人：何广强；曾贵华；曾文杰；周南润

专 利 号：ZL 2004 1 0017011.7

专利申请日：2004年3月18日

专利权人：上海交通大学

授权公告日：2007年4月25日

本发明经过本局依照中华人民共和国专利法进行审查，决定授予专利权，颁发本证书并在专利登记簿上予以登记。专利权自授权公告之日起生效。

本专利的专利权期限为二十年，自申请日起算。专利权人应当依照专利法及其实施细则规定缴纳年费。缴纳本专利年费的期限是每年03月18日前一个月内。未按照规定缴纳年费的，专利权自应当缴纳年费期满之日起终止。

专利证书记载专利权登记时的法律状况。专利权的转移、质押、无效、终止、恢复和专利权人的姓名或名称、国籍、地址变更等事项记载在专利登记簿上。

局长 田力普

中华人民共和国国家知识产权局

2007年4月25日

[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/14
H04L 9/32

[12] 发明专利申请公开说明书

[21] 申请号 200410017011.7

[43] 公开日 2005 年 1 月 12 日

[11] 公开号 CN 1564510A

[22] 申请日 2004.3.18
[21] 申请号 200410017011.7
[71] 申请人 上海交通大学
地址 200240 上海市闵行区东川路 800 号
[72] 发明人 何广强 曾贵华 曾文杰 周南润

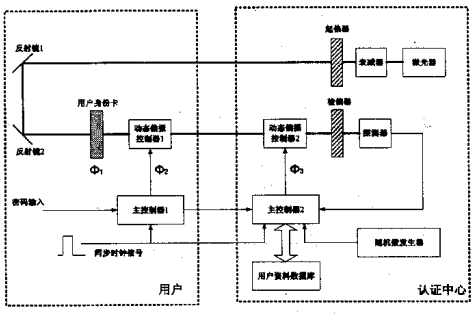
[74] 专利代理机构 上海交达专利事务所
代理人 毛翠莹

权利要求书 1 页 说明书 5 页 附图 1 页

[54] 发明名称 基于偏振调制的量子身份认证系统

[57] 摘要

一种基于偏振调制的量子身份认证系统，包括认证中心和用户端，半导体激光器和衰减器作为量子信号发生器，产生准单光子，经起偏器初始化为垂直偏振态后通过自由空间传输到用户端，再经两个反射镜传输到用户端和认证中心的动态偏振控制器，由检偏器检测变换后的准单光子的偏振态，由探测器探测单光子，用户端主控制器根据用户密码控制动态偏振控制器，两个主控制器通过经典信道通信，同步时钟发生器为主控制器提供同步时钟信号，随机数发生器产生注册时需要的随机数，用户资料数据库储存用户身份信息。 本发明不需利用 BB84 协议传输认证密钥，把量子信号的传输过程与认证过程同时进行，直接验证用户资料数据库中的用户信息，提高了认证效率。



ISSN1008-4274

1、一种基于偏振调制的量子身份认证系统，由认证中心和用户端两部分组成，其特征在于认证中心的光路部分由半导体激光器、衰减器、起偏器、中心动态偏振控制器、检偏器、光电探测器组成，认证中心的控制部分由中心主控制器、用户资料数据库、随机数发生器组成，用户端光路部分包括两个反射镜、用户端动态偏振控制器，用户端控制部分包括用户端主控制器、同步时钟发生器，半导体激光器和衰减器作为量子信号发生器，产生的作为信息载体的准单光子，经起偏器初始化为垂直偏振态，通过自由空间传输到用户端，经两个互为90度夹角布置的反射镜改变传输方向，经用户身份卡传输到用户端动态偏振控制器，再经自由空间传输到认证中心的动态偏振控制器，由检偏器检测变换后的准单光子的偏振态，由探测器探测单光子，检偏器的透光轴与起偏器的透光轴平行；用户端主控制器根据用户密码控制用户端动态偏振控制器，控制中心动态偏振控制器的中心主控制器和用户端的主控制器通过经典信道通信，同步时钟发生器分别与两个主控制器相连，随机数发生器与中心主控制器相连，为中心主控制器产生注册时需要的随机数，用户资料数据库为中心主控制器储存用户身份信息。

基于偏振调制的量子身份认证系统

技术领域

本发明涉及一种基于偏振调制的量子身份认证系统，解决信息安全领域中的用户身份认证问题，是一个结合密码学、光纤通信、量子光学、非线性光学和网络通信等多个学科的前沿课题。

背景技术

量子密码是以经典密码学和量子物理学为基础的新型密码体制，这种密码体制的安全性受到量子比特内秉属性（海森堡测不准性）的保证。量子不可克隆定理和海森堡测不准原理保证了量子密码具有无条件安全性和对窃听的可检测性，使得量子密码具有良好的性能和前景。

1969 年，S.Wiesner 首先提出量子密码思想。1984 年，美国 IBM 公司的科学家 C.H.Bennett 和加拿大密码学家 G.Brassard 提出国际上第一个量子密钥分发协议——BB84 协议。几年后，Bennett 和 Brassard 以及他们领导的小组利用 BB84 协议，采用微弱激光脉冲作为量子信号发生器在实验室首次实现了自由空间中的量子密钥分发。从此，建立在量子光通信基础上的量子密码成为国际上普遍关注的课题之一，各国学者和科学家在理论上从不同的角度开展量子密码研究，内容涉及量子密钥分发、量子密钥验证、量子数据加密、量子秘密共享、量子身份认证、量子签名、量子比特承诺、量子不经意传输、量子多方计算以及量子密码的信息理论，另外，量子纠错码也越来越受到人们的重视。

作为量子密码重要分支之一的量子身份认证引起各国学者越来越多的兴趣。Miloslav Dusek 报道了一种基于量子密钥分发和经典认证的身份认证系统（Miloslav Dusek,Ondrej Haderka,Martin Hendrych and Robert Myska,Phys.Rev. A **60**, 149（1999））, 该系统中，Alice 和 Bob 采用 BB84 协议交换量子密钥，然后利用该密钥采用经典方式实现身份认证。Miloslav Dusek 没有从根本上解决量子身份认证的理论和技术问题，他仅仅利用量子密钥分发的无条件安全性与对窃听的可探测性传输认证密码，然后利用经典的认证方案确认用户身份的合法性。经典

认证需要三次握手才能最终确认用户身份的合法性，导致认证效率很低。国际上，一般用微弱激光脉冲作为量子信号，采用调制相位的方式分发量子密钥，而偏振调制方式鲜有报道。

发明内容

本发明的目的在于针对现有技术的不足，提供一种新的全量子身份认证方案，弥补 Miloslav Dusek 身份认证方案中经典部分的不足，提高认证效率，促进我国信息安全基础建设。

为实现这样的目的，本发明提出一种基于偏振调制的量子身份认证系统，采用微弱激光脉冲作为量子信号，采用动态偏振控制器作为量子信号调制器，工作于盖格模式下的硅雪崩二极管作为单光子探测器，根据用户密码和身份卡动态地建立用户数据库资料，利用未知量子态的不可克隆定理保证系统的安全。

本发明基于偏振调制的量子身份认证系统由认证中心和用户两部分组成。认证中心包括光路部分和控制部分，光路部分由半导体激光器、衰减器、起偏器、中心动态偏振控制器、检偏器、光电探测器组成，认证中心的控制部分由中心主控制器、用户资料数据库、随机数发生器组成。用户端也包括控光路部分和控制部分，光路部分包括两个反射镜、用户身份卡、用户端动态偏振控制器，用户端控制部分包括用户端主控制器、同步时钟发生器。半导体激光器和衰减器作为量子信号发生器，产生的作为信息载体的准单光子，经起偏器初始化为垂直偏振态，通过自由空间传输到用户端，经两个互为 90 度夹角布置的反射镜改变传输方向，经用户身份卡后传输到用户端动态偏振控制器，再经自由空间传输到认证中心的动态偏振控制器，由检偏器检测变换后的准单光子的偏振态，由探测器探测单光子，检偏器的透光轴与起偏器的透光轴平行；用户端主控制器根据用户密码控制用户端动态偏振控制器，控制中心动态偏振控制器的中心主控制器和用户端的主控制器通过经典信道通信，同步时钟发生器分别与两个主控制器相连，随机数发生器与中心主控制器相连，为中心主控制器产生注册时需要的随机数，用户资料数据库为中心主控制器储存用户身份信息。

本发明系统的工作过程包括注册阶段和认证阶段。注册阶段：用户向认证

中心提出注册请求，认证中心制备垂直线偏振的单光子序列，用户身份卡和由密码驱动的动态偏振控制器对单光子的垂直线偏振态进行调制，认证中心根据随机数对载入用户身份信息的单光子序列（经过调制后的单光子序列的垂直线偏振已经发生了变化）再次进行操作，并把具体操作和随机数作为用户身份信息动态地建立用户数据库资料。认证阶段：认证中心收到用户的认证请求后，制备垂直线偏振的单光子序列，并从数据库中调出相应用户的资料，系统客户端根据身份卡和用户密码对单光子的垂直线偏振态进行调制，认证中心服务器端根据数据库中的资料对调制后的单光子序列的偏振态再次执行相应的变换，并进行测量，通过比较测量结果与用户资料中的随机数是否一致来验证用户身份的合法性。

本发明基于偏振调制的量子身份认证系统采用微弱激光脉冲作为量子信号，这个技术已经相当成熟，能较好地满足系统对单光子源的要求。采用国际上常用的工作于盖格模式下硅雪崩二极管作为单光子探测器，国内外的多次试验证明这个探测方法是切实可行的。动态偏振控制器通过旋转半波片调制入射光的线偏振方向，精度可以达到0.03°。本系统不需利用 BB84 协议传输认证密钥，把量子信号的传输过程与认证过程同时进行，直接验证用户资料数据库中的用户信息，不需要进行三次握手，提高了认证效率。

附图说明

图 1 为本发明量子身份认证系统示意图。

如图 1 所示，本发明基于偏振调制的量子身份认证系统由认证中心和用户两部分组成。认证中心的光路部分由激光器、衰减器、起偏器、动态偏振控制器 2、检偏器、光电探测器组成，认证中心的控制部分由主控制器 2、用户资料数据库、随机数发生器组成。用户端的光路部分包括反射镜 1、反射镜 2、用户身份卡、动态偏振控制器 1，用户端的控制部分包括主控制器 1、同步时钟发生器。

具体实施方式

以下结合附图和实施例对本发明的技术方案作进一步描述。

本发明量子身份认证系统如图 1 所示，由认证中心和用户两部分组成。认证中心包括光路部分和控制部分，认证中心的光路部分由DL-100半导体激光器、衰减器、起偏器、动态偏振控制器2、检偏器、光电探测器组成，认证中心的控制部分由主控制器 2、用户资料数据库、随机数发生器组成。DL-100 半导体激光器和衰减器作为量子信号发生器产生作为信息载体的准单光子。起偏器把准单光子初始化为垂直偏振态。从半导体激光器发出的激光被衰减器衰减后，被起偏器初始化为垂直偏振态，通过自由空间传输到用户端。由主控制器 2 控制的动态偏振控制器 2 变换从客户端传输来的准单光子，检偏器检测单光子的偏振态，硅雪崩二极管作为光电探测器探测单光子。随机数发生器为主控制器 2 产生注册时需要的随机数。主控制器 2 和用户端的主控制器 1 通过经典信道通信，控制动态偏振控制器 2。

用户端也包括光路部分和控制部分，光路部分包括反射镜 1、反射镜 2、动态偏振控制器 1。控制部分包括主控制器 1、同步时钟发生器。反射镜 1 和反射镜 2 改变光的传输方向构成光学回路，由主控制器 1 控制的动态偏振控制器 1 根据用户密码变换准单光子的偏振态。主控制器 1 和主控制器 2 通过经典信道通信。同步时钟发生器为主控制器 1 和主控制器 2 提供同步时钟信号。激光器、衰减器、起偏器、反射镜 1、反射镜 2、动态偏振控制器 1、动态偏振控制器 2、检偏器、光电探测器顺序连接构成量子身份认证系统的光学部分。主控制器 1、主控制器 2、用户资料数据库、随机数发生器构成量子身份认证系统的控制部分。

在认证中心端，本发明系统将从半导体激光器发出的激光脉冲大幅度衰减产生的准单光子作为信息载体——激光光源属相干光源，其光子数分布满足泊松分布，将脉冲激光衰减到平均每个脉冲 0.1 个光子时，每个脉冲含 1 个以上光子的概率仅为 0.5%，此时的光脉冲表现出不可克隆等量子属性，本发明把这种由激光器和衰减器构成的准单光子源作为量子信号发生器。准单光子经过起偏器后，其偏振态被初始化为垂直偏振态，把准单光子经自由空间传输到认证系统用户端。在用户端，反射镜 1、反射镜 2 改变光的传输方向构成光学回路。用户身份卡和由用户密码驱动的动态偏振控制器 1 对来自服务器端的垂直偏振态

的准单光子变换。检偏器的透光轴与起偏器的透光轴平行，工作于盖格模式下的雪崩二极管作为单光子探测器，若用户身份卡、动态偏振控制器 1、动态偏振控制器 2 把垂直偏振态变换为水平偏振态，则探测器探测到光子的概率为 0；若变换后仍为垂直偏振态，探测器探测到光子的概率为 1。认证中心收到用户的注册请求后，产生 n 比特的随机数 $R=(r_1,r_2,\cdots,r_n)$，用户插入身份卡，使准单光子的线偏振面旋转 Φ_1，输入 n 位密码，第 i 位密码通过用户端主控制器 1 控制动态偏振控制器 1 使准单光子的线偏振面再次旋转 Φ_{2i}，认证中心根据随机数的第 i 比特是 0 或 1 确定动态偏振控制器 2 对线偏振光再次旋转的角度 Φ_{3i}，

$$当 r_i=0 时，\ \Phi_1+\Phi_{2i}+\Phi_{3i}=0^{\circ} 或者 180^{\circ}$$

$$当 r_i=1 时，\ \Phi_1+\Phi_{2i}+\Phi_{3i}=90^{\circ} 或者 270^{\circ}$$

注册结束后，认证中心在数据库中建立以用户名为文件名的用户资料，文件内容为

$$R=(r_1,r_2,\cdots,r_n) 和 \Phi_3=(\Phi_{31},\Phi_{32},\cdots,\Phi_{3n})$$

在认证阶段，用户插入身份卡，输入密码，认证中心用户从用户资料数据库中调出对应的用户文件，用 $\Phi_3=(\Phi_{31},\Phi_{32},\cdots,\Phi_{3n})$ 驱动动态偏振控制器 2，监测光电探测器，按照规则：探测到光子对应 0；探测不到光子对应 1，把采集到的比特串与注册时的随机数比较，如果一致，则认证成功，否则，认证失败。

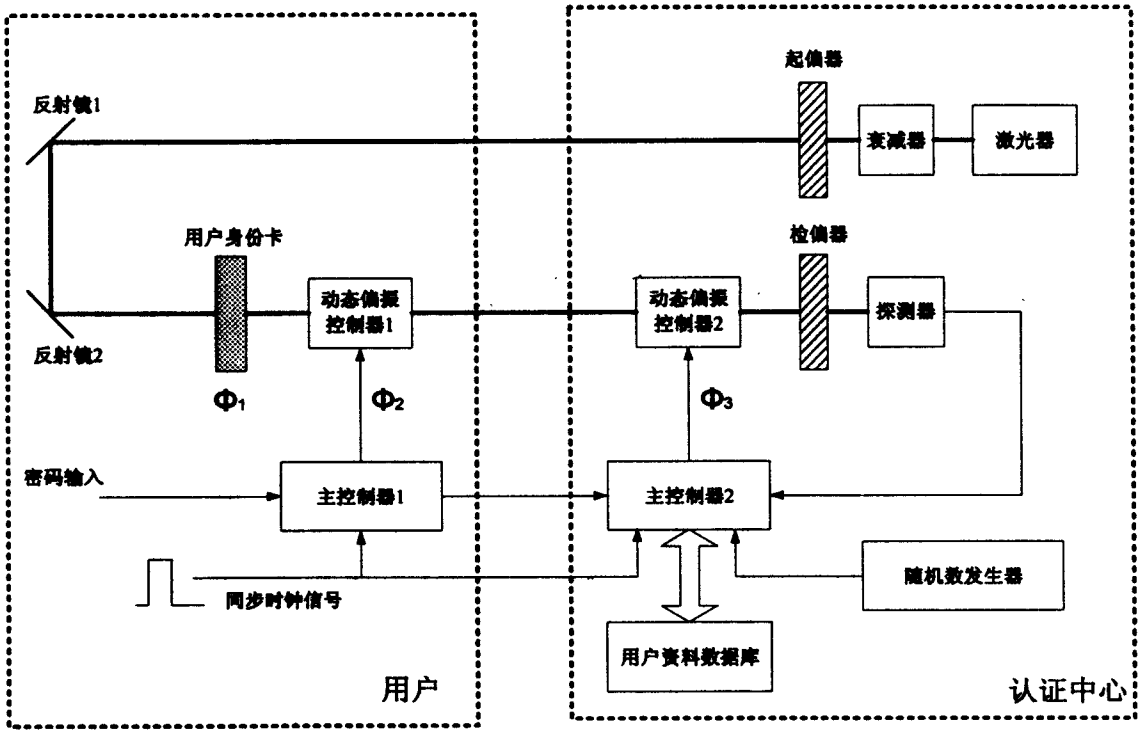

起偏器
反射镜1
衰减器
激光器
用户身份卡
检偏器
动态偏振控制器1
动态偏振控制器2
探测器
反射镜2
Φ1
Φ2
Φ3
密码输入
主控制器1
主控制器2
随机数发生器
同步时钟信号
用户资料数据库
用户
认证中心

图 1