(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 103248487 B
(45)授权公告日 2015.11.25

(21)申请号 201310155677.8

(22)申请日 2013.04.28

(73)专利权人 中国联合网络通信集团有限公司
地址 100033 北京市西城区金融大街21号

(72)发明人 李铭轩 王志军 顾旻霞 林敏 王蓉

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 刘芳

(51)Int.Cl.
H04L 9/32(2006.01)
H04B 5/00(2006.01)
H04L 9/28(2006.01)

(56)对比文件
CN 101739756 A,2010.06.16, 全文.
CN 101911581 A,2010.12.08, 全文.
EP 2490395 A1,2012.08.22, 全文.
苗雷. 基于智能卡的移动支付终端设计与实现.《中国优秀硕士学位论文全文数据库(电子期刊)》.2008,I136-407.

审查员 胡燕

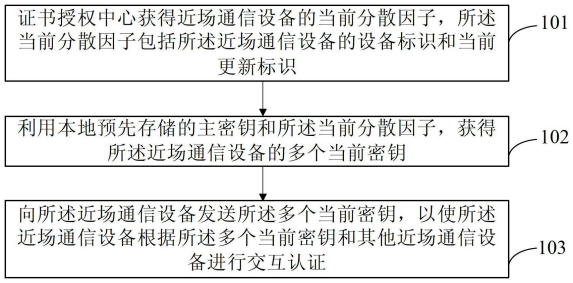
权利要求书3页 说明书11页 附图3页

(54)发明名称

近场通信认证方法、证书授权中心及近场通信设备

(57)摘要

本发明提供一种近场通信认证方法、证书授权中心及近场通信设备,方法包括:证书授权中心获得近场通信设备的当前分散因子,所述当前分散因子包括近场通信设备的设备标识和当前更新标识;利用本地预先存储的主密钥和所述当前分散因子,获得所述近场通信设备的多个当前密钥;向所述近场通信设备发送所述多个当前密钥,以使所述近场通信设备进行交互认证。本发明通过证书授权中心根据存储的主密钥获得近场通信设备的当前密钥,并向近场通信设备发送当前密钥,以使近场通信设备根据多个当前密钥和其他近场通信设备进行交互认证的方案,解决现有技术中存储在近场通信设备中的主密钥容易被破解导致的安全问题,从而有效提高近场通信的安全性。



CN 103248487 B

1.一种近场通信认证方法，其特征在于，包括：

证书授权中心获得近场通信设备的当前分散因子，所述当前分散因子包括所述近场通信设备的设备标识和当前更新标识；

利用本地预先存储的主密钥和所述当前分散因子，获得所述近场通信设备的多个当前密钥；

向所述近场通信设备发送所述多个当前密钥，以使所述近场通信设备根据所述多个当前密钥和其他近场通信设备进行交互认证。

2.根据权利要求1所述的方法，其特征在于，所述向所述近场通信设备发送所述多个当前密钥之后，还包括：

接收所述近场通信设备发送的第一认证请求，所述第一认证请求是另一近场通信设备发送给所述近场通信设备的，所述第一认证请求包括第一待认证密钥和所述另一近场通信设备的设备标识；

通过检测所述第一待认证密钥是否为所述另一近场通信设备的多个当前密钥之一，对所述另一近场通信设备进行认证，获得第一认证结果；

向所述近场通信设备返回所述第一认证结果。

3.根据权利要求1或2所述的方法，其特征在于，所述向所述近场通信设备发送所述多个当前密钥之后，还包括：

接收所述近场通信设备发送的密钥调用请求，所述密钥调用请求是所述近场通信设备在接收到另一近场通信设备发送的第一认证请求后发送的，所述第一认证请求包括第一待认证密钥和所述另一近场通信设备的设备标识；

向所述近场通信设备发送所述主密钥，以使所述近场通信设备根据所述主密钥和所述第一认证请求对所述另一近场通信设备进行认证。

4.一种近场通信认证方法，其特征在于，包括：

近场通信设备接收证书授权中心发送的多个当前密钥，所述多个当前密钥是所述证书授权中心根据本地预先存储的主密钥和所述近场通信设备的当前分散因子得到的，所述当前分散因子包括所述近场通信设备的设备标识和当前更新标识；

向另一近场通信设备发送第二认证请求，所述第二认证请求包括所述多个当前密钥之一和所述近场通信设备的设备标识，以使另一近场通信设备对所述近场通信设备进行认证。

5.根据权利要求4所述的方法，其特征在于，所述向另一近场通信设备发送第二认证请求之后，还包括：

接收所述另一近场通信设备发送的包括第一待认证密钥和所述另一近场通信设备的设备标识的第一认证请求，所述第一认证请求是所述另一近场通信设备在对所述近场通信设备认证成功后发送的；

根据所述第一认证请求对所述另一近场通信设备进行认证；

若对所述另一近场通信设备的认证成功，则与所述另一近场通信设备建立连接。

6.根据权利要求4所述的方法，其特征在于，所述向另一近场通信设备发送第二认证请求之前，还包括：

接收另一近场通信设备发送的包括第一待认证密钥和所述另一近场通信设备的设备

标识的第一认证请求；

根据所述第一认证请求对所述另一近场通信设备进行认证；

所述向另一近场通信设备发送第二认证请求，具体包括：

若对所述另一近场通信设备的认证成功，则向所述另一近场通信设备发送所述第二认证请求。

7. 根据权利要求 5 或 6 所述的方法，其特征在于，所述根据所述第一认证请求对所述另一近场通信设备进行认证，具体包括：

向所述证书授权中心发送所述第一认证请求，并接收所述证书授权中心返回的第一认证结果，所述第一认证结果是所述证书授权中心根据所述第一认证请求对所述另一近场通信设备进行认证后返回的；或者，

向所述证书授权中心发送密钥调用请求，并根据所述证书授权中心返回的所述主密钥和所述第一认证请求对所述另一近场通信设备进行认证。

8. 一种证书授权中心，其特征在于，包括：

获取模块，用于获得近场通信设备的当前分散因子，所述当前分散因子包括所述近场通信设备的设备标识和当前更新标识；

处理模块，还用于利用本地预先存储的主密钥和所述当前分散因子，获得所述近场通信设备的多个当前密钥；

发送模块，用于向所述近场通信设备发送所述多个当前密钥，以使所述近场通信设备根据所述多个当前密钥和其他近场通信设备进行交互认证。

9. 根据权利要求 8 所述的证书授权中心，其特征在于，所述证书授权中心还包括：

第一接收模块，用于接收所述近场通信设备发送的第一认证请求，所述第一认证请求是另一近场通信设备发送给所述近场通信设备的，所述第一认证请求包括第一待认证密钥和所述另一近场通信设备的设备标识；

认证模块，用于通过检测所述第一待认证密钥是否为所述另一近场通信设备的多个当前密钥之一，对所述另一近场通信设备进行认证，获得第一认证结果；

所述发送模块，还用于向所述近场通信设备返回所述第一认证结果。

10. 根据权利要求 8 或 9 所述的证书授权中心，其特征在于，所述证书授权中心还包括：

第二接收模块，用于接收所述近场通信设备发送的密钥调用请求，所述密钥调用请求是所述近场通信设备在接收到另一近场通信设备发送的第一认证请求后发送的，所述第一认证请求包括第一待认证密钥和所述另一近场通信设备的设备标识；

所述发送模块，还用于向所述近场通信设备发送所述主密钥，以使所述近场通信设备根据所述主密钥和所述第一认证请求对所述另一近场通信设备进行认证。

11. 一种近场通信设备，其特征在于，包括：

接收模块，用于接收证书授权中心发送的多个当前密钥，所述多个当前密钥是所述证书授权中心根据本地预先存储的主密钥和所述近场通信设备的当前分散因子得到的，所述当前分散因子包括所述近场通信设备的设备标识和当前更新标识；

发送模块，用于向另一近场通信设备发送第二认证请求，所述第二认证请求包括所述多个当前密钥之一和所述近场通信设备的设备标识，以使另一近场通信设备对所述近场通

信设备进行认证。

12.根据权利要求 11 所述的近场通信设备，其特征在于，所述接收模块，还用于接收所述另一近场通信设备发送的包括第一待认证密钥和所述另一近场通信设备的设备标识的第一认证请求，所述第一认证请求是所述另一近场通信设备在对所述近场通信设备认证成功后发送的；

所述近场通信设备，还包括：

认证模块，用于根据所述第一认证请求对所述另一近场通信设备进行认证；

处理模块，用于若对所述另一近场通信设备的认证成功，则与所述另一近场通信设备建立连接。

13.根据权利要求 11 所述的近场通信设备，其特征在于，

所述接收模块，还用于接收另一近场通信设备发送的包括第一待认证密钥和所述另一近场通信设备的设备标识的第一认证请求；

所述近场通信设备还包括：

认证模块，用于根据所述第一认证请求对所述另一近场通信设备进行认证；

所述发送模块，具体用于若对所述另一近场通信设备的认证成功，则向所述另一近场通信设备发送所述第二认证请求。

14.根据权利要求 12 或 13 所述的近场通信设备，其特征在于，所述认证模块具体包括：

第一发送单元，用于向所述证书授权中心发送所述第一认证请求；

第一接收单元，用于接收所述证书授权中心返回的第一认证结果，所述第一认证结果是所述证书授权中心根据所述第一认证请求对所述另一近场通信设备进行认证后返回的；

或者，所述认证模块具体包括：

第二发送单元，用于向所述证书授权中心发送密钥调用请求；

第二接收单元，用于接收所述证书授权中心返回的所述主密钥；

认证单元，用于根据所述证书授权中心返回的所述主密钥和所述第一认证请求对所述另一近场通信设备进行认证。

近场通信认证方法、证书授权中心及近场通信设备

技术领域

[0001] 本发明涉及通信领域，尤其涉及一种近场通信认证方法、证书授权中心及近场通信设备。

背景技术

[0002] 随着具备近场通信功能的设备逐渐普及，通过近场通信实现设备之间的数据传输也越发的频繁。如何确保近场通信的安全性，是目前近场通信技术发展过程中需要解决的问题。

[0003] 为此，现有的解决方案为，通过营业厅的专有设备将主密钥预先存入各设备，此后，当各设备之间需要进行通信交互时，则可根据本设备中预先存入的所述主密钥和预先设置在本设备中的随机数发生器生成的随机数，通过特定的密钥分散算法产生每次通信的会话密钥，从而实现对设备之间的通信数据进行加密，保证近场通信的安全性。

[0004] 但是，在上述现有方案中，用于产生对通信数据进行加密的会话密钥的主密钥被预先存储在设备本地，其被破解的可能性很大，即若所述主密钥被破解，则根据所述主密钥生成的，用于通信数据加密的会话密钥的安全性将同样无法保证，因此，该方案中仍存在很大的安全隐患。

发明内容

[0005] 本发明提供一种近场通信认证方法、证书授权中心及近场通信设备，用于解决现有近场通信技术中，近场通信设备中的主密钥容易被破解而导致的安全问题。

[0006] 一方面，本发明提供一种近场通信认证方法，包括：

[0007] 证书授权中心获得近场通信设备的当前分散因子，所述当前分散因子包括所述近场通信设备的设备标识和当前更新标识；

[0008] 利用本地预先存储的主密钥和所述当前分散因子，获得所述近场通信设备的多个当前密钥；

[0009] 向所述近场通信设备发送所述多个当前密钥，以使所述近场通信设备根据所述多个当前密钥和其他近场通信设备进行交互认证。

[0010] 另一方面，本发明提供一种证书授权中心，包括：

[0011] 获取模块，用于获得近场通信设备的当前分散因子，所述当前分散因子包括所述近场通信设备的设备标识和当前更新标识；

[0012] 处理模块，还用于利用本地预先存储的主密钥和所述当前分散因子，获得所述近场通信设备的多个当前密钥；

[0013] 发送模块，用于向所述近场通信设备发送所述多个当前密钥，以使所述近场通信设备根据所述多个当前密钥和其他近场通信设备进行交互认证。

[0014] 又一方面，本发明提供另一种近场通信认证方法，包括：

[0015] 近场通信设备接收证书授权中心发送的多个当前密钥，所述多个当前密钥是所述

证书授权中心根据本地预先存储的主密钥和所述近场通信设备的当前分散因子得到的，所述当前分散因子包括所述近场通信设备的设备标识和当前更新标识；

[0016] 向另一近场通信设备发送第二认证请求，所述第二认证请求包括所述多个当前密钥之一和所述近场通信设备的设备标识，以使另一近场通信设备对所述近场通信设备进行认证。

[0017] 又一方面，本发明提供一种近场通信设备，包括：

[0018] 接收模块，用于接收证书授权中心发送的多个当前密钥，所述多个当前密钥是所述证书授权中心根据本地预先存储的主密钥和所述近场通信设备的当前分散因子得到的，所述当前分散因子包括所述近场通信设备的设备标识和当前更新标识；

[0019] 发送模块，用于向另一近场通信设备发送第二认证请求，所述第二认证请求包括所述多个当前密钥之一和所述近场通信设备的设备标识，以使另一近场通信设备对所述近场通信设备进行认证。

[0020] 本发明提供的近场通信认证方法、证书授权中心及近场通信设备，通过将用于获得近场通信设备当前密钥的主密钥存储在证书授权中心，根据所述主密钥获得所述近场通信设备的当前密钥，并向所述近场通信设备发送所述当前密钥，以使所述近场通信设备根据所述多个当前密钥和其他近场通信设备进行交互认证的技术方案，解决了现有技术中存储在近场通信设备中的主密钥容易被破解而导致的安全问题，有效提高近场通信的安全性。

附图说明

[0021] 图 1 为本发明实施例一提供的一种近场通信认证方法的流程示意图；

[0022] 图 2 为本发明实施例二提供的一种近场通信认证方法的流程示意图；

[0023] 图 3 为本发明实施例三提供的一种近场通信认证方法的流程示意图；

[0024] 图 4 为本发明实施例四提供的一种近场通信认证方法的流程示意图；

[0025] 图 5 为本发明实施例六提供的一种证书授权中心的结构示意图；

[0026] 图 6 为本发明实施例七提供的一种近场通信设备的结构示意图。

具体实施方式

[0027] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述。

[0028] 图 1 为本发明实施例一提供的一种近场通信认证方法的流程示意图，如图 1 所示，所述方法包括：

[0029] 101、证书授权中心获得近场通信设备的当前分散因子，所述当前分散因子包括所述近场通信设备的设备标识和当前更新标识。

[0030] 其中，不同时刻的当前更新标识不同，具体的，所述当前更新标识可以为与当前时间对应的标识，例如，若当前时间为 2013 年 02 月 21 日 12 点整，则所述当前更新标识为 201302211200，再例如，若当前时间为 2013 年 02 月 21 日 11 点 40 分，则所述当前更新标识为 201302211140；进一步的，当前分散因子可以为设备标识和当前更新标识的简单组合，例如，若设备标识为 abc123，当前更新标识为 201302211140，则所述证书授权中心获得的

当前分散因子可以为 abc123201302211140，举例给出的只是一种具体的实施方式，并未对其它实施方式进行限制。

[0031] 具体的，101 可以包括：周期性地获得所述近场通信设备的当前分散因子；或者，

[0032] 根据所述近场通信设备的密钥请求，获得所述近场通信设备的当前分散因子。

[0033] 该实施方式的场景为，证书授权中心周期性地获得所述近场通信设备的当前分散因子，或者、证书授权中心根据所述近场通信设备的密钥请求，获得所述近场通信设备的当前分散因子，或者进一步的，证书授权中心在周期性地获得所述近场通信设备的当前分散因子的基础上，还可以根据所述近场通信设备的密钥请求，获得所述近场通信设备的当前分散因子。

[0034] 需要说明的是，在上述的第一种场景中，所述近场通信设备和另一近场通信设备的当前分散因子中的当前更新标识相同，具体的，101 的执行周期可以根据工作需要确定，例如，取所述周期为 30 分钟。同样需要说明的是，本发明各实施例中的所述获得当前分散因子均表示，根据设备标识和当前更新标识获得当前分散因子，可选的，所述当前更新标识与当前时间对应。

[0035] 102、利用本地预先存储的主密钥和所述当前分散因子，获得所述近场通信设备的多个当前密钥。

[0036] 具体的，102 可以包括：根据所述主密钥和所述当前分散因子，通过标准的中国金融集成电路卡规范（业内简称 PBOC2.0）密钥发散算法进行两级分散操作，获得所述近场通信设备的多个当前密钥。

[0037] 103、向所述近场通信设备发送所述多个当前密钥，以使所述近场通信设备根据所述多个当前密钥和其他近场通信设备进行交互认证。

[0038] 具体的，所述向所述近场通信设备发送所述多个当前密钥可以包括：通过空中下载技术（Over the Air Technology，简称 OTA）向所述近场通信设备发送所述多个当前密钥。

[0039] 其中，所述证书授权中心根据当前更新标识获得的当前分散因子，可以称为与所述当前更新标识对应的当前分散因子；相应的，根据该当前分散因子获得的当前密钥，可以称为与所述当前更新标识对应的当前密钥。

[0040] 本实施例提供的近场通信认证方法，通过将用于获得近场通信设备当前密钥的主密钥存储在证书授权中心，根据所述主密钥获得近场通信设备的当前密钥，并向所述近场通信设备发送所述当前密钥，以使所述近场通信设备根据所述多个当前密钥和其他近场通信设备进行交互认证的技术方案，解决了现有技术中存储在近场通信设备中的主密钥容易被破解而导致的安全问题，有效提高近场通信的安全性。

[0041] 图 2 为本发明实施例二提供的一种近场通信认证方法的流程示意图，如图 2 所示，根据实施例一所述的近场通信认证方法，在 103 之后，还可以包括：

[0042] 201、接收所述近场通信设备发送的第一认证请求，所述第一认证请求是另一近场通信设备发送给所述近场通信设备的，所述第一认证请求包括所述第一待认证密钥和所述另一近场通信设备的设备标识。

[0043] 202、通过检测所述第一待认证密钥是否为所述另一近场通信设备的多个当前密钥之一，对所述另一近场通信设备进行认证，获得第一认证结果。

[0044] 其中，所述另一近场通信设备的多个当前密钥可以预存在所述证书授权中心，或者，可以通过所述证书授权中心在接收到所述第一认证请求时，根据本地存储的主密钥和所述另一近场通信设备的当前分散因子获得。

[0045] 在后一种实施方式中，101 的实施场景可以为，证书授权中心周期性地获得所述近场通信设备的当前分散因子，或者、证书授权中心根据所述近场通信设备的密钥请求，获得所述近场通信设备的当前分散因子，或者进一步的，证书授权中心在周期性地获得所述近场通信设备的当前分散因子的基础上，还可以根据所述近场通信设备的密钥请求，获得所述近场通信设备的当前分散因子。具体的，当 101 的实施场景为后两种实施场景时，在所述后一种实施方式中，所述证书授权中心均可在获得近场通信设备的当前分散因子时，保存所述近场通信设备的当前分散因子对应的当前更新标识。

[0046] 203、向所述近场通信设备返回所述第一认证结果。

[0047] 可选的，在 103 之后，还可以包括 ：

[0048] 初始化对所述第一认证结果为认证失败的连续次数的计数 ；

[0049] 相应的，在 202 之后，还可以包括 ：

[0050] 若所述第一认证结果为认证失败的连续次数大于预设的门限值，则获得所述另一近场通信设备的当前分散因子 ；

[0051] 利用本地存储的主密钥和所述另一近场通信设备的当前分散因子，获得所述另一近场通信设备的多个当前密钥 ；

[0052] 向所述另一近场通信设备发送所述另一近场通信设备的多个当前密钥，并初始化所述第一认证结果为认证失败的连续次数的计数。

[0053] 所述门限值可以根据实际需要确定，例如，取所述门限值为 5。

[0054] 本实施方式的应用场景为，若证书授权中心对某近场通信设备认证失败的连续次数大于一定值，即表示该近场通信设备的当前密钥存在被试图破解的可能，则所述证书授权中心获得该近场通信设备的当前分散因子，并根据该当前分散因子获得当前密钥发送给该近场通信设备。

[0055] 本实施例提供的近场通信认证方法通过，证书授权中心根据接收到的近场通信设备的认证请求，通过检测所述认证请求中的待认证密钥是否为该近场通信设备的多个当前密钥之一，实现对近场通信设备进行认证，并在认证失败的连续次数大于预设的门限值时，重新获得该近场通信设备的当前密钥的技术方案，有效降低该近场通信设备的密钥被破解的可能性，从而进一步提高近场通信的安全性。

[0056] 图 3 为本发明实施例三提供的一种近场通信认证方法的流程示意图，如图 3 所示，根据实施例一所述的近场通信认证方法，在 103 之后，还可以包括 ：

[0057] 301、接收所述近场通信设备发送的密钥调用请求，所述密钥调用请求是所述近场通信设备在接收到另一近场通信设备发送的第一认证请求后发送的，所述第一认证请求包括第一待认证密钥和所述另一近场通信设备的设备标识 ；

[0058] 302、向所述近场通信设备发送所述主密钥，以使所述近场通信设备根据所述主密钥和所述第一认证请求对所述另一近场通信设备进行认证。

[0059] 可选的，在 302 之后，还可以包括 ：

[0060] 接收所述近场通信设备发送的携带所述另一近场通信设备的设备标识的密钥更

新请求，所述密钥更新请求是所述近场通信设备在对所述另一近场通信设备认证失败的连续次数大于预设的门限值后发送的；

[0061] 根据所述密钥更新请求，获得所述另一近场通信设备的当前分散因子；

[0062] 利用本地存储的主密钥和所述另一近场通信设备的当前分散因子，获得所述另一近场通信设备的多个当前密钥；

[0063] 向所述另一近场通信设备发送所述另一近场通信设备的多个当前密钥。

[0064] 本实施例提供的近场通信认证方法通过，证书授权中心在接收到近场通信设备根据接收到的另一近场通信设备的认证请求发送的密钥调用请求时，向所述近场通信设备发送本地存储的主密钥，从而使所述近场通信设备对另一近场通信设备进行认证，并在接收到所述近场通信设备在检测到对另一近场通信设备认证失败的连续次数大于预设的门限值时发送的，包括所述另一近场通信设备的设备标识的密钥更新请求时，获得所述近场通信设备的当前密钥并发送给所述另一近场通信设备的技术方案，有效降低该近场通信设备的密钥被破解的可能性，从而进一步提高近场通信的安全性。

[0065] 可选的，根据上述任一实施例所述的近场通信认证方法，在 103 之前，还可以包括：

[0066] 向所述近场通信设备发送密钥指令；

[0067] 相应的，103 具体可以包括：

[0068] 若在所述发送密钥指令之后的预设时间内接收到所述近场通信设备根据所述密钥指令返回的密钥响应，则向所述近场通信设备发送所述多个当前密钥。

[0069] 本实施方式通过，当接收到近场通信设备在接收到证书授权中心发送的密钥指令后的预设时间内返回的密钥响应时，则向该近场通信设备发送当前密钥的实施方式，对近场通信设备的当前收发状态预先进行检测，从而有效保证密钥发送的成功率。

[0070] 图 4 为本发明实施例四提供的一种近场通信认证方法的流程示意图，如图 4 所示，所述方法包括：

[0071] 401、近场通信设备接收证书授权中心发送的多个当前密钥，所述多个当前密钥是所述证书授权中心根据本地预先存储的主密钥和所述近场通信设备的当前分散因子得到的，所述当前分散因子包括所述近场通信设备的设备标识和当前更新标识。

[0072] 在实际应用中，所述近场通信设备可以将所述当前密钥存储在自身设备的安全模块内，需要说明的是，不同设备类型的设备，其安全模块可能不同，具体举例来说，所述近场通信设备的安全模块可以为设置在所述近场通信设备中的智能卡。

[0073] 402、向另一近场通信设备发送第二认证请求，所述第二认证请求包括所述多个当前密钥之一和所述近场通信设备的设备标识，以使另一近场通信设备对所述近场通信设备进行认证。

[0074] 可选的，在 402 之后，还可以包括：

[0075] 接收所述另一近场通信设备发送的包括第一待认证密钥和所述另一近场通信设备的设备标识的第一认证请求，所述第一认证请求是所述另一近场通信设备在对所述近场通信设备认证成功后发送的；

[0076] 根据所述第一认证请求对所述另一近场通信设备进行认证；

[0077] 若对所述另一近场通信设备的认证成功，则与所述另一近场通信设备建立连接。

[0078] 通常，两个近场通信设备在建立连接之前，需先进行相互认证，若相互认证均成功，则建立连接。

[0079] 在本实施例的一种实施方式中，所述根据所述第一认证请求对所述另一近场通信设备进行认证，具体可以包括：

[0080] 向所述证书授权中心发送所述第一认证请求，并接收所述证书授权中心返回的第一认证结果，所述第一认证结果是所述证书授权中心根据所述第一认证请求对所述另一近场通信设备进行认证后返回的。

[0081] 具体的，证书授权中心对近场通信设备进行认证的具体过程，与实施例一中的相关内容相似，本实施例在此不再赘述。

[0082] 在本实施例的另一种实施方式中，所述根据所述第一认证请求对所述另一近场通信设备进行认证，具体可以包括：

[0083] 向所述证书授权中心发送密钥调用请求，并根据所述证书授权中心返回的所述主密钥和所述第一认证请求对所述另一近场通信设备进行认证。

[0084] 可选的，在本实施方式下，所述第二认证请求还可以包括所述近场通信设备的当前更新标识，所述第一认证请求还可以包括所述另一近场通信设备的当前更新标识；所述根据所述证书授权中心返回的所述主密钥和所述第一认证请求对所述另一近场通信设备进行认证，具体可以包括：

[0085] 根据所述证书授权中心返回的所述主密钥、所述另一近场通信设备的当前更新标识和所述第一认证请求，获得所述另一近场通信设备的多个当前密钥，并通过检测所述第一待认证密钥是否为所述另一近场通信设备的多个当前密钥之一，对所述另一近场通信设备进行认证。

[0086] 本实施例中 401 之后，所述近场通信设备还可以根据接收到所述证书授权中心发送的当前密钥时的当前时间，确定自身的所述当前密钥对应的当前更新标识。进一步地，在对所述另一近场通信设备进行认证时，将自身的当前密钥对应的当前更新标识作为所述另一近场通信设备的当前密钥对应的当前更新标识。其中，所述近场通信设备接收到所述证书授权中心发送的当前密钥的时间，与所述证书授权中心生成所述近场通信设备的当前密钥所用的当前分散因子中当前更新标识对应的时间可能存在一定的时间差，即，所述近场通信设备确定的自身当前密钥对应的当前更新标识与所述近场通信设备的当前密钥实际对应的当前更新标识存在一定的误差。进一步地，所述证书授权中心生成所述近场通信设备的当前密钥所用的当前分散因子中当前更新标识对应的时间与生成所述另一近场通信设备的当前密钥所用的当前分散因子中当前更新标识对应的时间可能存在一定的时间差，即所述近场通信设备的当前密钥实际对应的当前更新标识与所述另一近场通信设备的当前密钥实际对应的当前更新标识存在一定的误差，因此，为了进一步提高认证的准确性，可以预先设定一个时间窗，即当前更新标识的误差范围。对应的，所述根据所述证书授权中心返回的所述主密钥和所述第一认证请求对所述另一近场通信设备进行认证，具体可以包括：

[0087] 根据预存的所述近场通信设备的当前更新标识和预设的时间窗，获得多个可认证更新标识，所述可认证更新标识的值不小于所述当前更新标识与所述预设的时间窗的差、且不大于所述当前更新标识与所述预设的时间窗的和；

[0088] 根据所述另一近场通信设备的设备标识、所述多个可认证更新标识和所述主密钥，分别获得所述另一近场通信设备的多个可认证当前密钥，并通过检测所述第一待认证密钥是否为所述另一近场通信设备的多个可认证当前密钥之一，对所述另一近场通信设备进行认证。

[0089] 其中，所述时间窗可以根据工作需要确定，例如，设所述时间窗为 2 分钟，则若所述近场通信设备的当前更新标识为 201302211200，则获得多个可认证更新标识包括 201302211158、201302211159、201302211200、201302211201 和 201302211202。

[0090] 可选的，所述根据所述证书授权中心返回的所述主密钥和所述第一认证请求对所述另一近场通信进行认证之后，还可以包括：

[0091] 若对所述另一近场通信的认证结果为认证失败的连续次数大于预设的门限值，则向所述证书授权中心发送携带所述另一近场通信设备的设备标识的密钥更新请求，以使所述证书授权中心根据所述密钥更新请求更新所述另一近场通信设备的当前密钥。

[0092] 其中，所述第二认证请求还可以包括所述近场通信设备的当前更新标识，所述第一认证请求还可以包括所述另一近场通信设备的当前更新标识。

[0093] 上述步骤的应用场景可以为，若近场通信设备对另一近场通信设备认证失败的连续次数大于预设的门限值，即表示该另一近场通信设备的当前密钥存在被试图破解的可能，则所述近场通信设备向证书授权中心请求更新该另一近场通信设备的当前密钥。

[0094] 可选的，在一种实施方式中，在 401 之前，还可以包括：

[0095] 接收所述证书授权中心发送的密钥指令，并向所述证书授权中心返回密钥响应。

[0096] 可选的，在另一种实施方式中，在 401 之前，还可以包括：

[0097] 向证书授权中心发送密钥请求，以使所述证书授权中心根据所述密钥请求获得所述近场通信设备的当前分散因子。

[0098] 在上述两种实施方式下，本实施例中的所述第二认证请求还可以包括所述近场通信设备的当前更新标识，所述第一认证请求还可以包括所述另一近场通信设备的当前更新标识。

[0099] 本实施例提供的近场通信认证方法，通过在近场通信设备与另一近场通信设备建立连接之前，向另一近场通信设备发送包括任一预先从证书授权中心接收到的当前密钥的认证请求，并在接收到所述另一近场通信设备返回的认证请求后，对所述另一近场通信设备进行认证的技术方案，实现在近场通信设备建立连接之前先进行交互认证，从而有效提高近场通信的安全性。

[0100] 本发明实施例五提供又一种近场通信认证方法，根据实施例四所述的近场通信认证方法，在 402 之前，还可以包括：

[0101] 接收另一近场通信设备发送的包括第一待认证密钥和所述另一近场通信设备的设备标识的第一认证请求；

[0102] 根据所述第一认证请求对所述另一近场通信设备进行认证；

[0103] 则相应的，402 具体包括：

[0104] 若对所述另一近场通信设备的认证成功，则向所述另一近场通信设备发送所述第二认证请求。

[0105] 具体的，上述步骤可以在 401 之前执行，或者在 401 之后 402 之前执行，本实施例

未对其进行限制。其中，所述根据所述第一认证请求对所述另一近场通信设备进行认证的具体方法与实施例四中的相关内容相似，故在此不再赘述。

[0106] 可选的，在本实施方式中，所述根据所述证书授权中心返回的所述主密钥和所述第一认证请求对所述另一近场通信设备进行认证之后，还可以包括：

[0107] 若第一认证结果为认证失败的连续次数大于所述门限值，则向所述证书授权中心发送携带所述另一近场通信设备的设备标识的密钥更新请求，以使所述证书授权中心根据所述密钥更新请求更新所述另一近场通信设备的当前密钥。

[0108] 本实施例中各实施方式的具体流程与前述各实施例中的相关内容相似，本实施例在此不再赘述。

[0109] 本实施例提供的近场通信认证方法，通过近场通信设备根据另一近场通信设备发送的认证请求，对所述另一近场通信设备认证成功后，根据本地从证书授权中心接收到的当前密钥，向所述另一近场通信设备发送包括任一所述当前密钥的认证请求，以实现所述另一近场通信设备对所述近场通信设备进行交互认证的技术方案，有效提高近场通信的安全性。

[0110] 图 5 为本发明实施例六提供的一种证书授权中心的结构示意图，如图 5 所示，所述证书授权中心包括：

[0111] 获取模块 51，用于获得近场通信设备的当前分散因子，所述当前分散因子包括所述近场通信设备的设备标识和当前更新标识；

[0112] 处理模块 52，还用于利用本地预先存储的主密钥和所述当前分散因子，获得所述近场通信设备的多个当前密钥；

[0113] 发送模块 53，用于向所述近场通信设备发送所述多个当前密钥，以使所述近场通信设备根据所述多个当前密钥和其他近场通信设备进行交互认证。

[0114] 可选的，在本实施例的一种实施方式中，所述证书授权中心还可以包括：

[0115] 第一接收模块，用于接收所述近场通信设备发送的第一认证请求，所述第一认证请求是另一近场通信设备发送给所述近场通信设备的，所述第一认证请求包括所述第一待认证密钥和所述另一近场通信设备的设备标识；

[0116] 认证模块，用于通过检测所述第一待认证密钥是否为所述另一近场通信设备的多个当前密钥之一，对所述另一近场通信设备进行认证，获得第一认证结果；

[0117] 发送模块 53，还用于向所述近场通信设备返回所述第一认证结果。

[0118] 在本实施方式下，处理模块 52，还用于初始化对所述第一认证结果为认证失败的连续次数的计数；

[0119] 获取模块 51，还用于若所述第一认证结果为认证失败的连续次数大于预设的门限值，则获得所述另一近场通信设备的当前分散因子；

[0120] 处理模块 52，还用于利用本地存储的主密钥和所述另一近场通信设备的当前分散因子，获得所述另一近场通信设备的多个当前密钥；

[0121] 发送模块 53，还用于向所述另一近场通信设备发送所述另一近场通信设备的多个当前密钥，并初始化所述第一认证结果为认证失败的连续次数的计数。

[0122] 可选的，在本实施例的另一种实施方式中，所述证书授权中心还可以包括：第二接收模块，用于接收所述近场通信设备发送的密钥调用请求，所述密钥调用请求是所述近场

通信设备在接收到另一近场通信设备发送的第一认证请求后发送的，所述第一认证请求包括第一待认证密钥和所述另一近场通信设备的设备标识；

[0123] 发送模块 53，还用于向所述近场通信设备发送所述主密钥，以使所述近场通信设备根据所述主密钥和所述第一认证请求对所述另一近场通信设备进行认证。

[0124] 在本实施方式下，所述第二接收模块，还用于接收所述近场通信设备发送的携带所述另一近场通信设备的设备标识的密钥更新请求，所述密钥更新请求是所述近场通信设备在对所述另一近场通信设备认证失败的连续次数大于预设的门限值后发送的；

[0125] 获取模块 51，还用于根据所述密钥更新请求，获得所述另一近场通信设备的当前分散因子；

[0126] 处理模块 52，还用于利用本地存储的主密钥和所述另一近场通信设备的当前分散因子，获得所述另一近场通信设备的多个当前密钥；

[0127] 发送模块 53，还用于向所述另一近场通信设备发送所述另一近场通信设备的多个当前密钥。

[0128] 可选的，在上述任一实施方式中，发送模块 53，还用于向所述近场通信设备发送密钥指令；所述证书授权中心还包括：第三接收模块，用于接收所述近场通信设备根据所述密钥指令返回的密钥响应；发送模块 53，还用于若在所述发送密钥指令之后的预设时间内接收到所述近场通信设备根据所述密钥指令返回的密钥响应，则向所述近场通信设备发送所述多个当前密钥。

[0129] 可选的，获取模块 51，具体用于周期性地获得所述近场通信设备的当前分散因子；或者，根据所述近场通信设备的密钥请求，获得所述近场通信设备的当前分散因子。

[0130] 本实施例提供的证书授权中心，通过将用于获得近场通信设备当前密钥的主密钥存储在所述证书授权中心，并且所述证书授权中心根据所述主密钥获得近场通信设备的当前密钥，并向所述近场通信设备发送所述当前密钥，以使所述近场通信设备根据所述多个当前密钥和其他近场通信设备进行交互认证的技术方案，解决了现有技术中存储在近场通信设备中的主密钥容易被破解而导致的安全问题，有效提高近场通信的安全性。

[0131] 图 6 为本发明实施例七提供的一种近场通信设备的结构示意图，如图 6 所示，所述近场通信设备包括：

[0132] 接收模块 61，用于接收证书授权中心发送的多个当前密钥，所述多个当前密钥是所述证书授权中心根据本地预先存储的主密钥和所述近场通信设备的当前分散因子得到的，所述当前分散因子包括所述近场通信设备的设备标识和当前更新标识；

[0133] 发送模块 62，用于向另一近场通信设备发送第二认证请求，所述第二认证请求包括所述多个当前密钥之一和所述近场通信设备的设备标识，以使另一近场通信设备对所述近场通信设备进行认证。

[0134] 可选的，接收模块 61，还用于接收所述另一近场通信设备发送的包括第一待认证密钥和所述另一近场通信设备的设备标识的第一认证请求，所述第一认证请求是所述另一近场通信设备在对所述近场通信设备认证成功后发送的；

[0135] 相应的，所述近场通信设备，还包括：

[0136] 认证模块，用于根据所述第一认证请求对所述另一近场通信设备进行认证；

[0137] 处理模块，用于若对所述另一近场通信设备的认证成功，则与所述另一近场通信

设备建立连接。

[0138] 在上述任一实施方式下，接收模块 61，还用于接收所述证书授权中心发送的密钥指令；发送模块 62，还用于根据所述密钥指令，向所述证书授权中心返回密钥响应。

[0139] 在上述任一实施方式下，发送模块 62，还用于向证书授权中心发送密钥请求，以使所述证书授权中心根据所述密钥请求获得所述近场通信设备的当前分散因子。

[0140] 本实施例提供的近场通信设备，通过在所述近场通信设备与另一近场通信设备建立连接之前，向另一近场通信设备发送包括任一预先从证书授权中心接收到的当前密钥的认证请求，并在接收到所述另一近场通信设备返回的认证请求后，对所述另一近场通信设备进行认证的技术方案，实现在近场通信设备建立连接之前先进行交互认证，从而有效提高近场通信的安全性。

[0141] 本发明实施例八提供另一种近场通信设备，根据实施例七所述的近场通信设备，

[0142] 接收模块 61，还用于接收另一近场通信设备发送的包括第一待认证密钥和所述另一近场通信设备的设备标识的第一认证请求；

[0143] 所述近场通信设备还包括：认证模块，用于根据所述第一认证请求对所述另一近场通信设备进行认证；

[0144] 发送模块 62，具体用于若对所述另一近场通信设备的认证成功，则向所述另一近场通信设备发送所述第二认证请求。

[0145] 根据实施例七或实施例八所述的近场通信设备，所述认证模块具体可以包括：

[0146] 第一发送单元，用于向证书授权中心发送所述第一认证请求，以使所述证书授权中心根据所述第一认证请求对所述另一近场通信设备进行认证；

[0147] 第一接收单元，用于接收所述证书授权中心根据所述第一认证请求对所述另一近场通信设备进行认证后返回的第一认证结果；

[0148] 或者，所述认证模块具体可以包括：

[0149] 第二发送单元，用于向所述证书授权中心发送密钥调用请求；

[0150] 第二接收单元，用于接收所述证书授权中心返回的所述主密钥；

[0151] 认证单元，用于根据所述证书授权中心返回的所述主密钥和所述第一认证请求对所述另一近场通信设备进行认证。

[0152] 在后一种实施方式中，所述第二发送单元，还用于若第一认证结果为认证失败的连续次数大于所述门限值，则向所述证书授权中心发送携带所述另一近场通信设备的设备标识的密钥更新请求，以使所述证书授权中心根据所述密钥更新请求更新所述另一近场通信设备的当前密钥。

[0153] 本实施例提供的近场通信设备，通过所述近场通信设备根据另一近场通信设备发送的认证请求，对所述另一近场通信设备认证成功后，根据本地从证书授权中心接收到的当前密钥，向所述另一近场通信设备发送包括任一所述当前密钥的认证请求，以实现所述另一近场通信设备对所述近场通信设备进行交互认证的技术方案，有效提高近场通信的安全性。

[0154] 需要说明的是，上述实施例提供的证书授权中心和近场通信设备均可实现本发明任一实施例提供的近场通信认证方法的步骤，具体实现方法在此不再赘述。

[0155] 本领域普通技术人员可以理解：实现上述各方法实施例的全部或部分步骤可以通

过程序指令相关的硬件来完成。前述的程序可以存储于一计算机可读取存储介质中。该程序在执行时，执行包括上述各方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0156] 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

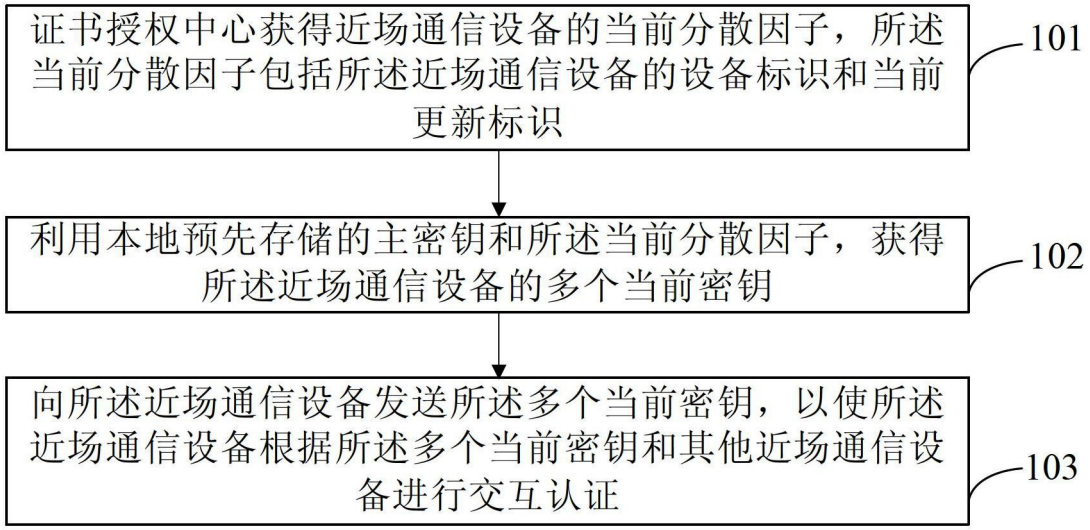

证书授权中心获得近场通信设备的当前分散因子，所述当前分散因子包括所述近场通信设备的设备标识和当前更新标识
101
利用本地预先存储的主密钥和所述当前分散因子，获得所述近场通信设备的多个当前密钥
102
向所述近场通信设备发送所述多个当前密钥，以使所述近场通信设备根据所述多个当前密钥和其他近场通信设备进行交互认证
103

图 1

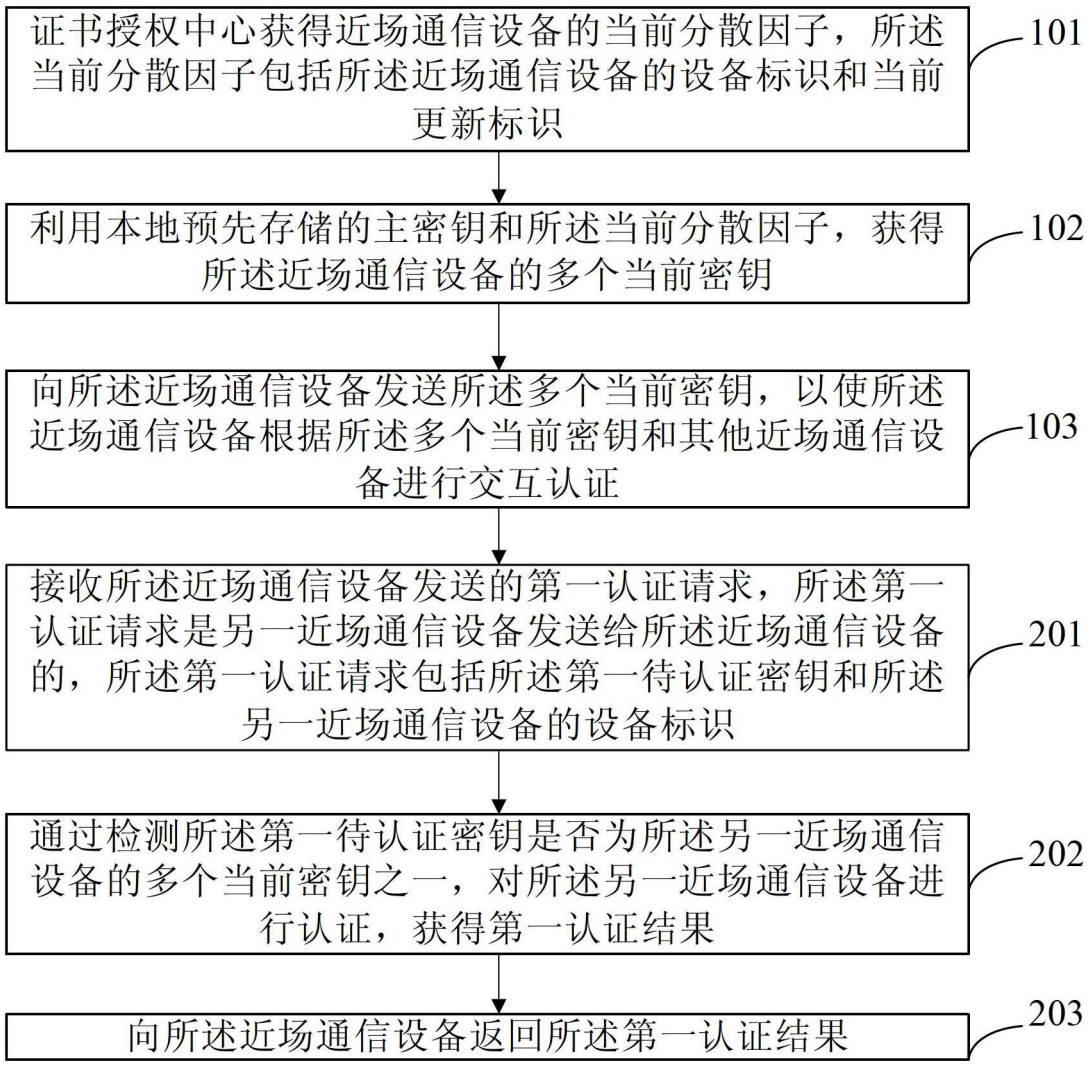

证书授权中心获得近场通信设备的当前分散因子，所述当前分散因子包括所述近场通信设备的设备标识和当前更新标识
101
利用本地预先存储的主密钥和所述当前分散因子，获得所述近场通信设备的多个当前密钥
102
向所述近场通信设备发送所述多个当前密钥，以使所述近场通信设备根据所述多个当前密钥和其他近场通信设备进行交互认证
103
接收所述近场通信设备发送的第一认证请求，所述第一认证请求是另一近场通信设备发送给所述近场通信设备的，所述第一认证请求包括所述第一待认证密钥和所述另一近场通信设备的设备标识
201
通过检测所述第一待认证密钥是否为所述另一近场通信设备的多个当前密钥之一，对所述另一近场通信设备进行认证，获得第一认证结果
202
向所述近场通信设备返回所述第一认证结果
203

图 2

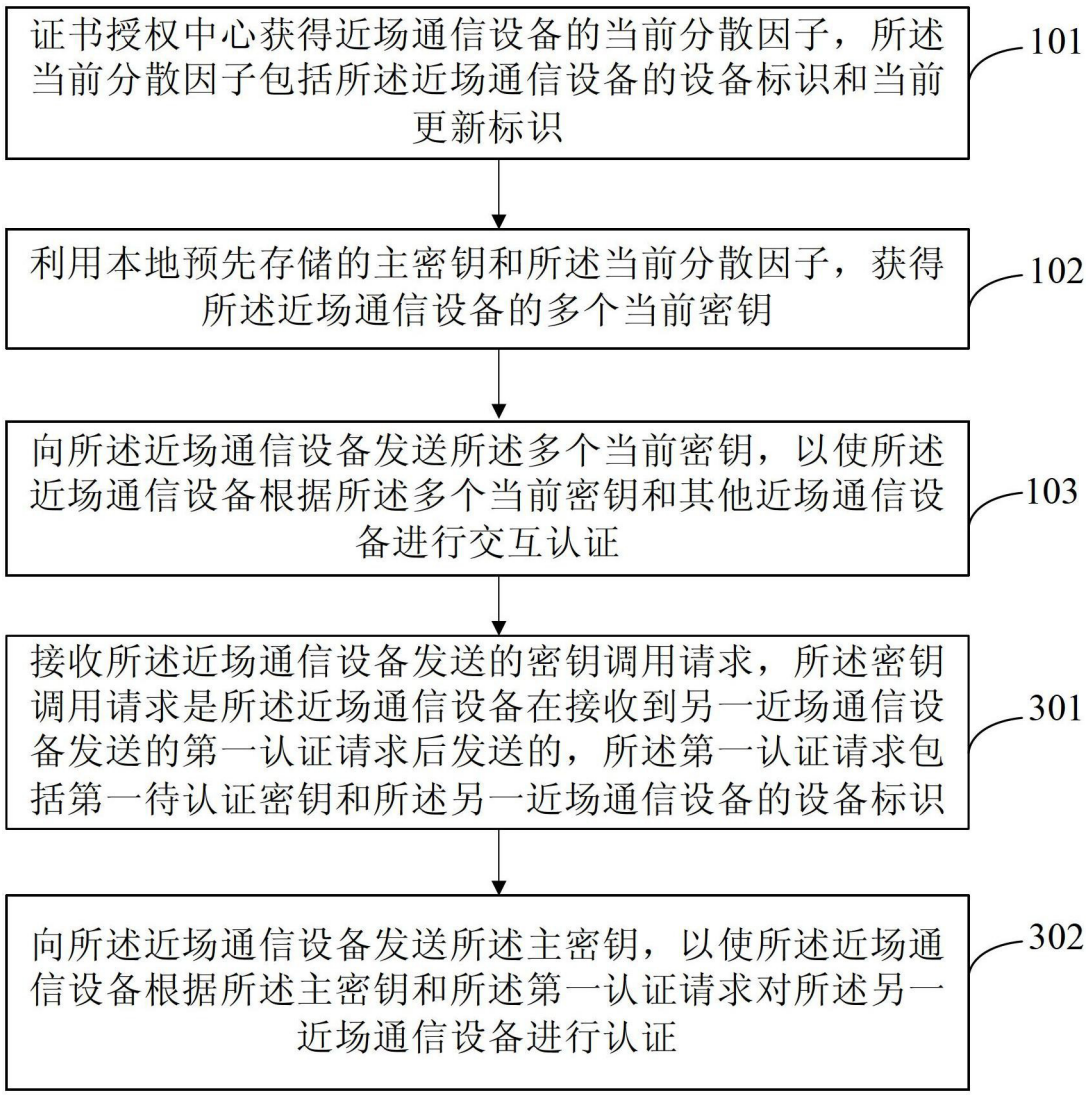

证书授权中心获得近场通信设备的当前分散因子，所述当前分散因子包括所述近场通信设备的设备标识和当前更新标识
101
利用本地预先存储的主密钥和所述当前分散因子，获得所述近场通信设备的多个当前密钥
102
向所述近场通信设备发送所述多个当前密钥，以使所述近场通信设备根据所述多个当前密钥和其他近场通信设备进行交互认证
103
接收所述近场通信设备发送的密钥调用请求，所述密钥调用请求是所述近场通信设备在接收到另一近场通信设备发送的第一认证请求后发送的，所述第一认证请求包括第一待认证密钥和所述另一近场通信设备的设备标识
301
向所述近场通信设备发送所述主密钥，以使所述近场通信设备根据所述主密钥和所述第一认证请求对所述另一近场通信设备进行认证
302

图 3

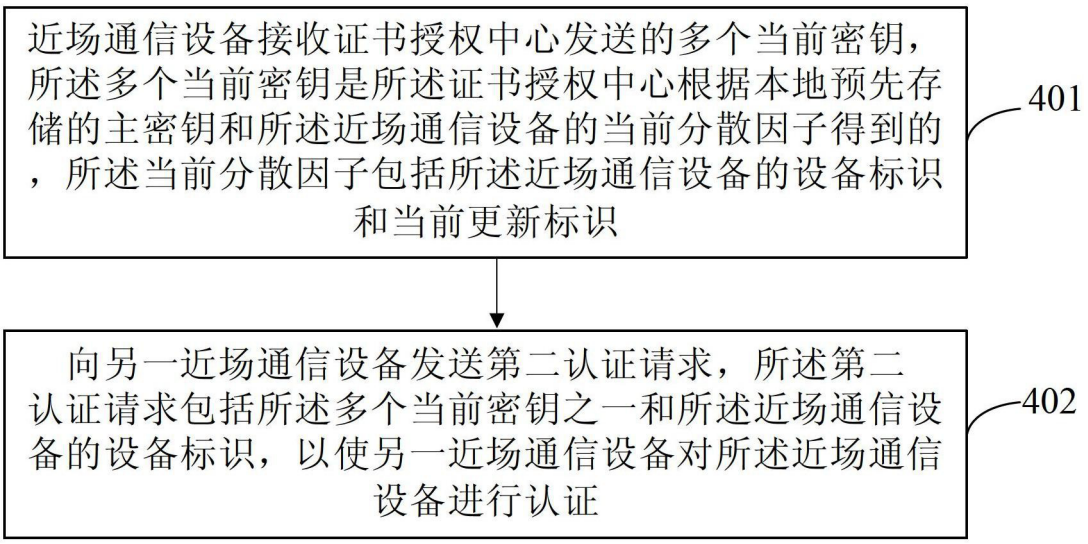

近场通信设备接收证书授权中心发送的多个当前密钥，所述多个当前密钥是所述证书授权中心根据本地预先存储的主密钥和所述近场通信设备的当前分散因子得到的，所述当前分散因子包括所述近场通信设备的设备标识和当前更新标识
401
向另一近场通信设备发送第二认证请求，所述第二认证请求包括所述多个当前密钥之一和所述近场通信设备的设备标识，以使另一近场通信设备对所述近场通信设备进行认证
402

图 4

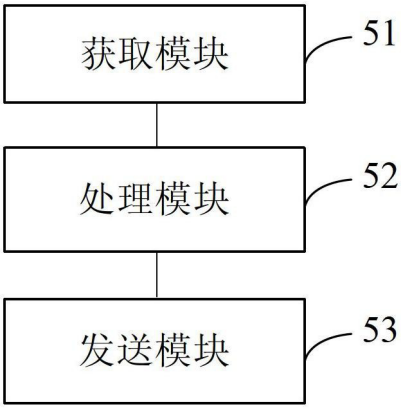

获取模块
51
处理模块
52
发送模块
53

图 5

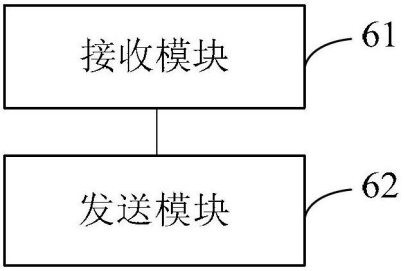

接收模块
61
发送模块
62

图 6