

[19] 中华人民共和国国家知识产权局



[12] 发明专利说明书

[51] Int. Cl.

G06K 17/00 (2006.01)

H04L 9/14 (2006.01)

G06K 19/077 (2006.01)

专利号 ZL 200710175850.5

[45] 授权公告日 2009 年 12 月 2 日

[11] 授权公告号 CN 1005655562C

[22] 申请日 2007.10.15

[21] 申请号 200710175850.5

[73] 专利权人 北京派瑞根科技开发有限公司

地址 100026 北京市朝阳区团结湖北路 2  
号 215 室

[72] 发明人 须 清

[56] 参考文献

CN1588386A 2005.3.2

CN101038630A 2007.9.19

US6412086B1 2002.6.25

审查员 夏贝贝

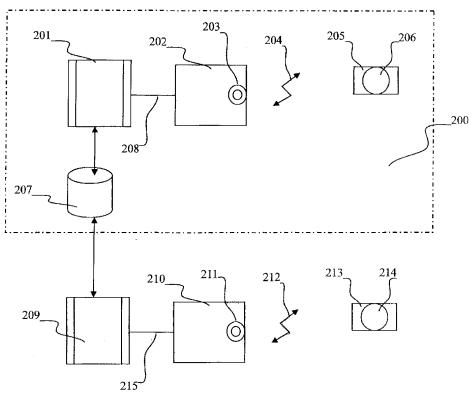
权利要求书 4 页 说明书 15 页 附图 6 页

[54] 发明名称

电子标签安全认证方法

[57] 摘要

本发明提出一种创新的电子标签安全认证方法，将 RFID 电子标签设计为未注册电路逻辑和已注册电路逻辑的两种工作逻辑，将 RFID 系统设计为包含注册子系统和认证子系统构成 RFID 安全认证系统结构。安全电子标签需要通过安全认证系统注册过后才能通过认证；安全电子标签的未注册电路逻辑和已注册电路逻辑的变化是单向的，即只能从未注册电路逻辑变化为已注册电路逻辑，而不能从已注册电路逻辑变化为未注册电路逻辑。解决电子标签被非法复制而被错误认证的问题，特别在诸如电子护照及电子护照认证系统、国家机密设施人员身份识别系统等应用环境中，保证身份认证的安全性和不可仿制性变得特别重要。



---

1. 电子标签安全认证方法，其特征是包含：

安全电子标签，所述安全电子标签包含未注册电路逻辑和已注册电路逻辑；

注册子系统，所述注册子系统是置于信息安全环境的服务器系统，由电子标签读写器、注册管理服务器和注册管理软件构成，所述的安全电子标签与注册子系统中所述的电子标签读写器通过无线射频信号进行通讯，所述注册子系统中的电子标签读写器连接到注册管理服务器，所述注册管理软件安装在注册管理服务器中，运行所述注册管理软件，按照注册流程，通过所述注册子系统中的电子标签读写器对于所述安全电子标签进行注册管理，将所述安全电子标签从未注册电路逻辑切换为已注册电路逻辑；

认证子系统，所述认证子系统是一种服务器系统，由电子标签读写器、认证管理服务器和认证管理软件构成，所述的安全电子标签与认证子系统中所述的电子标签读写器通过无线射频信号进行通讯，所述认证子系统中的电子标签读写器连接到认证管理服务器，所述认证管理软件安装在认证管理服务器中，运行所述认证管理软件，按照认证流程，通过所述认证子系统中的电子标签读写器对于所述的安全电子标签进行认证管理；

数据库存储设备，所述数据库存储设备是置于信息安全环境的数据存储设备，存储的数据包含所述安全电子标签的注册数据信息和认证数据信息，与所述的注册子系统通过安全的信息通道进行连接，与所述的认证子系统通过安全的信息通道进行连接；

所述的安全电子标签通过无线射频方式与注册子系统中电子标签读写器进行无线通讯连接，所述注册子系统中的电子标签读写器通过无线连接或有线连接方式与注册管理服务器进行通讯连接；

所述的安全电子标签通过无线射频方式与认证子系统中电子标签读写器进行无线通讯连接，所述认证子系统中的电子标签读写器通过无线连接或有线连接方式与认证管理服务器进行通讯连接；

在未注册电路逻辑工作状态下，所述安全电子标签的唯一标识信息是由电子标签地址信息和一组随机数构成，每次访问安全电子标签，随机数都会重新生成；

在已注册电路逻辑工作状态下，所述安全电子标签的随机数部分被锁定作为加

密的密钥。

2. 根据权利要求 1 所述的电子标签安全认证方法，其特征是所述的安全电子标签包含电子标识存储电路、密钥存储电路、随机数发生器电路、熔丝保护逻辑电路、加密算法逻辑电路、数据输出选择电路、控制处理逻辑电路、射频天线电路；

所述的随机数发生器电路通过熔丝保护逻辑电路与密钥存储电路连接，熔丝保护逻辑电路没有被熔断保护时，随机数发生器电路产生的随机数在控制处理逻辑电路的控制下存入到密钥存储电路，熔丝保护逻辑电路被熔断保护后，随机数发生器电路与密钥存储电路物理连接断开，密钥存储电路包含非易失存储体，其存储的数据不再发生变化；

同时密钥存储电路也通过熔丝保护逻辑电路与数据输出选择电路连接，熔丝保护逻辑电路没有被熔断保护时，密钥存储电路中存储的密钥在控制处理逻辑电路的控制下可以通过数据输出选择电路将数据发送到射频天线电路，熔丝保护逻辑电路的熔丝被熔断保护后，密钥存储电路与数据输出选择电路物理连接断开，密钥存储电路中存储的数据不能再发送到数据输出选择电路；

随机数发生器电路还与数据输出选择电路连接，在控制处理逻辑电路的控制下可以将随机数发生器电路生成的随机数发送到射频天线电路；

密钥存储电路与加密算法逻辑电路连接，作为加密算法逻辑电路的密钥，加密算法逻辑电路的输出连接到数据输出选择电路，在控制处理逻辑电路的控制下可以将数据发送到射频天线电路；

电子标识存储电路存储了电子标签的唯一标识信息，与数据输出选择电路连接，在控制处理逻辑电路的控制下可以将数据发送到射频天线电路。

3. 根据权利要求 2 所述的电子标签安全认证方法，其特征是所述的安全电子标签初始逻辑为未注册电路逻辑，即所述的熔丝保护逻辑电路的熔丝处于连通状态；所述的已注册电路逻辑是指所述的熔丝保护逻辑电路的熔丝被熔断后的工作逻辑。
4. 根据权利要求 1 所述的电子标签安全认证方法，其特征是所述的注册管理服务器是以个人电脑（PC）或计算机服务器为硬件，安装运行操作系统(OS)、数据库管理软件及应用软件的系统，其中应用软件至少包含专门处理安全电子标签注册应用的管理软件；所述的认证管理服务器是以个人电脑（PC）或计算机服务器为硬件，安装

运行操作系统(OS)、数据库管理软件及应用软件的系统，其中应用软件至少包含专门处理安全电子标签认证应用的管理软件；所述的数据库存储设备所存储的数据至少包含已经注册的安全电子标签的地址信息、密钥信息，所述的注册管理软件可以管理和访问所述的数据库存储设备所存储的数据；所述的认证管理软件可以访问所述的数据库存储设备所存储的数据。

5. 根据权利要求1所述的电子标签安全认证方法，其特征是对于安全电子标签进行安全认证的处理过程包括安全电子标签的注册流程和安全电子标签的认证流程；其中安全电子标签的注册流程以注册子系统为硬件平台，安全电子标签的认证流程以认证子系统为硬件平台。
6. 根据权利要求5所述的电子标签安全认证方法，其特征是所述的注册流程包含如下步骤：
  - a) 所述的注册子系统向所述的安全电子标签发送注册指令；
  - b) 所述的安全电子标签将安全电子标签的唯一标识信息和密钥存储电路存储的密钥信息发送到所述的注册子系统；
  - c) 所述的注册子系统接收所述安全电子标签的唯一标识信息和密钥存储电路存储的密钥信息并存储到所述的数据库存储设备；
  - d) 所述的注册子系统向所述的安全电子标签发送注册确认指令；
  - e) 所述的安全电子标签熔断熔丝保护逻辑电路的熔丝。
7. 根据权利要求6所述的电子标签安全认证方法，其特征是在所述的步骤a)之前包含对于电子标签进行单一化的操作指令步骤和获取电子标签的唯一标识信息的操作指令步骤；在步骤a)之前还包含从所述数据库存储设备检索到所述的安全电子标签是未注册过的，即处于未注册逻辑；在步骤c)包含对收到的密钥信息存储到所述的数据库存储设备之前进行加密运算；在步骤e)之后包含向注册子系统发送注册确认指令的响应信息，一般为电子标签的唯一标识信息或电子标签的唯一标识信息加上其它响应信息。
8. 根据权利要求5所述的电子标签安全认证方法，其特征是所述的认证流程包含如下步骤：
  - a) 所述的认证子系统生成一个随机数；

- 
- b) 所述的认证子系统向所述的安全电子标签发送认证指令和所述随机数;
  - c) 同时所述的认证子系统用所述的安全电子标签的标识信息从数据库存储设备中检索到密钥信息，与所述随机数进行加密运算得到结果 1;
  - d) 所述的安全电子标签接收到认证指令和所述随机数后，用存储在密钥存储电路的密钥和收到的所述随机数进行加密运算得到结果 2;
  - e) 所述的安全电子标签将结果 2 和唯一标识信息通过射频信号发送到所述的认证子系统;
  - f) 所述的认证子系统收到所述的安全电子标签发送的结果 2 和唯一标识信息，比较结果 1 与结果 2 是否相等，如果相等则认证成功，如果不相等，则认证失败;
9. 根据权利要求 8 所述的电子标签安全认证方法，其特征是在所述的步骤 a)之前包含对于电子标签进行单一化的操作指令步骤和获取电子标签的唯一标识信息的操作指令步骤；在步骤 a)之前还包含从所述数据库存储设备检索到所述的安全电子标签是已注册过的，即处于已注册逻辑；在步骤 f)之后所述认证子系统认证确认后可以允许安全电子标签的拥有者操作系统提供的其他操作。
10. 根据权利要求 1 至 9 中任一权利要求所述的电子标签安全认证方法，其特征是安全电子标签需要通过安全认证系统注册过后才能通过认证；安全电子标签的未注册电路逻辑和已注册电路逻辑的变化是单向的，即只能从未注册电路逻辑变化为已注册电路逻辑，而不能从已注册电路逻辑变化为未注册电路逻辑。

## 电子标签安全认证方法

### 技术领域

本发明涉及 **RFID** 电子标签、**RFID** 系统和一种提高 **RFID** 标签与 **RFID** 读写器之间通讯安全的方法，特别涉及将 **RFID** 电子标签设计为未注册电路逻辑和已注册电路逻辑的两种工作逻辑，将 **RFID** 系统设计为包含注册子系统和认证子系统构成 **RFID** 安全认证系统结构。属于电子标签技术领域和信息安全技术领域。

### 背景技术

**RFID** 是因英文 radio frequency identification 的缩写，称为射频识别器，或射频标签或射频电子标签或无线电子标签，通常也简称为电子标签，采用射频信号实现物品的自动识别，**RFID** 技术应用广泛，很多应用中需要提供较高的信息能力。

**RFID** 是带有射频天线的微电子电路芯片，分为主动式 **RFID** 和被动式 **RFID**。主动式 **RFID** 自带电池提供工作电源，但由于成本、尺寸、寿命等因素的影响，其应用范围较小，而被动式 **RFID** 相对廉价和小尺寸，可以用来标识各种物品，应用范围更广。**RFID** 通常存储一定数据，如用于标识 **RFID** 所表示物品的标识信息。被动式 **RFID** 通过射频天线信号被激活和提供工作电源，一旦激活后，可以通过射频天线收发数据信息并读写存储的数据信息。

通常 **RFID** 系统包含一个 **RFID** 读写器（或读卡器或阅读器或询问器）和 **RFID** 电子标签。**RFID** 读写器接收通过射频从 **RFID** 电子标签发来的数据，然后将数据传送到后台系统处理。**RFID** 读写器包括一个射频收发器，发送的射频信号为电子标签提供能量以启动电子标签。**RFID** 读写器可以对电子标签进行读操作和写操作。

上面已经说明，被动电子标签不需要电池。**RFID** 直接由射频收发器提供射频能量。**RFID** 系统的通讯距离较短，如符合 ISO- 14443 标准的 **RFID** 系统，电子标签和读写器之间的通讯距离不超过 10 厘米。

近距离可以看作是一种安全特性，但最近发现攻击 **RFID** 系统的距离比预期的大，如攻击 **RFID** 读写器向电子标签通讯的距离已经达到 50 米。更详细的报道，参见由 Z. Kfir and A. Wool 编写的 "Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems"（采用中继攻击非接触式智能卡系统窃取虚拟钱包），在互联网络地址 <http://eprmt.iacr.org/2005/052.pdf> 可以查看内容。在本说明书中

---

插入该文章作为参考。

有可能通过建立完全安全的通讯通道以提高安全性，但将需要完整的智能卡解决方案，其中用内嵌了 CPU、RAM、ROM 的真正智能卡替换相对简单的 RFID 电子标签，并采用加密算法，但该解决方案相对昂贵。

随着电子标签（RFID）技术的发展，其应用也越来越多，由于电子标签（RFID）相对于条码技术而言有很多优势，如信息量大、更安全、防污能力强、可一次阅读多个标签等。但随着电子技术的发展，电子标签（RFID）的设计和生产也变得越来越容易，虽然每个电子标签的地址应该是唯一的，且该地址信息很容易被读出，所以仍然不能排除电子标签信息被非法复制的可能。特别在一些信息安全级别要求很高的领域，如电子护照、无线支付等领域，电子标签（RFID）的信息如果被非法获取，将给电子标签持有者带来很大损失。

人们想出了加密的电子标签和加密算法，希望保证电子标签作为电子身份的安全。本专利文献包括一系列使用技术跟踪制造物品和完成物品认证的参考文献，如题为“Methods and System for Performing Article Authentication”的欧洲专利 0 710 934 A2；题为“Methods of Preventing Counterfeiting of Articles of Manufacture”的欧洲专利 0 889 448 A2；题为“System for Identifying, Authenticating, and Tracking Manufactured Article”的美国专利 No. 5,768,384；题为“认证标签的方法”的 PCT 专利号 00818777.0。在题为“认证标签的方法”的申请号为 00818777.0 提出了认证标签的方法。但是在这些和其他的参考文献中叙述的方法与本发明所提出的方法不同。上述方法不能解决电子标签被非法复制的问题。

本发明中提到的安全电子标签，是相对于一般电子标签而言，提供了一个新的功能特性来提高 RFID 系统的信息安全性，同时相应的 RFID 安全认证系统含注册子系统和认证子系统。

## 发明内容

本发明提出一种创新的安全电子标签，希望能够解决电子标签被非法复制而被错误认证的问题，特别在诸如电子护照及电子护照认证系统、国家机密设施人员身份识别系统等应用环境中，如何保证身份认证的安全性和不可仿制性变得特别重要。

为达到上述目的，本发明解决其技术问题所采用的技术方案是：

电子标签是专门设计的安全电子标签，可以工作在两种逻辑状态下，即未注册工

作状态和已注册工作状态，两种逻辑的工作状态是相互排斥的，也就是当电子标签工作在未注册工作状态逻辑时，已注册工作状态逻辑停止工作；当电子标签工作在已注册工作状态逻辑时，未注册工作状态逻辑停止工作。同时电子标签从未注册工作状态逻辑转变为已注册工作状态逻辑后，为了安全，可以设定该逻辑状态是不可逆转的，即只能从未注册工作状态逻辑转变为已注册工作状态逻辑，但不能从已注册工作状态逻辑转变为未注册工作状态逻辑。安全电子标签不同于普通电子标签之处还在于，在未注册工作状态逻辑工作状态下，安全电子标签的唯一标识信息是由电子标签地址信息和一组随机数构成，每次访问安全电子标签，随机数都会重新生成，因此每次访问未注册的安全电子标签，所得到的唯一标识信息中的随机数部分是变化的；而在已注册工作状态逻辑工作状态下，安全电子标签的随机数部分被锁定作为加密的密钥，由认证子系统中的认证管理服务器生成一个随机数，然后由电子标签地址信息加上该随机数构成认证指令发送给安全电子标签，安全电子标签将收到的随机数与安全电子标签内部存储用作加密密钥的随机数经过加密运算得到加密结果数据，然后安全电子标签将该加密结果数据与电子标签地址信息一起送回认证子系统中的认证管理服务器，由认证子系统中的认证管理服务器比较认证管理服务器的加密计算结果与安全电子标签的计算结果，如果相同，认证成功，否则认证失败。加密算法的选择与安全电子标签的设计难度和成本有关，当要求电子标签的成本较低时，可以采用简单的算法，如按位异或运算，只需要很少的逻辑电路模块即可实现一种对称加密算法，其缺点是攻击者经过一定时间的分析可以推测到所用的算法；随着半导体技术的发展，可以在成本增加一定的情况下，采用更复杂的加密算法，如通常采用对称加密算法，如 DES 算法，DES 算法全称为 Data Encryption Standard，即数据加密算法，它是 IBM 公司于 1975 年研究成功并公开发表的。

与本发明所对应的 RFID 注册认证系统是一种安全电子标签认证系统，包含注册子系统、认证子系统、数据库存储设备以及进行安全认证的处理软件。在这个系统中，本发明中的电子标签只有通过注册子系统注册过后的电子标签才能通过认证子系统的认证，而电子标签一旦注册成功后，其工作逻辑将被强制切换到已注册工作状态，且不可逆转回未注册工作状态。当有仿制相同标签地址的电子标签进行注册时，由于注册子系统中已经有该地址的电子标签地址存在，可以立即发现该电子标签是伪造电子标签，注册不会成功；同时由于电子标签支持加密算法，而密钥是在注册子系统进行注册时随机生成的，并存储于数据库存储设备和电子标签内部，同时存储于安全电子标签内部密钥数据的直接访问硬件电路在注册时已经把其中的熔丝保护电路中的熔丝熔断而永远

不可恢复，从而保证密钥信息不会通过电子标签的数据接口信息泄漏出来。由于一般数据库存储设备都有较强的信息处理能力，可以对于密钥数据进行加密，且放置在十分安全的环境中，可以保证密钥数据的信息安全。

电子标签工作在认证逻辑时，认证子系统先获得电子标签的识别号码，从数据库中搜索电子标签的密钥信息，然后生成一个随机数 Rand，用获得的识别号码、电子标签的密钥信息和随机数经过加密算法生成运算结果 Ra1。认证子系统将 Rand 发送到电子标签，电子标签经过同样的加密算生成运算结果 Ra1'，发送回认证子系统。认证子系统比较 Ra1 和 Ra1'，如果相同，则认证成功，否则不能认证。

安全电子标签的设计分为两种，一种是从射频信号中提取供电能源的无源电子标签，另一种是自带供电电池的有源电子标签。

根据上述设计思想，本发明的安全电子标签的电路设计说明如下：

一种可以防止被非法复制的安全电子标签，是一种专门设计的安全电子标签，可以工作于两种工作状态：未注册工作状态和已注册工作状态。安全逻辑处理电路与公知的电子标签设计是不一样，也是本发明的核心设计所在。

### 1. 电子标签安全认证方法，包含：

安全电子标签，所述安全电子标签包含未注册电路逻辑和已注册电路逻辑；

注册子系统，所述注册子系统是置于信息安全环境的服务器系统，由电子标签读写器、注册管理服务器和注册管理软件构成，所述注册子系统中的安全电子标签与注册子系统中所述的电子标签读写器通过无线射频信号进行通讯，所述注册子系统中的电子标签读写器连接到注册管理服务器，所述注册管理软件安装在注册管理服务器中，运行所述注册管理软件，按照注册流程，通过所述注册子系统中的电子标签读写器对于所述安全电子标签进行注册管理，将所述安全电子标签从未注册电路逻辑切换为已注册电路逻辑；

认证子系统，所述认证子系统是一种服务器系统，由电子标签读写器、认证管理服务器和认证管理软件构成，所述的安全电子标签与认证子系统中所述的电子标签读写器通过无线射频信号进行通讯，所述认证子系统中的电子标签读写器连接到认证管理服务器，所述认证管理软件安装在认证管理服务器中，运行所述认证管理软件，按照认证流程，通过所述认证子系统中的电子标签读写器对于所述安全电子标签进行认证管理；

数据库存储设备，所述数据库存储设备是置于信息安全环境的数据存储设备，存储的数据包含所述安全电子标签的注册数据信息和认证数据信息，与所述的注册子系统通过安全的信息通道进行连接，与所述的认证子系统通过安全的信息通道进行连接；

在未注册电路逻辑工作状态下，所述安全电子标签的唯一标识信息是由电子标签地址信息和一组随机数构成，每次访问安全电子标签，随机数都会重新生成；

在已注册电路逻辑工作状态下，所述安全电子标签的随机数部分被锁定作为加密的密钥。

2. 安全电子标签通过无线射频方式与注册子系统中电子标签读写器进行无线通讯连接，注册子系统中电子标签读写器通过无线连接或有线连接方式与注册管理服务器进行通讯连接；所述的安全电子标签通过无线射频方式与认证子系统中电子标签读写器进行无线通讯连接，认证子系统中电子标签读写器通过无线连接或有线连接方式与认证管理服务器进行通讯连接。
3. 安全电子标签包含电子标识存储电路、密钥存储电路、随机数发生器电路、熔丝保护逻辑电路、加密算法逻辑电路、数据输出选择电路、控制处理逻辑电路、射频天线电路，

所述的随机数发生器电路通过熔丝保护逻辑电路与密钥存储电路连接，熔丝保护逻辑电路没有被熔断保护时，随机数发生器电路产生的随机数在控制处理逻辑电路的控制下存入到密钥存储电路，熔丝保护逻辑电路被熔断保护后，随机数发生器电路与密钥存储电路物理连接断开，密钥存储电路包含非易失存储体，其存储的数据不再发生变化；

同时密钥存储电路也通过熔丝保护逻辑电路与数据输出选择电路连接，熔丝保护逻辑电路没有被熔断保护时，密钥存储电路中存储的密钥在控制处理逻辑电路的控制下可以通过数据输出选择电路将数据发送到射频天线电路，熔丝保护逻辑电路的熔丝被熔断保护后，密钥存储电路与数据输出选择电路物理连接断开，密钥存储电路中存储的数据不能再发送到数据输出选择电路；

随机数发生器电路还与数据输出选择电路连接，在控制处理逻辑电路的控制下可以将随机数发生器电路生成的随机数发送到射频天线电路；

密钥存储电路与加密算法逻辑电路连接，作为加密算法逻辑电路的密钥，加密

算法逻辑电路的输出连接到数据输出选择电路，在控制处理逻辑电路的控制下可以将数据发送到射频天线电路；

电子标识存储电路存储了电子标签的唯一标识信息，与数据输出选择电路连接，在控制处理逻辑电路的控制下可以将数据发送到射频天线电路。

4. 安全电子标签初始逻辑为未注册电路逻辑，即所述的熔丝保护逻辑电路的熔丝处于连通状态；所述的已注册电路逻辑是指所述的熔丝保护逻辑电路的熔丝被熔断后的工作逻辑。
5. 对于安全电子标签进行安全认证的处理过程包括安全电子标签的注册流程和安全电子标签的认证流程；其中安全电子标签的注册流程以注册子系统为硬件平台，安全电子标签的认证流程以认证子系统为硬件平台。
6. 安全电子标签在注册子系统进行注册的注册流程包含如下步骤：
  - a) 所述的注册子系统向所述的安全电子标签发送注册指令；
  - b) 所述的安全电子标签将安全电子标签的唯一标识信息和密钥存储电路存储的密钥信息发送到所述的注册子系统；
  - c) 所述的注册子系统接收所述安全电子标签的唯一标识信息和密钥存储电路存储的密钥信息并存储到所述的数据存储设备；
  - d) 所述的注册子系统向所述的安全电子标签发送注册确认指令；
  - e) 所述的安全电子标签熔断熔丝保护逻辑电路的熔丝。
7. 上述的步骤 a)之前包含对于电子标签进行单一化（Singulation）的操作指令步骤和获取电子标签的唯一标识信息的操作指令步骤。
8. 上述的步骤 a)之前包含从所述数据存储设备检索到所述的安全电子标签是未注册过的，即处于未注册逻辑。
9. 上述的步骤 c)包含对收到的密钥信息存储到所述的数据存储设备之前进行加密运算。这种加密运算仅仅是注册子系统保存数据的一种安全方式，读取存储的信息时需要使用对应的解密算法进行解密。由注册子系统的软件决定算法。如可以采用简单数据移位处理等算法。
10. 上述的步骤 e)之后包含向注册子系统发送注册确认指令的响应信息，一般为电子标签的唯一标识信息或电子标签的唯一标识信息加上其它响应信息。

11. 当所述的安全电子标签工作于未注册电路逻辑，则所述的随机数发生器电路每次收到一条注册指令都要生成一个新的随机数并存储到密钥存储电路中，使密钥存储电路的密钥总是在随机变化，并与所述的随机数发生器电路产生的随机数相同，同时所述密钥存储电路也通过熔丝保护逻辑电路与数据输出选择电路连接，可以正确；当所述的安全电子标签工作于已注册电路逻辑，则所述的随机数发生器电路与所述的密钥存储电路物理连接断开，同时所述密钥存储电路与数据输出选择电路物理连接断开，使密钥存储电路的密钥不会跟随所述的随机数发生器电路生成的新随机数的变化而变化，并且防止了密钥存储电路的密钥被输出，此时在步骤 c)中电子标签响应注册指令的输出是安全电子标签的唯一标识信息和随机数发生器电路生成的新随机数。
12. 安全电子标签载认证子系统的认证流程包含如下步骤：
  - a) 所述的认证子系统生成一个随机数；
  - b) 所述的认证子系统向所述的安全电子标签发送认证指令和所述随机数；
  - c) 同时所述的认证子系统用所述的安全电子标签的标识信息从数据库存储设备中检索到密钥信息，与所述随机数进行加密运算得到结果 1；
  - d) 所述的安全电子标签接收到认证指令和所述随机数后，用存储在密钥存储电路的密钥和收到的所述随机数进行加密运算得到结果 2；
  - e) 所述的安全电子标签将结果 2 和唯一标识信息通过射频信号发送到所述的认证子系统；
  - f) 所述的认证子系统收到所述的安全电子标签发送的结果 2 和唯一标识信息，比较结果 1 与结果 2 是否相等，如果相等则认证成功，如果不相等，则认证失败；
13. 认证流程的步骤 a)之前包含对于电子标签进行单一化（Singulation）的操作指令步骤和获取电子标签的唯一标识信息的操作指令步骤。
14. 认证流程的步骤 a)之前包含从所述数据库存储设备检索到所述的安全电子标签是已注册过的，即处于已注册逻辑。
15. 认证流程的步骤 f)之后所述认证子系统认证确认后允许安全电子标签的拥有者操作系统提供的其他操作。
16. 所述的安全电子标签工作于未注册电路逻辑，则所述的随机数发生器电路每次收到

一条指令都要生成一个新的随机数并存储到密钥存储电路中，使密钥存储电路的密钥总是在随机变化，因此加密运算的结果2总是在随机变化；当所述的安全电子标签工作于已注册电路逻辑，则所述的随机数发生器电路与所述的密钥存储电路物理连接断开，使密钥存储电路的密钥总是保持不变。

17. 安全电子标签需要通过安全认证系统注册过后才能通过认证。
18. 安全电子标签可以工作在两种工作状态：未注册工作状态和已注册工作状态。
19. 安全电子标签的未注册电路逻辑和已注册电路逻辑的变化是单向的，即只能从未注册电路逻辑变化为已注册电路逻辑，而不能从已注册电路逻辑变化为未注册电路逻辑。
20. 电子标签读写器是通过无线射频信号与安全电子标签进行信息的通讯，包括读取、写入、修改安全电子标签的存储信息。
21. 注册管理服务器是以个人电脑（PC）或计算机服务器为硬件，安装运行操作系统（OS）、数据库管理软件及应用软件的系统，其中应用软件至少包含专门处理安全电子标签注册应用的管理软件。
22. 认证管理服务器是以个人电脑（PC）或计算机服务器为硬件，安装运行操作系统（OS）、数据库管理软件及应用软件的系统，其中应用软件至少包含专门处理安全电子标签认证应用的管理软件。
23. 数据库存储设备所存储的数据至少包含已经注册的安全电子标签的地址信息、密钥信息，所述的注册管理软件可以管理和访问所述的数据库存储设备所存储的数据；所述的认证管理软件可以访问所述的数据库存储设备所存储的数据。
24. 注册管理服务器、认证管理服务器的硬件平台可以采用一个硬件平台，数据库存储设备也可以用注册管理服务器或认证管理服务器的硬盘替代。

本发明的有益效果是：由于所采用的安全电子标签是通过专门设计的，其用于加密算法的密钥数据只有在进行注册确认后才被确定下来，可以确保密钥信息的动态生成与安全，而且将电子标签设计为未注册状态的工作逻辑和已注册状态下的工作逻辑，未注册的安全电子标签在认证子系统中是无法通过认证的，保证了系统的安全。整个安全电子标签在进行认证过程中，由认证子系统生成随机数发送到安全电子标签，然后读取经过加密计算的结果，避免了加密密钥在传输中的泄漏，被其他人仿制。相比已有技术的安全电子标签是将标签地址或信息数据通过加密后传输以防止信息泄漏的技术方案，

但随着半导体设计技 制造技术及反向工程技术的发展，复制出拥有完全相同的标签地址和加密算法的电子标签是完全可以做到，因此无法避免电子标签被复制，并可能被非法使用，给合法电子标签拥有者造成巨大损失。而采用本发明的安全电子标签，即使有人可以非法复制一模一样的电子标签，如果复制的逻辑状态是未注册状态，由于安全认证系统中已经存在该标签的地址，因此不可能通过认证；如果复制的逻辑状态是已注册逻辑状态，由于原合法的安全电子标签的密码是在注册时随机生成的，且一旦注册成功，该信息也不会经过电子标签向外传送，只要保证安全认证系统的数据库数据安全，密码数据就不会被泄漏，所以无法复制安全电子标签的密码，因此非法复制的电子标签也不可能通过认证，从而有效解决了电子标签被非法复制带来的信息安全问题。作为安全认证系统的数据库数据通常被认为是最机密的数据，只要有高度的安全保密管理制度即可解决系统数据的安全性问题。

#### 附图说明：

图 1 是电子标签安全认证系统的一种实现的系统框图

图 2 是由注册子系统和认证子系统与安全电子标签构成安全认证系统示意图。

图 3 是安全电子标签的一种实现框图。

图 4 是安全电子标签的安全逻辑处理电路的一种实现示意图。

图 5 是安全电子标签在未注册状态下向电子标签读写器发送标识信息的流程示意图。

图 6 是安全电子标签在未注册状态下收到电子标签读写器发出的注册确认信息后的处理流程示意图。

图 7 是安全电子标签在已注册状态下收到电子标签读写器发出的认证信息后的处理流程示意图。

图 8 是电子标签认证系统的注册子系统注册安全电子标签过程中进行信息交互的示意图。

图 9 是电子标签认证系统的认证子系统认证安全电子标签过程中进行信息交互的示意图。

#### 具体实施方式：

下面结合附图对本发明的结构原理和工作原理进行详细说明。

图 1 是将安全电子标签具体应用中的电子标签认证系统的一种实现的系统框图，注册子系统 102 和认证子系统 104 都与数据库存储设备 101 电连接，在大型系统应用中，通常数据库存储设备 101 可用采用硬盘存储阵列，注册子系统 102 和认证子系统 104 一般都采用服务器电脑外接电子标签读写器构成硬件平台，运行电脑操作系统如 Windows 或 Unix 或 Linux，并安装运行电子标签信息管理软件：进行安全认证的处理软件。注册子系统 102 可以只安装管理注册的处理软件，认证子系统 104 可以只安装管理认证的处理软件。未注册的安全电子标签 103 通过无线射频信号与注册子系统 102 的电子标签读写器之间进行信息通讯，已注册的安全电子标签 105 通过无线射频信号与认证子系统 104 的电子标签读写器之间进行信息通讯。由于本发明中所用的电子标签是需要专门设计的安全电子标签，其注册之前和注册之后的运行逻辑不一样。

图 2 是由注册子系统和认证子系统与安全电子标签构成安全认证系统示意图。由注册管理服务器 201 和电子标签读写器 202 构成注册子系统，其中电子标签读写器 202 上有射频天线 203，注册管理服务器 201 和电子标签读写器 202 之间的连接 208 可以是有线连接，如局域以太网络连接，也可以采用无线连接，如无线局域网络（WLAN、Wi-Fi、Bluetooth、WIMAX、UWB 等）；与电子标签读写器 202 通过射频信号 204 连接的安全电子标签 205 之间进行无线通讯，在安全电子标签 205 上有射频天线 206，当安全电子标签 205 设计为被动式电子标签时，射频天线 206 除了收发数据信息外，还感应出安全电子标签 205 工作的供电能量。注册管理服务器 201 通过高速数据连接线与数据库存储设备 207 连接。为了保证安全电子标签的注册过程是在一个信息安全的环境中进行，避免信息被攻击，通常将注册子系统的注册管理服务器 201 和电子标签读写器 202、安全电子标签 205、数据库存储设备 207 放置在具有信息安全的环境 200 中。如用一个足以容纳下这些设备的法拉第金属网屏蔽内部信号的泄漏。而认证子系统通常工作在具体应用环境，由认证管理服务器 209 和电子标签读写器 210 构成注册子系统，其中电子标签读写器 210 上有射频天线 211，认证管理服务器 209 和电子标签读写器 210 之间的连接 215 可以是有线连接，如局域以太网络连接，也可以采用无线连接，如无线局域网络（WLAN、Wi-Fi、Bluetooth、WIMAX、UWB 等）；与电子标签读写器 210 通过射频信号 212 连接的安全电子标签 213 之间进行无线通讯，在安全电子标签 213 上有射频天线 214，当安全电子标签 213 设计为被动式电子标签时，射频天线 214 除了收发数据信息外，还感应出安全电子标签 213 工作的供电能量。认证管理服务器 209 通过高速数据连接线与数据库存储设备 207 连接，为了保证这个连接的信息安全，通常要增加防火墙软件安装在认

证管理服务器 209 中。

图 3 是安全电子标签的一种逻辑示意图，以被动式电子标签为实现实例，天线耦合与阻抗匹配电路 301 通过天线感应射频信号分别送到整流电路 302 和信号解调电路与时钟提取电路 304，整流电路 302 从射频信号得到感应电流和感应电压并经供电电路 303 进行电压调整合供电分配供电子标签其他逻辑电路的工作。信号解调电路与时钟提取电路 304 用于从射频信号中解调出数据信息，然后送到数据提取电路 305 提取从射频信号收到的指令信息和数据送到数据分析逻辑处理电路 309 进行指令执行和数据处理，在已有的电子标签产品中也称该部分电路为控制电路或状态机电路，如 ATTEL 公司的 ATA5590 RFID 电子标签称该部分电路为状态机电路(Finite State Machines)，在 Infineon 公司的 SRF 66V10RFID 电子标签称该部分电路为数字逻辑电路(Digital Logic)。数据分析逻辑处理电路 309 进行信号分析，由于通过射频信号接收的信号种类只有几种：获取电子标签的标识信息、电子标签注册确认信息、电子标签认证信息等，而且通过射频信号发送的信号种类也只有几种：未注册状态下的电子标签标识信息、已注册状态下的电子标签标识信息，其中未注册状态下的电子标签标识信息是电子标签的地址信息附加一组随机数构成，已注册状态下的电子标签标识信息是电子标签的地址信息附加经过加密计算的加密信息，所以数据分析逻辑处理电路 309 用硬件逻辑电路完全可以实现，不需要复杂的信息处理电路或处理器。电子标签标识地址存储电路 307 存储了为每个电子标签分配的唯一标识信息，通常存放在非易失只读存储体(ROM)中，不可更改。电子标签标识地址存储电路 307 与数据分析逻辑处理电路 309 电连接，可以控制唯一标识信息的输出。数据存储电路 308 一般为非易失存储体，如电可擦写可编程只读存储体(EEPROM)或闪存存储体(FLASH Memory)。数据存储电路 308 与数据分析逻辑处理电路 309 电连接，可以通过射频信号由 RFID 读写器修改或读取数据存储电路 308 的数据。数据分析逻辑处理电路 309 对于接收信息的响应需要通过与其连接的信号调制器 306 将数据进行调制处理后送到天线耦合与阻抗匹配电路 301，然后通过射频天线发送到 RFID 读写器。与一般 RFID 电子标签设计不同的是增加了与数据分析逻辑处理电路 309 连接的安全逻辑处理电路 310，实现一种安全的电子标签的设计。在图 4 给出安全逻辑处理电路 310 的一种实现。

图 4 是安全电子标签的安全逻辑处理电路的一种实现示意图。图中的密钥存储电路 401、熔丝保护逻辑电路 402、随机数存储逻辑电路 403、随机数发生器逻辑电路 404

构成安全电子标签的密钥产生和保护机制电路。在数据分析逻辑处理电路 309 输出的控制信号 411 的控制下随机数发生逻辑电路产生新的随机数，然后存储到随机数存储逻辑电路 403 中，当熔丝保护逻辑电路 402 连通状态下，产生的随机数也存储到密钥存储电路 401，产生新的密钥，如果熔丝保护逻辑电路 402 的熔丝被熔断，则熔丝保护逻辑电路 402 处于物理连接断开状态，随机数就不能存储到密钥存储电路 401 中，从而保证一旦注册成功后密钥数据不变化。加密算法逻辑电路 406 输入的数据包括来自数据分析逻辑处理电路 309 提供的需要加密的数据 407 和来自数据选择电路 405 的密钥数据，数据选择电路 405 在数据分析逻辑处理电路 309 输出的控制信号 411 的控制下选择密钥的来源，可以增强系统的安全性：当安全电子标签处于已注册逻辑状态，如果攻击者想知道存储的密钥，发送认证指令时，输入的数据不是随机数，而是基本相同的数据，数据分析逻辑处理电路 309 检测到这种状态，表明是受到攻击，因此通过数据选择电路 405 选择随机数存储逻辑电路 403 随机数作为密钥参加加密运算以误导攻击者，提高安全性。数据选择电路 405 的输出还通过熔丝保护逻辑电路 408 与数据输出选择电路 409 连接，当电子标签处于未注册状态时，熔丝保护逻辑电路 408 处于物理连通状态，可以将密钥存储电路 401 存储的密钥通过数据选择电路 405、熔丝保护逻辑电路 408 和数据输出选择电路 409 将数据通过信号线 410 送到数据分析逻辑处理电路 309，由数据分析逻辑处理电路 309 再将数据送出电子标签。但当电子标签处于已注册状态后，熔丝保护逻辑电路 408 的物理连接断开，保证密钥存储电路 401 存储的密钥不会泄露出去。同时随机数存储逻辑电路 403 与数据输出选择电路 409 也有连接，可以进一步提高电子标签的安全性：当安全电子标签处于已注册逻辑状态，如果攻击者想知道存储的密钥，发送注册指令时，数据分析逻辑处理电路 309 检测到这种状态，表明是受到攻击，因此通过数据输出选择电路 409 选择随机数存储逻辑电路 403 随机数作为密钥输出以误导攻击者，提高安全性。

在安全电子标签处于未注册状态时，如果数据分析逻辑处理电路 309 收到电子标签注册确认信息，数据分析逻辑处理电路 309 将发出控制信息给熔丝保护逻辑电路 402 和熔丝保护逻辑电路 408 熔断各自的保险丝，此时随机数存储逻辑电路 403 与密钥存储电路 401 的物理连接被断开，密钥存储电路 401 存储的数据将保持不变，同时密钥存储电路 401 与数据输出选择电路 409 的物理电连接被断开，密钥存储电路 401 存储的数据不会被泄漏，因此可以将密钥存储电路 401 存储的数据作为加密算法的密钥信息。数据分析逻辑处理电路 309 的控制下将来自电子标签标识地址存储电路 307 的信息通过信号

调制器 306 和天线耦合与阻抗匹配电路 301 以及射频天线发送到电子标签读写器中。

在安全电子标签处于已注册状态时，如果数据分析逻辑处理电路 309 收到电子标签认证信息，首先数据分析逻辑处理电路 309 从所接收的信息中提取出认证子系统生成的随机数据信息并送到加密算法逻辑电路 406，同时密钥存储电路 401 的数据也通过数据选择电路 405 被送到加密算法逻辑电路 406 中，然后加密算法逻辑电路 406 将加密计算的结果送到数据输出选择电路 409 中，在数据分析逻辑处理电路 309 的控制下将来加密算法逻辑电路 406 的数据信息和来自电子标签标识地址存储电路 307 的信息组合在一起通过信号调制器 306 和天线耦合与阻抗匹配电路 301 以及射频天线发送到电子标签读写器中。

加密算法逻辑电路 406 的算法选择，可以根据成本要求，成本要求较高时，可以采用单纯的按位异或运算的算法进行加密，实现逻辑电路容易，当成本要求不高时，可以采用 DES 算法或 3DES（Triple DES）算法。其中 3DES（即 Triple DES）是 DES 向 AES 过渡的加密算法（1999 年，NIST 将 3-DES 指定为过渡的加密标准），是 DES 的一个更安全的变形。关于 DES 算法或 3DES（Triple DES）算法或 RSA 算法在 RFID 电子标签的实现可以参考飞利浦创立的独立半导体公司 NXP 半导体推出的新型非接触式智能卡 IC — MIFARE® DESFire8 中的加密算法的实现，作为本发明引用的设计内容。

随机数发生器逻辑电路 404 的逻辑实现可以参考 ATMEL 公司的 ATA5590 电子标签的中随机数发生器的实现，作为本发明引用的设计内容。

图 5 是安全电子标签在未注册状态下向电子标签读写器发送标识信息的流程示意图，安全电子标签收到阅读器发出的获取标识信息的指令 501 后，先判断安全电子标签的当前状态：电子标签是否已注册？502，如果已经注册过，则电子标签可以不做任何响应以减少电子标签之间的信号干扰，也可以如图示进入随机数发生器生成随机数 507，转入读取标识读取电子标签地址信息 505 步骤；如果没有注册过，则进入流程：随机数发生器生成随机数 503，然后将该随机数写入存储密钥信息的非易失存储体 504，读取标识读取电子标签地址信息 505，最后将随机数和标识信息发送给阅读器 506 完成对于处于未注册状态下向电子标签读写器发送标识信息的流程。注册子系统将收到的随机数存储到数据库存储体中对该电子标签地址的密钥数据字段中。该流程中，相比较普通电子标签而言，在电子标签的标识信息中除了电子标签地址信息外添加了一组随机数数据，在电子标签读写器没有发出注册确认信息之前，每次获取的电子标签标识信息

中的随机数都是变化的。

图 6 是安全电子标签在未注册状态下收到电子标签读写器发出的注册确认信息后的处理流程示意图，安全电子标签收到阅读器发出的注册确认信息的指令 601 后，先判断安全电子标签的当前状态：电子标签是否已注册？602，如果已经注册过，则电子标签可以不做任何响应以减少电子标签之间的信号干扰；如果没有注册过，则进入流程：判断地址信息是否与电子标签相同？603，若不同，则表明不是发送给该电子标签的注册确认信息，不做任何响应以减少电子标签之间的信号干扰；若相同，则表明是发送给该电子标签的注册确认信息，进入后续流程。接下来的流程是熔断熔丝保护逻辑电路的熔丝 604，然后读取标识读取电子标签地址信息 605，最后将电子标签地址信息和注册响应标志信息发送给阅读器 606 完成对于处于未注册状态下进行注册确认并向电子标签读写器发送回馈信息的流程。

图 7 是安全电子标签在已注册状态下收到电子标签读写器发出的认证信息后的处理流程示意图，安全电子标签收到阅读器发出的认证信息的指令 701 后，先判断安全电子标签的当前状态：电子标签是否已注册？702，如果未注册过，则电子标签可以不做任何响应以减少电子标签之间的信号干扰；如果已经注册过，则进入后续认证流程：提取认证信息中地址信息和随机数信息 703，然后判断地址信息是否与电子标签相同？704，若不同，则表明不是发送给该电子标签的认证信息，不做任何响应以减少电子标签之间的信号干扰；若相同，则表明是发送给该电子标签的认证信息，进入后续流程。用随机数、存储的密钥信息进行加密运算 705，这里的密钥信息是在注册确认时电子标签锁定的随机数，且在注册子系统中已经存储到数据库存储体中。然后读取加密运算结果 706，并读取电子标签地址信息 707，最后将加密运算结果和电子标签地址信息发送给阅读器 708 完成对于处于已注册状态下收到电子标签读写器发出的电子标签认证信息的处理流程。该流程中，相比较普通电子标签而言，在电子标签的标识信息中除了电子标签地址信息外添加了一组随机数数据，在电子标签读写器没有发出注册确认信息之前，每次获取的电子标签标识信息中的随机数都是变化的。在具体实现中，加密运算的算法可以采用按位异或运算或 DES 算法，也可以采用其它对称加密算法。

在本发明中的安全电子标签涉及安全电子标签与注册子系统的信息交互，也涉及安全电子标签与认证子系统的信息交互。下面对于注册过程和认证过程的交互实现进行进一步说明。

图 8 是电子标签认证系统的注册子系统注册安全电子标签过程中进行信息交互的示意图。在注册子系统与安全电子标签的信息交互中，注册子系统先发送读取标识信息的指令给安全电子标签，安全电子标签返回地址信息和随机数，如果返回的只有地址信息（图中虚线所示），则表明电子标签不是本系统中可用的电子标签，注册失败；注册子系统收到安全电子标签返回的地址信息和随机数后，注册子系统发出注册确认信息指令给安全电子标签，安全电子标签完成注册处理后返回地址信息和注册响应标志信息，如果返回的只有地址信息（图中虚线所示），则表明电子标签不是本系统中可用的电子标签，注册失败；注册子系统收到安全电子标签返回的地址信息和注册响应标志信息，则注册成功。

图 9 是电子标签认证系统的认证子系统认证安全电子标签过程中进行信息交互的示意图。在认证子系统与安全电子标签的信息交互中，认证子系统先发送读取标识信息的指令给安全电子标签，安全电子标签返回地址信息，如果返回的是地址信息和随机数（图中虚线所示），则表明电子标签没有注册，认证失败；认证子系统收到安全电子标签返回的地址信息后，认证子系统发出认证信息指令和随机数给安全电子标签，安全电子标签完成加密运算处理后返回加密运算结果和地址信息，如果返回的只有地址信息（图中虚线所示），则表明电子标签不是本系统中可用的电子标签，认证失败；认证子系统收到安全电子标签返回的加密运算结果和地址信息，比较认证子系统计算的加密运算结果与电子标签返回的加密运算结果，如果相等则认证成功，否则认证失败。

在本发明的描述和实现中，涉及到一些信息指令的定义，需要事先约定，包括读取标识信息的指令、注册确认信息指令、注册响应标志信息、认证信息指令。在具体实现中，可以这样规定，约定连续 10 个字节的全 00、连续 10 个字节的全 ff、连续 10 个字节的 55、连续 10 字节的全 aa 作为约定的指令信息，在注册子系统、认证子系统以及安全电子标签中生成的随机数如果是上述约定指令的数据，则需要重新生成以避开与指令信息冲突，同样在生产安全电子标签时，固化的电子标签地址信息也需要避开这些特定的数据。具体的可以规定，连续 10 个字节的全 ff 表示注册子系统或认证子系统发出的读取标识信息的指令，连续 10 个字节的全 00 作为安全电子标签返回的注册响应标志信息，连续 10 个字节的 55 表示注册子系统发出的注册确认信息指令，连续 10 字节的全 aa 表示认证子系统发出的认证信息指令。

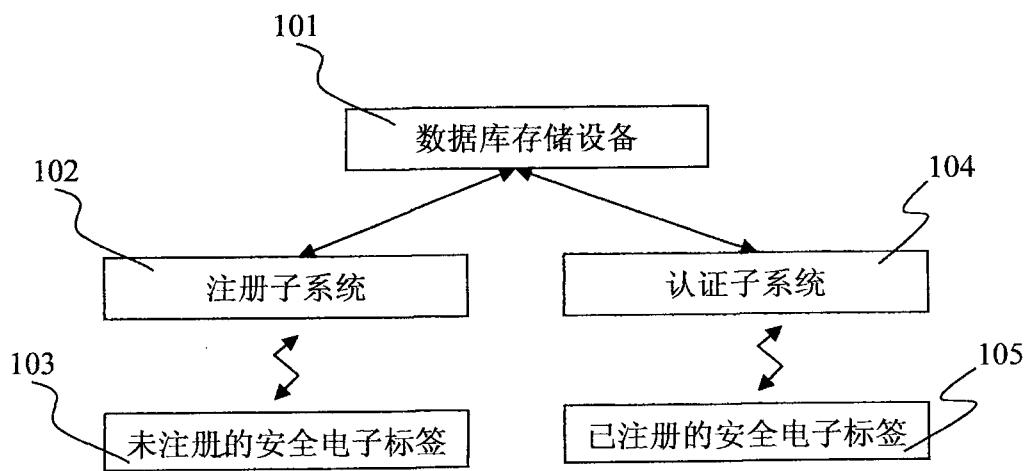


图 1

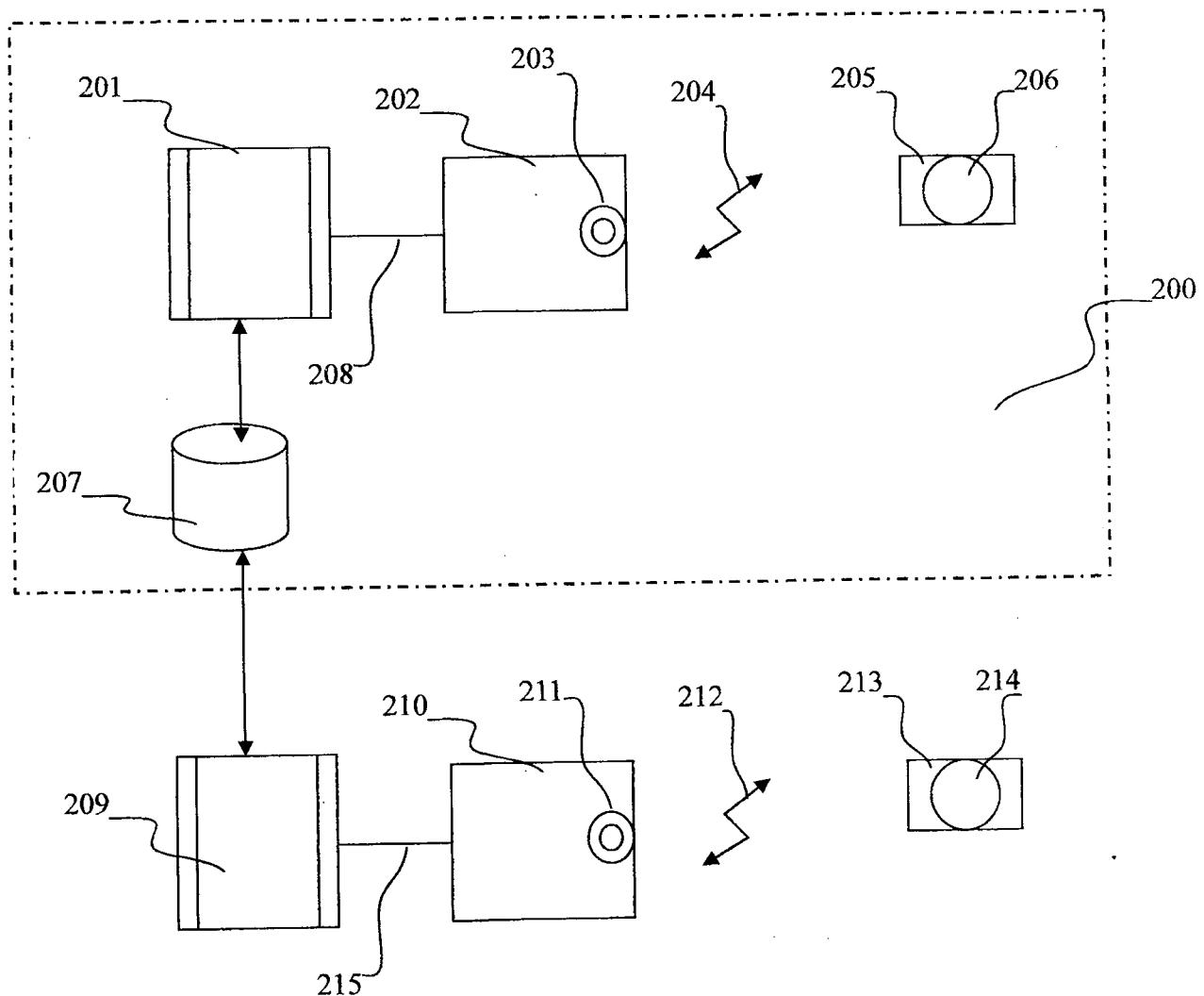


图 2

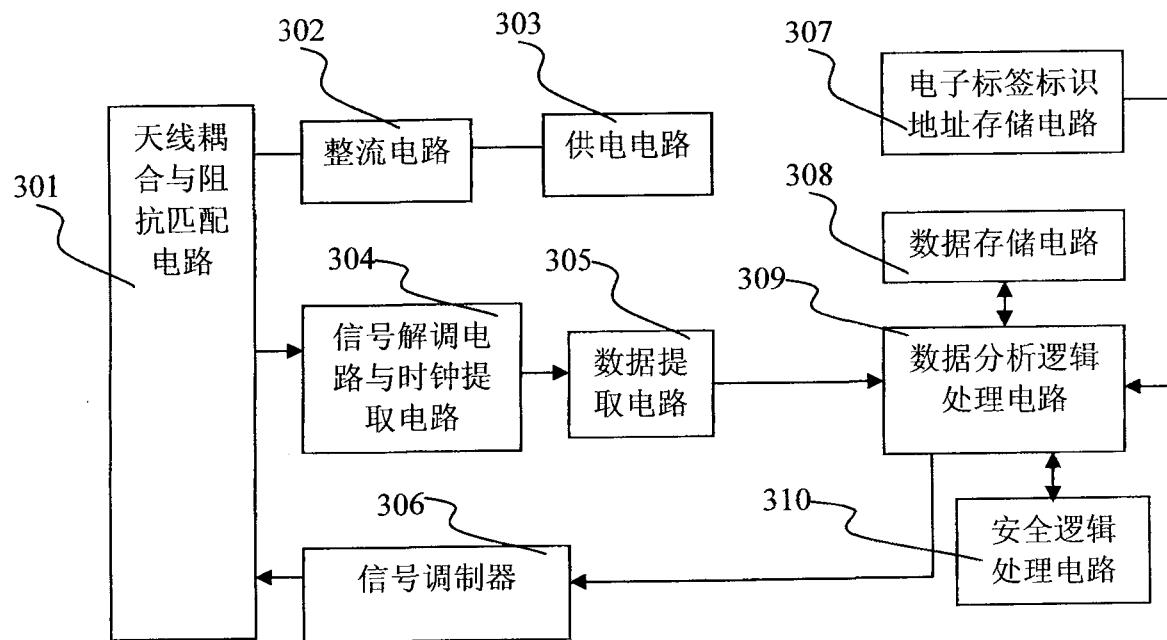


图 3

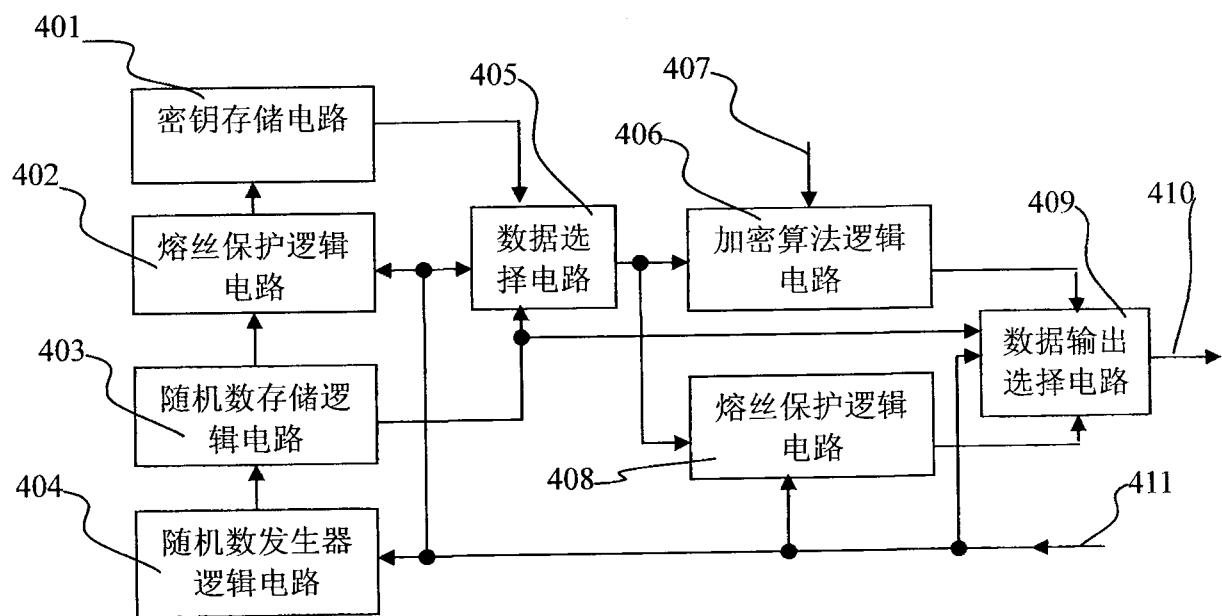


图 4

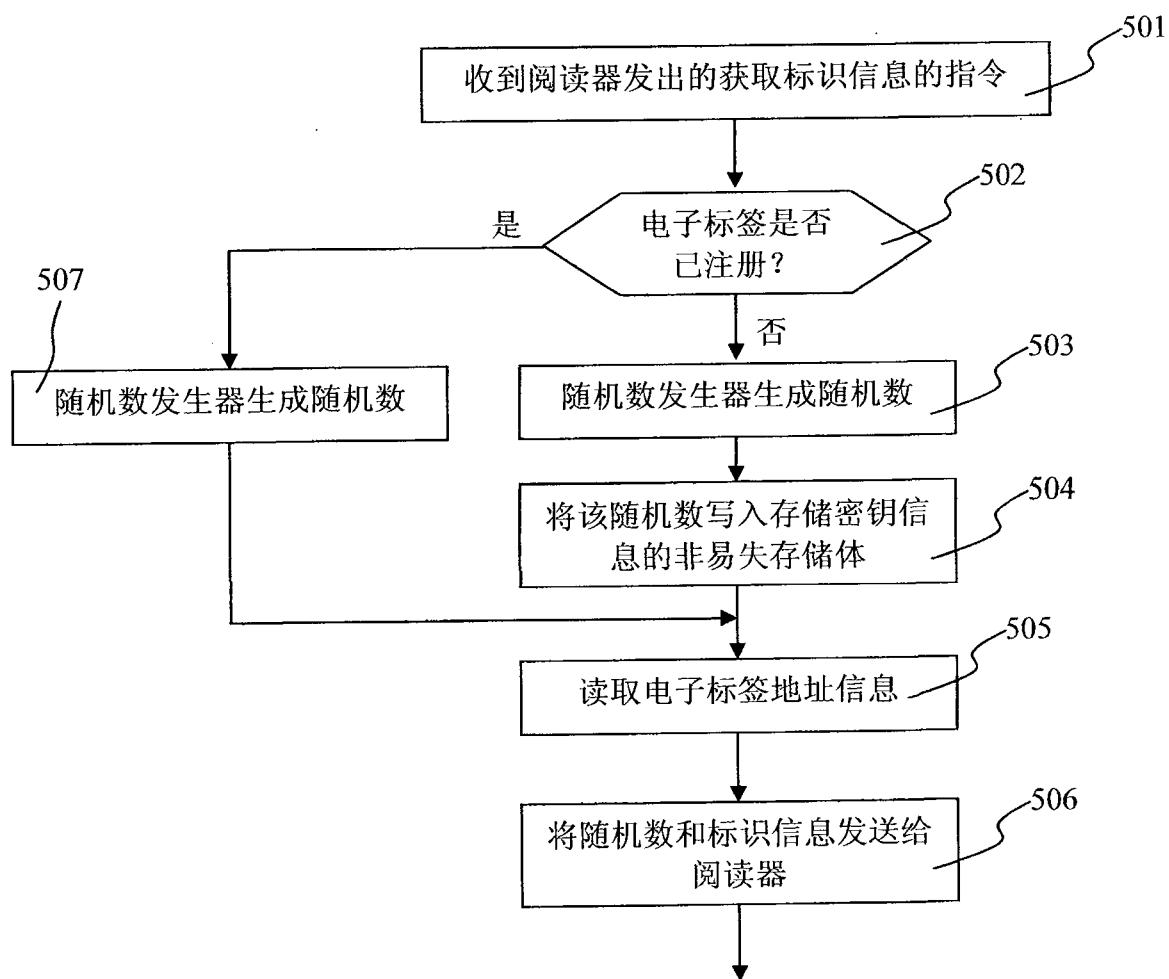


图 5

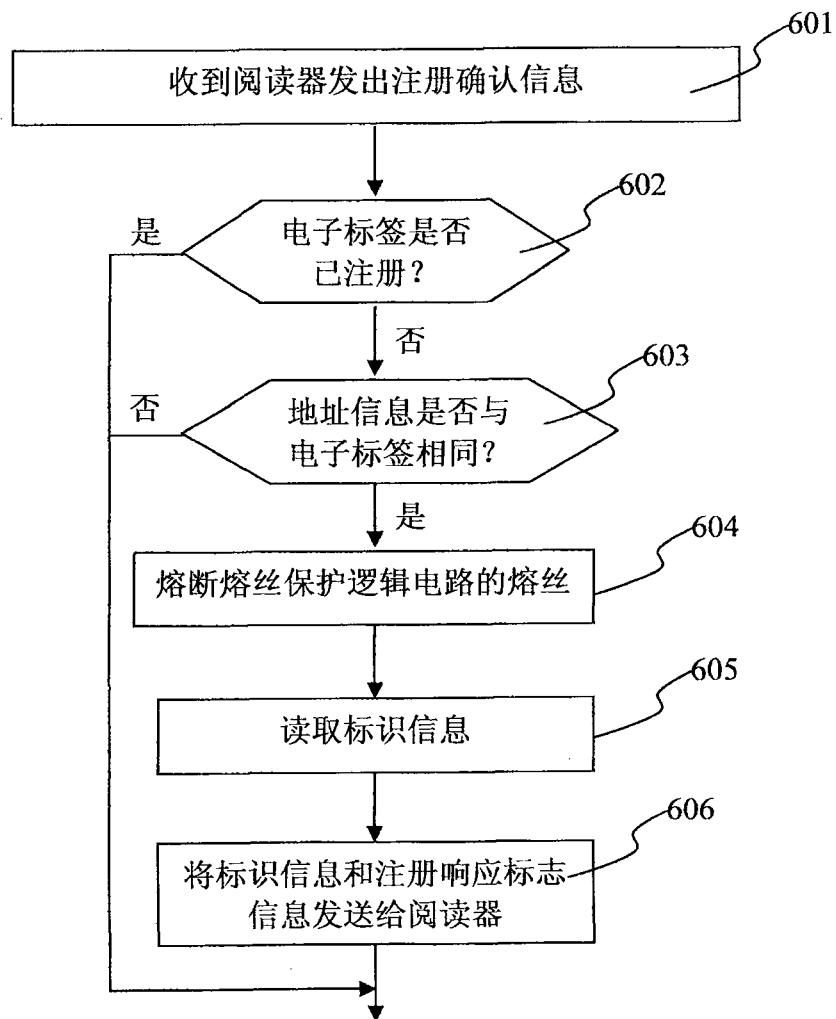


图 6

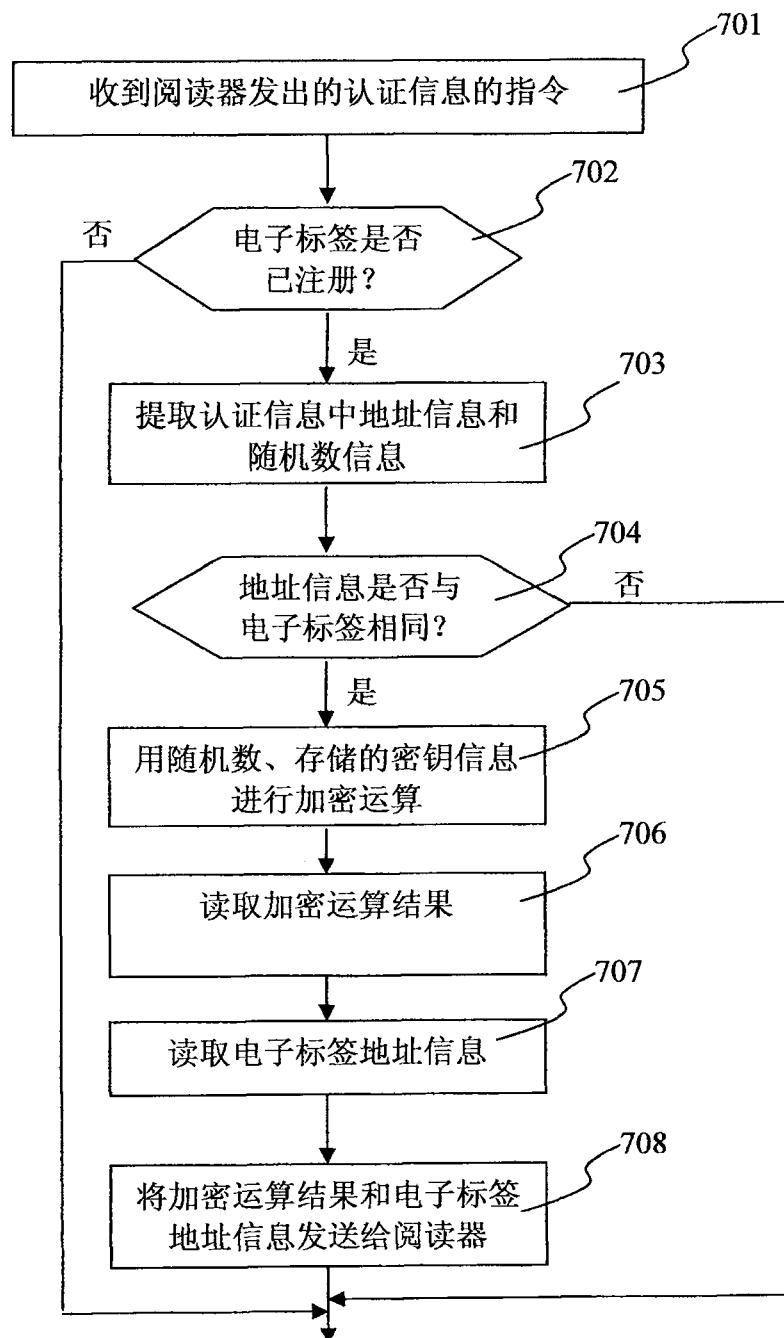


图 7

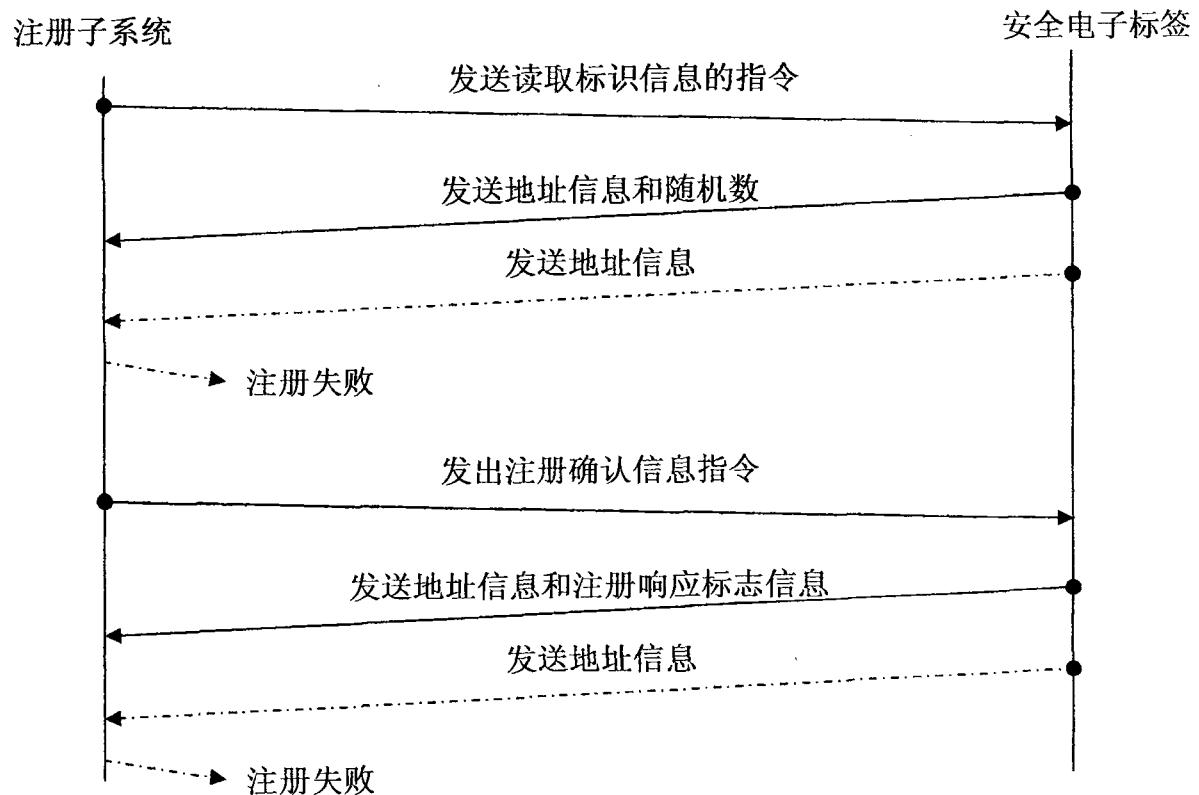


图 8

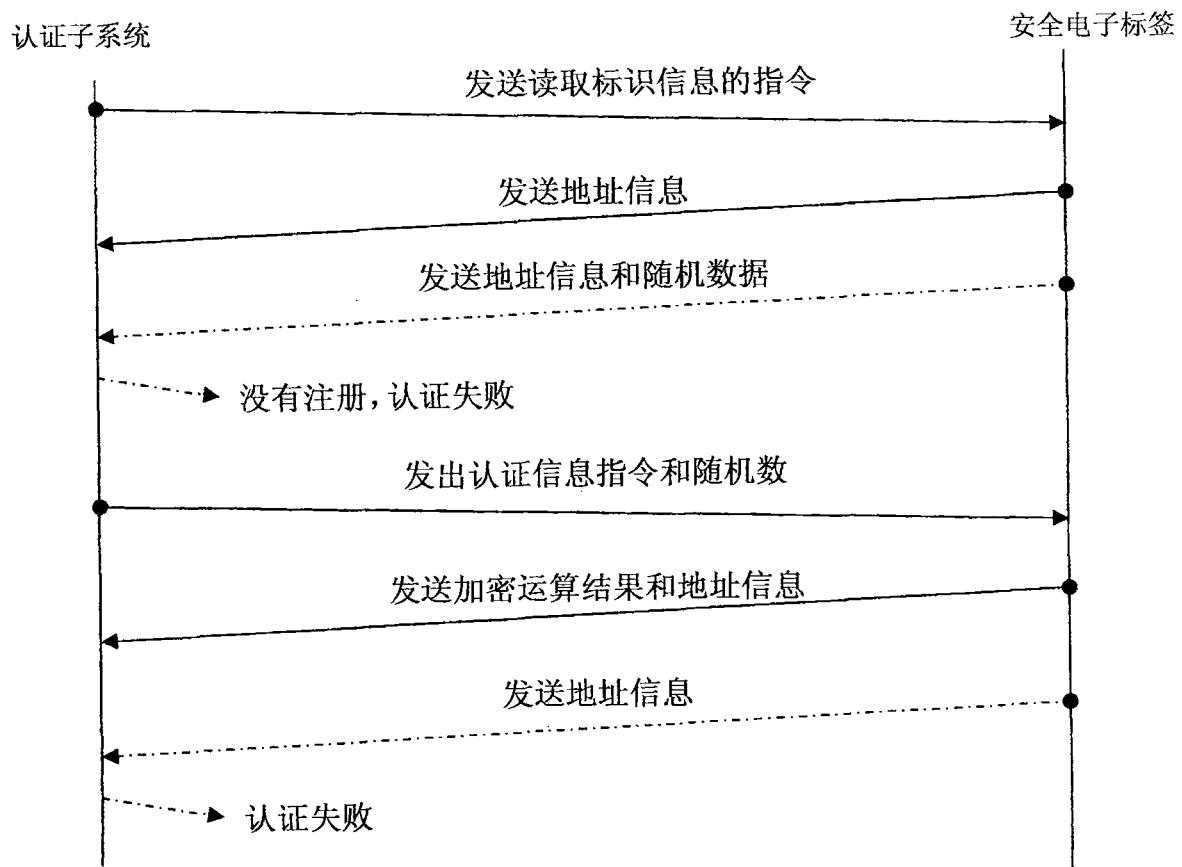


图 9