证书号第375150号

北京市海淀区地方税务局 印花税 代扣专用章 国家知识产权局

发明专利证书

发明名称：基于相位调制的量子身份认证系统

发明人：何广强；曾贵华

专利号：ZL 2004 1 0067582.1

专利申请日：2004年10月28日

专利权人：上海交通大学

授权公告日：2008年1月30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10月28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

2008年1月30日

[19] 中华人民共和国国家知识产权局

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

[12] 发明专利申请公开说明书

[21] 申请号 200410067582.1

[43] 公开日 2005 年 4 月 6 日

[11] 公开号 CN 1604524A

[22] 申请日 2004.10.28
[21] 申请号 200410067582.1
[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

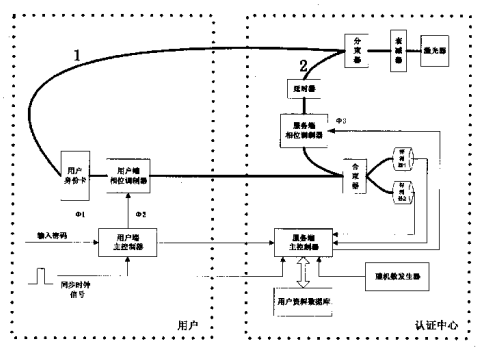
[74] 专利代理机构 上海交达专利事务所
代理人 毛翠莹

权利要求书 1 页 说明书 5 页 附图 1 页

[54] 发明名称 基于相位调制的量子身份认证系统

[57] 摘要

一种基于相位调制的量子身份认证系统，包括认证中心和用户端，激光器和衰减器产生的准单光子经 50/50 分束器后，经第一个光纤臂传输到用户端的光束经用户身份卡、相位调制器后传输到合束器，经第二个光纤臂传输的光束经延时后传输到相位调制器，最终到达合束器。 采用两个探测器探测单光子。 用户端主控制器根据用户密码控制相位调制器，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，采用相位编码，同时进行量子信号的传输过程与认证过程，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、一种基于相位调制的量子身份认证系统，由认证中心和用户两部分组成，其特征在于认证中心的光路部分由半导体激光器、衰减器、50/50 分束器、延时器、服务端相位调制器、50/50 合束器及两个探测器组成，认证中心的控制部分由服务端主控制器、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用户身份卡、用户端相位调制器，用户端的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 50/50 分束器后，分别进入 M-Z 光纤干涉仪的两个光纤臂，第一组光束通过第一个光纤臂传输到用户端，经用户身份卡后，改变光束的相位，经光纤传输到用户端相位调制器，然后经光纤传输到服务端的合束器，第二组光束通过第二个光纤臂传输到认证中心的延时器，经延时后再通过光纤传输到服务端相位调制器，最终到达合束器；第一组光束及经延时器调节的第二组光束的光程相等，两组光束在合束器处产生单光子干涉现象；合束器的两个输出口分别与两个探测器连接，两个探测器的输出分别连接服务端主控制器；用户端主控制器根据用户密码控制用户端相位调制器，服务端主控制器控制服务端相位调制器，服务端主控制器和用户端主控制器与同步时钟发生器相连，并通过经典信道通信，随机数发生器与服务端主控制器相连，为服务端主控制器产生注册时需要的随机数，用户资料数据库为服务端主控制器储存用户身份信息。

基于相位调制的量子身份认证系统

技术领域

本发明涉及一种基于相位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。申请号为

200410017011.7 的中国发明专利提出一种基于偏振调制的量子身份认证系统，采用偏振编码，以光纤作为量子信道传输准单光子。该系统第一次采用全量子的方式实现了量子身份认证，利用物理规律保证了该方案的安全性，但光纤的双折射效应影响光子的偏振态，使误码率升高，偏振相关损耗缩短了传输距离，影响了认证系统的性能。

在国际上，与基于量子身份认证相关的量子密钥分发技术已经比较成熟，瑞士日内瓦大学已经开发出基于相位调制的量子密钥分发产品。针对基于偏振编码的量子身份认证系统的上述弱点，利用量子信号的产生、传输、检测技术，设计一种基于相位调制的量子身份认证系统，使系统受外界条件的影响较小，性能稳定，认证速率高成为可能。但是目前这部分工作未见有相关文献报道。

发明内容

本发明的目的在于针对现有技术的不足，提供一种新的基于相位调制的量子身份认证系统，弥补 Miloslav Dusek 身份认证方案中经典部分的不足，提高认证效率，同时克服基于偏振调制的量子身份认证系统中各种偏振相关损害给认证系统性能带来的不利影响，提高系统性能。

为实现这样的目的，本发明提出一种基于相位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，采用动态相位调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。

本发明基于相位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、50/50 分束器、延时器、服务端相位调制器、50/50 合束器及两个探测器组成，认证中心的控制部分由服务端主控制器、用户资料数据库、随机数发生器组成。用户端也包括光路部分和控制部分，光路部分包括用户身份卡、用户端相位调制器，用户端的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，产生作为信息载体的准单光子，经 50/50 分束器后，分别进入 M-Z 光纤干涉仪的两个光纤臂，第一组光束通过第一个光纤臂传输到用户端，经用户身份卡后，改变光束的相位 Φ_1，经光纤传输到用户端相位调制器，然后经光纤传输到服务端的合束器。第二组光束通过第二个

光纤臂传输到认证中心的延时器，经延时后再通过光纤传输到服务端相位调制器，最终到达合束器。调节延时器使第一组光束与第二组光束的光程相等，两组光束在合束器处产生单光子干涉现象。合束器的两个输出口分别与两个探测器连接，两个探测器的输出分别连接服务端主控制器。

由于单光子干涉现象。两个探测器中第一个探测器探测到光子的概率为 $P_1=\cos^2\left|\frac{\Phi_1+\Phi_2-\Phi_3+k\Delta L}{2}\right|$，第二个探测器探测到光子的概率为 $P_2=\sin^2\left|\frac{\Phi_1+\Phi_2-\Phi_3+k\Delta L}{2}\right|$，其中Φ1和Φ2分别为用户端用户身份卡与用户端相位调制器引入的相位延迟，Φ3为服务端相位调制器引入的相位延迟，k为波数，ΔL为M-Z干涉仪的两臂光程差，调节认证中心端的延迟器使$\Delta L=0$。

当$\Phi1+\Phi2-\Phi3=\frac{\pi}{2}+n\pi$（$n$为整数）时，$P_1=P_2=\frac{1}{2}$；

当$\Phi_1+\Phi_2-\Phi_3=0$时，$P_1=1$，$P_2=0$；

当$\Phi_1+\Phi_2-\Phi_3=\pi$时，$P_1=0$，$P_2=1$。

用户端主控制器根据用户密码控制用户端相位调制器，服务端主控制器根据用户资料数据库中的用户信息控制服务端相位调制器，并监测两个探测器，服务端主控制器和用户端主控制器与同步时钟发生器相连，并通过经典信道通信。随机数发生器与服务端主控制器相连，为服务端主控制器产生注册时需要的随机数，用户资料数据库为服务端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，认证中心制备初始单光子序列，被分束器分为两组光束，即经第一个光纤臂传输的单光子脉冲1和经第二个光纤臂传输的单光子脉冲2。用户身份卡和由密码驱动的相位调制器调制单光子脉冲 1 的相位延迟；服务端调节延迟器使M-Z干涉仪的两个光纤臂的光程相等，然后根据随机数对经第二个光纤臂传输的单光子脉冲 2 进行调节，通过调节单光子脉冲 2 的相位延迟，使在合束器处出现的单光子干涉现象与随机数满足一一对应的关系，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，制备单光子序列，并从数据库中调出相应用户的资料，系统用户端根

据身份卡和用户密码对经过 M-Z 干涉仪第一个光纤臂的单光子脉冲 1 的相位延迟进行调节，认证中心服务器端根据数据库中的资料对经过 M-Z 干涉仪第二个光纤臂的单光子脉冲 2 的相位延迟进行调节，单光子脉冲 1 与单光子脉冲 2 经过相同的光程传输后，同时到达合束器，发生单光子干涉现象，通过两个监视单光子探测器进行单光子测量，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。

本发明基于相位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。本发明采用相位调制方式对量子信息进行编码，可以通过光纤传输，相对于偏振调制方式，对光纤的偏振模色散、偏振相关损耗等偏振相关损害不敏感，因此具有较好的性能。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。

具体实施方式

以下结合附图对本发明的技术方案作进一步描述。

本发明基于相位调制的量子身份认证系统由认证中心和用户两部分组成，如图 1 所示。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、50/50 分束器、延时器、服务端相位调制器、50/50 合束器、探测器 1 和探测器 2 组成，认证中心的控制部分由服务端主控制器、用户资料数据库、随机数发生器组成。用户端也包括光路部分和控制部分，光路部分包括用户身份卡、用户端相位调制器，用户端控制部分包括用户端主控制器、同步时钟发生器。用户端主控制器根据用户密码控制用户端相位调制器，服务端主控制器控制服务端相位调制器，服务端主控制器和用户端主控制器与同步时钟发生器相连，并通过经典信道通信，随机数发生器与服务端主控制器相连，为服务端主控制器产生注册时需要的随机数，用户资料数据库为服务端主控制器储存用户身份信息。

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。准单光子脉冲经过 50/50 分束器后，进入 M-Z 光纤干涉仪的光纤臂 1 和光纤臂 2，光束 1 通过光纤臂 1 传输用户端，经用户身份卡后，改变光束的相位 Φ_1，经光纤传输到用户端相位调制器，然后经光纤传输到服务端的合束器。光束 2 通过光纤臂 2 传输到延时器后，调节延时器使光纤臂 1 与光纤臂 2 的光程相等，通过光纤传输到服务端相位调制器，最终到达合束器。光束 1 和光束 2 在合束器处产生单光子干涉现象。探测器 1 和探测器 2 分别与合束器的输出口 1 和输出口 2 连接。探测器 1 和探测器 2 为工作于盖格模式下的雪崩二极管，若用户身份卡、用户端相位调制器、服务器端相位调制器使经过光纤臂 1 和光纤臂 2 的单光子脉冲的相位差为 0 时，则探测器 1 探测到光子；若相位差为 π 时，探测器 2 探测到光子。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，使经过光纤臂 1 的单光子脉冲的相位延迟为 Φ_1，输入 n 位密码，第 i 位密码通过用户端主控制器 1 控制用户端相位控制器 1 使单光子脉冲 1 的的相位延迟为 Φ_{2i}，认证中心根据随机数的第 i 比特是 0 或 1 确定经过光纤臂 2 的单光子脉冲 2 的相位延迟的值 Φ_{3i}，

$$当 r_i=0 时，\ \Phi_1+\Phi_{2i}-\Phi_{3i}=0$$

$$当 r_i=1 时，\ \Phi_1+\Phi_{2i}-\Phi_{3i}=\pi$$

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 $\Phi_3=(\Phi_{31},\Phi_{32},\cdots,\Phi_{3n})$ 驱动服务器端相位调制器，监测探测器 1 和探测器 2，按照规则：探测器 1 探测到光子对应 0；探测器 2 探测到光子对应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。

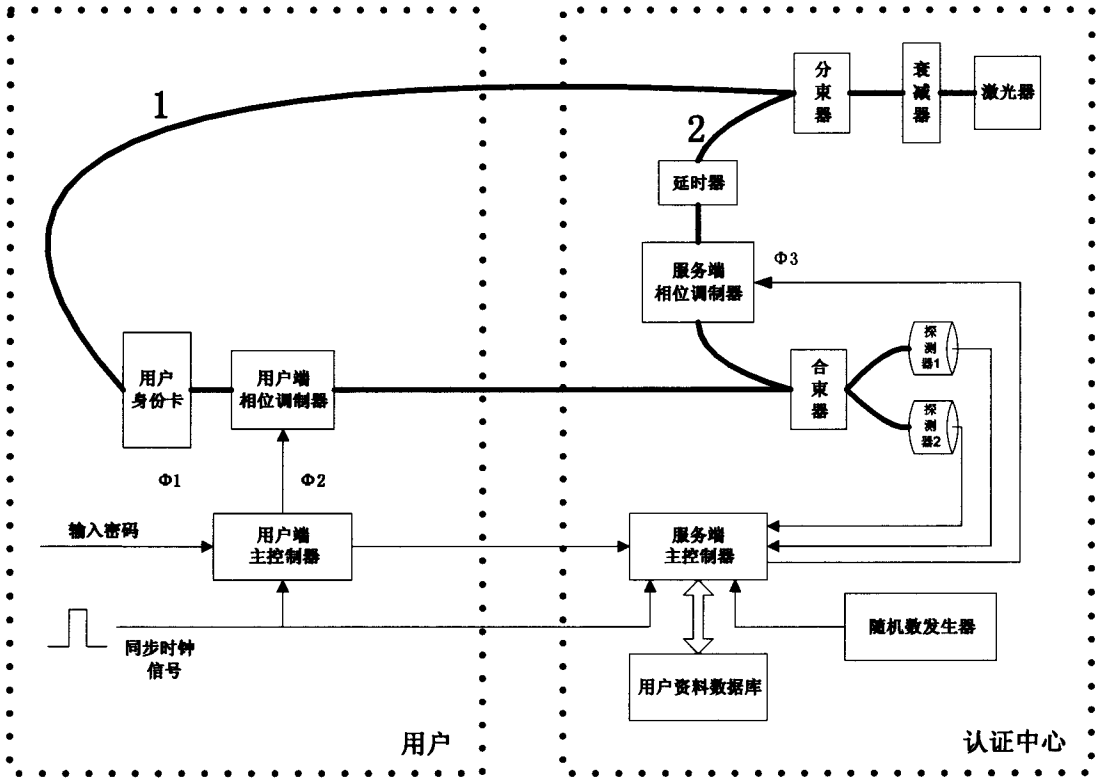

1
2
分束器
衰减器
激光器
延时器
服务端相位调制器
Φ3
用户身份卡
用户端相位调制器
合束器
探测器1
探测器2
Φ1
Φ2
输入密码
用户端主控制器
服务端主控制器
随机数发生器
同步时钟信号
用户资料数据库
用户
认证中心

图 1