(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 105608775 B
(45)授权公告日 2018.12.28

(21)申请号 201610055129.1

(22)申请日 2016.01.27

(65)同一申请的已公布的文献号
申请公布号 CN 105608775 A

(43)申请公布日 2016.05.25

(73)专利权人 大唐微电子技术有限公司
地址 100094 北京市海淀区永嘉北路6号
专利权人 大唐半导体设计有限公司

(72)发明人 徐桂 周清 焦华清

(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 李红爽 栗若木

(51)Int.Cl.
G07C 9/00(2006.01)

(56)对比文件
CN 102800141 A,2012.11.28,
CN 104917614 A,2015.09.16,
KR 20150139405 A,2015.12.11,

审查员 蔡伊青

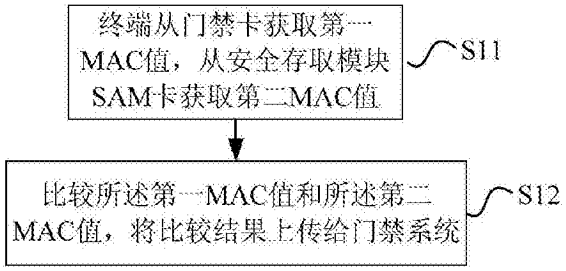
权利要求书3页 说明书8页 附图3页

(54)发明名称

一种鉴权的方法、终端、门禁卡及SAM卡

(57)摘要

一种鉴权的方法、终端、门禁卡及SAM卡，该方法应用于门禁系统，包括：终端从门禁卡获取第一消息鉴别码MAC值，从安全存取模块SAM卡获取第二MAC值；比较所述第一MAC值和所述第二MAC值，将比较结果上传给门禁系统。本技术方案采用当前最先进的CPU卡技术，采用只可硬件实现的国密SM1算法，通过设计一套完善的鉴权流程，解决门禁卡的防篡改和不可复制性；提升门禁卡的安全性。



CN 105608775 B

1.一种鉴权的方法,应用于门禁系统,包括:

终端获取门禁卡生成的第一随机数发送给安全存取模块SAM卡,获取所述SAM卡生成的第二随机数发送给所述门禁卡;

所述终端指示所述门禁卡和所述SAM卡分别根据所述第一随机数产生用于对用户身份信息进行加解密的会话密钥,并指示所述门禁卡和所述SAM卡分别根据所述第二随机数和采用所述会话密钥加密后的门禁卡用户身份信息生成第一消息鉴别码MAC值和第二MAC值;

所述终端从所述门禁卡获取所述第一MAC值,从所述SAM卡获取所述第二MAC值;比较所述第一MAC值和所述第二MAC值,当判断所述第一MAC值和所述第二MAC值一致时,将所述门禁卡用户身份信息上传给门禁系统。

2.如权利要求1所述的方法,其特征在于:所述终端从门禁卡获取第一MAC值之前,还包括:

所述终端指示所述SAM卡根据所述第二随机数生成第三MAC值;

从所述SAM卡获取所述第三MAC值,将所述述第三MAC值发送给所述门禁卡,指示所述门禁卡鉴别所述第三MAC值;所述门禁卡鉴别所述第三MAC值,通过后才生成所述第一MAC值。

3.如权利要求2所述的方法,其特征在于:在所述门禁卡鉴别所述第三MAC值通过后,将所述门禁卡用户身份信息上传给门禁系统前,还包括:

所述终端从所述门禁卡获取采用所述会话密钥加密后的用户身份信息,将所述加密后的用户身份信息发给所述SAM卡,指示所述SAM卡对所述加密后的用户身份信息进行解密;

从所述SAM卡获取采用所述会话密钥解密后的用户身份信息,对所述用户身份信息进行加工处理。

4.一种终端,应用于门禁系统,其特征在于,包括:

获取模块,用于获取门禁卡生成的第一随机数发送给安全存取模块SAM卡,获取所述SAM卡生成的第二随机数发送给所述门禁卡;

处理模块,用于指示所述门禁卡和所述SAM卡分别根据所述第一随机数产生用于对用户身份信息进行加解密的会话密钥,并指示所述门禁卡和所述SAM卡分别根据所述第二随机数和采用所述会话密钥加密后的门禁卡用户身份信息生成第一消息鉴别码MAC值和第二MAC值;从所述门禁卡获取所述第一MAC值,从所述SAM卡获取所述第二MAC值;比较所述第一MAC值和所述第二MAC值,当判断所述第一MAC值和所述第二MAC值一致时,将所述门禁卡用户身份信息上传给门禁系统。

5.如权利要求4所述的终端,其特征在于:

所述处理模块,还用于:在从所述门禁卡获取第一MAC值之前,指示所述SAM卡根据所述第二随机数生成第三MAC值;从所述SAM卡获取所述第三MAC值,将所述述第三MAC值发送给所述门禁卡,指示所述门禁卡鉴别所述第三MAC值;在所述门禁卡鉴别所述第三MAC值,通过后才从所述门禁卡获取所述第一MAC值。

6.如权利要求5所述的终端,其特征在于:

所述获取模块,还用于在所述门禁卡鉴别所述第三MAC值通过后,将所述门禁卡用户身份信息上传给门禁系统前,从所述门禁卡获取采用所述会话密钥加密后的用户身份信息,将所述加密后的用户身份信息发给所述SAM卡,指示所述SAM卡对所述加密后的用户身份信息进行解密;

从所述SAM卡获取采用所述会话密钥解密后的用户身份信息，对所述用户身份信息进行加工处理。

7.一种鉴权的方法，应用于门禁系统，包括，

门禁卡生成第一随机数发送给终端，根据所述第一随机数产生会话密钥对用户身份信息进行加密；

所述门禁卡接收所述终端发送的第二随机数，根据所述第二随机数和加密后的用户身份信息生成第一消息鉴别码MAC值，将所述第一MAC值发送给所述终端；

其中，所述第二随机数是由安全存取模块SAM卡生成并传送给所述终端的。

8.如权利要求7所述的方法，其特征在于：

所述门禁卡根据所述第一随机数产生会话密钥对用户身份信息进行加密之前，还包括：

所述门禁卡接收所述终端发送的第三MAC值；

根据所述第二随机数生成第四MAC值，对所述第三MAC值和所述第四MAC值进行比对，如一致，则鉴别通过，才利用所述会话密钥对用户身份信息进行加密；

其中，所述第三MAC值是所述SAM卡根据所述第二随机数生成并传送给所终端的。

9.一种门禁卡，其特征在于，包括：

生成模块，用于生成第一随机数发送给终端，根据所述第一随机数产生会话密钥；接收所述终端发送的第二随机数，根据所述第二随机数和加密后的用户身份信息生成第一消息鉴别码MAC值

加密模块，用于利用所述会话密钥对用户身份信息进行加密；

发送模块，用于将所述第一MAC值发送给所述终端；

其中，所述第二随机数是由安全存取模块SAM卡生成并传送给所述终端的。

10.如权利要求9所述的门禁卡，其特征在于：还包括鉴权模块，

所述生成模块，还用于接收所述终端发送的第三MAC值，根据所述第二随机数生成第四MAC值；

所述鉴权模块，用于对所述第三MAC值和所述第四MAC值进行比对，如一致，则鉴别通过，才通知所述加密模块利用所述会话密钥对用户身份信息进行加密；

其中，所述第三MAC值是所述SAM卡根据所述第二随机数生成并传送给所终端的。

11.一种鉴权的方法，应用于门禁系统，包括，

安全存取模块SAM卡生成第二随机数发送给终端；

根据所述第二随机数和所述终端发送的加密后的门禁卡用户身份信息生成第二消息鉴别码MAC值；将所述第二MAC值发送给终端；

其中，所述终端发送的加密后的门禁卡用户身份信息是由门禁卡根据所述门禁卡生成的第一随机数产生会话密钥，并对门禁卡用户身份信息进行加密后传送给所述终端的。

12.如权利要求11所述的方法，其特征在于：

所述SAM卡还接收所述终端发送的第一随机数；根据所述第一随机数生成会话密钥，利用所述会话密钥对所述加密后的门禁卡用户身份信息进行解密。

13.如权利要求12所述的方法，其特征在于：所述SAM卡生成所述第二MAC值之前，还包括：

所述SAM卡接收所述终端的指令后，根据所述第二随机数生成第三MAC值；

将所述第三MAC值发送给所述终端；

在所述终端鉴别所述第三MAC值后，将解密后的门禁卡用户身份信息发送给所述终端。

14.一种安全存取模块SAM卡，安装在终端中，应用于门禁系统，包括：

生成模块，用于生成第二随机数发送给终端；根据所述第二随机数和所述终端发送的加密后的门禁卡用户身份信息生成第二消息鉴别码MAC值；

发送模块，用于将所述第二MAC值发送给所述终端；

其中，所述终端发送的加密后的门禁卡用户身份信息是由门禁卡根据所述门禁卡生成的第一随机数产生会话密钥，并对门禁卡用户身份信息进行加密后传送给所述终端的。

15.如权利要求14所述的SAM卡，其特征在于：还包括解密模块，

所述生成模块，还用于接收所述终端发送的第一随机数，根据所述第一随机数生成会话密钥；

所述解密模块，用于根据所述会话密钥对所述加密后的门禁卡用户身份信息进行解密。

16.如权利要求15所述的SAM卡，其特征在于：

所述生成模块，还用于：在生成所述第二MAC值之前，接收所述终端的指令后，根据所述第二随机数生成第三MAC值；

所述发送模块，还用于将所述第三MAC值发送给所述终端；在所述终端鉴别所述第三MAC值后，将解密后的门禁卡用户身份信息发送给所述终端。

一种鉴权的方法、终端、门禁卡及SAM卡

技术领域

[0001] 本发明涉及通信领域，特别是涉及一种鉴权的方法、终端、门禁卡及SAM(Security Access module，安全存取模块)卡。

背景技术

[0002] 目前的门禁卡主要都是采用ID卡(Identification Card，身份识别卡)、M1卡，随着ID卡的可复制性，M1卡算法的被破解，这些门禁卡可以低成本的进行复制、篡改，门禁卡的安全性已经大大降低，

[0003] 智能卡内的集成电路中带有微处理器CPU(Central Processing Unit，中央处理单元)、存储单元(包括RAM(Random-Access Memory，随机存取存储器)、程序存储器ROM(Read-Only Memory，只读存储器)(Flash(闪存))、用户数据存储器EEPROM(Electrically Erasable Programmable Read-Only Memory，电可擦可编程只读存储器)以及芯片操作系统COS(China Operating System，中国自主操作系统)。装有COS的CPU卡相当于一台微型计算机，不仅具有数据存储功能，同时具有命令处理和数据安全保护等功能。

[0004] 智能卡内部具有CPU芯片，在具有数据判断能力的同时，也具备了数据分析处理能力，因此智能卡可以随时区分合法和非法读写设备，并且由于有了CPU芯片，具备数据运算能力，还可以对数据进行加密解密处理，因此具有非常高的安全性。CPU卡是在将EEPROM芯片封装在卡片上的同时，将微处理器芯片(CPU)也封装在里面。这样，EEPROM的数据接口在任何情况下都不会与IC卡的对外数据线相连接。外部读写设备只能通过CPU与IC卡(Integrated Circuit Card，集成电路卡)内的EEP-ROM进行数据交换，在任何情况下都不能再访问到EEP-ROM中的任何一个单元。

[0005] 因为CPU卡的高安全性，越来越多的安全级别高的场景开始采用CPU卡作为门禁卡，这种门禁卡一般采用其他行业标准(如PBOC(People's Bank of China，中国人民银行)，社保卡、公交一卡通等)的应用规范，将其内外部认证流程应用到门禁方案中，通过控制文件的读写权限来实现门禁的控制。这种解决方案不需要定制开发COS，仅需要将现有应用转移到门禁应用领域，卡商、读卡器厂家升级工作少，流程简易明了。采用CPU芯片的门禁卡，安全级别得到了质的提升。

[0006] 目前我国80％左右的门禁卡采用的是ID卡或M1卡的UID(User Identification，用户身份标识)号，这种产品只是读取卡片的一个固定号作为身份识别数据，其中没有对数据进行加工或加密认证等，非常容易被复制。稍先进一些的是采用M1卡的扇区进行数据操作，利用每个扇区独立的密钥进行读写校验，但其个人化包括敏感数据和各扇区密钥的更新，都是直接以明文的形式更新的，存在被窃取的风险，另外M1卡的校验机制只能解决卡片对终端的认证，而无法解决终端对卡片的认证，即存在有“伪卡”的风险。

[0007] 随着CPU卡技术的发展，一些高安全要求的门禁卡已经选择CPU卡，这些CPU卡通过文件读写权限控制，内外部认证等方法可以杜绝被篡改、复制的风险，但仍然还存在漏洞，如通过特殊设备采集交互数据，再定制特殊卡片，响应终端的指令，并返回某些特定数据，

进而达到冒充某些高权限门禁卡的“假卡”。

发明内容

[0008] 本发明要解决的技术问题是提供一种鉴权的方法、终端、门禁卡及SAM卡，以提升门禁卡的安全性。

[0009] 为了解决上述技术问题，本发明实施例提供了一种鉴权的方法，应用于门禁系统，包括：

[0010] 终端从门禁卡获取第一消息鉴别码MAC值，从安全存取模块SAM卡获取第二MAC值；

[0011] 比较所述第一MAC值和所述第二MAC值，将比较结果上传给门禁系统。

[0012] 可选地，上述方法还包括：

[0013] 所述终端从所述门禁卡获取第一随机数，将所述第一随机数传输给所述SAM卡，指示所述SAM卡根据所述第一随机数产生会话密钥。

[0014] 可选地，上述方法还包括：所述终端从门禁卡获取第一MAC值之前，还包括：

[0015] 所述终端指示所述SAM卡根据第二随机数生成第三MAC值；

[0016] 从所述SAM卡获取所述第三MAC值，将所述述第三MAC值发送给所述门禁卡，指示所述门禁卡鉴别所述第三MAC值，接收到所述门禁卡的鉴别通过消息后才从所述门禁卡获取第一MAC值。

[0017] 可选地，上述方法还包括：所述终端从门禁卡获取第一MAC值之前，所述终端从所述SAM卡获取所述第二随机数，将所述第二随机数发送给所述门禁卡，指示所述门禁卡根据所述第二随机数生成MAC值对所述第三MAC值进行鉴别。

[0018] 可选地，上述方法还包括：所述终端接收到所述门禁卡的鉴别通过消息后，

[0019] 所述终端从所述门禁卡获取电子身份标识，将所述电子身份标识发给所述SAM卡，指示所述SAM卡对所述电子身份标识进行解密；

[0020] 接收所述SAM卡解密后的电子身份标识。

[0021] 可选地，上述方法还包括：所述终端从所述门禁卡获取加密的电子身份标识之后：

[0022] 指示所述SAM卡根据所述第二随机数和/或所述电子身份标识生成所述第二MAC值。

[0023] 本发明实施例还提供了一种终端，应用于门禁系统，其中，包括：

[0024] 获取模块，用于从门禁卡获取第一消息鉴别码MAC值，从安全存取模块SAM卡获取第二MAC值；

[0025] 处理模块，用于比较所述第一MAC值和所述第二MAC值，将比较结果上传给门禁系统。

[0026] 可选地，上述终端还包括：所述获取模块，从所述门禁卡获取第一随机数，将所述第一随机数传输给所述SAM卡，指示所述SAM卡根据所述第一随机数产生会话密钥。

[0027] 可选地，上述终端还包括：所述获取模块，从门禁卡获取第一MAC值之前还用于：指示所述SAM卡根据第二随机数生成第三MAC值；从所述SAM卡获取所述第三MAC值，将所述述第三MAC值发送给所述门禁卡，指示所述门禁卡鉴别所述第三MAC值，接收到所述门禁卡的鉴别通过消息后才从所述门禁卡获取第一MAC值。

[0028] 可选地，上述终端还包括：

[0029] 所述获取模块，从门禁卡获取第一MAC值之前还用于，从所述SAM卡获取所述第二随机数，将所述第二随机数发送给所述门禁卡，指示所述门禁卡根据所述第二随机数生成MAC值对所述第三MAC值进行鉴别。

[0030] 可选地，上述终端还包括：

[0031] 所述获取模块，接收到所述门禁卡的鉴别通过消息后还用于，从所述门禁卡获取电子身份标识，将所述电子身份标识发给所述SAM卡，指示所述SAM卡对所述电子身份标识进行解密；接收所述SAM卡解密后的电子身份标识。

[0032] 可选地，上述终端还包括：

[0033] 所述获取模块，从所述门禁卡获取加密的电子身份标识之后还包括：指示所述SAM卡根据所述第二随机数和/或所述电子身份标识生成所述第二MAC值。

[0034] 本发明实施例还提供了一种鉴权的方法，应用于门禁系统，包括，

[0035] 门禁卡生成会话密钥和第一消息鉴别码MAC值；

[0036] 利用所述会话密钥对用户身份信息进行加密，得到电子身份标识；

[0037] 将所述电子身份标识和所述第一MAC值发送给所述终端。

[0038] 可选地，所述方法还包括：

[0039] 所述门禁卡是利用第一随机数生成所述会话密钥的。

[0040] 可选地，所述方法还包括：所述门禁卡生成第一消息鉴别码MAC值之前：

[0041] 所述门禁卡接收所述终端发送的第二随机数和第三MAC值；

[0042] 根据所述第二随机数生成第四MAC值，对所述第三MAC值和所述第四MAC值进行比对，如一致，则鉴别通过，才利用所述会话密钥对用户身份信息进行加密，才生成所述第一MAC值。

[0043] 可选地，所述方法还包括：所述门禁卡是根据所述第二随机数和/或所述电子身份标识生成所述第一MAC值的。

[0044] 本发明实施例还提供一种门禁卡，其中，包括：

[0045] 生成模块，用于生成会话密钥和第一消息鉴别码MAC值；

[0046] 加密模块，用于利用所述会话密钥对用户身份信息进行加密，得到电子身份标识；

[0047] 发送模块，用于将所述电子身份标识和所述第一MAC值发送给所述终端。

[0048] 可选地，上述门禁卡还包括：

[0049] 所述生成模块，是利用第一随机数生成所述会话密钥的。

[0050] 可选地，上述门禁卡还包括：还包括鉴权模块，

[0051] 所述生成模块，生成第一消息鉴别码MAC值之前还用于：接收所述终端发送的第二随机数和第三MAC值，根据所述第二随机数生成第四MAC值；

[0052] 所述鉴权模块，用于对所述第三MAC值和所述第四MAC值进行比对，如一致，则鉴别通过，才通知所述加密模块利用所述会话密钥对用户身份信息进行加密，才通知所述生成模块生成所述第一MAC值。

[0053] 可选地，上述门禁卡还包括：

[0054] 所述生成模块，是根据所述第二随机数和/或所述电子身份标识生成所述第一MAC值的。

[0055] 本发明实施例还提供一种鉴权的方法，应用于门禁系统，包括，

[0056] 安全存取模块SAM卡生成会话密钥和第二MAC值；

[0057] 通过所述会话密钥对接收到的电子身份标识进行解密；

[0058] 将解密后的电子身份标识和所述第二MAC值发送给终端。

[0059] 可选地，上述方法还包括，所述SAM卡生成所述第二MAC值之前：

[0060] 所述SAM卡接收所述终端的指令后，根据第二随机数生成第三MAC值；

[0061] 将所述第二随机数和所述第三MAC值发送给所述终端。

[0062] 可选地，上述方法还包括，所述SAM卡是根据所述第二随机数和/或所述电子身份标识生成所述第二MAC值的。

[0063] 本发明实施例还提供一种安全存取模块SAM卡，安装在终端中，应用于门禁系统，包括：

[0064] 生成模块，用于生成会话密钥和第二MAC值；

[0065] 解密模块，用于通过所述会话密钥对接收到的电子身份标识进行解密；

[0066] 发送模块，用于将解密后的电子身份标识和所述第二MAC值发送给所述终端。

[0067] 可选地，上述SAM卡还包括：

[0068] 所述生成模块，还用于接收所述终端发送的第一随机数，是根据所述第一随机数生成所述会话密钥的。

[0069] 可选地，上述SAM卡还包括：

[0070] 所述生成模块，生成所述第二MAC值之前还用于：接收所述终端的指令后，根据第二随机数生成第三MAC值；

[0071] 所述发送模块，还用于将所述第二随机数和所述第三MAC值发送给所述终端。

[0072] 可选地，上述SAM卡还包括：

[0073] 所述生成模块，是根据所述第二随机数和/或所述电子身份标识生成所述第二MAC值的。

[0074] 综上，本发明提供一种鉴权的方法、终端、门禁卡及SAM卡，采用当前最先进的CPU卡技术，采用只可硬件实现的国密SM1算法，通过设计一套完善的鉴权流程，可以解决以下几个问题：解决门禁卡的防篡改和不可复制性；采用芯片硬实现的国密SM1算法，提升门禁卡的安全性；在充分发挥CPU卡的功能前提下，通过“一卡一密，一次一密”的特点，进一步提升门禁卡的安全性。

附图说明

[0075] 图1为本发明实施例的终端侧进行鉴权的方法的流程图。

[0076] 图2为本发明实施例的门禁卡侧进行鉴权的方法的流程图。

[0077] 图3为本发明实施例的SAM卡侧进行鉴权的方法的流程图。

[0078] 图4为本发明应用示例的鉴权的方法的流程图。

[0079] 图5为本发明实施例的终端的示意图。

[0080] 图6为本发明实施例的门禁卡的示意图。

[0081] 图7为本发明实施例的SAM卡的示意图。

具体实施方式

[0082] 为使本发明的目的、技术方案和优点更加清楚明白，下文中将结合附图对本发明的实施例进行详细说明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

[0083] 本发明实施例提出一种采用国密算法的CPU卡技术应用到门禁系统中进行鉴权的方法，本方案自主开发双向鉴权流程，每次鉴权都通过随机数产生会话密钥，再使用该会话密钥进行鉴权和数据加解密，在充分发挥CPU卡的功能前提下，通过“一卡一密，一次一密”的特点，进一步提升门禁卡的安全性。

[0084] 图1为本发明实施例的终端侧进行鉴权的方法的流程图，如图1所示，本实施例的方法包括：

[0085] S11、终端从门禁卡获取第一消息鉴别码(Message Authentication Code，简称MAC)值，从安全存取模块SAM卡获取第二MAC值；

[0086] S12、比较所述第一MAC值和所述第二MAC值，将比较结果上传给门禁系统。

[0087] 本实施例中，所述终端从所述门禁卡获取第一随机数，将所述第一随机数传输给所述SAM卡，指示所述SAM卡根据所述第一随机数产生会话密钥。这样可以保证每次的会话密钥都不一样。

[0088] 在一优选实施例中，所述终端指示所述SAM卡根据第二随机数生成第三MAC值；

[0089] 所述终端从所述SAM卡获取所述第三MAC值，将所述述第三MAC值发送给所述门禁卡，指示所述门禁卡鉴别所述第三MAC值。

[0090] 所述终端从所述SAM卡获取所述第二随机数，将所述第二随机数发送给所述门禁卡，指示所述门禁卡根据所述第二随机数生成MAC值对所述第三MAC值进行鉴别。

[0091] 所述终端是接收到所述门禁卡的鉴别通过消息后，才从所述门禁卡获取第一MAC值的。

[0092] 图2为本发明实施例的门禁卡侧进行鉴权的方法的流程图，如图2所示，本实施例的方法包括：

[0093] S21、门禁卡生成会话密钥和第一MAC值；

[0094] S22、利用所述会话密钥对用户身份信息进行加密，得到电子身份标识；

[0095] S23、将所述电子身份标识和所述第一MAC值发送给所述终端。

[0096] 本实施例中，所述门禁卡是利用第一随机数生成所述会话密钥的。

[0097] 在一优选实施例中，所述门禁卡生成第一消息鉴别码MAC值之前，还接收所述终端发送的第二随机数和第三MAC值；

[0098] 根据所述第二随机数生成第四MAC值，对所述第三MAC值和所述第四MAC值进行比对，如一致，则鉴别通过，才将所述第一MAC值发送给所述终端。

[0099] 图3为本发明实施例的SAM卡侧进行鉴权的方法的流程图，如图3所示，本实施例的方法包括：

[0100] S31、SAM卡生成会话密钥和第二MAC值；

[0101] S32、通过所述会话密钥对接收到的电子身份标识进行解密；

[0102] S33、将解密后的电子身份标识和所述第二MAC值发送给终端。

[0103] 本实施例中，所述SAM卡生成会话密钥之前，还包括：

[0104] 所述SAM卡接收所述终端发送的第一随机数；

[0105] 所述SAM卡是根据所述第一随机数生成所述会话密钥的。

[0106] 本发明实施例的鉴权方法充分利用卡内密钥体系，通过进行互认证，建立每次会话密钥，确保流程的不可重复性。同时为提升门禁系统的刷卡速度，尽量精简指令，具体应用流程如图4所示，包括以下步骤：

[0107] 步骤101、终端从门禁卡获取随机数R1，将R1传输给SAM卡；

[0108] 步骤102、终端从SAM卡获取随机数R2，将R2传输给门禁卡；

[0109] 步骤103、终端向SAM卡发送产生会话密钥的指令，分散因子是R1。

[0110] 步骤104，SAM卡接收到终端的产生会话密钥的指令后，根据分散因子R1产生会话密钥，这样确保每次鉴权流程的密钥都不一样，即一次一密。

[0111] 步骤105、终端向SAM卡发送指令，要求SAM卡对读文件命令及数据域R2计算MAC1值，初始值为全0；

[0112] 步骤106、SAM卡根据R2计算MAC1值(相当于上文的第三MAC值)。

[0113] 步骤107、终端读取用户身份信息，同时传入R2和MAC1值；将R2和MAC1值发送给门禁卡；

[0114] 步骤108、门禁卡利用R1产生会话密钥，对读文件命令及数据域R2计算MAC1’(相当于上文的第四MAC值)，比对与MAC1是否相等，如相等，则读取用户身份信息，用会话密钥对用户身份信息进行加密得到EID(Electronic Identity，电子身份标识)，根据读文件命令、EID和数据域R2计算MAC2；然后将EID和MAC2发送给终端；如不相等，则鉴权识别，门禁权限不能使用。

[0115] 步骤109、终端获得EID和MAC2后，向SAM卡发送指令，要求SAM卡计算MAC2’值，R2作为MAC2计算初始值。

[0116] 步骤110、SAM卡接收到指令后，根据R2和/或EID计算MAC2’值(相当于上文的第二MAC值)，并用会话密钥解密EID数据，获得用户身份信息，将MAC2’值和用户身份信息发送给终端。

[0117] 步骤111、终端比较SAM卡计算的MAC2’值与门禁卡返回的MAC2是否一致，如正确一致，则处理用户身份信息；如不一致，则鉴权失败，不能获得门禁权限，结束流程。

[0118] 步骤112、终端对用户身份信息进行加工处理，并将处理后数据传递给门禁系统，进行后续门禁控制操作，结束流程。

[0119] 本发明实施例中涉及到的计算MAC值、加解密算法，均可以采用国密算法SM1。

[0120] 本实施例的方法，将SM1算法引入到门禁应用领域，提升门禁应用的安全性；

[0121] 本实施例的方法可以实现一卡一密，一次一密，可以有效防止任何窃取、篡改、复制等行为。

[0122] 本实施例的方法引入高安全的智能卡芯片和COS，并针对门禁系统的特点，重点保护门禁卡内关键数据的安全性。现在智能卡芯片的成本逐年下降，本发明实施例提供的方案不会给客户带来更高的成本代价。

[0123] 图5为本发明实施例的终端的示意图，如图5所示，本实施例的终端包括：

[0124] 获取模块，用于从门禁卡获取第一消息鉴别码MAC值，从安全存取模块SAM卡获取第二MAC值；

[0125] 处理模块，用于比较所述第一MAC值和所述第二MAC值，将比较结果上传给门禁系

统。

[0126] 在一优选实施例中，所述获取模块，从所述门禁卡获取第一随机数，将所述第一随机数传输给所述SAM卡，指示所述SAM卡根据所述第一随机数产生会话密钥。

[0127] 在一优选实施例中，所述获取模块，从门禁卡获取第一MAC值之前还可以用于：指示所述SAM卡根据第二随机数生成第三MAC值；从所述SAM卡获取所述第三MAC值，将所述述第三MAC值发送给所述门禁卡，指示所述门禁卡鉴别所述第三MAC值，接收到所述门禁卡的鉴别通过消息后才从所述门禁卡获取第一MAC值。

[0128] 在一优选实施例中，所述获取模块，从门禁卡获取第一MAC值之前还可以用于，从所述SAM卡获取所述第二随机数，将所述第二随机数发送给所述门禁卡，指示所述门禁卡根据所述第二随机数生成MAC值对所述第三MAC值进行鉴别。

[0129] 在一优选实施例中，所述获取模块，接收到所述门禁卡的鉴别通过消息后还可以用于，从所述门禁卡获取电子身份标识，将所述电子身份标识发给所述SAM卡，指示所述SAM卡对所述电子身份标识进行解密；接收所述SAM卡解密后的电子身份标识(即用户身份信息)。

[0130] 在一优选实施例中，所述获取模块，从所述门禁卡获取加密的电子身份标识之后还包括：指示所述SAM卡根据所述第二随机数和/或所述电子身份标识生成所述第二MAC值。

[0131] 图6为本发明实施例的门禁卡的示意图，如图6所示，本实施例的门禁卡包括：

[0132] 生成模块，用于生成会话密钥和第一消息鉴别码MAC值；

[0133] 加密模块，用于利用所述会话密钥对用户身份信息进行加密，得到电子身份标识；

[0134] 发送模块，用于将所述电子身份标识和所述第一MAC值发送给所述终端。

[0135] 在一优选实施例中，所述生成模块，是利用第一随机数生成所述会话密钥的。

[0136] 在一优选实施例中，所述门禁卡还包括鉴权模块，

[0137] 所述生成模块，生成第一消息鉴别码MAC值之前还用于：接收所述终端发送的第二随机数和第三MAC值，根据所述第二随机数生成第四MAC值；

[0138] 所述鉴权模块，用于对所述第三MAC值和所述第四MAC值进行比对，如一致，则鉴别通过，才通知所述加密模块利用所述会话密钥对用户身份信息进行加密，才通知所述生成模块生成所述第一MAC值。

[0139] 在一优选实施例中，所述生成模块，是根据所述第二随机数和/或所述电子身份标识生成所述第一MAC值的。

[0140] 图7为本发明实施例的SAM卡的示意图，本实施例的SAM卡安装在终端中，如图7所示，本实施例的SAM卡包括：

[0141] 生成模块，用于生成会话密钥和第二MAC值；

[0142] 解密模块，用于通过所述会话密钥对接收到的电子身份标识进行解密；

[0143] 发送模块，用于将解密后的电子身份标识和所述第二MAC值发送给所述终端。

[0144] 在一优选实施例中，所述生成模块，还用于接收所述终端发送的第一随机数，是根据所述第一随机数生成所述会话密钥的。

[0145] 在一优选实施例中，所述生成模块，生成所述第二MAC值之前还用于：接收所述终端的指令后，根据第二随机数生成第三MAC值；

[0146] 所述发送模块，还用于将所述第二随机数和所述第三MAC值发送给所述终端。

[0147] 在一优选实施例中，所述生成模块，是根据所述第二随机数和/或所述电子身份标识生成所述第二MAC值的。

[0148] 本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序来指令相关硬件完成，所述程序可以存储于计算机可读存储介质中，如只读存储器、磁盘或光盘等。可选地，上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现。相应地，上述实施例中的各模块/单元可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。本发明不限制于任何特定形式的硬件和软件的结合。

[0149] 以上仅为本发明的优选实施例，当然，本发明还可有其他多种实施例，在不背离本发明精神及其实质的情况下，熟悉本领域的技术人员当可根据本发明作出各种相应的改变和变形，但这些相应的改变和变形都应属于本发明所附的权利要求的保护范围。

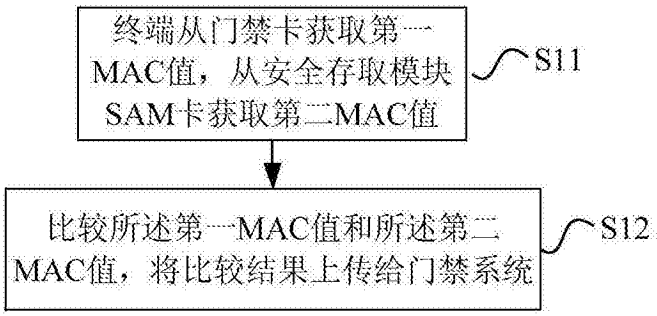

终端从门禁卡获取第一MAC值，从安全存取模块SAM卡获取第二MAC值
S11
比较所述第一MAC值和所述第二MAC值，将比较结果上传给门禁系统
S12

图1

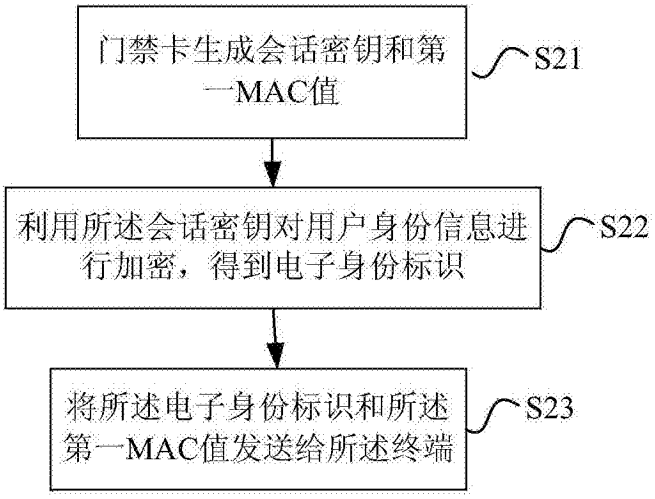

门禁卡生成会话密钥和第一MAC值
S21
利用所述会话密钥对用户身份信息进行加密，得到电子身份标识
S22
将所述电子身份标识和所述第一MAC值发送给所述终端
S23

图2

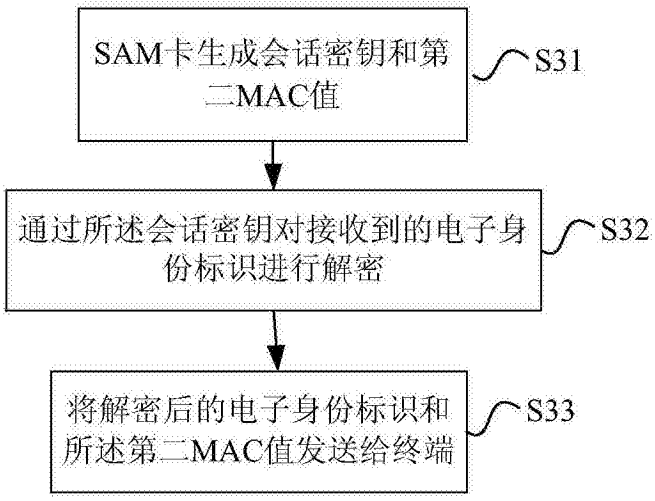

SAM卡生成会话密钥和第二MAC值
S31
通过所述会话密钥对接收到的电子身份标识进行解密
S32
将解密后的电子身份标识和所述第二MAC值发送给终端
S33

图3

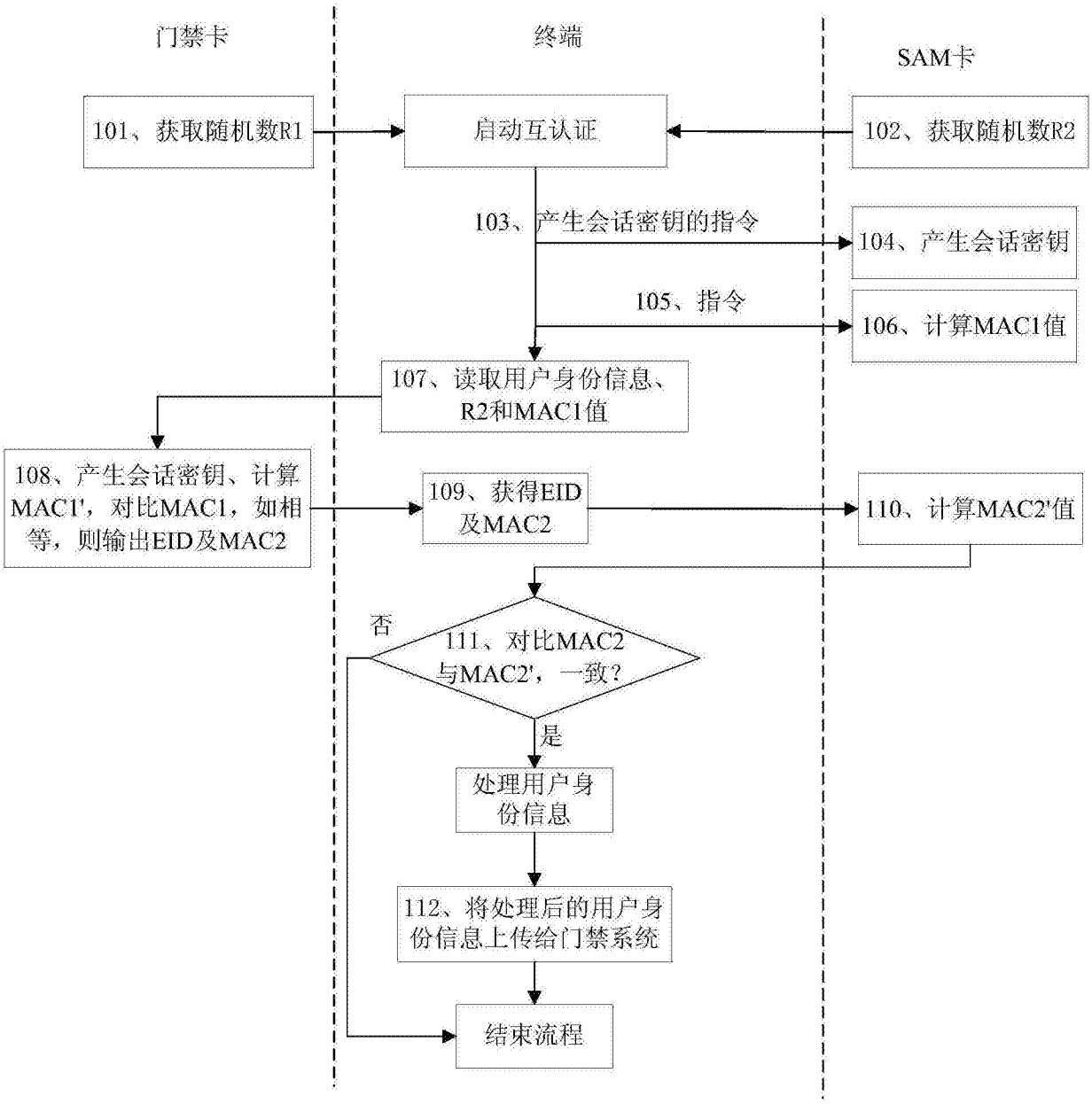

门禁卡
终端
SAM卡
101、获取随机数R1
启动互认证
102、获取随机数R2
103、产生会话密钥的指令
104、产生会话密钥
105、指令
106、计算MAC1值
107、读取用户身份信息、R2和MAC1值
108、产生会话密钥、计算MAC1'，对比MAC1，如相等，则输出EID及MAC2
109、获得EID及MAC2
110、计算MAC2'值
否
111、对比MAC2与MAC2'，一致？
是
处理用户身份信息
112、将处理后的用户身份信息上传给门禁系统
结束流程

图4

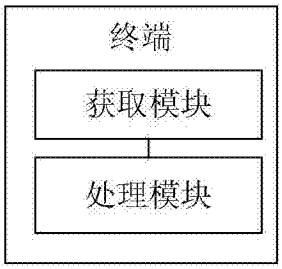

终端
获取模块
处理模块

图5

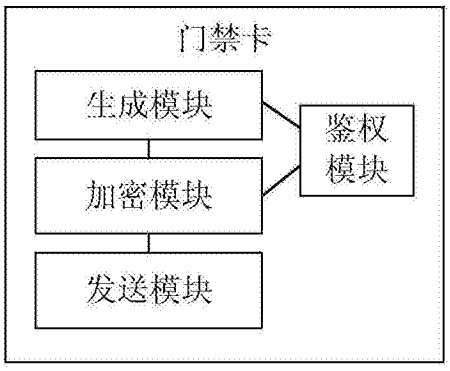


图6

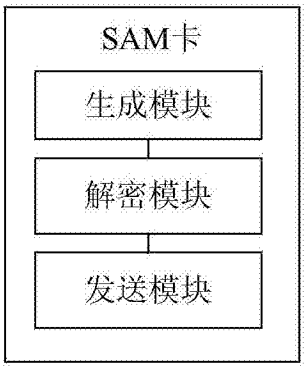


图7