(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 104637117 B
(45)授权公告日 2017.06.30

(21)申请号 201310548132.3

(22)申请日 2013.11.07

(65)同一申请的已公布的文献号
申请公布号 CN 104637117 A

(43)申请公布日 2015.05.20

(73)专利权人 国家电网公司
地址 100031 北京市西城区西长安街86号
专利权人 北京南瑞智芯微电子科技有限公司

(72)发明人 赵羡龙 王维彬 杨立新

(74)专利代理机构 北京中誉威圣知识产权代理有限公司 11279
代理人 郭振兴 丛芳

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

(56)对比文件
US 5055701 A,1991.10.08,全文.
JP 特开平9-268820 A,1997.10.14,全文.

审查员 郭毓敏

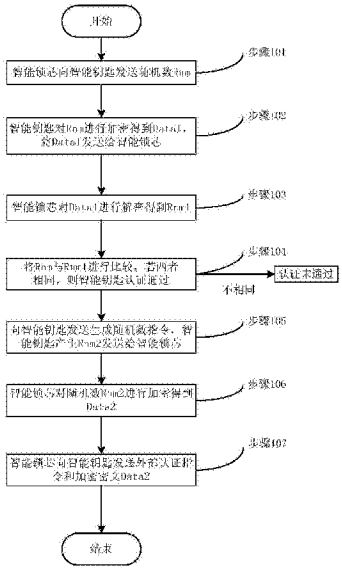
权利要求书1页 说明书5页 附图4页

(54)发明名称

智能锁芯和钥匙实现的方法、智能锁芯、锁具和钥匙

(57)摘要

本发明公开了一种智能锁芯和智能钥匙实现的方法、智能锁芯、锁具和钥匙，其中，该方法包括：智能锁芯向智能钥匙发送随机数Rnm，接收智能钥匙对随机数Rnm加密后得到的密文Data1；对密文Data1进行解密得到Rnm1；将随机数Rnm与Rnm1进行比较，若两者相同，则智能钥匙认证通过。本发明实施例的智能锁芯实现的方法、智能锁芯和锁具，通过ESAM对锁芯与钥匙进行身份认证、数据加/解密、安全存储、通讯保密等可以发挥锁具独到的安全控制作用和管理作用。新型的智能锁芯不仅具有MCU，还增加了专门的ESAM(嵌入式安全认证模块)安全芯片，使锁具的安全性得到提升。



CN 104637117 B

1.一种智能锁芯实现的方法,其特征在于,包括:

向智能钥匙发送随机数Rnm,接收所述智能钥匙对所述随机数Rnm加密后得到的密文Data1;

对所述密文Data1进行解密得到Rnm1;

将所述随机数Rnm与所述Rnm1进行比较,若两者相同,则所述智能钥匙认证通过;

向所述智能钥匙发送生成随机数指令,接收所述智能钥匙产生的随机数Rnm2;

对所述随机数Rnm2进行加密得到加密密文Data2,向所述智能钥匙发送所述加密密文Data2。

2.一种智能锁芯,其特征在于,包括:

随机数发送模块,用于向智能钥匙发送随机数Rnm,接收所述智能钥匙对所述随机数Rnm加密后的密文Data1;

随机数解密模块,用于对所述密文Data1进行解密得到Rnm1;

随机数比较模块,用于将所述随机数Rnm与所述Rnm1进行比较,若两者相同,则所述智能钥匙认证通过;

随机数接收模块,用于向所述智能钥匙发送生成随机数指令,接收所述智能钥匙产生的随机数Rnm2;

随机数加密发送模块,用于对所述随机数Rnm2进行加密得到加密密文Data2,向所述智能钥匙发送所述加密密文Data2。

3.一种智能锁具,其特征在于,包括权利要求2所述的智能锁芯。

4.一种智能钥匙实现的方法,其特征在于,包括:

自智能锁芯接收生成随机数指令,生成随机数Rnm2,将所述Rnm2发送给所述智能锁芯;自所述智能锁芯接收所述智能锁芯对所述Rnm2加密得到的密文Data2,对所述密文Data2进行解密得到明文Rnm3;

将所述随机数Rnm2和所述明文Rnm3进行比较,如果两者相同,则所述智能锁芯认证通过;

自所述智能锁芯接收随机数Rnm;

对所述随机数Rnm进行加密得到加密密文Data1,将所述Data1发送回所述智能锁芯进行认证。

5.一种智能钥匙,其特征在于,包括:

随机数生成发送模块,用于自智能锁芯接收生成随机数指令,生成随机数Rnm2,将所述随机数Rnm2发送给所述智能锁芯;

随机数接收解密模块,用于自所述智能锁芯接收所述智能锁芯对所述Rnm2加密得到的密文Data2,对所述密文Data2进行解密得到明文Rnm3;

随机数比较模块,用于将所述随机数Rnm2和所述Rnm3进行比较,如果两者相同,则所述智能锁芯认证通过;

随机数接收模块,用于自所述智能锁芯接收随机数Rnm;

随机数加密发送模块,用于对所述随机数Rnm进行加密得到加密密文Data1,将所述Data1发送回所述智能锁芯进行认证。

智能锁芯和钥匙实现的方法、智能锁芯、锁具和钥匙

技术领域

[0001] 本发明涉及锁具技术领域，具体地，涉及智能锁芯、锁具及智能钥匙的领域。

背景技术

[0002] 智能锁是近年来出现的新型智能化锁具，它与传统的机械锁有很大不同，在用户识别、安全性、管理性等方面都具有智能化特征。这些智能化特征依赖于智能锁的关键部件－智能锁芯。相对于传统的机械锁的锁芯，智能锁芯增加了微控制单元(MCU)等能够实现自动化、智能运算的部件从而实现了锁具的智能化。目前市面上普通的智能锁锁芯只具有简单的逻辑、存储及密钥电路，无法实现锁功能的扩展，并且由于电路简单，通常锁的密钥易于破解，容易出现安全性差的问题。

发明内容

[0003] 本发明是为了克服现有技术中智能锁安全性差的缺陷，根据本发明的一个方面，提出一种智能锁芯实现的方法。

[0004] 根据本发明实施例的智能锁芯实现的方法，包括：

[0005] 向智能钥匙发送随机数Rnm，接收智能钥匙对随机数Rnm加密后得到的密文Data1；

[0006] 对密文Data1进行解密得到Rnm1；

[0007] 将随机数Rnm与Rnm1进行比较，若两者相同，则智能钥匙认证通过。

[0008] 本发明是为了克服现有技术中智能锁安全性差的缺陷，根据本发明的另一个方面，提出一种智能锁芯。

[0009] 根据本发明实施例的智能锁芯，包括：

[0010] 随机数发送模块，用于向智能钥匙发送随机数Rnm，接收智能钥匙对随机数Rnm加密后的密文Data1；

[0011] 随机数解密模块，用于对密文Data1进行解密得到Rnm1；

[0012] 随机数比较模块，用于将随机数Rnm与Rnm1进行比较，若两者相同，则智能钥匙认证通过。

[0013] 本发明是为了克服现有技术中智能锁安全性差的缺陷，根据本发明的另一个方面，提出一种智能锁具。

[0014] 根据本发明实施例的智能锁具，包括：上述智能锁芯。

[0015] 本发明实施例的智能锁芯实现的方法、智能锁芯和锁具，通过ESAM对锁芯与钥匙进行身份认证、数据加/解密、安全存储、通讯保密等可以发挥锁具独到的安全控制作用和管理作用。新型的智能锁芯不仅具有MCU，还增加了专门的ESAM(嵌入式安全认证模块)安全芯片，使锁具的安全性得到提升。

[0016] 由于采用ESAM模块构建智能锁芯及锁具，使安全性大大提升，更易于管理，且使用简单。只有管理部门才能使用主密钥修改钥匙将ESAM模块中密钥修改为运行主密钥，密钥泄露的可能性很小。使用时，工作人员只需将用户钥匙插入锁中，由用户钥匙与锁中的ESAM

模块自动完成密钥的安全认证和数据存取工作。由于锁内部的安全认证过程完全是在钥匙内完成的，外人很难攻击，安全级别高，且核心主密钥严密控制，保证了锁系统的安全性运营。

[0017] 通过由ESAM模块构建的智能锁芯，智能锁具及与之匹配的智能钥匙，可以实现智能锁生产过程的安全性、运行管理的安全性。从而为锁具在安全性和可操作性方面得到保证，并可应用到各类安全等级高的防护设备上，从而增加了防护设备的安全管理等级。

[0018] 本发明是为了克服现有技术中智能锁安全性差的缺陷，根据本发明的另一个方面，提出一种智能钥匙实现的方法。

[0019] 根据本发明实施例的智能钥匙实现的方法，包括：

[0020] 自智能锁芯接收生成随机数指令，生成随机数Rnm2，将Rnm2发送给智能锁芯；自智能锁芯接收智能锁芯对Rnm2加密得到的密文Data2，对密文Data2进行解密得到明文Rnm3；

[0021] 将随机数Rnm2和明文Rnm3进行比较，如果两者相同，则智能锁芯认证通过。

[0022] 本发明是为了克服现有技术中智能锁安全性差的缺陷，根据本发明的另一个方面，提出一种智能钥匙。

[0023] 根据本发明实施例的智能钥匙，包括：

[0024] 随机数生成发送模块，用于自智能锁芯接收生成随机数指令，生成随机数Rnm2，将随机数Rnm2发送给智能锁芯；

[0025] 随机数接收解密模块，用于自智能锁芯接收智能锁芯对Rnm2加密得到的密文Data2，对密文Data2进行解密得到明文Rnm3；

[0026] 随机数比较模块，用于将随机数Rnm2和Rnm3进行比较，如果两者相同，则智能锁芯认证通过。

[0027] 本发明实施例的智能钥匙实现的方法和智能钥匙，通过ESAM对锁芯与钥匙进行身份认证、数据加/解密、安全存储、通讯保密等可以发挥锁具独到的安全控制作用和管理作用。新型的智能锁芯不仅具有MCU，还增加了专门的ESAM(嵌入式安全认证模块)安全芯片，使锁具的安全性得到提升。

[0028] 由于采用ESAM模块构建智能锁芯及锁具，使安全性大大提升，更易于管理，且使用简单。只有管理部门才能使用主密钥修改钥匙将ESAM模块中密钥修改为运行主密钥，密钥泄露的可能性很小。使用时，工作人员只需将用户钥匙插入锁中，由用户钥匙与锁中的ESAM模块自动完成密钥的安全认证和数据存取工作。由于锁内部的安全认证过程完全是在钥匙内完成的，外人很难攻击，安全级别高，且核心主密钥严密控制，保证了锁系统的安全性运营。

[0029] 通过由ESAM模块构建的智能锁芯，智能锁具及与之匹配的智能钥匙，可以实现智能锁生产过程的安全性、运行管理的安全性。从而为锁具在安全性和可操作性方面得到保证，并可应用到各类安全等级高的防护设备上，从而增加了防护设备的安全管理等级。

[0030] 本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

[0031] 下面通过附图和实施例，对本发明的技术方案做进一步的详细描述。

附图说明

[0032] 附图用来提供对本发明的进一步理解，并且构成说明书的一部分，与本发明的实施例一起用于解释本发明，并不构成对本发明的限制。在附图中：

[0033] 图1为本发明实施例的智能锁芯对智能钥匙认证的流程示意图；

[0034] 图2为本发明实施例智能锁芯的结构示意图；

[0035] 图3为本发明实施例的智能钥匙对智能锁芯认证的流程示意图；

[0036] 图4为本发明实施例智能钥匙的结构示意图。

具体实施方式

[0037] 下面结合附图，对本发明的具体实施方式进行详细描述，但应当理解本发明的保护范围并不受具体实施方式的限制。

[0038] 本发明是针对现有技术中存在的智能锁芯与智能钥匙之间无有效身份认证的问题，而提出的一种智能锁芯和智能钥匙之间进行有效身份认证的方法。

[0039] 根据本发明实施例，如图1所示，提供了一种智能锁芯对智能钥匙进行鉴权认证的方法，具体实施步骤如下：

[0040] 步骤101：智能锁芯向智能钥匙发送随机数Rnm和内部认证指令；

[0041] 步骤102：智能钥匙基于主密钥Mkey对随机数Rnm进行加密得到加密密文Data1，将加密密文Data1发送给智能锁芯；

[0042] 步骤103：智能锁芯基于主密钥Mkey对加密密文Data1进行解密，得到解密后的数据Rnm1；

[0043] 步骤104：将随机数Rnm与Rnm1进行比较，如果两者相同，则智能锁芯判断智能钥匙为真，智能锁芯与智能钥匙之间的内部认证通过；如果两者不同，则智能锁芯与智能钥匙之间的内部认证未通过；

[0044] 步骤105：智能锁芯向智能钥匙发送生成随机数指令，智能钥匙产生随机数Rnm2发送给智能锁芯；

[0045] 步骤106：智能锁芯基于主密钥Mkey对随机数Rnm2进行加密得到加密密文Data2；

[0046] 步骤107：智能锁芯向智能钥匙发送外部认证指令和加密密文Data2，该加密密文Data2用于智能钥匙对智能锁芯进行外部认证；

[0047] 根据本发明实施例，如图2所示，提供了一种智能锁芯，该智能锁芯包括以下模块：

[0048] 随机数发送模块201，用于向智能钥匙发送随机数Rnm，接收智能钥匙对随机数Rnm加密后的密文Data1；

[0049] 随机数解密模块202，用于对密文Data1进行解密得到Rnm1；

[0050] 随机数比较模块203，用于将随机数Rnm与Rnm1进行比较，若两者相同，则智能钥匙认证通过。

[0051] 上述智能锁芯还包括以下模块：

[0052] 随机数接收模块204，用于向智能钥匙发送生成随机数指令，接收智能钥匙产生的随机数Rnm2；

[0053] 随机数加密发送模块205，用于对随机数Rnm2进行加密得到加密密文Data2，向智

能钥匙发送加密密文Data2。

[0054] 根据本发明实施例，提供了一种智能锁具，该智能锁具包括：

[0055] 上述智能锁芯。

[0056] 本发明实施例的智能锁芯实现的方法、智能锁芯和锁具，通过ESAM对锁芯与钥匙进行身份认证、数据加/解密、安全存储、通讯保密等可以发挥锁具独到的安全控制作用和管理作用。新型的智能锁芯不仅具有MCU，还增加了专门的ESAM(嵌入式安全认证模块)安全芯片，使锁具的安全性得到提升。

[0057] 根据本发明实施例，如图3所示，提供了一种智能钥匙实现的方法，该方法包括以下步骤：

[0058] 步骤301：智能钥匙自智能锁芯接收生成随机数指令；

[0059] 步骤302：智能钥匙生成随机数Rnm2，将Rnm2发送给智能锁芯；

[0060] 步骤303：智能锁芯对Rnm2加密得到的密文Data2，并将Data2发送给智能钥匙；

[0061] 步骤304：智能钥匙自智能锁芯接收Data2，并对密文Data2进行解密得到明文Rnm3；

[0062] 步骤305：将随机数Rnm2和明文Rnm3进行比较，如果两者相同，则智能锁芯认证通过；如果两者不同，则智能锁芯认证未通过；

[0063] 步骤306：智能钥匙自智能锁芯接收随机数Rnm；

[0064] 步骤307：智能钥匙对随机数Rnm进行加密得到加密密文Data1，将Data1发送回所述智能锁芯进行认证。

[0065] 根据本发明实施例，如图4所示，提供了一种智能钥匙，该智能钥匙包括以下模块：

[0066] 随机数生成发送模块401，用于自智能锁芯接收生成随机数指令，生成随机数Rnm2，将随机数Rnm2发送给智能锁芯。

[0067] 随机数接收解密模块402，用于自智能锁芯接收智能锁芯对Rnm2加密得到的密文Data2，对密文Data2进行解密得到明文Rnm3；

[0068] 随机数比较模块403，用于将随机数Rnm2和Rnm3进行比较，如果两者相同，则智能锁芯认证通过；如果两者不同，则智能锁芯认证未通过。

[0069] 上述智能钥匙还包括以下模块：

[0070] 随机数接收模块404，用于自智能锁芯接收随机数Rnm；

[0071] 随机数加密发送模块405，用于对随机数Rnm进行加密得到加密密文Data1，将Data1发送回智能锁芯进行认证。

[0072] 本发明实施例的智能钥匙实现的方法和智能钥匙，只有管理部门才能使用主密钥修改钥匙将ESAM模块中密钥修改为运行主密钥，密钥泄露的可能性很小。使用时，工作人员只需将用户钥匙插入锁中，由用户钥匙与锁中的ESAM模块自动完成密钥的安全认证和数据存取工作。由于锁内部的安全认证过程完全是在钥匙内完成的，外人很难攻击，安全级别高，且核心主密钥严密控制，保证了锁系统的安全性运营。

[0073] 本发明能有多种不同形式的具体实施方式，上面以图1-图4为例结合附图对本发明的技术方案作举例说明，这并不意味着本发明所应用的具体实例只能局限在特定的流程或实施例结构中，本领域的普通技术人员应当了解，上文所提供的具体实施方案只是多种优选用法中的一些示例，任何体现本发明权利要求的实施方式均应在本发明技术方案所要

求保护的范围之内。

[0074] 最后应说明的是：以上所述仅为本发明的优选实施例而已，并不用于限制本发明，尽管参照前述实施例对本发明进行了详细的说明，对于本领域的技术人员来说，其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

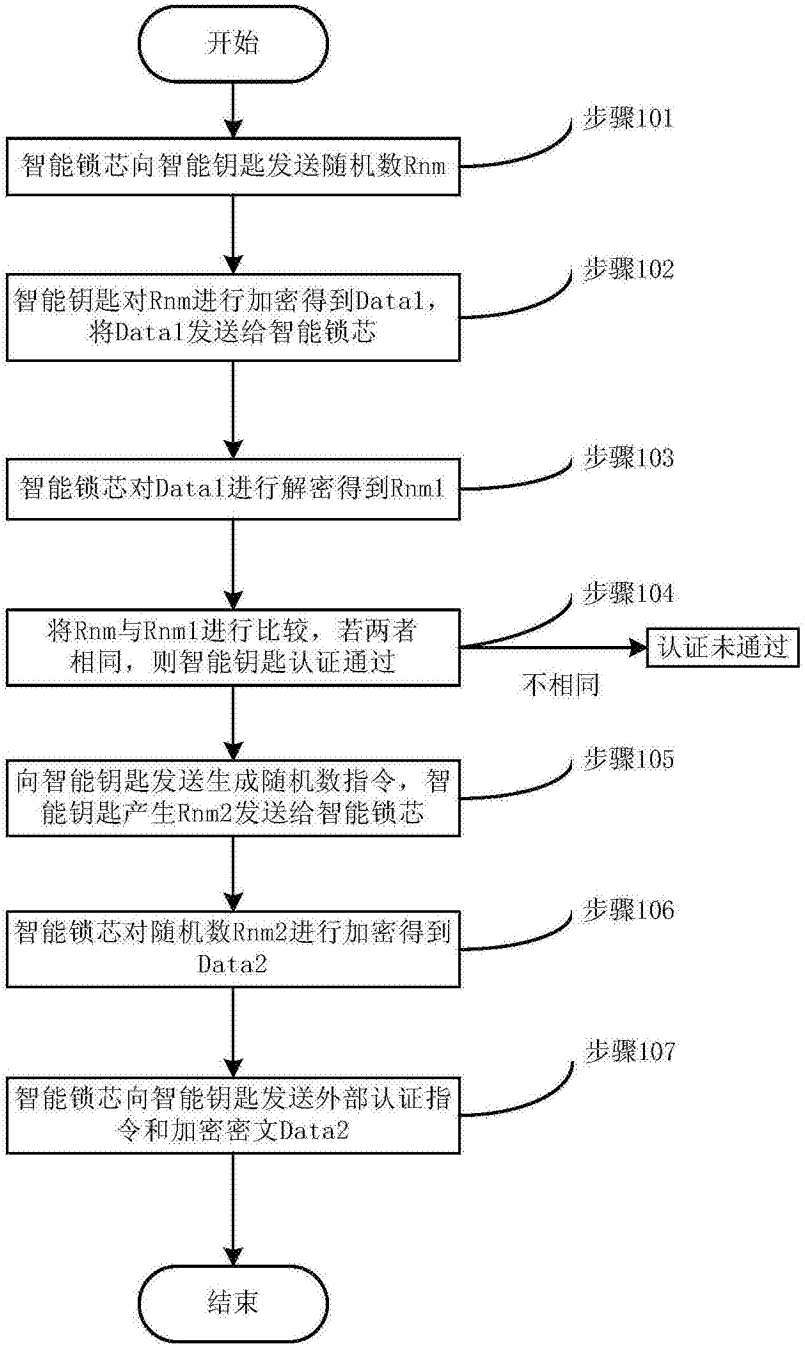

开始
步骤101
智能锁芯向智能钥匙发送随机数Rnm
步骤102
智能钥匙对Rnm进行加密得到Data1，将Data1发送给智能锁芯
步骤103
智能锁芯对Data1进行解密得到Rnm1
步骤104
将Rnm与Rnm1进行比较，若两者相同，则智能钥匙认证通过
认证未通过
不相同
步骤105
向智能钥匙发送生成随机数指令，智能钥匙产生Rnm2发送给智能锁芯
步骤106
智能锁芯对随机数Rnm2进行加密得到Data2
步骤107
智能锁芯向智能钥匙发送外部认证指令和加密密文Data2
结束

图1

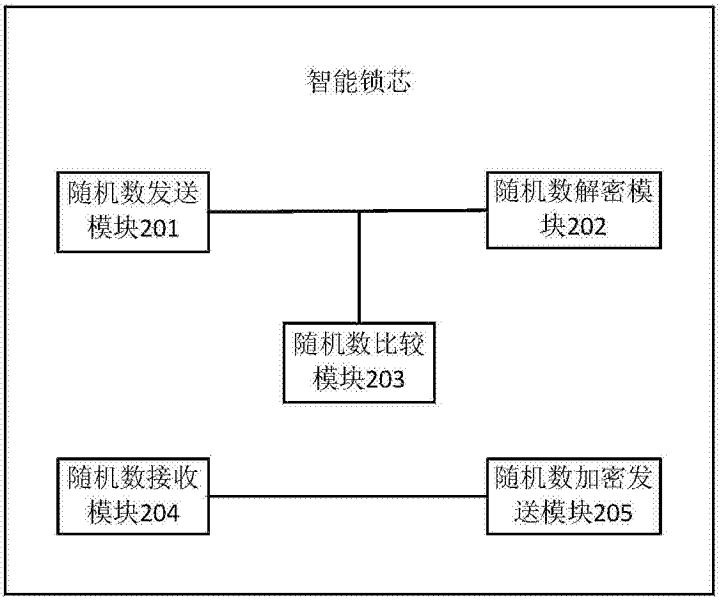

智能锁芯
随机数发送模块201
随机数解密模块202
随机数比较模块203
随机数接收模块204
随机数加密发送模块205

图2

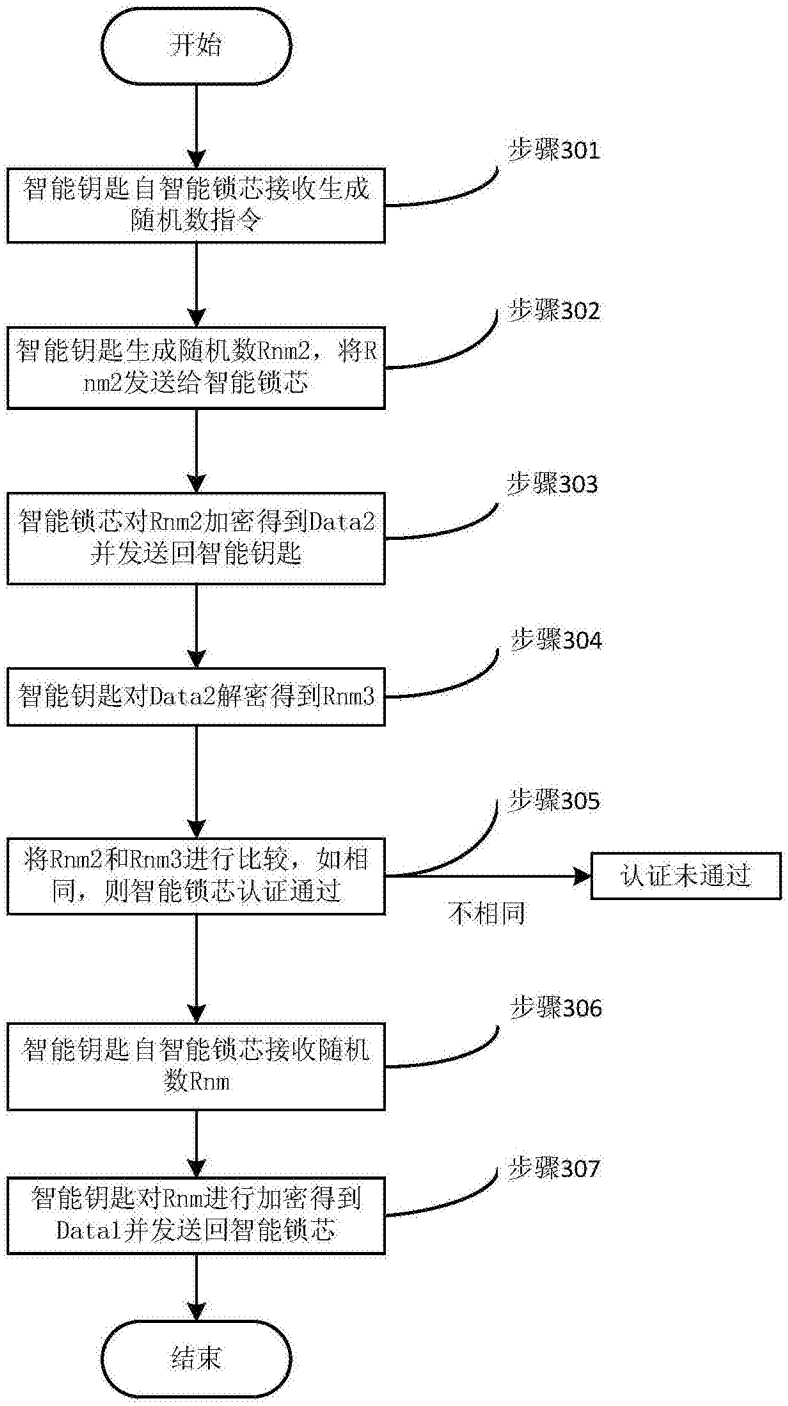

开始
步骤301
智能钥匙自智能锁芯接收生成随机数指令
步骤302
智能钥匙生成随机数Rnm2，将Rnm2发送给智能锁芯
步骤303
智能锁芯对Rnm2加密得到Data2并发送回智能钥匙
步骤304
智能钥匙对Data2解密得到Rnm3
步骤305
将Rnm2和Rnm3进行比较，如相同，则智能锁芯认证通过
认证未通过
不相同
步骤306
智能钥匙自智能锁芯接收随机数Rnm
步骤307
智能钥匙对Rnm进行加密得到Data1并发送回智能锁芯
结束

图3

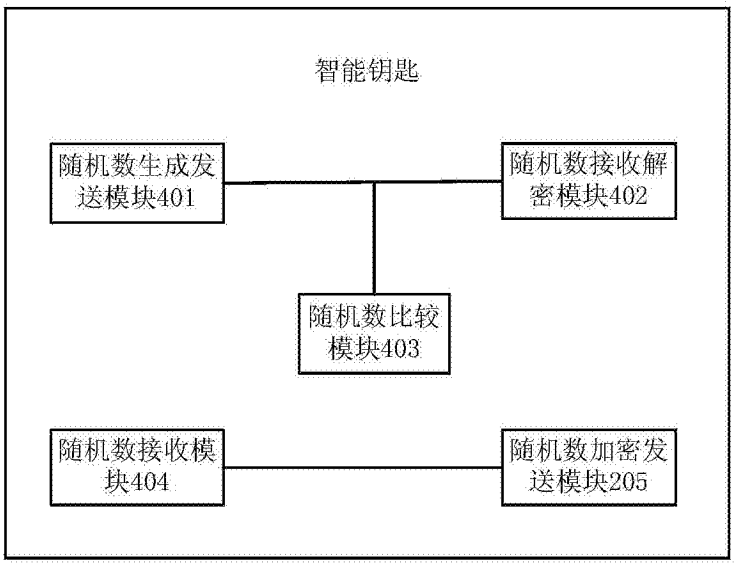

智能钥匙
随机数生成发送模块401
随机数接收解密模块402
随机数比较模块403
随机数接收模块404
随机数加密发送模块205

图4