(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104113411 B
(45)授权公告日 2017.09.29

(21)申请号 201310139644.4

(22)申请日 2013.04.22

(65)同一申请的已公布的文献号
申请公布号 CN 104113411 A

(43)申请公布日 2014.10.22

(73)专利权人 中国银联股份有限公司
地址 200135 上海市浦东新区含笑路36号银联大厦

(72)发明人 郑建宾 周钰

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 臧霁晨 朱海煜

(51)Int.Cl.
H04L 9/32(2006.01)
G06F 21/31(2013.01)

(56)对比文件
WO 2012106757 A1,2012.08.16,
CN 102377570 A,2012.03.14,
US 8095113 B2,2012.01.10,
闫振威.基于IC卡的改进型对称密码认证方法.《计算机应用》.2012,第32卷(第S1期),全文.
Steven J Murdoch等."Chip an PIN is Broken".《2010 IEEE Symposium and Privacy》.2010,摘要,第1部分-第4部分.

审查员 陈晨

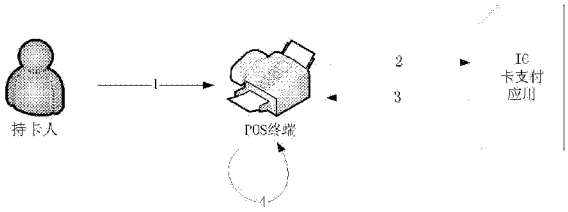
权利要求书3页 说明书7页 附图3页

(54)发明名称

一种IC卡脱机PIN验证方法以及IC卡脱机验证系统

(57)摘要

本发明涉及脱机PIN认证以及脱机PIN认证系统。该方法包括:向POS终端输入脱机PIN1,POS终端生成动态挑战码,并且动态挑战码和脱机PIN1发送给卡片应用:卡片应用验证第一脱机PIN1和第二脱机PIN2是否一致;在一致的情况下,对第一脱机PIN1和第二脱机PIN2进行数字签名将签名数据和成功状态码返回到POS终端;POS终端在收到成功状态码的情况下对签名数据进行验证,并且在签名数据验证成功的情况下开始后续交易处理。根据本发明,不仅能够实现IC卡对脱机PIN的验证,同时也能够实现了终端对脱机PIN的验证。该方法实现简单、实用且安全可靠。



CN 104113411 B

1.一种IC卡脱机PIN验证方法,其特征在于,包括下述步骤:

步骤a:POS终端获得第一脱机PIN1,并且POS终端生成动态挑战码,将所述动态挑战码和所述第一脱机PIN1进行异或运算得到第一异或值和所述动态挑战码发送给IC卡的卡片应用,其中,所述第一脱机PIN1是持卡人输入到POS终端的密码;

步骤b:卡片应用对所述动态挑战码和第二脱机PIN2进行异或运算得到第二异或值,并验证所述第一异或值和第二异或值是否一致,其中,所述第二脱机PIN2是在IC卡预先储存的该IC卡的真实密码;

步骤c:在步骤b的判断为一致的情况下,卡片应用对所述第二异或值进行签名,并且将该第二异或值的签名数据以及成功状态码返回到POS终端;在步骤b的判断为不一致的情况下,向POS终端返回错误状态码;

步骤d:POS终端在收到成功状态码的情况下对该第二异或值的签名数据进行验证,并且在该第二异或值的签名数据验证成功的情况下开始后续交易处理,而在该第二异或值的签名数据验证失败的情况下执行异常处理;另一方面POS终端在收到错误状态码的情况下,执行异常处理。

2.如权利要求1所述的IC卡脱机PIN验证方法,其特征在于,

在所述步骤a中,POS终端生成随机数作为动态挑战码,并产生第一异或值。

3.如权利要求2所述的IC卡脱机PIN验证方法,其特征在于,

在所述步骤c中,用私钥对该第二异或值进行数据签名,生成该第二异或值的签名数据,

在所述步骤d中,POS终端在收到成功状态码的情况下对该第二异或值的签名数据进行如下验证:

用公钥对该第二异或值的签名数据进行签名验证;

比较第一异或值和第二异或值是否一致。

4.一种IC卡脱机PIN验证方法,其特征在于,包括下述步骤:

步骤a:POS终端获得第一脱机PIN1,并且POS终端生成动态挑战码,将所述动态挑战码和所述第一脱机PIN1发送给IC卡的卡片应用,其中,所述第一脱机PIN1是持卡人输入到POS终端的密码;

步骤b:卡片应用验证所述第一脱机PIN1和第二脱机PIN2是否一致,其中,所述第二脱机PIN2是在IC卡预先储存的该IC卡的真实密码;

步骤c:在步骤b的判断为一致的情况下,卡片应用对所述第二脱机PIN2和上述动态挑战码进行规定计算获得第一签名数据,并且将该第一签名数据和成功状态码返回到POS终端;在步骤b的判断为不一致的情况下,向POS终端返回错误状态码;

步骤d:POS终端在收到成功状态码的情况下对第一签名数据进行验证,并且在第一签名数据验证成功的情况下开始后续交易处理而在第一签名数据验证失败的情况下执行异常处理;另一方POS终端在收到错误状态码的情况下,执行异常处理。

5.如权利要求4所述的IC卡脱机PIN验证方法,其特征在于,

在所述步骤a中,POS终端生成随机数作为动态挑战码。

6.如权利要求5所述的IC卡脱机PIN验证方法,其特征在于,

在所述步骤a中,POS终端将所述第一脱机PIN1和所述动态挑战码组成验证指令一起发

送给卡片应用。

7.如权利要求5所述的IC卡脱机PIN验证方法，其特征在于，

在所述步骤a中，POS终端先将所述动态挑战码发送给卡片应用，然后再将第一脱机PIN1发送给卡片应用。

8.如权利要求6或7所述的IC卡脱机PIN验证方法，其特征在于，

在所述步骤a中，POS终端生成动态挑战码并且和所述第一脱机PIN1一起储存在POS终端中。

9.如权利要求8所述的IC卡脱机PIN验证方法，其特征在于，

在所述步骤c中，卡片应用对所述动态挑战码和所述第二脱机PIN2进行下述计算获得第一签名数据：

计算动态挑战码和第二脱机PIN2的第一异或值；

用私钥对该第一异或值进行数据签名，生成第一签名数据，

在所述步骤d中，POS终端在收到成功状态码的情况下对第一签名数据进行如下验证：

计算动态挑战码和第一脱机PIN1的第二异或值；

用公钥对第一签名数据进行签名验证；

比较所述第一异或值和所述第二异或值是否一致。

10.一种IC卡脱机PIN验证系统，其特征在于，包括POS终端(100)和IC卡的卡片应用模块(200)，

其中，所述POS终端(100)包括：

密码获取模块(101)，用于获取持卡人输入的密码作为第一脱机PIN1；

动态挑战码生成模块(102)，用于随机生成动态挑战码；

第一储存模块(102)，用于储存所述第一脱机PIN1和所述动态挑战码；

第一接收/发送模块(103)，用于执行POS终端和IC卡的卡片应用模块之间的数据发送接收；

动态挑战码验证模块(104)，用于在从第一接收/发送模块收到下述的成功状态码的情况下对第一签名数据进行验证，并且在第一签名数据验证成功的情况下使得开始后续交易处理而在第一签名数据验证失败的情况下执行异常处理；

第一接收/发送模块(105)，用于执行POS终端和IC卡的卡片应用模块之间的数据发送接收，

所述IC卡的卡片应用模块(200)包括：

密码验证模块(201)，用于验证从所述POS终端收到的所述第一脱机PIN1和IC卡中预先储存的第二脱机PIN2是否一致并且在验证为不一致的情况下输出错误状态码，其中，所述第二脱机PIN2是该IC卡的真实密码；

数字签名模块(202)，用于在所述密码验证模块验证所述第一脱机PIN1和第二脱机PIN2是为一致的情况下，对所述动态挑战码和和所述第二脱机PIN2进行规定计算获得第一签名数据；

第二接收/发送模块(203)，用于执行POS终端和IC卡的卡片应用模块之间的数据发送接收，在密码验证模块验证成功的情况下将该第一签名数据和成功状态码返回到所述第一接收/发送模块而在密码验证模块验证失败的情况下将错误状态码发送到所述第一接收/

发送模块。

11.如权利要求10所述的IC卡脱机PIN验证系统，其特征在于，

所述第一接收/发送模块将由所述动态挑战码生成模块生成并且储存在第一储存模块中的所述动态挑战码和所述第一脱机PIN1一起发送给所述第二接收/发送模块。

12.如权利要求10所述的IC卡脱机PIN验证系统，其特征在于，

所述第一接收/发送模块将由所述动态挑战码生成模块生成并且储存在第一储存模块中的所述动态挑战码先发送给第二接收/发送模块，然后再将所述第一脱机PIN1发送给所述第二接收/发送模块。

13.如权利要求11或12所述的IC卡脱机PIN验证系统，其特征在于，

所述数字签名模块用于计算动态挑战码和第二脱机PIN2的第一异或值，用私钥对该第一异或值进行数据签名，生成第一签名数据，

所述动态挑战码验证模块用于计算动态挑战码和第一脱机PIN1的第二异或值，用公钥对第一签名数据进行验证，比较所述第一异或值和所述第二异或值是否一致。

一种IC卡脱机PIN验证方法以及IC卡脱机验证系统

技术领域

[0001] 本发明涉及信息安全技术，具体地涉及一种提高IC卡脱机交易安全性的验证方法以及验证系统。

背景技术

[0002] 目前，在IC卡脱机PIN验证过程中，在输入向终端输入PIN之后，如果PIN正确的话，终端返回成功状态码“9000”，也就是说，终端仅通过返回状态码是否为“9000”来判断IC卡是否通过了对持卡人的身份合法性认证。在整个认证过程中，终端只能被动的被通知，而不能主动的进行验证，从而使整个认证过程很容易遭受中间人攻击。

[0003] 下面，对于现有技术的这种IC卡脱机PIN验证过程进行说明。

[0004] 图1是表示现有技术中脱机PIN认证的流程图。如图1所示，目前脱机PIN认证的流程包括下述步骤：

[0005] 步骤1：持卡人在POS终端上输入PIN；

[0006] 步骤2：POS终端组织认证PIN指令并发送给IC卡支付应用进行验证；

[0007] 步骤3：IC卡验证通过后，返回验证状态码给POS终端，告知其验证是否通过，其中，若是验证状态码为9000，则表示成功，若是验证状态为非9000，则表示验证出错；

[0008] 步骤4：POS终端通过判断返回的验证状态码是否为9000，从而判断持卡人身份的合法性，并执行后续的交易流程。

[0009] 从上述流程可以看出，POS终端仅凭状态码是否为9000来判断持卡人身份的合法性，且为明文。这就很容易导致错误的返回状态码被修改为9000的中间人攻击，从而导致POS终端认为当前输入PIN的持卡人是合法的假象。

[0010] 典型的针对脱机持卡人认证过程进行攻击的流程如下，此处以接触式电子现金为例描述。图2是表示现有技术中接触式电子现金认证的流程图。如图2所示，首先终端向接触式PBOC电子现金发起卡片认证、并且获取PIN尝试次数，接着，在终端任意输入一个PIN码，通过恶意攻击的中间人向终端返回状态码“9000”，终端根据该状态码“9000”判断为认证成功并同意进行后续交易流程。

[0011] 从上述图2的描述和PBOC借代记标准的描述可知，不管在终端上输入什么值的PIN码，通过恶意攻击的中间人都能返回验证成功的“9000”码并继续完成后续脱机扣款交易，因此，会给持卡人造成财产损失。

[0012] 进一步拓展后，可知只要后续的在线操作以智能卡的脱机PIN认证为前提，则会存在同样的安全隐患，如以智能卡脱机PIN为要素的客户端登陆操作。在此条件下，当不法分子捡到一带支付功能的客户端后，一旦通过中间人攻击的方式骗取客户端的信任后，则客户端的所有功能都会暴露给不法分子，说不定就可以通过验证码的方式修改用户的相关信息、甚至重置支付密码。

发明内容

[0013] 鉴于上述问题，本发明旨在提供一种能有效防止针对脱机PIN认证流程的攻击的安全可靠的IC卡脱机PIN验证方法和验证系统。

[0014] 本发明的IC卡脱机PIN验证方法，其特征在于，包括下述步骤：

[0015] 步骤a：POS终端获得第一脱机PIN1，并且POS终端生成动态挑战码，将所述动态挑战码和所述第一脱机PIN1进行异或运算得到第一异或值和所述动态挑战码发送给IC卡的卡片应用，其中，所述第一脱机PIN1是持卡人输入到POS终端的密码；

[0016] 步骤b：卡片应用对所述动态挑战码和第二脱机PIN2进行异或运算得到第二异或值，并验证所述第一异或值和第二异或值是否一致，其中，所述第二脱机PIN2是在IC卡预先储存的、该IC卡的真实密码；

[0017] 步骤c：在步骤b的判断为一致的情况下，卡片应用对所述第二异或值进行签名，并且将该第二异或值的签名数据以及成功状态码返回到POS终端；在步骤b的判断为不一致的情况下，向POS终端返回错误状态码；

[0018] 步骤d：POS终端在收到成功状态码的情况下对该第二异或值的签名数据进行验证，并且在该第二异或值的签名数据验证成功的情况下开始后续交易处理而在该第二异或值的签名数据验证失败的情况下执行异常处理；另一方面POS终端在收到错误状态码的情况下，执行异常处理。

[0019] 优选地，在所述步骤a中，POS终端生成随机数作为动态挑战码，并产生第一异或值。

[0020] 优选地，在所述步骤c中，用私钥对该第二异或值进行数据签名，生成该第二异或值的签名数据，在所述步骤d中，POS终端在收到成功状态码的情况下对该第二异或值的签名数据进行如下验证：用公钥对该第二异或值的签名数据进行签名验证；比较第一异或值和第二异或值是否一致。

[0021] 根据本发明的IC卡脱机认证方法，通过利用数字签名技术和动态挑战码，不仅能够实现IC卡对脱机PIN的验证，同时也能够实现了终端对脱机PIN的验证。尤其是，在卡片和终端的交互过程中不会出现明文的脱机PIN，因此，能够进一步提高安全性。

[0022] 本发明的另一方面的IC卡脱机PIN验证方法，其特征在于，包括下述步骤：

[0023] 步骤a：POS终端获得第一脱机PIN1，并且POS终端生成动态挑战码，将所述该动态挑战码、所述脱机PIN1发送给IC卡的卡片应用，其中，所述第一脱机PIN1是持卡人输入到POS终端的密码；步骤b：卡片应用验证所述第一脱机PIN1和第二脱机PIN2是否一致，其中，所述第二脱机PIN2是在IC卡预先储存的、该IC卡的真实密码；步骤c：在步骤b的判断为一致的情况下，卡片应用对所述第一脱机PIN1和所述第二脱机PIN2进行规定计算获得第一签名数据，并且将该第一签名数据和成功状态码返回到POS终端；在步骤b的判断为不一致的情况下，向POS终端返回错误状态码；步骤d：POS终端在收到成功状态码的情况下对第一签名数据进行验证，并且在第一签名数据验证成功的情况下开始后续交易处理而在第一签名数据验证失败的情况下执行异常处理；另一方POS终端在收到错误状态码的情况下，执行异常处理。

[0024] 优选地，在所述步骤a中，POS终端生成随机数作为动态挑战码。

[0025] 优选地，在所述步骤a中，POS终端将所述第一脱机PIN1和所述动态挑战码组成验证指令一起发送给卡片应用。

[0026] 优选地，在所述步骤a中，POS终端先将所述动态挑战码发送给卡片应用，然后再将第一脱机PIN1发送给卡片应用。

[0027] 优选地，在所述步骤a中，POS终端生成动态挑战码并且和所述第一脱机PIN1一起储存在POS终端中。

[0028] 优选地，在所述步骤c中，卡片应用对所述动态挑战码和所述第二脱机PIN进行下述计算算获得第一签名数据：计算动态挑战码和第二脱机PIN2的第一异或值；用私钥对该第一异或值进行数据签名，生成第一签名数据，在所述步骤d中，POS终端在收到成功状态码的情况下对第一签名数据进行如下验证：计算动态挑战码和第一脱机PIN1的第二异或值；用公钥对该第二异或值进行数据签名，生成第二签名数据；比较所述第一签名数据和所述第二签名数据是否一致。

[0029] 本发明的IC卡脱机PIN验证系统，其特征在于，包括POS终端和IC卡的卡片应用模块，其中，所述POS终端包括：密码获取模块，用于获取持卡人输入的密码作为第一脱机PIN1；动态挑战码生成模块，用于随机生成动态挑战码；第一储存模块，用于储存所述第一脱机PIN1和所述动态挑战码；第一接收/发送模块，用于执行POS终端和IC卡的卡片应用模块之间的数据发送接收；动态挑战码验证模块，用于在从第一接收/发送模块收到下述的成功状态码的情况下对第一签名数据进行验证，并且在第一签名数据验证成功的情况下使得开始后续交易处理而在第一签名数据验证失败的情况下执行异常处理；第一接收/发送模块，用于执行POS终端和IC卡的卡片应用模块之间的数据发送接收，

[0030] 所述IC卡的卡片应用模块包括：密码验证模块，用于验证从所述POS终端收到的所述第一脱机PIN1和IC卡中预先储存的第二脱机PIN2是否一致并且在验证为不一致的情况下输出错误状态码，其中，所述第二脱机PIN2是该IC卡的真实密码；数字签名模块，用于在所述密码验证模块验证所述第一脱机PIN1和第二脱机PIN2是为一致的情况下，对所述第一脱机PIN1和所述第二脱机PIN2进行规定计算获得第一签名数据；第二接收/发送模块，用于执行POS终端和IC卡的卡片应用模块之间的数据发送接收，在密码验证模块验证成功的情况下将该第一签名数据和成功状态码返回到所述第一接收/发送模块而在密码验证模块验证失败的情况下将错误状态码发送到所述第一接收/发送模块。

[0031] 优选地，所述第一接收/发送模块将由所述动态挑战码生成模块生成并且储存在第一储存模块中的生成动态挑战码、所述第一脱机PIN1一起发送给所述第二接收/发送模块。

[0032] 优选地，所述第一接收/发送模块将由所述动态挑战码生成模块生成并且储存在第一储存模块中的生成动态挑战码先发送给第二接收/发送模块，然后再将所述第一脱机PIN1发送给所述第二接收/发送模块。

[0033] 优选地，所述数字签名模块用于计算动态挑战码和第二脱机PIN2的第一异或值，用私钥对该第一异或值进行数据签名，生成第一签名数据，所述动态挑战码验证模块用于计算动态挑战码和第一脱机PIN1的第二异或值，用公钥对该第二异或值进行数据签名，生成第二签名数据。比较所述第一签名数据和所述第二签名数据是否一致。

[0034] 根据本发明的IC卡脱机认证方法以及认证系统，通过利用数字签名技术和动态挑战码，不仅能够实现IC卡对脱机PIN的验证，同时也能够实现了终端对脱机PIN的验证。该方法实现简单、实用且安全可靠，能有效防止针对脱机PIN认证流程的攻击，保证IC卡支付过

程中的安全性。

附图说明

[0035] 图1是表示现有技术中脱机PIN认证的流程图。

[0036] 图2是表示现有技术中接触式电子现金认证的流程图。

[0037] 图3是表示本发明的脱机PIN认证的流程图。

[0038] 图4是将本发明的脱机PIN认证方法应用于接触式PBOC电子现金的流程图。

[0039] 图5是表示本发明的脱机PIN认证系统的构造框图。

具体实施方式

[0040] 下面介绍的是本发明的多个实施例中的一些，旨在提供对本发明的基本了解。并不旨在确认本发明的关键或决定性的要素或限定所要保护的范围。

[0041] 图3是表示本发明的脱机PIN认证的流程图。如图3所示，本发明的脱机PIN认证方法包括下述步骤：

[0042] 步骤1：持卡人向POS终端输入脱机PIN1。

[0043] 步骤2：POS终端产生一随机数Rnd作为动态挑战码，并且将该动态挑战码和脱机PIN1一起存储到POS中的加密芯片中。这里，由POS中终端的硬件产生一随机数Rnd，随机数可以为任意位数，例如，8位字节的随机数。

[0044] 步骤3：POS终端将该动态挑战码Rnd附在脱机PIN1之后并且组成验证指令发送给卡片应用。这里“卡片应用”具体指装载并运行在IC卡芯片中的应用程序。

[0045] 步骤4：卡片应用验证该脱机PIN1和预先存储在IC卡内的、IC卡的真实密码PIN2是否一致。如果不一致，则向POS终端直接返回错误状态码，如果一致则进行下述步骤：

[0046] (1)计算随机数Rnd和脱机PIN2的异或值Tdata1，即Tdata1＝Rnd异或PIN2；

[0047] (2)用私钥SkTdata1进行数字签名，得到数字签名数据Sig1；

[0048] (3)向POS终端返回Sig1＋9000(成功状态码)。

[0049] 步骤5：POS终端在收到来自卡片应用的响应后，判断返回的状态码是为成功状态码还是错误状态码，若为错误状态码的话，则执行相应的异常处理逻辑，若为成功状态码9000的话，则执行如下的验证动作：

[0050] (1)计算随机数Rnd和脱机PIN1的异或值Tdata2，即Tdata2＝Rnd异或PIN1；

[0051] (2)用存储在POS终端的公钥Pk验证数字签名Sig1并且比较Tdata2和Tdata1是否一致。如果两者一致，则说明卡片应用确收执行了POS终端所发送的PIN1验证指令；如果不一致则说明受到中间人攻击。

[0052] 另一方面，在上述的步骤3中，POS终端将该动态挑战码Rnd附在脱机PIN1之后一起发送给卡片应用，当然也可以将动态挑战码Rnd和脱机PIN1一前一后发送给卡片应用，这种方式的情况下，POS终端应当先将动战码发送给卡片应用，然后再将脱机PIN1发送给卡片应用。

[0053] 在上述的步骤4、5中采用了一对私钥Sk和公钥Pk进行验证，即在本发明中能够利用这样的非对称密钥体系进行认证，例如具体地可以采用RSA算法等。非对称密钥体系的优势主要体现在安全性和可扩展性更好。除此之外，在本发明中的上述步骤4、5中当然也能够

采用对称密钥体系进行认证。

[0054] 根据本发明的IC卡脱机认证方法，通过利用数字签名技术和动态挑战码，不仅能够实现IC卡对脱机PIN的验证，同时也能够实现了终端对脱机PIN的验证。该方法实现简单、实用且安全可靠，能有效防止针对脱机PIN认证流程的攻击，保证IC卡支付过程中的安全性。

[0055] 下面，对于将本发明的脱机认证方法应用于接触式PBOC电子现金的认证过程进行说明。

[0056] 图4是将本发明的脱机PIN认证方法应用于接触式PBOC电子现金的流程图。

[0057] 如图4所示，该认证过程包括下述步骤：

[0058] 步骤1：从终端向接触式PBOC电子现金发起卡片认证(不属于本发明的范畴)。

[0059] 步骤2：终端获取PIN尝试次数(不属于本发明的范畴)。

[0060] 步骤3：终端产生随机数，

[0061] 步骤4：终端将该随机数和PIN码发送到接触式PBOC电子现金。

[0062] 步骤5：接触式PBOC电子现金对该输入PIN码进行认证，并且对该PIN码和随机数进行数据签名。

[0063] 步骤6：接触式PBOC电子现金向终端返回状态码和数字签名，其中，，其中，在PIN码认证成功的情况下返回成功状态码和数字签名，而在PIN码认证失败的情况下仅返回错误状态码。

[0064] 步骤7：终端对验证状态码和数字签名，在获得成功状态码的情况下对数字签名进行验证，而在获得错误状态码的情况下，执行异常处理；

[0065] 步骤8：在终端通过对状态码和数字签名验证都成功的情况下，开始后续的交易处理流程。

[0066] 通过将上述本发明的脱机PIN认证方法应用于接触式PBOC电子现金，也能够有效防止针对脱机PIN认证流程的攻击，保证接触式PBOC电子现金的安全性。

[0067] 接着，对于本发明的脱机PIN认证系统进行简单说明。

[0068] 接着，对于本发明的另一个实施方式进行说明。该实施方式与上述实施方式的区别在于，在POS终端生成动态挑战码后，在POS终端就将该动态挑战码与第一脱机PIN1进行异或运算得到第一异或值，在卡片应用进行验证时，将动态挑战码和第二脱机PIN2进行异或运算生成第二异或值，然后比较第一异或值和第二异或值是否一致来判断卡片PIN验证是否通过，然后用私钥对该第二异或值进行签名后返回到POS终端，在POS终端用公钥对该第二异或值的签名数据进行验证，然后比较该第一异或值和第二异或值是否一致来判断持卡人PIN验证是否通过。

[0069] 该实施方式的IC卡脱机PIN验证方法具体地包括下述步骤：

[0070] 步骤a：POS终端获得第一脱机PIN1，并且POS终端生成动态挑战码，将所述动态挑战码和所述第一脱机PIN1进行异或运算得到第一异或值和所述动态挑战码发送给IC卡的卡片应用，其中，所述第一脱机PIN1是持卡人输入到POS终端的密码；

[0071] 步骤b：卡片应用对所述动态挑战码和第二脱机PIN2进行异或运算得到第二异或值，并验证所述第一异或值和第二异或值是否一致，其中，所述第二脱机PIN2是在IC卡预先储存的、该IC卡的真实密码；

[0072] 步骤c：在步骤b的判断为一致的情况下，卡片应用对所述第二异或值进行签名，并且将该第二异或值的签名数据以及成功状态码返回到POS终端；在步骤b的判断为不一致的情况下，向POS终端返回错误状态码；

[0073] 步骤d：POS终端在收到成功状态码的情况下对该第二异或值的签名数据进行验证，并且在该第二异或值的签名数据验证成功的情况下开始后续交易处理而在该第二异或值的签名数据验证失败的情况下执行异常处理；另一方面POS终端在收到错误状态码的情况下，执行异常处理。

[0074] 在所述步骤a中，POS终端生成随机数作为动态挑战码，并产生第一异或值。

[0075] 在所述步骤c中，用私钥对该第二异或值进行数据签名，生成该第二异或值的签名数据，在所述步骤d中，POS终端在收到成功状态码的情况下对该第二异或值的签名数据进行如下验证：用公钥对该第二异或值的签名数据进行签名验证；比较第一异或值和第二异或值是否一致。

[0076] 根据该实施方式的IC卡脱机认证方法，通过利用数字签名技术和动态挑战码，不仅能够实现IC卡对脱机PIN的验证，同时也能够实现了终端对脱机PIN的验证。尤其是，在卡片和终端的交互过程中不会出现明文的脱机PIN，因此，能够进一步提高安全性。

[0077] 图5是表示本发明的脱机PIN认证系统的构造框图。如图5所示，本发明的IC卡脱机PIN验证系统，包括POS终端100和IC卡的卡片应用模块200。

[0078] POS终端100包括：密码获取模块101、动态挑战码生成模块102、第一储存模块103、第一接收/发送模块104、动态挑战码验证模块105。所述IC卡的卡片应用模块200包括：密码验证模块201、数字签名模块202、第二接收/发送模块203。

[0079] 密码获取模块101用于作为第一脱机PIN1获取持卡人输入的密码。

[0080] 动态挑战码生成模块102用于随机生成动态挑战码，随机生成的动态挑战码可以是任意字节的数据，例如，8位字节的一个随机数。

[0081] 第一储存模块103用于储存所述第一脱机PIN1和所述动态挑战码。

[0082] 第一接收/发送模块104用于执行POS终端和IC卡的卡片应用模块之间的数据发送接收。

[0083] 动态挑战码验证模块105用于在从第一接收/发送模块收到下述的成功状态码的情况下对第一签名数据进行验证，并且在第一签名数据验证成功的情况下使得开始后续交易处理而在第一签名数据验证失败的情况下执行异常处理。

[0084] 第一接收/发送模块104用于执行POS终端和IC卡的卡片应用模块之间的数据发送接收，即将第一存储模块103中存储的动态挑战码、第一脱机PIN1发送到下述IC卡的卡片应用模块200的第二接收/发送模块203，并且，对应地也从下述IC卡的卡片应用模块200的第二接收/发送模块203接收数据。其中，第一接收/发送模块104将由动态挑战码生成模块102生成且储存在第一储存模块103中的生成动态挑战码、第一脱机PIN1一起发送给第二接收/发送模块203。或者也可以是，第一接收/发送模块104将由动态挑战码生成模块102生成并且储存在第一储存模块103中的生成动态挑战码先发送给第二接收/发送模块203，然后再将第一脱机PIN1发送给第二接收/发送模块203。

[0085] 另一方面，密码验证模块201用于验证从POS终端收到的第一脱机PIN1和IC卡中预先储存的第二脱机PIN2(第二脱机PIN2是该IC卡的真实密码)是否一致并且在验证为不一

致的情况下输出错误状态码，而在验证成功的情况下输出成功状态码9000。

[0086] 数字签名模块202用于在密码验证模块201验证第一脱机PIN1和第二脱机PIN2为一致的情况下，对第一脱机PIN1和第二脱机PIN2进行规定计算获得第一签名数据。

[0087] 第二接收/发送模块203用于执行POS终端100和IC卡的卡片应用模块200之间的数据发送接收，在密码验证模块201验证成功的情况下将该第一签名数据和成功状态码返回到第一接收/发送模块105而在密码验证模块201验证失败的情况下将错误状态码发送到第一接收/发送模块104。

[0088] 作为具体地一个实施方式，数字签名模块202用于计算动态挑战码和第二脱机PIN2的第一异或值，用私钥对该第一异或值进行数据签名，生成第一签名数据。与此相应地，动态挑战码验证模块105计算动态挑战码和第一脱机PIN1的第二异或值，用公钥对该第二异或值进行数据签名，生成第二签名数据，并且比较第一签名数据和所述第二签名数据是否一致，比较结果为两者一致的情况下，则说明卡片应用确收执行了POS终端所发送的PIN1验证指令；比较结果为两者不一致则说明受到中间人攻击。

[0089] 根据本发明的IC卡脱机认证系统，通过利用数字签名技术和动态挑战码，不仅能够实现IC卡对脱机PIN的验证，同时也能够实现了终端对脱机PIN的验证。该方法实现简单、实用且安全可靠，能有效防止针对脱机PIN认证流程的攻击，保证IC卡支付过程中的安全性。

[0090] 本发明的脱机PIN认证以及脱机PIN认证系统具有如下特性：不仅实现卡片对持卡人的认证，同时也实现终端对持卡人的认证。进一步提高的交易的安全性；终端不再仅仅通过返回的状态码获知持卡人认证是否成功，而是通过本创意在上述基础上进一步验证卡片是否真正执行了脱机PIN的认证；能够进一步提高受理环境的安全性。

[0091] 以上例子主要说明了本发明的脱机PIN认证方法以及脱机PIN认证系统。尽管只对其中一些本发明的具体实施方式进行了描述，但是本领域普通技术人员应当了解，本发明可以在不偏离其主旨与范围内以许多其他的形式实施。因此，所展示的例子与实施方式被视为示意性的而非限制性的，在不脱离如所附各权利要求所定义的本发明精神及范围的情况下，本发明可能涵盖各种的修改与替换。

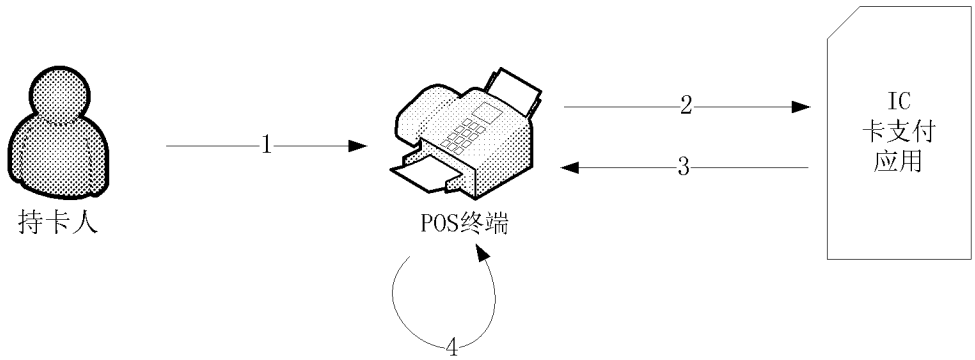

持卡人
1
POS终端
2
3
IC
卡支付
应用
4

图 1

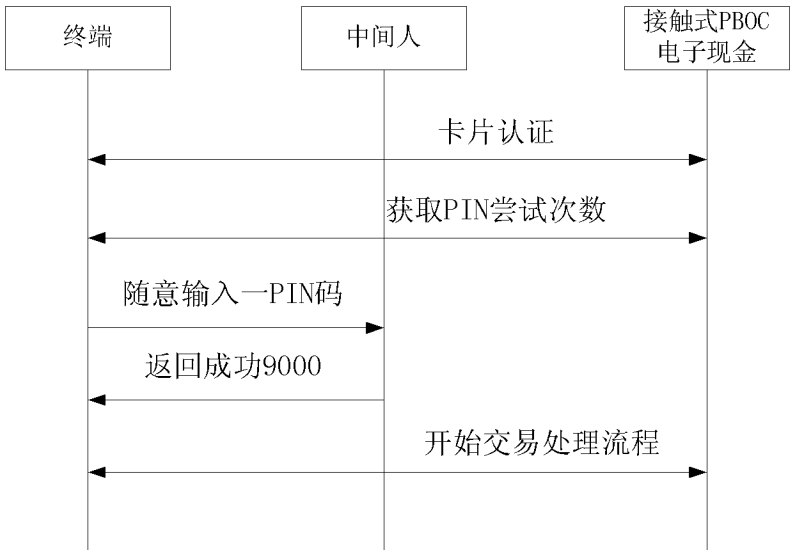

终端
中间人
接触式PBOC
电子现金
卡片认证
获取PIN尝试次数
随意输入一PIN码
返回成功9000
开始交易处理流程

图 2

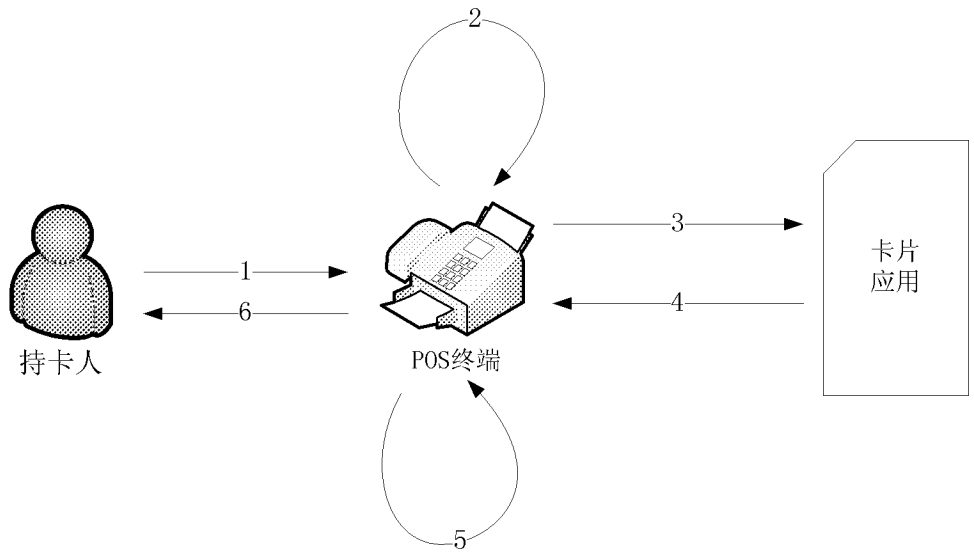

2
3
卡片
应用
1
4
6
持卡人
POS终端
5

图 3

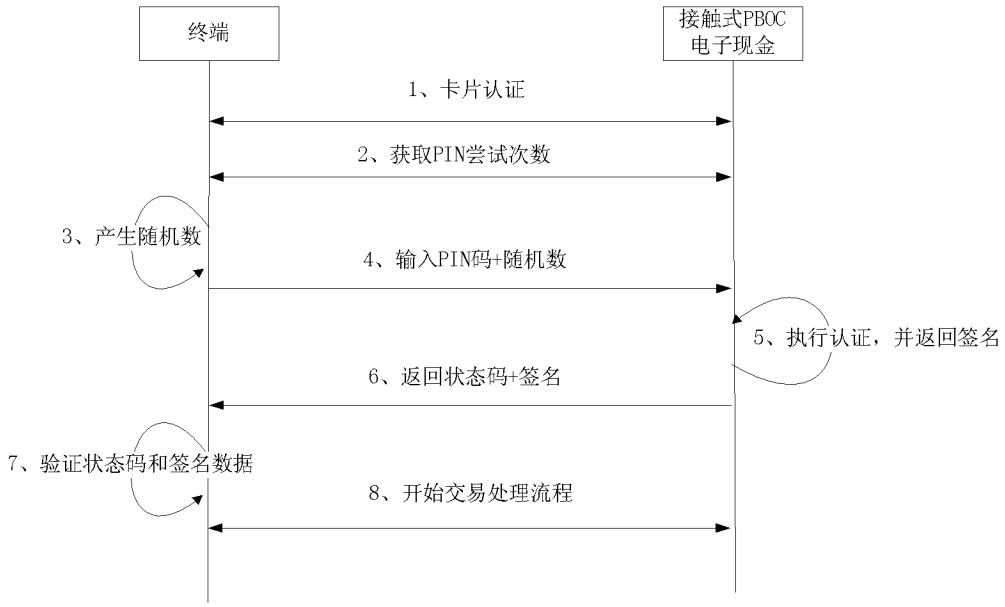

终端
接触式PBOC
电子现金
1、卡片认证
2、获取PIN尝试次数
3、产生随机数
4、输入PIN码+随机数
5、执行认证，并返回签名
6、返回状态码+签名
7、验证状态码和签名数据
8、开始交易处理流程

图 4

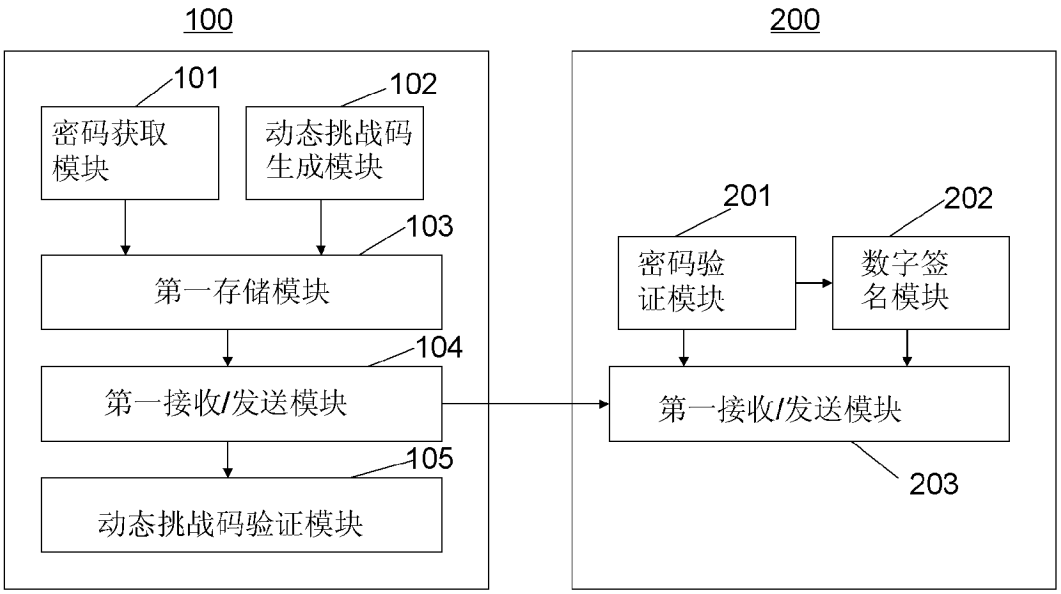

100
200
101
密码获取模块
102
动态挑战码生成模块
103
第一存储模块
104
第一接收/发送模块
105
动态挑战码验证模块
201
密码验证模块
202
数字签名模块
第一接收/发送模块
203

图 5