(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 102171970 B
(45)授权公告日 2014.02.26

(21)申请号 201080002786.0
(22)申请日 2010.07.07
(30)优先权数据
2009-171626 2009.07.22 JP
(85)PCT国际申请进入国家阶段日
2011.03.31
(86)PCT国际申请的申请数据
PCT/JP2010/004440 2010.07.07
(87)PCT国际申请的公布数据
WO2011/010432 JA 2011.01.27
(73)专利权人 松下电器产业株式会社
地址 日本大阪府
(72)发明人 张毅波
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 黄剑锋
(51)Int.Cl.
H04L 9/08(2006.01)
G06F 21/30(2013.01)
H04B 3/54(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 101411113 A,2009.04.15, 全文.
US 6570857 B1,2003.05.27, 全文.
JP 特开 2009-94768 A,2009.04.30, 全文.
CN 1522517 A,2004.08.18, 全文.
US 2004/0158333 A1,2004.08.12, 全文.
CN 1838623 A,2006.09.27, 全文.
CN 1496631 A,2004.05.12, 全文.
JP 特开 2008-154133 A,2008.07.03, 全文.
CN 1855865 A,2006.11.01, 全文.

审查员 张攀

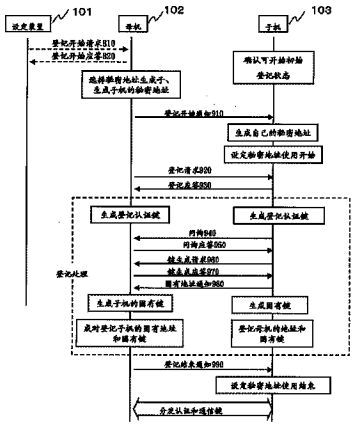
权利要求书4页 说明书17页 附图27页

(54)发明名称

母机及子机

(57)摘要

提供一种用确保安全的方法来登记子机的通信装置。秘密地址生成/设定部生成秘密地址生成子，根据秘密地址生成子和子机的识别信息来生成暂时使用的子机的秘密地址，以代替子机的固有地址。第二通信部通过广播将存储有秘密地址生成子的登记开始通知发送给子机。登记处理部生成登记认证键，在与子机之间发送、接收用登记认证键进行了加密的固有键生成信息，来生成子机的固有键，从子机接收用登记认证键进行了加密的子机的固有地址，并使子机的识别信息、子机的固有地址和子机的固有键相对应之后，保存在登记信息保存部中。



CN 102171970 B

1. 一种母机，管理子机的登记，其特征在于：

该母机包括：

第一通信部，受理所述子机的识别信息的输入；

秘密地址生成 / 设定部，生成每次作为不同值所生成的秘密地址生成符，根据该所生成的秘密地址生成符和所述子机的识别信息，来生成暂时被使用的子机的秘密地址，以代替所述子机的固有地址，所述秘密地址生成符为由所述母机选择的随机数或由随机数与所述母机的 BSSID 所结合的生成符；

第二通信部，与所述子机之间发送、接收与登记处理有关的通知，同时，通过广播将存储有所述秘密地址生成符的登记开始通知发送给所述子机，并且在将与登记处理有关的通知发送给所述子机时，将所述子机的秘密地址记载为所述子机的接收侧地址，将所述母机的固有地址记载为发送源地址；

登记信息保存部，保存所述子机的登记信息；以及

登记处理部，通过生成在对与所述子机之间的通信进行加密时所用的加密密钥即登记认证密钥，并在与所述子机之间发送、接收用该所生成的登记认证密钥进行加密后的固有密钥生成信息，来生成所述子机的固有密钥，并从所述子机接收用所述登记认证密钥或所述子机的固有密钥进行加密后的所述子机的固有地址，使所述子机的识别信息、所述子机的固有地址和所述子机的固有密钥相对应，保存在所述登记信息保存部中。

2. 根据权利要求 1 所述的母机，其特征在于：

所述登记处理部将登记认证密钥生成信息作为登记请求发送给所述子机，从所述子机将登记认证密钥生成信息作为登记应答接收，根据该所发送的登记认证密钥生成信息、该接收到的登记认证密钥生成信息和所述子机的识别信息来生成所述登记认证密钥。

3. 根据权利要求 2 所述的母机，其特征在于：

所述登记处理部通过从所述子机接收问询纯文本，将用所述登记认证 密钥对该接收到的问询纯文本进行加密后的问询密码文发送给所述子机，来确认在所述母机和所述子机之间生成了共通的所述登记认证密钥的情况。

4. 根据权利要求 1 所述的母机，其特征在于：

所述登记处理部从所述子机接收作为密钥生成请求而用所述登记认证密钥进行加密后的固有密钥生成信息，将作为密钥生成应答而用所述登记认证密钥进行加密后的固有密钥生成信息发送给所述子机，根据该接收到的固有密钥生成信息和该所发送的固有密钥生成信息，来生成所述子机的固有密钥。

5. 根据权利要求 4 所述的母机，其特征在于：

所述登记处理部当从所述子机接收所述子机的固有地址被加密后的固有地址通知时，用所述登记认证密钥或所述子机的固有密钥对被加密后的所述子机的固有地址进行解密，使所述子机的识别信息、所述子机的固有地址和所述子机的固有密钥相对应，并保存在所述登记信息保存部中，结束所述子机的登记处理。

6. 根据权利要求 5 所述的母机，其特征在于：

所述登记处理部在被连接在所述母机的所有子机的登记处理结束时，通过广播将结束所述秘密地址的使用的登记结束通知发送给所述子机。

7. 根据权利要求 1 所述的母机，其特征在于：

所述登记处理部判断在所述登记信息保存部中是否存在所述子机的识别信息、所述子机的固有地址及所述子机的固有密钥，当存在有所述子机的识别信息、所述子机的固有地址及所述子机的固有密钥时，在保持有所述子机的识别信息及所述子机的固有地址的状态下仅对所述子机的固有密钥进行更新。

8. 一种子机，连接在管理登记的母机上，其特征在于：

该子机包括：

第二通信部，与所述母机之间发送、接收与登记处理有关的通知，同时，从所述母机接收设定有每次作为不同值所生成的秘密地址生成符的登记开始通知，并在将与登记处理有关的通知发送给所述母机时，将从所述秘密地址生成符所生成的所述子机的秘密地址记载为所述子机的发送源地址，将所述母机的固有地址记载为接收侧地址，所述秘密地址生成符为由所述母机选择的随机数或由随机数与所述母机的 BSSID 所结合的生成符；

秘密地址生成 / 设定部，根据从所述母机接收到的所述秘密地址生成符和所述子机的识别信息来生成暂时被使用的所述子机的秘密地址，以代替所述子机的固有地址；

登记信息保存部，保存与所述母机有关的信息；以及

登记处理部，通过生成在对与所述母机之间的通信进行加密时所用的加密密钥即登记认证密钥，并在与所述母机之间发送、接收使用该所生成的登记认证密钥进行加密后的固有密钥生成信息，来生成所述子机的固有密钥，将用所述登记认证密钥或所述子机的固有密钥进行加密后的所述子机的固有地址发送给所述母机，使所述子机的固有密钥与所述母机的固有地址相对应，保存在所述登记信息保存部中。

9. 根据权利要求 8 所述的子机，其特征在于：

所述登记处理部从所述母机将登记认证密钥生成信息作为登记请求接收，并将登记认证密钥生成信息作为登记应答发送给所述母机，根据该接收到的登记认证密钥生成信息、该所发送的登记认证密钥生成信息和所述子机的识别信息来生成所述登记认证密钥。

10. 根据权利要求 9 所述的子机，其特征在于：

所述登记处理部将随机生成的问询纯文本发送给所述母机，用所述登记认证密钥将从所述母机接收到的问询密码文解密为问询纯文本，在该生成的问询纯文本与该解密后的问询纯文本一致时，确认在所述母机与所述子机之间生成了共通的所述登记认证密钥的情况。

11. 根据权利要求 8 所述的子机，其特征在于：

所述登记处理部将作为密钥生成请求而用所述登记认证密钥进行加密后的固有密钥生成信息发送给所述子机，并从所述母机接收作为密钥生成应答而用所述登记认证密钥进行加密后的固有密钥生成信息，根据该发送的固有密钥生成信息和该接收到的固有密钥生成信息来生成所述子机的固有密钥。

12. 根据权利要求 11 所述的子机，其特征在于：

所述登记处理部当从所述母机接收所述密钥生成应答时，用所述登记认证密钥或所述子机的固有密钥对所述子机的固有地址进行加密，并将设定有该被加密后的所述子机的固有地址的固有地址通知发送给所述母机。

13. 根据权利要求 12 所述的子机，其特征在于：

所述登记处理部使所述子机的固有密钥与所述母机的固有地址相对应并保存在所述

登记信息保存部中。

14. 根据权利要求 13 所述的子机，其特征在于：

所述登记处理部在从所述母机接收到结束所述秘密地址的使用的登记结束通知的时刻，结束所述秘密地址的使用。

15. 根据权利要求 12 所述的子机，其特征在于：

所述登记处理部判断在所述登记信息保存部中是否保存有所述母机的固有地址以及所述子机的固有密钥，在保存有所述母机的固有地址以及所述子机的固有密钥时，判断为所述母机已保持有所述子机的固有地址，不将所述固有地址通知发送给所述母机。

16. 一种方法，是母机管理子机的登记的方法，其特征在于：

所述母机包括保存所述子机的登记信息的登记信息保存部；

所述方法包括如下步骤：

生成每次作为不同值所生成的秘密地址生成符，根据所述秘密地址生 成符和所述子机的识别信息，来生成暂时被使用的子机的秘密地址，以代替所述子机的固有地址的步骤，所述秘密地址生成符为由所述母机选择的随机数或由随机数与所述母机的 BSSID 所结合的生成符，

通过广播将存储有所述秘密地址生成符的登记开始通知发送给所述子机的步骤，

与所述子机之间发送、接收与登记处理有关的通知，同时，在将与登记处理有关的通知发送给所述子机时，将所述子机的秘密地址记载为所述子机的接收侧地址，并将所述母机的固有地址记载为发送源地址的步骤，

生成在对与所述子机之间的通信进行加密时所用的加密密钥即登记认证密钥，并在与所述子机之间发送、接收用该所生成的登记认证密钥进行加密后的固有密钥生成信息的步骤，

从所述子机接收用所述登记认证密钥进行加密后的所述子机的固有地址的步骤，

从所述固有密钥生成信息生成所述子机的固有密钥的步骤，以及

使所述子机的识别信息、所述子机的固有地址和所述子机的固有密钥相对应，并保存在所述登记信息保存部中的步骤。

17. 一种方法，是连接在管理登记的母机上的子机对所述母机进行确认的方法，其特征在于：

所述子机包括保存与所述母机有关的信息的登记信息保存部；

所述方法包括如下步骤：

从所述母机接收设定有每次作为不同值所生成的秘密地址生成符的登记开始通知的步骤，所述秘密地址生成符为由所述母机选择的随机数或由随机数与所述母机的 BSSID 所结合的生成符，

根据从所述母机接收到的所述秘密地址生成符和所述子机的识别信息，来生成暂时被使用的所述子机的秘密地址，以代替所述子机的固有地址的步骤，

在将与登记处理有关的通知发送给所述母机时，将所述子机的秘密地址记载为所述子机的发送源地址，将所述母机的固有地址记载为接收侧地址的步骤，

生成在对与所述母机之间的通信进行加密时所用的加密密钥即登记认证密钥，并在与所述母机之间发送、接收用该所生成的登记认证密钥进行加密后的固有密钥生成信息的步

骤，

将用所述登记认证密钥进行加密后的所述子机的固有地址发送给所述母机的步骤，

生成所述子机的固有密钥的步骤，以及

使所述子机的固有密钥与所述母机的固有地址相对应，并保存在所述登记信息保存部中的步骤。

母机及子机

技术领域

[0001] 本发明涉及能够在通信网络中使通信装置（母机）简单地实现多个通信装置（子机）的登记的技术。

背景技术

[0002] 在无线通信、PLC(Power Line Communications) 通信等通信网络中，一般采用如下方法：为了防止信息泄露到外部，而在已加入到网络中的通信装置与即将加入到网络中的通信装置之间进行共有用于通信中的加密密钥的认证处理，并在认证处理结束后，用该共有的加密密钥加密数据来进行通信。

[0003] 作为认证处理的一个例子，存在有如下例子：用户对请求认证的子机和认证子机的母机双方设定共通的认证密钥，在母机可确认到子机保持有相同认证密钥的情况时，将加密密钥散发给该子机。但是，在该子机不具备从外部受理认证密钥的输入时，由于该子机所保持的认证密钥不能从制造该子机时所设定的认证密钥来改变，因此有可能不能确保安全性。

[0004] 作为解决这样的课题的方法，例如，存在有记载在专利文献 1 和 2 中的技术。专利文献 1 中所记载的技术是通过在规定时间内按下母机和子机各自具有的按钮，来在规定时间内仅在按钮被按下的母机和子机之间进行认证的。但是，专利文献 1 中所记载的技术在同时认证多个子机时，必须要对每台子机重复如下工作：在规定时间内按下母机和子机各自具有的按钮，等待认证结束。由于这样的工作对于用户来说负担较大，因此期望能够减轻负担。

[0005] 专利文献 2 中所记载的技术是将客户的 ID、密码等固有信息预先设定在服务器中，认证时，客户用从服务器所散布的公开密钥加密固有信息并发送给服务器，当服务器接收到的固有信息与预先所设定的信息一致时确认客户。但是，专利文献 2 中所记载的技术中存在这样的问题：在网络上在客户与服务器之间存在中间者，在该中间者对服务器的公开密钥进行窜改时不能确保安全性。并且，由于在使用公开密钥方式时，加密、解密的处理所需的时间与共通密钥加密方式相比较长，因此在与 CPU 能力较低的多个子机进行认证时，认证所有子机所需的时间变长。

[0006] 先行技术文献

[0007] 专利文献

[0008] 专利文献 1：日本特开 2003-377072 号公报

[0009] 专利文献 2：日本特开平 7 － 325785 号公报

发明概要

[0010] 发明要解决的问题

[0011] 在节约用户的设定时间而谋求便利性的同时，为了缩短子机的认证所需的时间，还可想到这样的方法：将子机的 MAC 地址预先登记在母机中，在认证请求从子机发送到母

机时，如果认证请求中所含的子机的 MAC 地址与预先登记的地址一致，则母机许可子机的认证请求。但是，存在如下课题：由于 MAC 地址是作为子机发送通常的包的发送源地址信息所记载的信息，只要是位于可接收该包的位置的通信装置，都能取得，因此难以避免冒充等情况，不能确保安全性。

[0012] 发明内容

[0013] 因此，本案是鉴于上述状况的发明，目的在于：提供一种当在母机管理多个子机的网络中一次增设多个子机时，可谋求用户的便利性，短时间且可确保安全性的子机的登记处理。

[0014] 用于解决问题的手段

[0015] 本发明面向管理子机的登记的母机。并且，为了达到上述目的，本发明的一方式所涉及的母机包括：第一通信部，受理子机的识别信息的输入；秘密地址生成 / 设定部，生成每次作为不同值所生成的秘密地址生成符，根据该所生成的秘密地址生成符和子机的识别信息，来生成暂时被使用的子机的秘密地址，以代替子机的固有地址；第二通信部，与子机之间发送、接收与登记处理有关的通知，同时，通过广播将设定有秘密地址生成符的登记开始通知发送给子机，并且在将与登记处理有关的通知发送给子机时，将子机的秘密地址记载为子机的接收侧地址，将母机的固有地址记载为发送源地址；登记信息保存部，保存子机的登记信息；以及登记处理部，通过生成在对与子机之间的通信进行加密时所用的加密密钥即登记认证密钥，并在与子机之间发送、接收用该所生成的登记认证密钥进行加密后的固有密钥生成信息，来生成子机的固有密钥，并从子机接收用登记认证密钥或子机的固有密钥进行加密后的子机的固有地址，使子机的识别信息、子机的固有地址和子机的固有密钥相对应，保存在登记信息保存部中。

[0016] 优选的是，登记处理部将登记认证密钥生成信息作为登记请求发送给子机，从子机将登记认证密钥生成信息作为登记应答接收，根据该所发送的登记认证密钥生成信息、该接收到的登记认证密钥生成信息和子机的识别信息来生成登记认证密钥。

[0017] 登记处理部通过从子机接收问询纯文本，将用登记认证密钥对该接收到的问询纯文本进行加密后的问询密码文发送给子机，来确认在母机和子机之间生成了共通的登记认证密钥的情况。

[0018] 登记处理部从子机接收作为密钥生成请求而用登记认证密钥进行加密后的固有密钥生成信息，将作为密钥生成应答而用登记认证密钥进行加密后的固有密钥生成信息发送给子机，根据该接收到的固有密钥生成信息和该所发送的固有密钥生成信息，来生成子机的固有密钥。

[0019] 登记处理部当从子机接收子机的固有地址被加密后的固有地址通知时，用登记认证密钥或子机的固有密钥对被加密后的子机的固有地址进行解密，使子机的识别信息、子机的固有地址和子机的固有密钥相对应，并保存在登记信息保存部中，结束子机的登记处理。

[0020] 登记处理部在被连接在母机的所有子机的登记处理结束时，通过广播将结束秘密地址的使用的登记结束通知发送给子机。

[0021] 登记处理部判断在登记信息保存部中是否存在子机的识别信息、子机的固有地址及子机的固有密钥，当存在有子机的识别信息、子机的固有地址及子机的固有密钥时，在保

持有子机的识别信息及子机的固有地址的状态下仅对子机的固有密钥进行更新。

[0022] 并且，本发明还面向连接在管理登记的母机上的子机。并且，为了达到上述目的，本发明的子机包括：第二通信部，与母机之间发送、接收与登记处理有关的通知，同时，从母机接收设定有每次作为不同值所生成的秘密地址生成符的登记开始通知，并在将与登记处理有关的通知发送给母机时，将从秘密地址生成符所生成的子机的秘密地址记载为子机的发送源地址，将母机的固有地址记载为接收侧地址；秘密地址生成 / 设定部，根据从母机接收到的秘密地址生成符和子机的识别信息来生成暂时被使用的子机的秘密地址，以代替子机的固有地址；登记信息保存部，保存与母机有关的信息；以及登记处理部，通过生成在对与母机之间的通信进行加密时所用的加密密钥即登记认证密钥，并在与母机之间发送、接收使用该所生成的登记认证密钥进行加密后的固有密钥生成信息，来生成子机的固有密钥，将用登记认证密钥或子机的固有密钥进行加密后的子机的固有地址发送给母机，使子机的固有密钥与母机的固有地址相对应，保存在登记信息保存部中。

[0023] 登记处理部从母机将登记认证密钥生成信息作为登记请求接收，并将登记认证密钥生成信息作为登记应答发送给母机，根据该接收到的登记认证密钥生成信息、该所发送的登记认证密钥生成信息和子机的识别信息来生成登记认证密钥。

[0024] 登记处理部将随机生成的问询纯文本发送给母机，用登记认证密钥将从母机接收到的问询密码文解密为问询纯文本，在该生成的问询纯文本与该解密后的问询纯文本一致时，确认在母机与子机之间生成了共通的登记认证密钥的情况。

[0025] 登记处理部将作为密钥生成请求而用登记认证密钥进行加密后的固有密钥生成信息发送给子机，并从母机接收作为密钥生成应答而用登记认证密钥进行加密后的固有密钥生成信息，根据该发送的固有密钥生成信息和该接收到的固有密钥生成信息来生成子机的固有密钥。

[0026] 登记处理部当从母机接收所述密钥生成应答时，用登记认证密钥或子机的固有密钥对子机的固有地址进行加密，并将存储有该被加密后的子机的固有地址的固有地址通知发送给母机。

[0027] 登记处理部使子机的固有密钥与母机的固有地址相对应并保存在登记信息保存部中。

[0028] 登记处理部在从母机接收到结束秘密地址的使用的登记结束通知的时刻，结束秘密地址的使用。

[0029] 登记处理部判断在登记信息保存部中是否保存有母机的固有地址以及子机的固有密钥，在保存有母机的固有地址以及子机的固有密钥时，判断为母机已保持有子机的固有地址，不将固有地址通知发送给母机。

[0030] （发明的效果）

[0031] 根据上述方式，在新增设子机时，仅对母机输入各子机的识别信息，就能够进行子机的登记处理，将子机连接在已设置的网络上。并且，即使在子机的登记处理后的子机的认证处理中，由于使用共通加密密钥（固有密钥），因此即使在登记对象子机的台数较多的情况下，仍能够在短时间内完成子机的认证。

附图说明

[0032] 图 1 是表示本发明的 PLC 网络的系统结构的图；

[0033] 图 2 是表示母机 102 的物理结构的方块图；

[0034] 图 3 是表示子机 103 的物理结构的方块图；

[0035] 图 4 是表示母机 102 的功能结构的方块图；

[0036] 图 5 是表示子机 103 的功能结构的方块图；

[0037] 图 6 是表示整个登记处理的流程的序列图；

[0038] 图 7 是表示详细的初始登记处理的序列图；

[0039] 图 8 是表示设定装置 101 与母机 102 之间所交换的外部指令的格式的图；

[0040] 图 9 是表示在母机 102 与子机 103 之间所交换的消息的格式的图；

[0041] 图 10 是表示母机 102 所执行的初期登记处理的流程图；

[0042] 图 11 是表示子机 103a ～ 103n 所执行的初期登记处理的流程图；

[0043] 图 12 是表示详细的第一再登记处理的序列图；

[0044] 图 13 是表示登记开始通知 1310 的格式的图；

[0045] 图 14 是表示母机 102 所执行的第一再登记处理的流程图；

[0046] 图 15 是表示子机 103a ～ 103n 所执行的第一再登记处理的流程图；

[0047] 图 16 是表示详细的第二再登记处理的流程图；

[0048] 图 17 是表示登记开始请求 1710 的格式的图；

[0049] 图 18 是表示登记请求 1810 的格式的图；

[0050] 图 19 是表示母机 102 所执行的第二再登记处理的流程图；

[0051] 图 20 是表示子机 103a ～ 103n 所执行的第二再登记处理的流程图；

[0052] 图 21 是表示母机 102 所执行的初期登记处理的流程图；

[0053] 图 22 是表示子机 103a ～ 103n 所执行的初期登记处理的流程图；

[0054] 图 23 是表示母机 102 所执行的第一再登记处理的流程图；

[0055] 图 24 是表示子机 103a ～ 103n 所执行的第一再登记处理的流程图；

[0056] 图 25 是表示母机 102 所执行的第二再登记处理的流程图；

[0057] 图 26 是表示子机 103a ～ 103n 所执行的第二再登记处理的流程图；

[0058] 图 27 是表示母机 102 的功能块图；

[0059] 图 28 是表示子机 103 的功能块图；

[0060] 图 29 是表示在无线通信网络中进行设定时的系统结构的图；

[0061] 图 30 是表示在 PLC 网络与无线通信网络结合后的网络中进行设定时的系统结构的图。

具体实施方式

[0062] 以下，在参照附图的同时，对由本发明的各个实施例所涉及的通信装置（母机及子机）所构成的网络进行说明。另外，在本发明中，进行如下处理：首先，在母机与子机之间共有最初按照子机固有生成的固有密钥，其次，在母机与子机之间共有在母机正在管理的网路中所用的通信密钥。以下，将为了在母机与子机之间使固有密钥共通化而进行的处理称为登记处理，将为了在结束了固有密钥的共有的母机与子机之间共有通信密钥所进行的处理称为认证处理。

[0063] (1) 系统结构

[0064] 图 1 为表示本发明的 PLC 网络的系统结构的图。在图 1 中，本实施方式中的 PLC 网络由设定装置 101（例如，PC 或 IC 读卡器 / 打字机）、母机 102 及多个子机 103a ～ 103n 构成。

[0065] 设定装置 101 和母机 102 通过 Ethernet（注册商标）或近距离无线相连接，通过经由 Ethernet（注册商标）或近距离无线的通信交换与登记处理有关的规定的外部指令。另外，通过其它方法来保证在设定装置 101 与母机 102 之间所进行的外部指令的交换时的通信安全性。并且，也可以通过上述以外的通信，例如，USB(Universal Serial Bus) 等连接设定装置 101 和母机 102。

[0066] 母机 102 和各子机 103a ～ 103n 之间通过电灯线连接，利用经由电灯线的通信，进行与登记处理及认证处理有关的消息交换、数据传输。对母机 102 及子机 103a ～ 103n 分别设定有固定的固有地址。母机 102 和各子机 103a ～ 103n 能够通过发送包，来判断该包是在哪一终端之间进行的通信的包，该包是将自终端的固有地址及作为通信对象的终端的固有地址分别记载为发送源地址及目的地的包。作为固有地址，例如，能够利用 MAC 地址。

[0067] (2) 装置的结构

[0068] 图 2 为表示母机 102 的物理结构的图。在图 2 中，母机 102 包括 CPU201、存储部 202、以太 I / F203 和 PLC I / F204。另外，母机 102 也可以代替以太 I / F，包括近距离无线 I / F。母机 102 用 CPU201 执行被存储在存储部 202 中的程序，经由与 Ethernet（注册商标）连接的以太 I / F203 与设定装置 101 之间进行通信，经由与 PLC 网络连接的 PLC I / F204 与子机 103a ～ 103n 之间进行通信。

[0069] 图 3 为表示子机 103 的物理结构的方块图。在图 3 中，子机 103 包括 CPU301、存储部 302 及 PLC I / F303。子机 103 用 CPU301 执行被存储在存储部 302 中的程序，经由与 PLC 网络连接的 PLC I / F303 与母机 102 进行通信。另外，在图 3 所示的例子中，子机 103 虽为不包括以太 I / F 的结构，但也可以为与母机 102 一样包括以太 I / F 的结构。以下，将子机 103a ～ 103n 的总称记为子记 103。

[0070] （第一实施方式）

[0071] 在第一实施方式中，对在母机 102 与子机 103a ～ 103n 之间进行的登记处理进行说明。图 4 为用与图 2 中的物理结构相对应的方式来表示母机 102 所具有的功能的功能方块图。在图 4 中，CPU201 具有登记处理部 401、秘密地址生成 / 设定部 404 的功能。存储部 202 具有登记信息保存部 405 的功能。以太 I / F203 具有第一通信部 407 的功能。PLC I / F204 具有第二通信部 408 的功能。登记信息保存部 405 保存被登记的子机 103 的固有地址、固有密钥（即，子机 103 的登记信息）。

[0072] 登记处理部 401 对经由第一通信部 407 所输入的指令进行处理，根据处理结果来经由第一通信部 407 进行应答。并且，登记处理部 401 用秘密地址生成 / 设定部 404 来生成子机 103 的秘密地址。被生成的子机 103 的秘密地址在之后的登记处理中作为送给子机 103 的消息的目的地而被使用。登记处理结束后，登记处理部 401 将子机 103 的固有地址、固有密钥等保存在登记信息保存部 405 中。这里，子机的秘密地址是代替子机的固有地址而暂时使用的地址。秘密地址生成 / 设定部 404 生成子机 103 的秘密地址，并通知给登记处理部 401。

[0073] 图 5 为以与图 3 中的物理结构相对应的方式表示子机 103 所具有的功能的功能方块图。在图 5 中，CPU301 具有登记处理部 501 以及秘密地址生成 / 设定部 503 的功能。存储部 302 具有登记信息保存部 504 的功能。PLCI / F303 具有第二通信部 506 的功能。登记信息保存部 504 保存有母机 102 的固有地址、识别信息（例如，BSSID）以及自身的固有密钥。

[0074] 登记处理部 501 对从母机 102 经由第二通信部 506 所接收到的与登记有关的消息（后述）进行解析处理。并且，秘密地址生成 / 设定部 503 生成自身的秘密地址并通知给登记处理部 501。登记处理部 501 将秘密地址生成 / 设定部 503 所生成的自身的秘密地址设定在第二通信部 506。子机 103 在登记处理中代替固有地址而将该秘密地址作为自己的发送、接收地址使用。登记处理结束后，登记处理部 501 将母机 102 的固有地址、识别信息（例如，BSSID）以及自己的固有密钥等保存在登记信息保存部 504 中。

[0075] (3) 关于登记处理的概要

[0076] 其次，在图 6、图 8、图 9 中，对登记处理的概要进行说明。图 6 为表示登记处理的整个流程的序列图。并且，图 8 为表示在设定装置 101 与母机 102 之间被交换的外部指令的格式的图。图 9 为表示在母机 102 与子机 103 之间被交换的与登记处理有关的消息的格式的图。

[0077] 参照图 6，设定装置 101 在从用户输入包含进行登记的子机 103a ～ 103n 的识别信息的登记对象子机表时，根据登记对象子机表来将子机的信息表存储在登记开始请求 810 中并发送给母机 102。对于设定装置 101 所进行的登记对象子机表的输入既可以是用户直接输入，也可以通过扫描装置、近距离无线装置等来进行输入。这里，子机的识别信息为子机的固有地址以外的固有信息，例如，为子机制造号、子机品号 + 制造号、PIN(Personal Identification Number) 等。

[0078] 母机 102 根据含在登记开始请求 810 中的子机的信息表 814，生成登记开始通知 910，并通过广播将登记开始通知 910 发送给子机 103a ～ 103n。然后，母机 102 对于含在子机的信息表 814 中的各个子机 103a ～ 103n 依次发送登记请求 920，并分别对子机 103 进行登记处理，取得各个子机的固有地址，同时共有固有密钥。母机 102 在与含在子机的信息表 814 中的所有子机 103 之间结束登记处理后，将登记结束通知 990 发送给子机 103a ～ 103n。

[0079] 母机 102 当从设定装置 101 接收登记结果取得请求时，将包含子机的固有地址、固有密钥等的登记结束子机表转送给设定装置 101。设定装置 101 将从母机 102 接收到的登记结束子机表保存在外部存储装置中，在进行再登记时使用。并且，母机 102 在登记处理中当从设定装置 101 送来进展状态确认请求时，向设定装置 101 应答该时点的登记处理的进展状态。

[0080] (4) 初始登记方法

[0081] 图 7 为表示初始登记处理的详细情况的序列图。这里，初始登记是指以没有完成登记的子机 103（即，在登记信息保存部 504 中没有登记信息的子机 103）为对象所实施的登记处理。图 10 为表示母机 102 所执行的初始登记处理的流程图。图 11 为表示子机 103a ～ 103n 所执行的初始登记处理的流程图。

[0082] 以下，用图 7、图 10 及图 11 对初始登记方法进行详细说明。

[0083] 参照图 7，母机 102 在从设定装置 101 接收登记开始请求 810 时，对是否已处于登

记处理中、可登记的子机的台数是否已满、含在子机的信息表 814 中的子机 103 是否已被登记、或子机 103 的识别信息是否异常等进行确认，并将确认结果存储在登记开始应答 820 中发送给设定装置 101。母机 102 在可执行登记执行类型中所指定的初始登记，且子机的信息表没有异常时，开始以下的初始登记处理。

[0084] 在步骤 S1001（参照图 10）中，母机 102 根据含在登记开始请求 810 的子机的信息表 814 中的各个子机的识别信息，来选择秘密地址生成符及生成子机的秘密地址（在后说明其方法，以下一样）。

[0085] 在步骤 S1101（参照图 11）中，子机 103a ～ 103n 在确认自身与母机 102 的登记处理没有结束，且与其它母机不处于登记处理中的状态之后，等待来自母机 102 的登记开始通知 910。

[0086] 在步骤 S1002（参照图 10）中，母机 102 通过广播将存储有秘密地址生成符 913 等的登记开始通知 910（参照图 9）发送给子机 103a ～ 103n。另外，也可将被存储在登记开始通知 910 中的这些信息总称为秘密地址生成信息。

[0087] 在步骤 S1102（参照图 11）中，子机 103a ～ 103n 接收来自母机 102 的登记开始通知 910。然后，在步骤 S1103（参照图 11）中，子机 103a ～ 103n 从所接收到的登记开始通知 910 读取秘密地址生成符 913，并根据该读取的秘密地址生成符 913 和自身的识别信息来生成自身的秘密地址。然后，子机 103a ～ 103n 进行该生成了的秘密地址的使用开始设定。

[0088] 在步骤 S1003（参照图 10）中，母机 102 对在子机的信息表 814 中所记载的子机中的还没有完成登记处理的子机的台数进行确认，当没有完成登记处理的子机的台数为 0 时，转移到步骤 S1014，当没有完成登记处理的子机的台数在 1 以上时，转移到步骤 S1004。

[0089] 在步骤 S1004（参照图 10）中，母机 102 从子机的信息表 814 取得其次进行登记处理的子机的信息。这里，假设取得了子机 103a ～ 103n 中的子机 103a 的信息。在步骤 S1005（参照图 10）中，母机 102 将在步骤 S1004 中取得了信息的子机 103a 的秘密地址记载为目的地，并发送存储有登记认证密钥生成算法编号 922、密码算法编号 923 以及登记认证密钥生成符 A924 的登记请求 920（参照图 9），该登记认证密钥生成算法编号 922 表示用于生成登记认证密钥的算法，该密码算法编号 923 表示用于使登记处理中的消息加密的算法，该登记认证密钥生成符 A924 为用于生成登记认证密钥的信息。

[0090] 这里，登记认证密钥被用作对与子机 103 之间的通信进行加密的加密密钥。并且，对于登记认证密钥生成算法编号 922 例如设定表示母机 102 和子机 103 事先所共有的登记认证密钥生成算法的种类的号码。对于密码算法编号 923 例如设定表示母机 102 和子机 103 事先所共有的密码算法的种类的号码。并且，对于登记认证密钥生成符 A924 设定任意值（也可以为随机数）。也可将被存储在登记请求 920 中的这些信息总称为登记认证密钥生成信息。

[0091] 在步骤 S1104（参照图 11）中，子机 103a 对自身的秘密地址被作为目的地记载的登记请求 920 进行接收。其次，在步骤 S1105 中，子机 103a 对所接收到的登记请求 920（参照图 9）中的各个字段的内容进行确认，在没有异常时，将登记认证密钥生成符 B933 存储在登记应答 930（参照图 9）中，并发送给母机 102。这里，对于登记认证密钥生成符 B933 设定任意值（也可以为随机数）。并且，也可以将被存储在登记应答 930 中的这些信息总称为登记认证密钥生成信息。

[0092] 在步骤 S1006（参照图 10）中，母机 102 对子机 103a 所发送的登记应答 930（参照图 9）进行接收，并转移到步骤 S1007。另外，在步骤 S1006 中，母机 102 也可以确认登记应答 930 中的各个字段的内容，当有异常时，中止子机 103a 的登记处理，返回到步骤 S1003，从子机的信息表 814 取得其次进行登记处理的子机的信息，并将登记请求 920 发送给该子机。在步骤 S1007（参照图 10）中，母机 102 利用通过登记认证密钥生成算法编号 922 所指定的登记认证密钥生成算法来从登记认证密钥生成符 A924 和登记认证密钥生成符 B933 生成登记认证密钥。

[0093] 在步骤 S1106（参照图 11）中，子机 103a 利用登记认证密钥生成算法编号 922 所指定的登记认证密钥生成算法来从登记认证密钥生成符 A924 和登记认证密钥生成符 B933 生成登记认证密钥。在步骤 S1107（参照图 11）中，子机 103a 将存储有问询纯文本 942 的问询 940（参照图 9）发送给母机 102，该问询纯文本 942 用于判断母机 102 和子机 103a 是否生成了共通的登记认证密钥，为随机所生成的文本数据。

[0094] 在步骤 S1008（参照图 10）中，母机 102 接收从子机 103a 所发送的问询 940，并用登记认证密钥和通过密码算法编号 923 所指定的密码算法来对该接收到的问询 940 中的问询纯文本 942 进行加密。其次，在步骤 S1009（参照图 10）中，母机 102 将问询应答 950（参照图 9）发送给子机 103a，该问询应答 950 为存储有被加密的问询密码文 952 的问询应答。

[0095] 在步骤 S1108（参照图 11）中，子机 103a 接收母机 102 所发送的问询应答 950。子机 103a 通过登记认证密钥用由密码算法编号 923 所指定的密码算法来对所接收到的问询应答 950 中的问询密码文 952 进行解密，将该被解密的问询密码文 952 与自己发送给母机 102 的问询纯文本 942 进行对照，确认被解密的问询密码文 952 与问询纯文本 942 是否一致。

[0096] 在确认对照的结果之后，子机 103a 转移到步骤 S1109，将存储有固有密钥生成算法 962 和固有密钥生成符 A963 的密钥生成请求 960（参照图 9）发送给母机 102。这里，对固有密钥生成算法编号 962 设定例如表示母机 102 与子机 103 事先共有的固有密钥生成算法的种类的号码。并且，对固有密钥生成符 A963 设定任意值（也可以是随机数）。也可以将存储在密钥生成请求 960 的这些信息总称为固有密钥生成信息。另外，在步骤 S1108 中，子机 103a 在对照的结果是被解密的问询密码文 952 与问询纯文本 942 不一致时，也可以中止登记处理，转移到步骤 S1115。

[0097] 在步骤 S1010（参照图 10）中，母机 102 从子机 103a 接收密钥生成请求 960，并转移到步骤 S1011。另外，在步骤 S1010 中，母机 102 也可以确认所接收到的密钥生成请求 960 中的各字段，在有异常时，中止子机 103a 的登记处理，返回到步骤 S1003，并从子机的信息表 814 取得其次进行登记处理的子机的信息，将登记请求 920 发送给该子机。在步骤 S1011 中，母机 102 将存储有固有密钥生成符 B973 等的密钥生成应答 970（参照图 9）发送给子机 103。这里，对固有密钥生成符 B973 设定任意值（也可以为随机数）。另外，在密钥生成应答 970 中也可以进一步存储表示可否生成固有密钥的固有密钥生成可否标志 972。并且，也可以将存储在密钥生成应答 970 中的这些信息总称为密钥生成信息。

[0098] 在步骤 S1110（参照图 11）中，子机 103a 接收密钥生成应答 970。其次，在步骤 S1111（参照图 11）中，子机 130a 用登记认证来使自身的固有地址加密，并将存储有该被加密的固有地址 982 的固有地址通知 980（参照图 9）发送给母机 102。

[0099] 在步骤S1012(参照图10)中,母机102接收子机103a所发送的固有地址通知980,并用登记认证密钥对存储在该接收到的固有地址通知980的子机103a的固有地址进行解密。另外,在步骤S1012中,母机102也可以在不能准确接收到固有地址通知980时,中止子机103a的登记处理,返回到步骤S1003,从子机的信息表814取得其次进行登记处理的子机的信息,将登记请求920发送给该子机。

[0100] 在步骤S1013(参照图10)中,母机102根据固有密钥生成符A963和固有密钥生成符B973,用被指定的固有密钥生成算法来生成子机103的固有密钥,并使该生成的固有密钥与子机103的固有地址或识别信息相对应,保存在登记信息保存部405中。母机102在多个子机被设定在子机的信息表814中时,对于所有子机,反复进行从步骤S1003到步骤S1013为止的登记处理。其次,在步骤S1014(参照图10)中,母机102在所有子机的登记处理结束时,用广播将登记结束通知990(参照图9)发送给子机103a～103n,结束初始登记处理。

[0101] 在步骤S1113(参照图11)中,子机103根据固有密钥生成符A963和固有密钥生成符B973,用被指定的固有密钥生成算法来生成子机103的固有密钥,使该所生成的固有密钥与母机102的固有地址相对应,保存在登记信息保存部504中。另外,子机103a也可以在步骤S1113的固有密钥生成处理之后执行步骤S1111的固有密钥通知发送处理,用固有密钥对自身的固有地址进行加密,将存储有该被加密的固有地址982的固有地址通知980(参照图9)发送给母机102。

[0102] 在步骤S1114(参照图11)中,子机103从母机102接收登记结束通知990。在步骤S1115(参照图11)中,子机103a在从母机102接收到登记结束通知990的时点设定秘密地址使用结束,来结束初始登记处理。以上内容是在母机102与子机103a～103n之间所进行的初始登记处理的一个例子。

[0103] 另外,母机102也可以在与所有子机103a～103n的登记处理结束后,将所有子机103a～103n的固有密钥和固有地址或识别信息一起保存在登记信息保存部405中。

[0104] 并且,在步骤S1115(参照图11)中,子机103a可以在从母机102接收到登记结束通知990的时点结束秘密地址的使用,也可以代替它,构成为在与母机102之间结束了登记处理的时点结束秘密地址的使用。并且,子机103a也可以构成为当从登记开始通知的接收开始经过规定时间,发生超时时,结束秘密地址的使用。并且,也可以将这些判断组合在一起使用。例如,子机103a也可以构成为在发生了如下情况的任一情况时,结束秘密地址的使用,所述如下情况为:从母机102接收登记结束通知990,或从登记开始通知的接收开始经过规定时间,发生超时。

[0105] 并且,用登记请求920中的登记认证密钥生成算法编号922所指定的登记认证密钥的生成算法和用密钥生成请求960中的固有密钥生成算法编号962所指定的固有密钥的生成算法既可以用公开的密钥生成算法,也可以用未公开的密钥生成算法。作为被公开的密钥生成算法的一个例子,能够举出Diffie－Hellman算法。而且,也可以通过子机的制造号或含在产品编号中的信息来对子机进行范畴划分,以范畴的不同,来使用不同的密钥生成算法,或生成不同密钥长度的加密密钥。

[0106] (5)第一再登记处理

[0107] 以下,对在初始登记处理结束了的子机103与母机102之间所进行的第一再登记

处理进行说明。图 12 为表示第一再登记处理的详细情况的序列图。这里，第一再登记处理是在与已登记结束的子机（即，登记信息保持在登记信息保存部 504 的子机）之间所进行的登记处理。例如，在母机 102 因故障而进行交换或恢复（登记信息损坏）时等施行第一再登记处理。以下，将交换及故障前的母机记为源母机。

[0108] 参照图 12，母机 102 在从设定装置 101 接收登记开始请求 810 时，确认是否已处于登记处理中，可进行登记的子机的台数是否已满，含在子机的信息表 814 中的子机是否已被登记，或者该子机的识别信息中是否有异常等，并将确认结果存储在登记开始应答 820 中，发送给设定装置 101。但是，与初始登记处理时不同，第一再登记处理中的登记开始请求 810 作为子机的信息表 814，并不仅是子机的识别信息，还含有子机的固有地址和固有密钥。母机 102 能够执行在登记执行类型 811 中所指定的再登记，并且在子机的信息表 814 中没有异常时，开始第一再登记处理。

[0109] 图 14 为表示母机 102 所执行的第一再登记处理的流程图。图 15 为表示子机 103a ～ 103n 所执行的第一再登记处理的流程图。在图 14 中，对第一再登记处理中与初始登记处理相同的处理标注与图 10 相同的符号。图 14 的第一再登记处理中与初始登记处理不同之处在于 :进行步骤 S1401 来代替步骤 S1002。

[0110] 在图 15 中，对与第一再登记处理中与初始登记处理相同的处理标注与图 10 相同的符号。图 15 的第一再登记处理中与初始登记处理不同之处在于 :进行步骤 S1501 来代替步骤 S1101，进行步骤 S1502 来代替步骤 S1102，在步骤 S1502 之后追加步骤 S1503。

[0111] 图 13 为表示在第一再登记处理中母机 102 与子机 103 之间被交换的消息中登记开始通知 1310 的格式的图。有关其它消息，由于为与初始登记时被交换的消息的格式相同，因此省略附图。

[0112] 以下，仅对第一再登记处理中与初始登记处理不同的处理进行说明，省略其它处理的说明。在步骤 1401（参照图 14）中，母机 102 用广播将登记开始通知 1310（参照图 13）发送给子机 103a ～ 103n，该登记开始通知 1310 存储有秘密地址生成符 1313、源母机的固有地址 1314 和登记结束证明信息 1315。这里，登记结束证明信息 1315 用于证明母机 102 的正当性。另外，在本实施方式中，作为登记结束证明信息 1315，对登记开始通知 1310 前方的各个字段计算单向函数（例如，Hash 函数），并且对用各子机的固有密钥进行加密后的信息，仅存储子机 103a ～ 103n 的台数。

[0113] 在步骤 S1501（参照图 15）中，子机 103a ～ 103n 自身已结束登记处理，并且在对检测出母机 102 故障之后被交换或被恢复的状态进行了确认之后，等待接收来自母机 102 的登记开始通知 1310。在步骤 S1502（参照图 15）中，子机 103a ～ 103n 从母机 102 接收登记开始通知 1310。

[0114] 接着，在步骤 S1503（参照图 15），子机 103 根据所接收到的登记开始通知 1310，与母机 102 一样计算单向函数，用自身的固有密钥生成登记结束证明信息，并且确认在登记开始通知 1310 中是否包含与自身所生成的登记结束证明信息一致的信息。子机 103 在不包含与自身所生成的登记结束证明信息一致的信息时，将母机 102 判断为不正当，无视所接收到的登记开始通知 1310，结束再登记处理。

[0115] 而在步骤 S1503（参照图 15）中，子机 103 在包含与自身所生成的登记结束证明信息一致的信息时，将母机 102 判断为正当，转移到步骤 S1103，根据含在登记开始通知 1310

中的秘密地址生成符 1313 来生成自身的秘密地址，设定该所生成的秘密地址的使用。关于其它处理，由于与初始登记处理相同，因此在此省略说明。

[0116] 另外，母机 102 也可以是在登记信息保存部 405 中存在有子机 103 的识别信息、子机 103 的固有地址和子机 103 的固有密钥时，也可以在保持子机 103 的识别信息和子机 103 的固有地址的状态下仅更新子机 103 的固有密钥的装置。并且，在从设定装置 101 输入到母机 102 的子机的信息表中包含子机的固有地址（或在子机 103 的登记信息保存部 504 中保存有母机 102 的固有地址及子机的固有密钥）时，由于母机 102 已保有子机的固有地址，因此子机 103 也可以进行步骤 S1111 的处理。像这样，根据本实施方式，能够简单地进行通过母机 102 的交换等再登记处理。

[0117] (6) 第二再登记处理

[0118] 也可以代替第一再登记处理使用以下所说明的第二再登记处理。图 16 为表示第二再登记处理的详细情况的序列图。图 17 为表示第二再登记处理中在设定装置 101 与母机 102 之间被交换的外部指令中登记开始请求 1710 的格式的图。有关其它消息，由于为与第一再登记处理时被交换的外部指令的格式相同的格式，因此省略说明。

[0119] 母机 102 在从设定装置 101 接收登记开始请求 1710 时，确认是否已在登记处理中、可登记的台数是否已满、含在子机的信息表 1715 中的子机是否已被登记、或者该子机的识别信息是否存在异常等，并将确认结果存储在登记开始应答 820 中，发送给设定装置 101。但是，在第二再登记处理中，在登记开始请求 1710（参照图 17）中含有以前登记时所用的秘密地址生成符 1713。并且，在子机的信息表 1715 中不仅含有子机的识别信息，还含有子机的固有地址和固有密钥。能够执行在登记执行类型 1711 中所指定的再登记，且在子机的信息表 1715 没有异常时，开始第二再登记处理。

[0120] 图 19 为表示母机 102 所执行的第二再登记处理的流程图。图 20 为表示子机 103a ～ 103n 所执行的第二再登记处理的流程图。在图 19 中，对于第二再登记处理中与第一再登记处理一样的处理标注与图 14 相同的符号。图 19 中的第二再登记处理中与图 14 的第一再登记处理的不同之处在于：步骤 S1014 及 S1401 被删除之处，代替步骤 S1005 而执行步骤 S1902 之处。

[0121] 在图 20 中，对于第二再登记处理中与第一再登记处理一样的处理标注与图 15 相同的符号。图 20 中的第二再登记处理中与图 15 的第一再登记处理的不同之处在于：步骤 S1502 及步骤 S1104 被删除，在步骤 S1501 之后追加步骤 S2001，代替步骤 S1103 而执行步骤 S2002。

[0122] 图 18 为表示在第二再登记处理中，在母机 102 与子机 103 之间被交换的消息中登记请求 1810 的格式的图。由于其它消息的格式与在第一再登记处理时被交换的消息的格式相同，因此省略说明。

[0123] 以下，仅对第二再登记处理中与第一再登记处理不同的处理进行说明，省略有关其它处理的说明。在步骤 S1902（参照图 19），母机 102 将登记请求 1810（参照图 18）发送给子机的秘密地址，该登记请求存储有登记执行类型 1812、登记认证密钥生成算法编号 1813、后续登记的消息的加密用密码算法编号 1814、登记认证密钥生成符 A1815 以及登记结束证明信息 1816。这里，登记结束证明信息 1816 为对于登记请求前方的各个字段计算单向函数（例如，Hash 函数），且用子机的固有密钥进行了加密的信息。

[0124] 在步骤S2001(参照图20)中,子机103从母机102接收登记请求1810。在步骤S1503(参照图20)中,子机103根据所接收到的登记请求1810与母机102一样计算单向函数,用自身的固有密钥生成登记结束证明信息,并确认在登记请求1810中是否含有与自身生成的登记结束证明信息一致的信息。子机103在不含与自身所生成的登记结束证明信息一致的信息时,将母机102判断为不正当,无视所接收到的登记开始通知1310,结束再登记处理。

[0125] 而在步骤S1503(参照图15)中,子机103在含有与自身所生成的登记结束证明信息一致的信息时,将母机102判断为正当,转移到步骤S2002。在步骤S2002(参照图20)中,子机103进行秘密地址的使用开始设定。由于其它处理与第一再登记处理一样,因此省略说明。

[0126] 另外,在从设定装置101输入到母机102的子机的信息表中含有子机的固有地址时,由于母机102已保有子机的固有地址,因此子机103也可以不进行步骤S1111的处理。由于其它处理与第一再登记处理一样,因此省略说明。

[0127] (7)秘密地址生成符的选择方法及秘密地址的生成方法

[0128] 以下,将秘密MAC地址的生成方法的一个例子表示为秘密地址。

[0129] 秘密MAC地址(系列ID部分):=Hash(变换主码‖识别信息‖秘密地址生成符)

[0130] 不过,Hash为Hash函数,例如,SHA-1。变换主码为规定的固定文字列。秘密地址生成符为用母机选择的随机数或由随机数与母机的BSSID所结合的生成符,每次生成不同的值。确认所算出的登记对象子机的秘密MAC地址(系列ID)之间没有重复的情况。当存在重复时,母机再次选择秘密地址生成符,再次计算对象子机的秘密MAC地址。并且,秘密MAC地址整个由厂商ID、机种和系列ID构成。但是,厂商ID与机种由统一的专用识别值决定。随机ID取上述Hash值的右端16位使用。

[0131] 根据上述实施例,在对母机102增设子机103时,仅通过向母机102输入各个子机103的识别信息,就能够进行子机103的登记处理,将子机103连接在已设的网络上。因此,能够谋求用户的方便性,同时,提供短时间且能够确保安全的子机103的登记处理。

[0132] (第二实施方式)

[0133] 第二实施方式与第一实施方式的不同之处在于:在母机102与子机103a-103n之间进行的初始登记处理和再登记处理的处理顺序。由于母机102及子机103的功能块图与第一实施方式一样,因此援用图4及图5。以下,仅对与第一实施方式不同的动作进行说明。

[0134] 图21为表示第二实施方式所涉及的母机102所执行的初始登记处理的流程图。在图21中,母机102从第一实施方式所涉及的初始登记处理(参照图10)中省略步骤S1003、S1004、S1014的动作。图22为表示第二实施方式所涉及的子机103所执行的初始登记处理的流程图。在图22中,子机103从第一实施方式所涉及的初始登记处理(参照图11)中省略步骤S1101、S1114、S1115的动作。以下,对第二实施方式所涉及的初始登记处理进行说明。

[0135] (1)初始登记处理

[0136] 在步骤S1001(参照图21)中,母机102根据含在登记开始请求810(参照图8)的子机的信息表814中的各个子机的识别信息,来选择秘密地址生成符,生成子机的秘密地

址。

[0137] 在步骤 S1002(参照图 21)中,母机 102 用广播将存储有秘密地址生成符 913 的登记开始通知 910(参照图 9)发送给子机 103a ～ 103n。

[0138] 在步骤 S1102(参照图 22)中,子机 103a ～ 103n 接收来自母机 102 的登记开始通知 910。然后,在步骤 S1103(参照图 22)中,子机 103a ～ 103n 从所接收到的登记开始通知 910 读取秘密地址生成符 913,根据该读取的秘密地址生成符 913 与自身的识别信息来生成自身的秘密地址。并且,子机 103a ～ 103n 进行该生成的秘密地址的使用开始设定。

[0139] 在步骤 S1005(参照图 21)中,母机 102 从子机的信息表 814 取得进行登记处理的子机的信息。这里,假设取得了子机 103a 的信息。母机 102 将在步骤 S1004 中取得的子机 103a 的秘密地址作为接收目的地记载并发送登记请求 920(参照图 9),该登记请求 920 存储有表示用于登记认证密钥的生成的算法的登记认证密钥生成算法编号 922、表示用于登记处理中的消息的加密的算法的密码算法编号 923 以及作为用于登记认证密钥的生成的信息的登记认证密钥生成符 A924。

[0140] 在步骤 S1104(参照图 22)中,子机 103a 接收将自身的秘密地址作为接收目的地记载的登记请求 920。其次,在步骤 S1105 中,子机 103a 确认所接收到的登记请求 920(参照图 9)中的各个字段的内容,在没有异常时,将登记认证密钥生成符 B933 存储在登记应答 930(参照图 9)中,并发送给母机 102。

[0141] 在步骤 S1006(参照图 21)中,母机 102 接受子机 103a 所发送的登记应答 930(参照图 9),并转移到步骤 S1007。另外,也可以在步骤 S1006 中,母机 102 确认登记应答 930 中的各个字段的内容,在有异常时,停止子机 103a 的登记处理,返回到步骤 S1005,从子机的信息表 814 取得其次进行登记处理的子机的信息,并将登记请求 920 发送给该子机。在步骤 S1007(参照图 21)中,母机 102 使用通过登记认证密钥生成算法编号 922 所指定的登记认证密钥生成算法,来从登记认证密钥生成符 A924 和登记认证密钥生成符 B933 生成登记认证密钥。

[0142] 在步骤 S1106(参照图 22)中,子机 103a 使用通过登记认证密钥生成算法编号 922 所指定的登记认证密钥生成算法,来从登记认证密钥生成符 A924 和登记认证密钥生成符 B933 生成登记认证密钥。在步骤 S1107(参照图 22)中,子机 103a 将存储有问询纯文本 942 的问询 940(参照图 9)发送给母机 102,该问询纯文本用于判断母机 102 和子机 103a 是否生成了共同的登记认证密钥,为随机生成的文本数据。

[0143] 在步骤 S1008(参照图 21)中,母机 102 接收从子机 103a 所发送的问询 940,并用登记认证密钥和由密码算法编号 923 所指定的密码算法对该接收到的问询 940 中的问询纯文本 942 进行加密。其次,在步骤 S1009(参照图 21)中,母机 102 将存储有被加密的问询密码文 952 的问询应答 950(参照图 9)发送给子机 103a。

[0144] 在步骤 S1108(参照图 22)中,子机 103a 接收母机 102 所发送的问询应答 950。子机 103a 用登记认证密钥通过由密码算法编号 923 所指定的密码算法对所接收到的问询应答 950 中的问询密码文 952 进行解密,并将该被解密的问询密码文 952 与自身发送给母机 102 的问询纯文本 942 进行对照,确认被解密后的问询密码文 952 与问询纯文本 942 是否一致。在确认对照的结果之后,子机 103a 转移到步骤 S1109,将存储有固有密钥生成算法编号 962 和固有密钥生成符 A963 的密钥生成请求 960(参照图 9)发送给母机 102。另外,在

步骤 S1108 中，也可以是子机 103a 在对照的结果是被解密的问询密码文 952 和问询纯文本 942 不一致时，中止登记处理，结束处理。

[0145] 在步骤 S1010（参照图 21）中，母机 102 从子机 103a 接收密钥生成请求 960，并转移到步骤 S1011。另外，在步骤 S1010 中，也可以是母机 102 确认所接收到的密钥生成请求 960 中的各个字段，当有异常时，中止子机 103a 的登记处理，返回到步骤 S1005，从子机的信息表 814 中取得其次进行登记处理的子机的信息，并将登记请求 920 发送给该子机。在步骤 S1011（参照图 21）中，母机 102 将存储有固有密钥生成符 B973 等的密钥生成应答 970（参照图 9）发送给子机 103。

[0146] 在步骤 S1110（参照图 22）中，子机 103a 接收密钥生成应答 970。其次，在步骤 S1111（参照图 22）中，子机 130a 用登记认证密钥加密自机的固有地址，并将存储有被加密的固有地址 982 的固有地址通知 980（参照图 9）发送给母机 102。

[0147] 在步骤 S1012（参照图 21）中，母机 102 接收子机 103a 所发送的固有地址通知 980。另外，在步骤 S1012 中，也可以是母机 102 在不能准确接收固有地址通知 980 时，中止子机 103a 的登记处理，并返回到步骤 S1005，从子机的信息表 814 取得其次进行登记处理的子机的信息，将登记请求 920 发送给该子机。

[0148] 在步骤 S1013（参照图 21）中，母机 102 根据固有密钥生成符 A963 和固有密钥生成符 B973，用所指定的固有密钥生成算法来生成子机 103 的固有密钥，将该所生成的固有密钥与子机 103 的固有地址或识别信息一起保存在登记信息保存部 405 中。另外，母机 102 在子机的信息表 814 中设定有多个子机时，也可以对所有子机，反复进行步骤 S1005 到步骤 S1013 为止的登记处理。

[0149] 在步骤 S1113（参照图 22）中，子机 103 根据固有密钥生成符 A963 和固有密钥生成符 B973，用被指定的固有密钥生成算法来生成子机 103 的固有密钥，并将该生成的固有密钥与母机 102 的固有地址一起保存在登记信息保存部 504 中。并且，子机 103a 设定秘密地址使用结束，结束初始登记处理。以上为在母机 102 与子机 103a ～ 103n 之间所进行的初始登记处理的一个例子。另外，也可以是子机 103a 在步骤 S1113 的固有密钥生成处理之后执行步骤 S1111 的固有地址通知发送处理，用固有密钥加密自机的固有地址，将存储有该被加密的固有地址 982 的固有地址通知 980（参照图 9）发送给母机 102。

[0150] (5) 第一再登记处理

[0151] 以下，对第二实施方式所涉及的第一再登记处理中的与初始登记处理不同的动作进行说明。图 23 为表示第二实施方式所涉及的母机 102 所执行的第一再登记处理的流程图。图 24 为表示第二实施方式所涉及的子机 103a ～ 103n 所执行的第一再登记处理的流程图。在图 23 中，对第一再登记处理中与初始处理相同的处理标注与图 21 一样的符号。图 23 中的第一再登记处理中与图 21 的初始登记处理不同之处在于进行步骤 S1401 来代替步骤 S1002。并且，图 23 中的第一再登记处理为从第一实施方式所涉及的第一再登记处理（参照图 14）中省略了步骤 S1003、S1004、S1014 的动作的处理。

[0152] 在图 24 中，对于第一再登记处理中与初始登记处理相同的处理标注与图 22 一样的符号。图 24 中的第一再登记处理中与图 22 的第一初始登记处理不同之处在于进行步骤 S1502 来代替步骤 S1102、以及在步骤 S1502 之后追加了步骤 S1503。即，图 24 中的第一再登记处理为从第一实施方式所涉及的第一再登记处理（参照图 15）中省略了步骤 S1501、

S1115 的动作的处理。

[0153] 以下，仅对第一再登记处理中与初始登记处理不同的处理进行说明，而省略其它处理的说明。在步骤 S1401（参照图 23）中，母机 102 通过广播将存储有秘密地址生成符 1313、源母机的固有地址 1314 和登记结束证明信息 1315 的登记开始通知 1310（参照图 13）发送给子机 103a ～ 103n。另外，在本实施方式中，作为登记结束证明信息 1315，对于登记开始通知中位于前方的各个字段，计算单向函数（例如，Hash 函数），并且仅存储子机 103a ～ 103n 数目的用各个子机的固有密钥加密后的。

[0154] 在步骤 S1502（参照图 24）中，子机 103a ～ 103n 从母机 102 接收登记开始通知 1310。接着，在步骤 S1503（参照图 24）中，子机 103 根据接收到的登记开始通知 1310 与母机 102 一样计算单向函数，用自身的固有密钥生成登记结束证明信息，确认在登记开始通知 1310 中是否含有与自机所生成的登记结束证明信息一致的信息。子机 103 在不含与自机所生成的登记结束证明信息一致的信息时，无视所接收到的登记开始通知 1310，结束在登记处理。而在步骤 S1503（参照图 24）中，子机 103 在包含有与自机所生成的登记结束证明信息一致的信息时，判断为母机 102 正当，并转移到步骤 S1103，根据含在登记开始通知 1310 中的秘密地址生成符 1313，生成自机的秘密地址，设定该生成的秘密地址的使用。由于其它处理与初始登记处理相同，因此在此省略说明。

[0155] 另外，当在从设定装置 101 输入到母机 102 的子机的信息表中含有子机的固有地址时，由于母机 102 已保有子机的固有地址，因此子机 103 也可以不进行步骤 S1111 的处理。像这样，根据本实施方式，还能够简单地进行基于母机的交换等的再登记处理。

[0156] (6) 第二再登记处理

[0157] 以下，对第二实施方式所涉及的第二再登记处理中与第一再登记处理不同的动作进行说明。图 25 为表示第二实施方式所涉及的母机 102 执行的第二再登记处理的流程图。图 26 为表示第二实施方式所涉及的子机 103a ～ 103n 执行的第二再登记处理的流程图。在图 25 中，对第二再登记处理中与第一再登记处理相同的处理标注与图 23 一样的符号。图 25 中的第二再登记处理中与图 23 的第一再登记处理不同之处在于删除了步骤 S1401、以及进行步骤 S1902 来代替步骤 S1005。并且，图 25 中的第二再登记处理为从第一实施方式所涉及的第二再登记处理（参照图 19）中省略了步骤 S1003、S1004 的动作的处理。

[0158] 在图 26 中，对第二再登记处理中与第一再登记处理一样的处理，标注与图 24 相同的符号。图 26 的第二再登记处理中与图 24 的第一再登记处理的不同之处在于删除了步骤 S1502 及步骤 S1104、追加步骤 S2001 以及进行步骤 S2002 来代替步骤 S1103。即，图 26 中的第二再登记处理为从第一实施方式所涉及的第二再登记处理（参照图 20）中省略了步骤 S1501、S1115 的动作的处理。

[0159] 以下，仅说明第二再登记处理中与第一再登记处理不同的处理，省略其它处理的说明。在步骤 S1902（参照图 25）中，母机 102 将存储有登记执行类型 1812、登记认证密钥生成算法编号 1813、后续登记的消息的加密用的密码算法编号 1814、登记认证密钥生成符 A1815 以及登记结束证明信息 1816 的登记请求 1810（参照图 18）发送给子机的秘密地址。这里，登记结束证明信息 1816 为对于登记请求前方的各个字段计算单向函数（例如，Hash 函数），且用子机的固有密钥加密后的信息。

[0160] 在步骤 S2001（参照图 26）中，子机 103 从母机 102 接收登记请求 1810。在步骤

S2002(参照图 20)中,子机 103 进行秘密地址的使用开始设定。对于其它处理,由于与第一再登记处理相同,因此在此省略说明。

[0161] 另外,在从设定装置 101 输入到母机 102 的子机的信息表中包含子机的固有地址时,由于母机 102 已保有子机的固有地址,因此子机 103 也可以不进行步骤 S1111 的处理。对于其它处理,由于与第一再登记处理相同,因此在此省略说明。

[0162] (第三实施方式)

[0163] 在第三实施方式中,对在固有密钥的共有完成了的母机与子机之间共有通信密钥用的认证处理进行说明。如果初始登记处理结束,则子机 103a ～ 103n 能够将母机 102 的固有地址指定为接收地址,向母机 102 请求认证处理,从母机 102 接收通信密钥的分发。以下,对进行初始登记处理、再登记处理以及认证处理的母机 102 及子机 103 的结构进行说明。图 27 为第三实施方式所涉及的母机 102 的功能块图。在图 27 中,CPU201 除了具有登记处理部 401、秘密地址生成 / 设定部 404 之外,还具有通信认证部 402 的功能。存储部 202 除了具有登记信息保存部 405 之外,还具有通信密钥保存部 406 的功能。以太 I / F203 具有第一通信部 407 的功能,PLC I / F204 具有第二通信部 408 的功能,这与第一及第二实施方式相同。

[0164] 通信密钥保存部 406 保存母机 102 所管理的网络的通信密钥。通信认证部 402 在从登记完成后的子机 103 经由第二通信部 408 接收通信认证请求之后,基于被保存在登记信息保存部 405 中的子机 103 的固有地址及固有密钥,进行对子机 103 的认证,在认证成功时,将保存在通信密钥保存部 406 中的通信密钥分发给子机 103。

[0165] 图 28 为第三实施方式所涉及的子机 103 的功能块图。在图 28 中,CPU301 除了登记处理部 501 以及秘密地址生成 / 设定部 503 之外,还具有通信认证部 502 的功能。存储部 302 除了登记信息保存部 504 之外,还具有通信密钥保存部 505 的功能。PLC I / F303 具有第二通信部 506 的功能与第一及第二实施方式一样。通信密钥保存部 505 保存母机 102 所分发的通信密钥。通信认证部 502 在与母机 102 之间的登记处理结束后,经由第二通信部 506 向母机 102 发送通信认证请求,在从母机 102 分发允许认证后的通信密钥之后,将该通信密钥保存在通信密钥保存部 505。

[0166] 根据上述实施方式,由于即使在子机 103 的登记处理后的子机 103 的认证处理中,也使用共通加密密钥(固有密钥),因此即使在登记对象子机 103 的台数较多时,也能够短时间结束子机 103 的认证。

[0167] 另外,在上述各实施方式中,以适用于 PLC 网络的情况为例进行了说明,但本发明并于限于 PLC 网络,不用说还可适用于图 29 所示的无线网络、其它网络。在将本发明适用于无线网络中时,母机及子机包括无线 I / F 来代替 PLC I / F,经由无线网络发送、接收经由 PLC 网络发送、接收到的消息。并且,不用说作为可适用本发明的网络的结构,还包括通过图 30 所示的电桥所结合的 PLC 网络、通过无线网络以及 / 或电桥所结合的多个 PLC 网络(无图示)、和通过电桥所结合的多个无线网络(无图示)。

[0168] 并且,对于本发明的各个实施方式中所公开的母机和子机所具备的各个功能块执行的各个处理顺序,也可以通过 CPU 来解释执行可执行存储在存储装置 (ROM、RAM、硬盘等)中的上述处理顺序的规定程序数据来实现。此时,程序数据既可以经由存储介质导入存储装置内,也可以从存储介质上直接执行。另外,存储介质是指 ROM、RAM、快闪存储器等半导

体存储器、软盘、硬盘等磁盘存储器、CD－ROM、DVD、BD 等光盘存储器以及存储卡等。并且，存储介质为包括电话线路、搬送路径等的通信介质。

[0169] （工业上的利用可能性）

[0170] 本发明所涉及的通信装置及通信装置的登记方法具有在增设新设备时可安全连接到已设的网络上的效果等，作为进行用于通信装置之间的秘密通信的共通秘密密钥的设定的登记方法及通信装置等有用。另外，所公开的方法并不限于 PLC 网络，还可适用于包含无线通信网络的各种局域通信网络。

[0171] 符号的说明

[0172] 101－设定装置；102－母机；103－子机；201－CPU；202－存储部；203－以太 I/F；204－PLC I/F；301－CPU；302－存储部；303－PLC I/F；401－登记处理部；402－通信认证部；404－秘密地址生成/设定部；405－登记信息保存部；406－通信密钥保存部；407－第一通信部；408－第二通信部；501－登记处理部；502－通信认证部；503－秘密地址生成/设定部；504－登记信息保存部；505－通信密钥保存部；506－第二通信部。

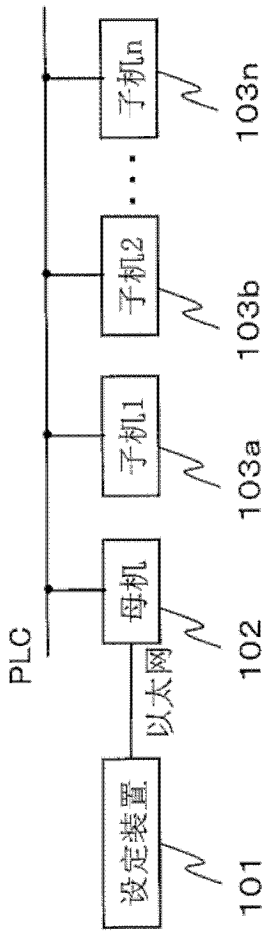

PLC
设定装置
101
以太网
母机
102
子机1
103a
子机2
103b
子机n
103n

图 1

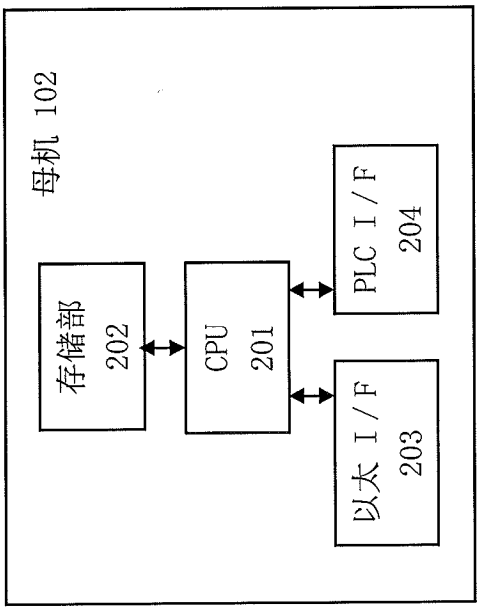

母机 102
存储部
202
CPU
201
以太 I/F
203
PLC I/F
204

图 2

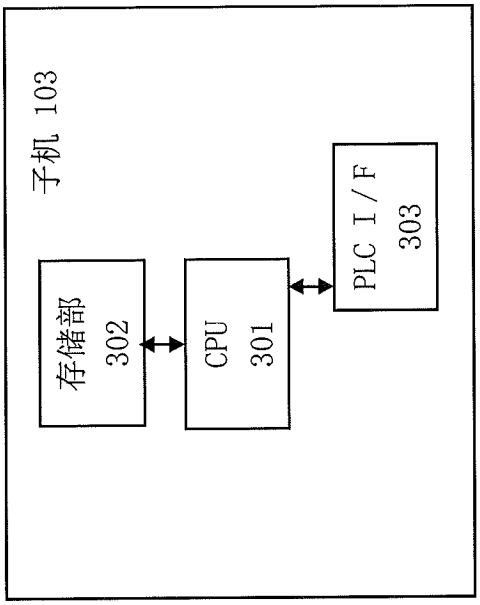


图 3

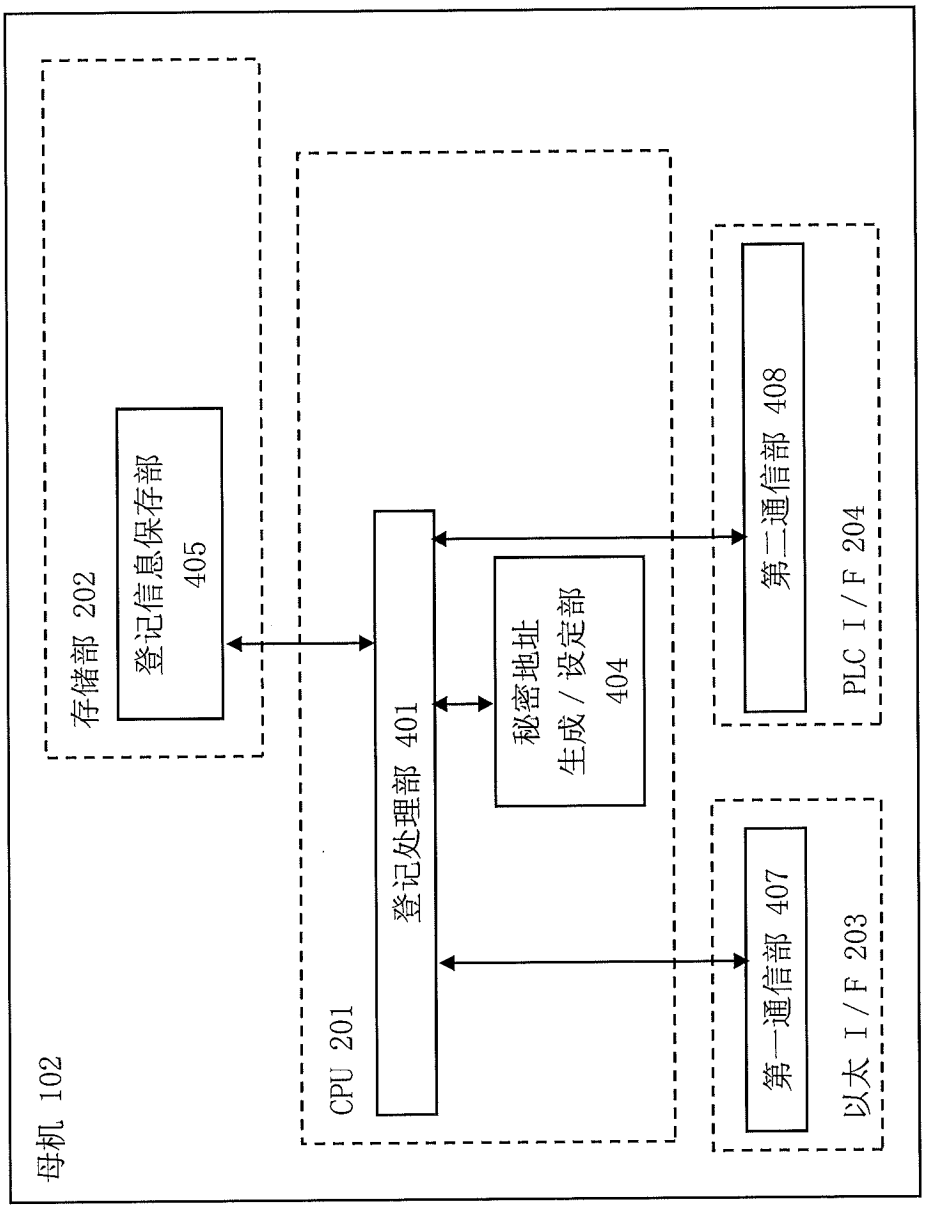

母机 102
存储部 202
登记信息保存部 405
CPU 201
登记处理部 401
秘密地址 生成 / 设定部 404
PLC I / F 204
第二通信部 408
以太 I / F 203
第一通信部 407

图 4

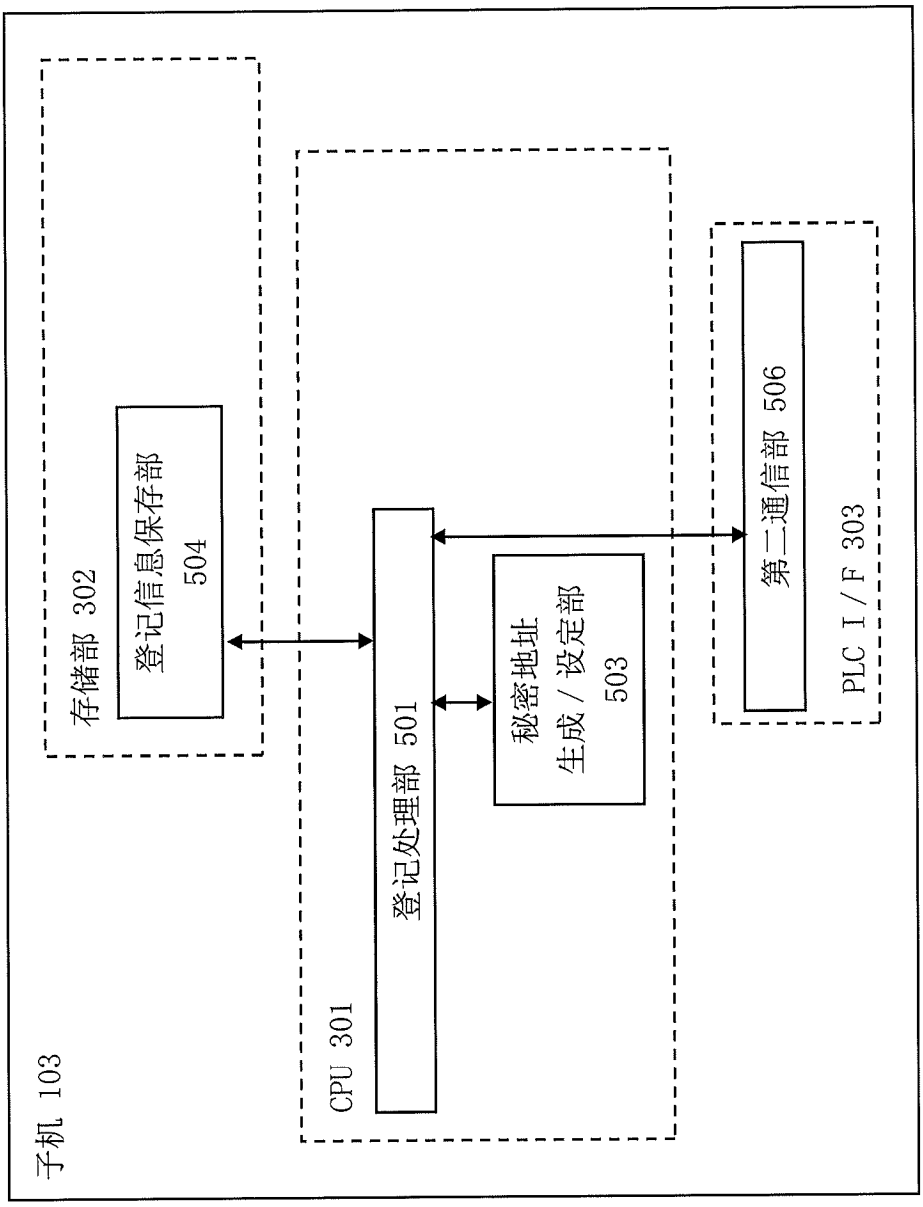

子机 103
存储部 302
登记信息保存部
504
CPU 301
登记处理部 501
秘密地址
生成 / 设定部
503
PLC I / F 303
第二通信部 506

图 5

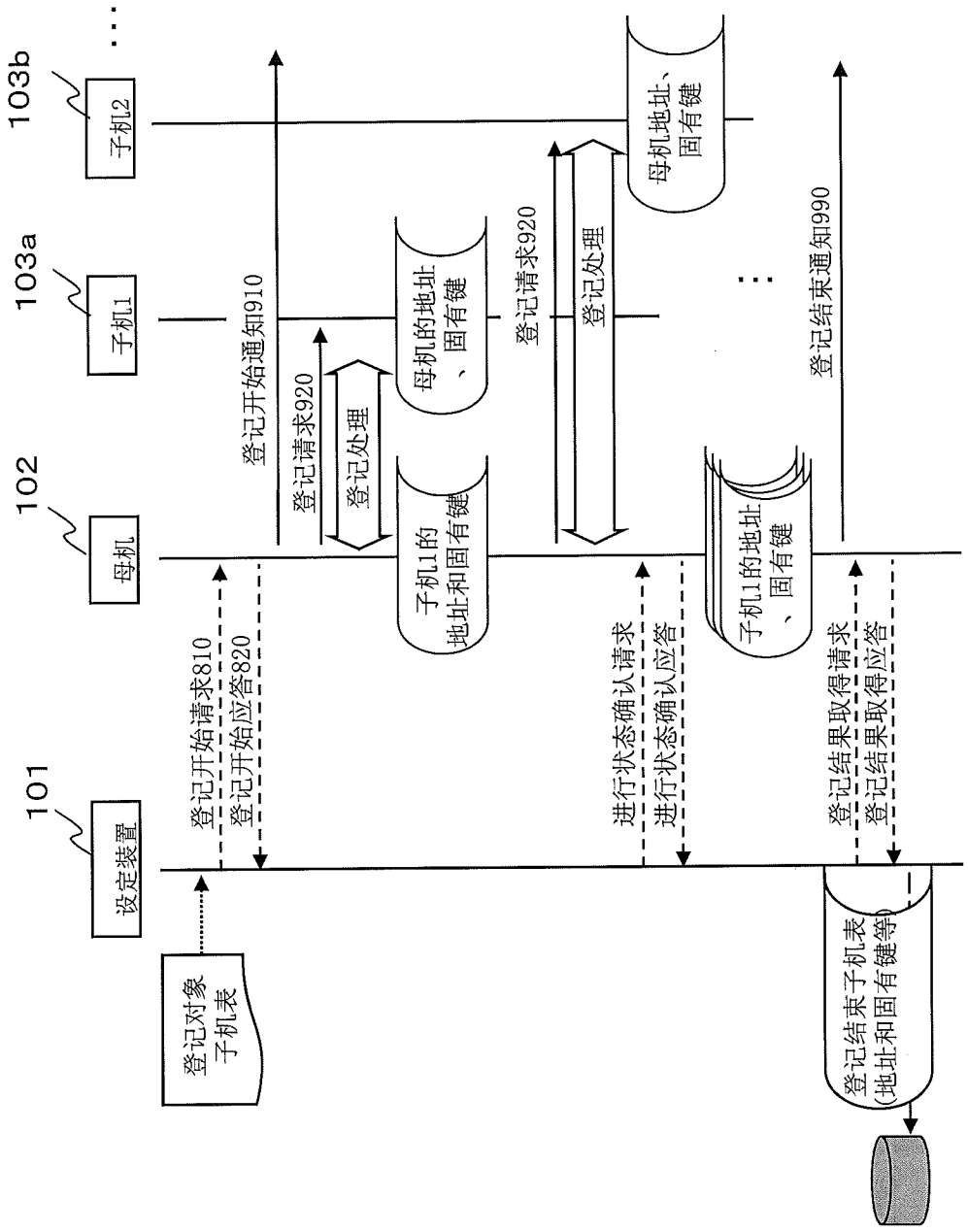

101
设定装置
102
母机
103a
子机1
103b
子机2
登记对象子机表
登记开始请求810
登记开始应答820
登记开始通知910
登记请求920
登记处理
子机1的地址和固有键
母机的地址、固有键
登记请求920
登记处理
母机地址、固有键
子机1的地址、固有键
进行状态确认请求
进行状态确认应答
登记结束通知990
登记结果取得请求
登记结果取得应答
登记结束子机表(地址和固有键等)

图 6

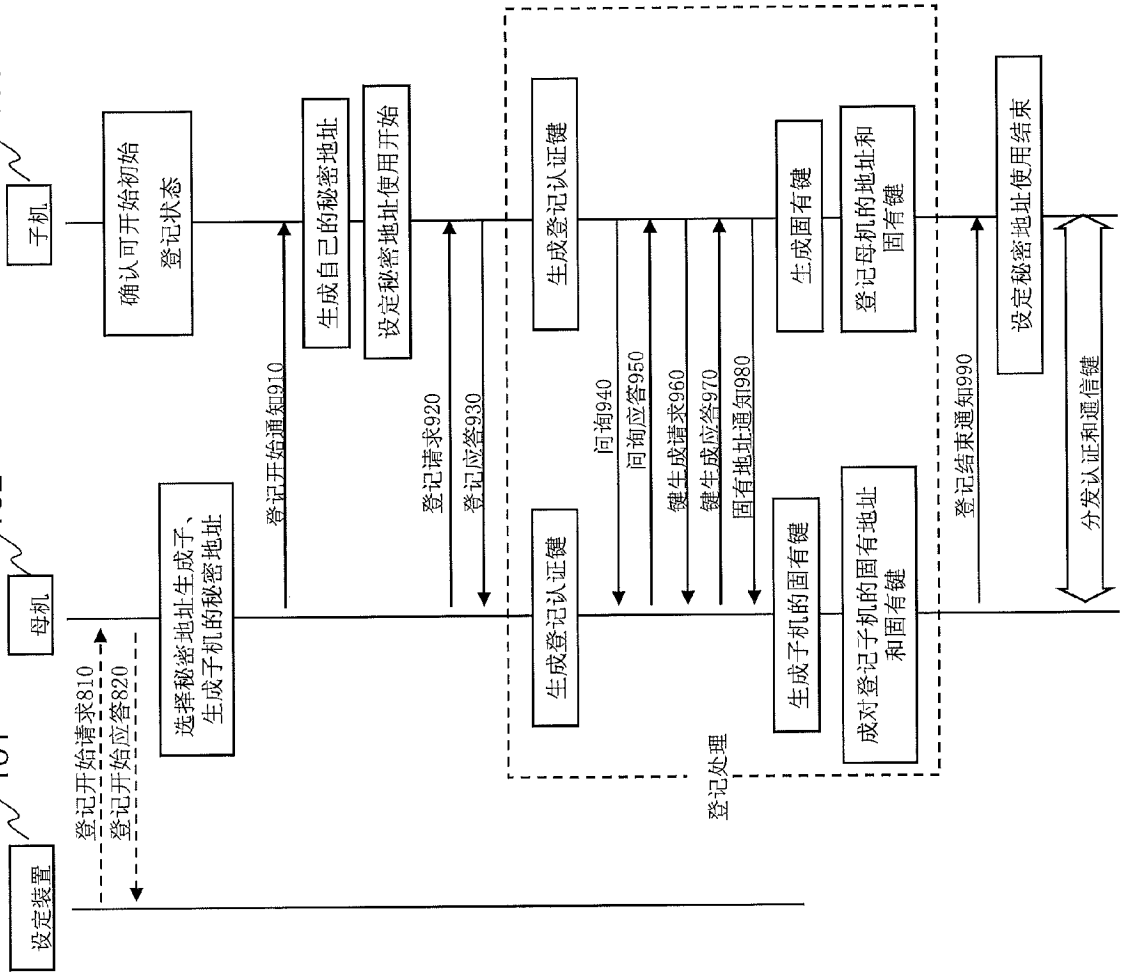

101
设定装置
102
母机
103
子机
登记开始请求810
登记开始应答820
选择秘密地址生成子、生成子机的秘密地址
确认可开始初始登记状态
登记开始通知910
生成自己的秘密地址
设定秘密地址使用开始
登记请求920
登记应答930
生成登记认证键
生成登记认证键
问询940
问询应答950
键生成请求960
键生成应答970
固有地址通知980
生成固有键
生成子机的固有键
登记母机的地址和固有键
成对登记子机的固有地址和固有键
登记处理
登记结束通知990
设定秘密地址使用结束
分发认证和通信键

图 7

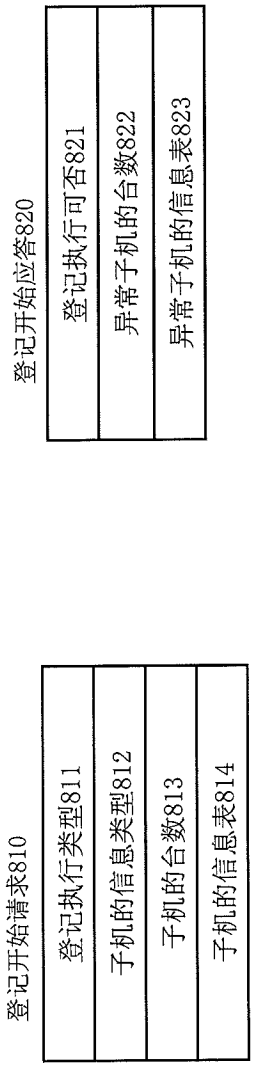

登记开始请求810
登记执行类型811
子机的信息类型812
子机的台数813
子机的信息表814
登记开始应答820
登记执行可否821
异常子机的台数822
异常子机的信息表823

图 8

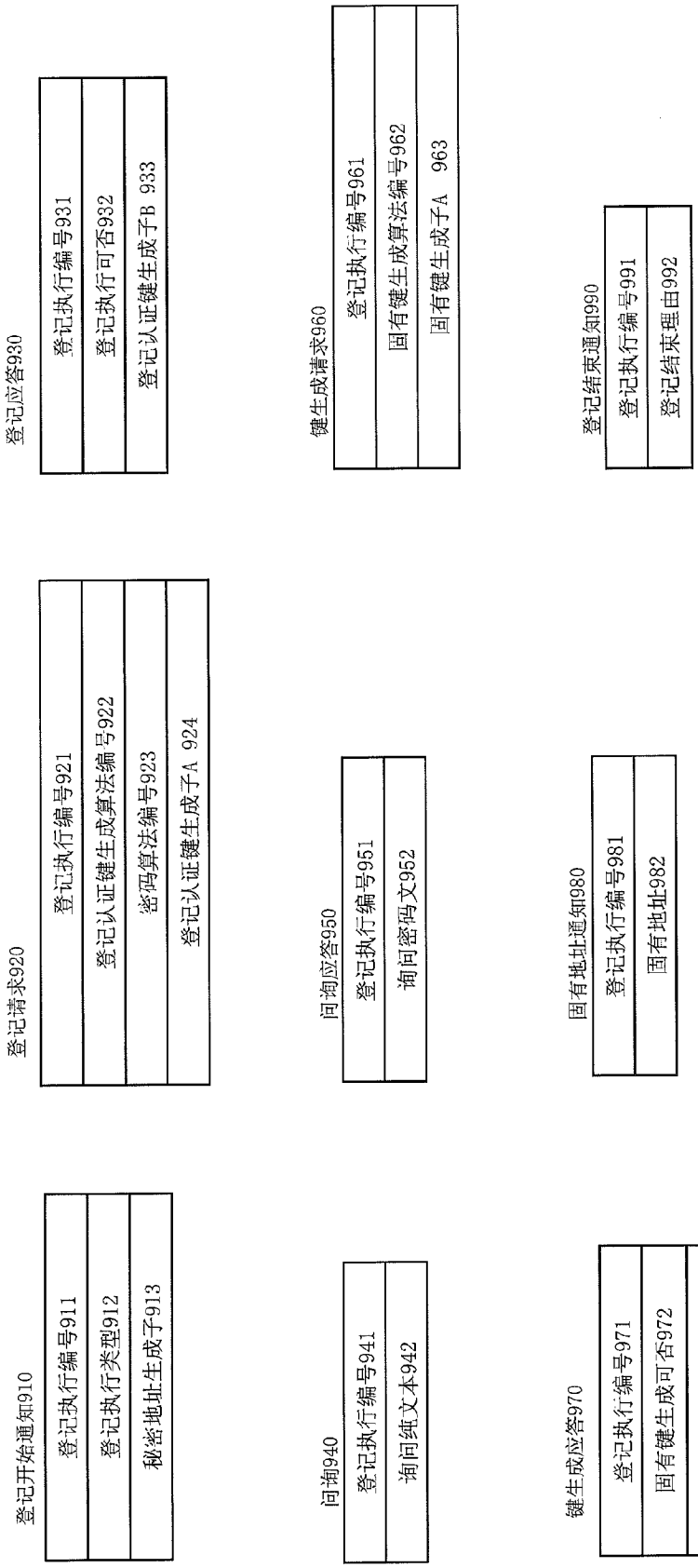

登记开始通知910
登记执行编号911
登记执行类型912
秘密地址生成子913
登记请求920
登记执行编号921
登记认证键生成算法编号922
密码算法编号923
登记认证键生成子A 924
登记应答930
登记执行编号931
登记执行可否932
登记认证键生成子B 933
问询940
登记执行编号941
询问纯文本942
问询应答950
登记执行编号951
询问密码文952
键生成请求960
登记执行编号961
固有键生成算法编号962
固有键生成子A 963
键生成应答970
登记执行编号971
固有键生成可否972
固有键生成子B 973
固有地址通知980
登记执行编号981
固有地址982
登记结束通知990
登记执行编号991
登记结束理由992

图 9

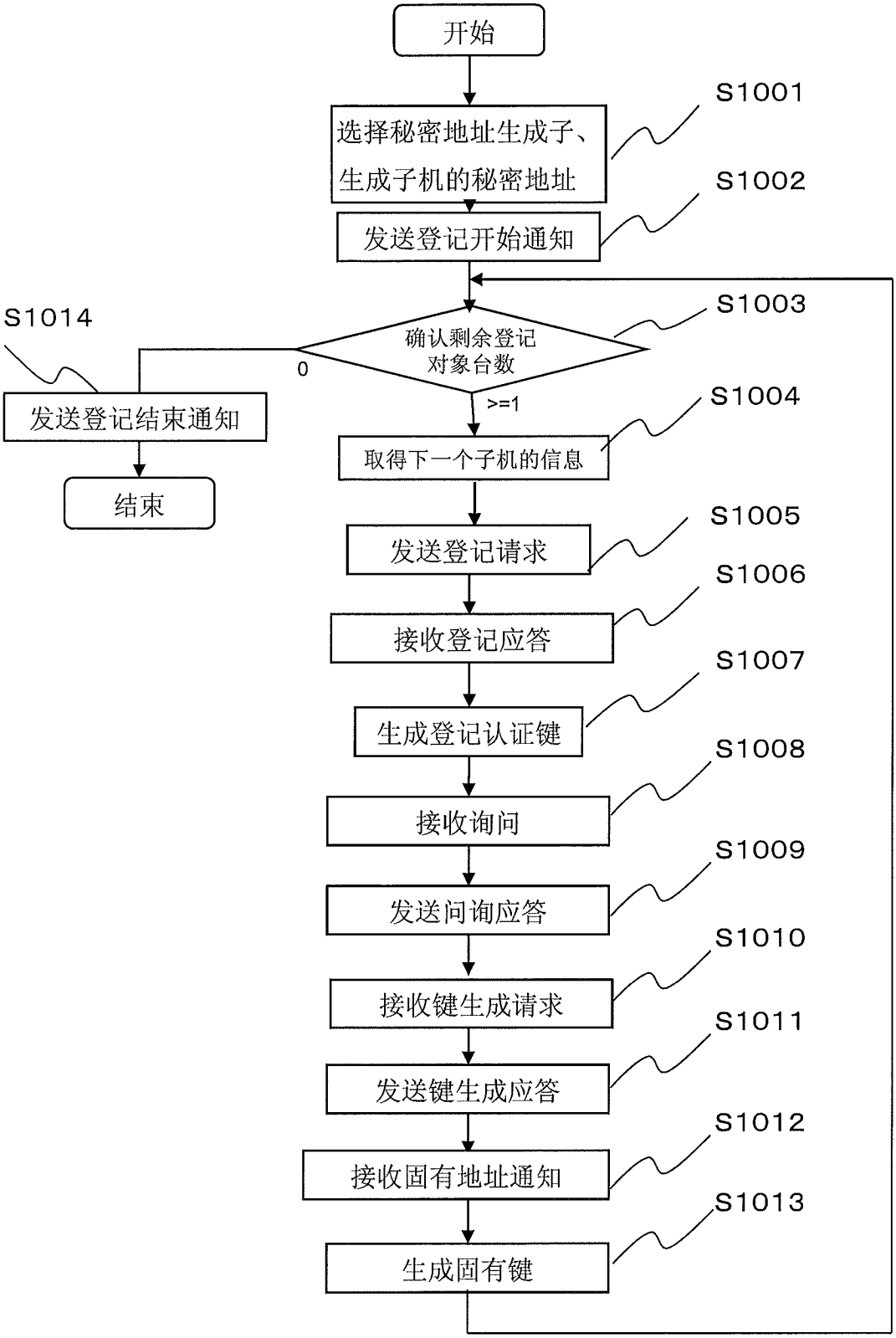

开始
S1001
选择秘密地址生成子、
生成子机的秘密地址
S1002
发送登记开始通知
S1003
确认剩余登记
对象台数
0
>=1
S1014
发送登记结束通知
结束
S1004
取得下一个子机的信息
S1005
发送登记请求
S1006
接收登记应答
S1007
生成登记认证键
S1008
接收询问
S1009
发送问询应答
S1010
接收键生成请求
S1011
发送键生成应答
S1012
接收固有地址通知
S1013
生成固有键

图 10

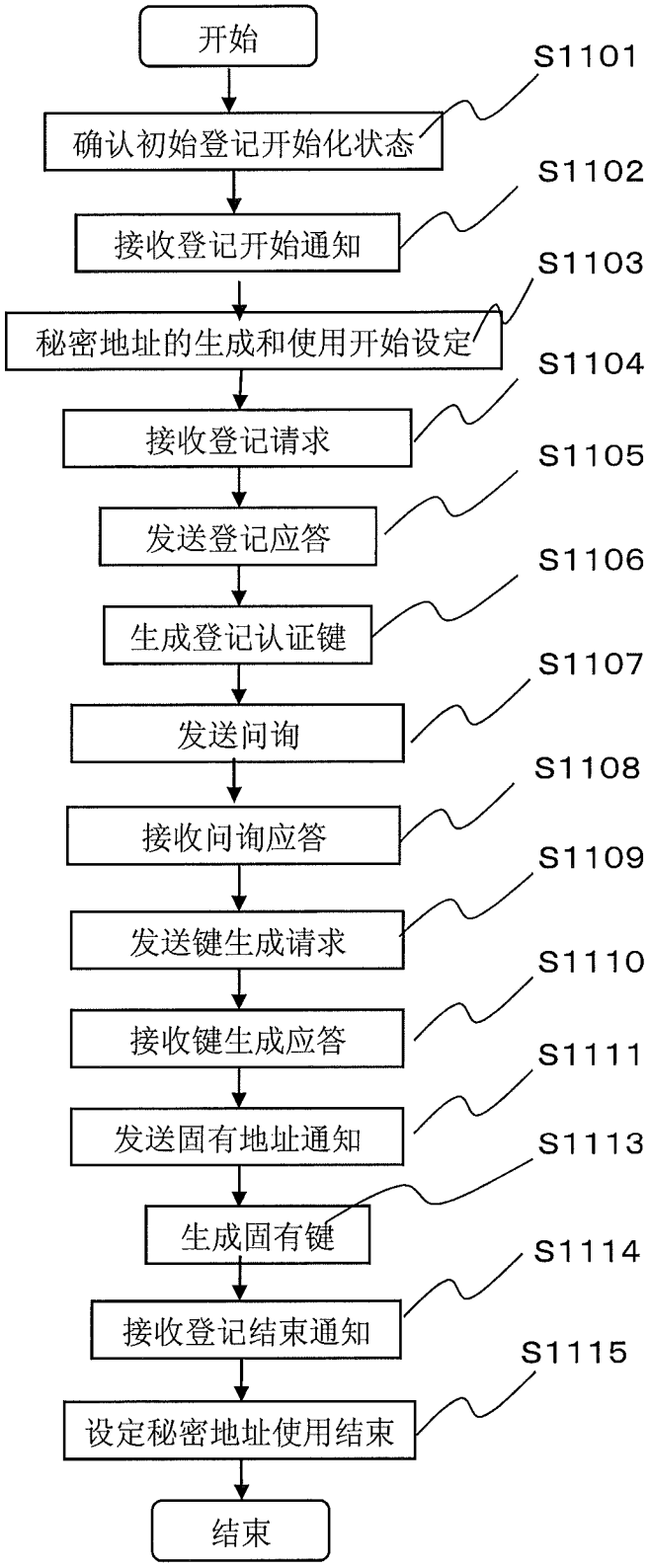

开始
S1101
确认初始登记开始化状态
S1102
接收登记开始通知
S1103
秘密地址的生成和使用开始设定
S1104
接收登记请求
S1105
发送登记应答
S1106
生成登记认证键
S1107
发送问询
S1108
接收问询应答
S1109
发送键生成请求
S1110
接收键生成应答
S1111
发送固有地址通知
S1113
生成固有键
S1114
接收登记结束通知
S1115
设定秘密地址使用结束
结束

图 11

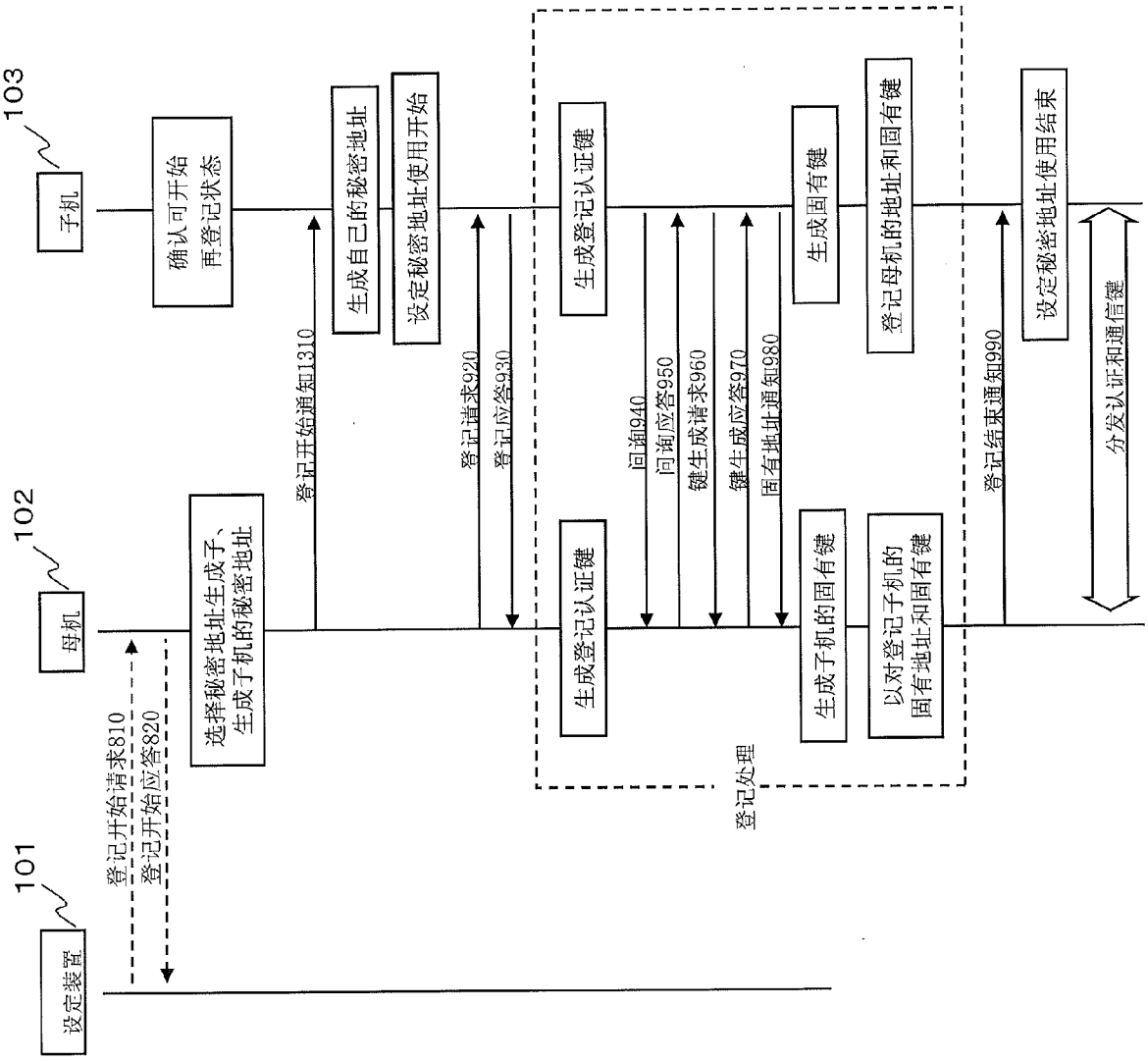

101
设定装置
102
母机
103
子机
登记开始请求810
登记开始应答820
选择秘密地址生成子、生成子机的秘密地址
确认可开始再登记状态
登记开始通知1310
生成自己的秘密地址
设定秘密地址使用开始
登记请求920
登记应答930
生成登记认证键
生成登记认证键
问询940
问询应答950
键生成请求960
键生成应答970
固有地址通知980
生成固有键
生成子机的固有键
以对登记子机的固有地址和固有键
登记母机的地址和固有键
登记处理
登记结束通知990
设定秘密地址使用结束
分发认证和通信键

图 12

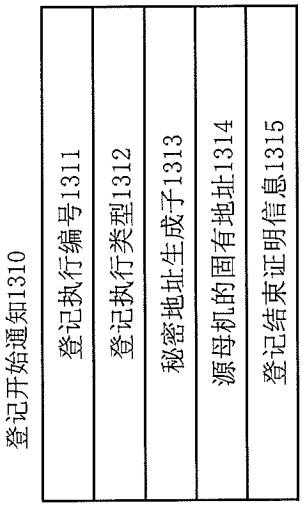

登记开始通知1310
登记执行编号1311
登记执行类型1312
秘密地址生成子1313
源母机的固有地址1314
登记结束证明信息1315

图 13

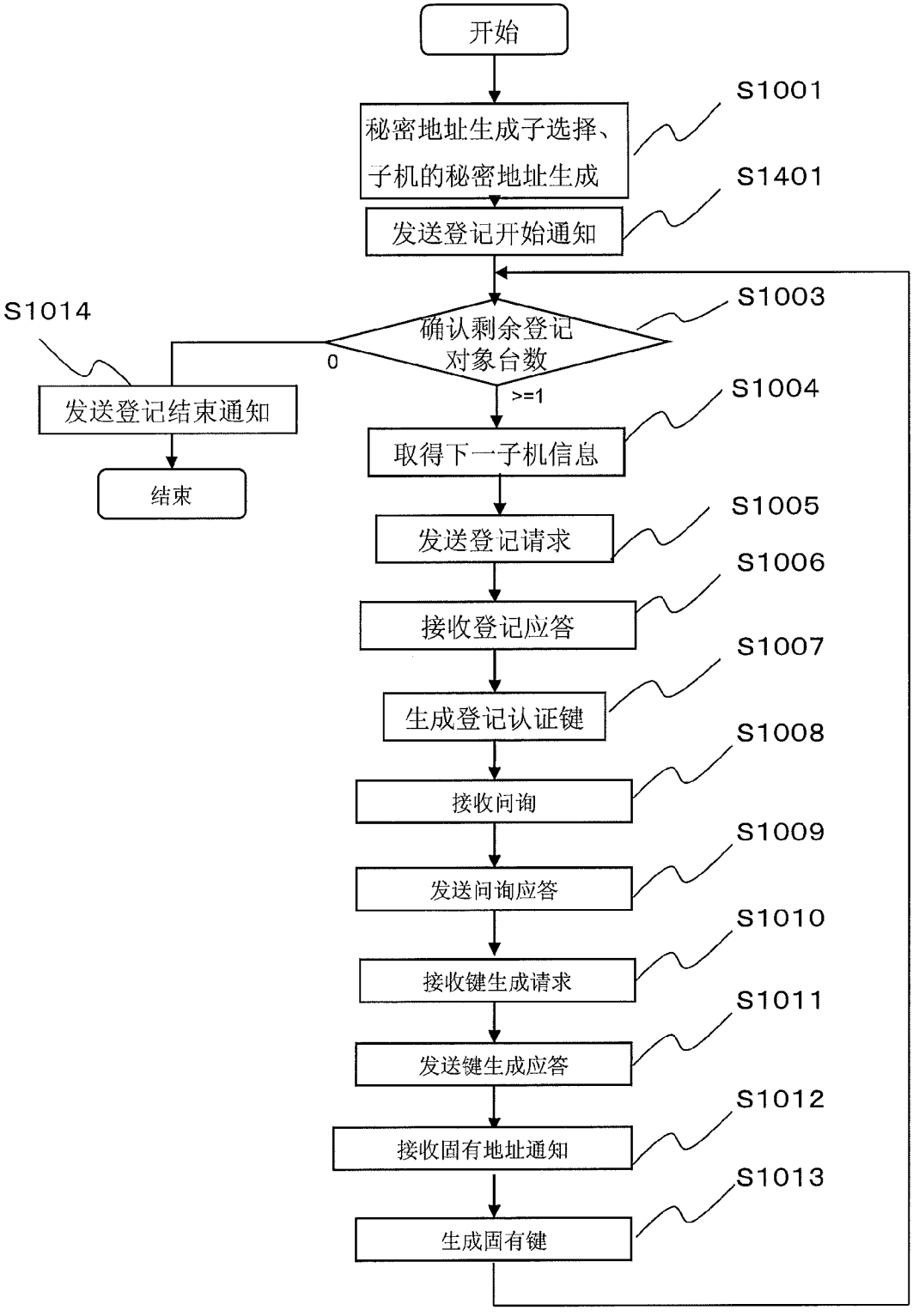

开始
S1001
秘密地址生成子选择、子机的秘密地址生成
S1401
发送登记开始通知
S1003
确认剩余登记对象台数
S1014
0
>=1
发送登记结束通知
结束
S1004
取得下一子机信息
S1005
发送登记请求
S1006
接收登记应答
S1007
生成登记认证键
S1008
接收问询
S1009
发送问询应答
S1010
接收键生成请求
S1011
发送键生成应答
S1012
接收固有地址通知
S1013
生成固有键

图 14

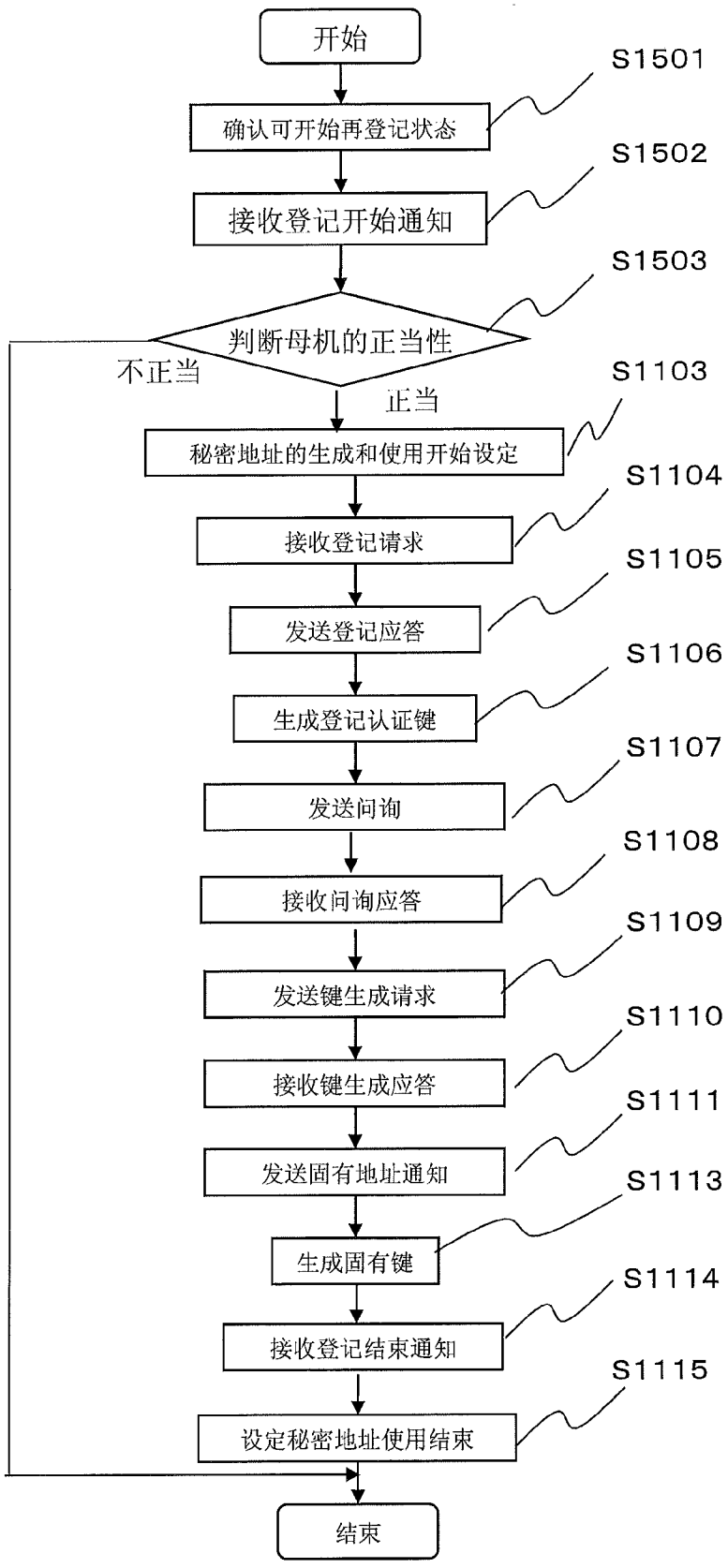

开始
S1501
确认可开始再登记状态
S1502
接收登记开始通知
S1503
判断母机的正当性
不正当
正当
S1103
秘密地址的生成和使用开始设定
S1104
接收登记请求
S1105
发送登记应答
S1106
生成登记认证键
S1107
发送问询
S1108
接收问询应答
S1109
发送键生成请求
S1110
接收键生成应答
S1111
发送固有地址通知
S1113
生成固有键
S1114
接收登记结束通知
S1115
设定秘密地址使用结束
结束

图 15

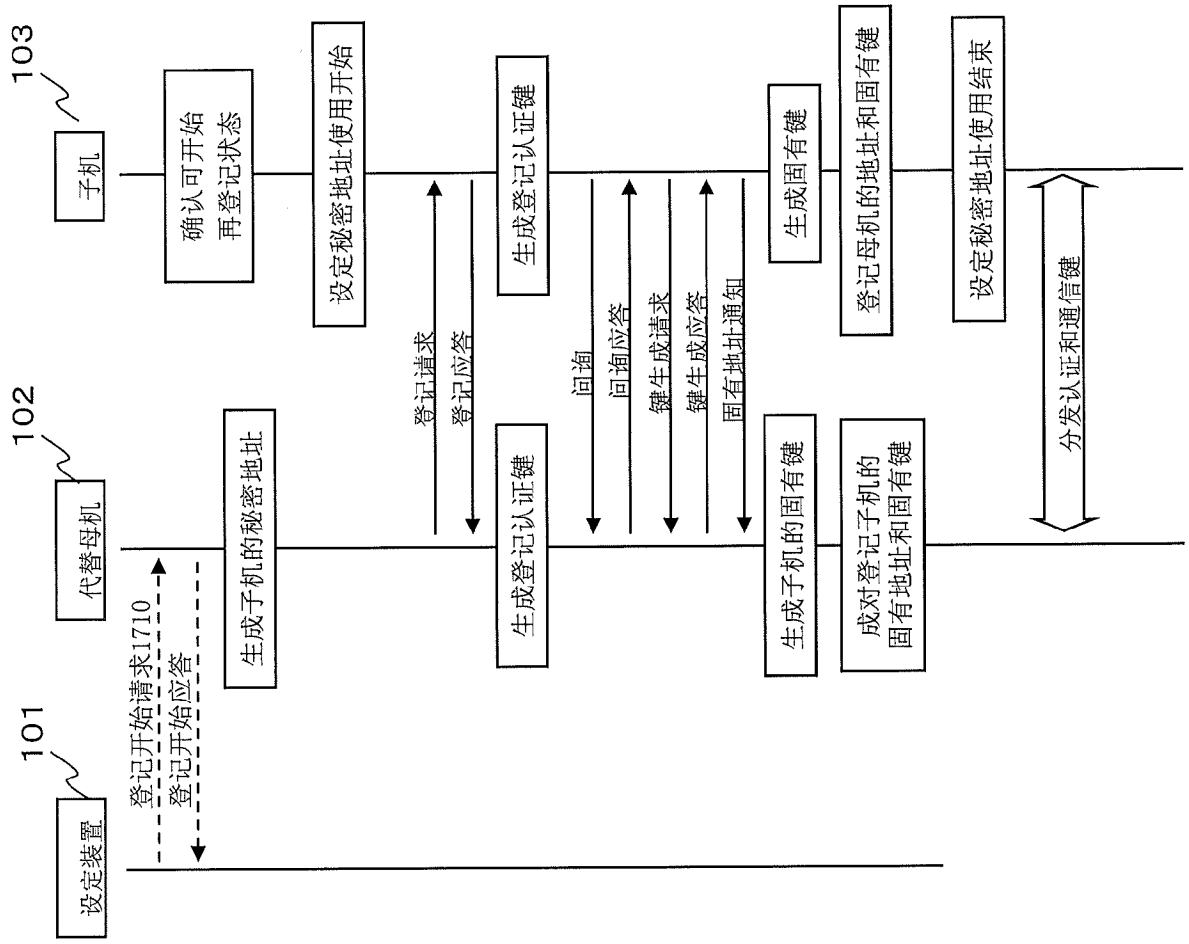

101
设定装置
102
代替母机
103
子机
登记开始请求1710
登记开始应答
生成子机的秘密地址
确认可开始
再登记状态
设定秘密地址使用开始
登记请求
登记应答
生成登记认证键
问询
问询应答
键生成请求
键生成应答
固有地址通知
生成登记认证键
生成子机的固有键
生成固有键
成对登记子机的
固有地址和固有键
登记母机的地址和固有键
设定秘密地址使用结束
分发认证和通信键

图 16

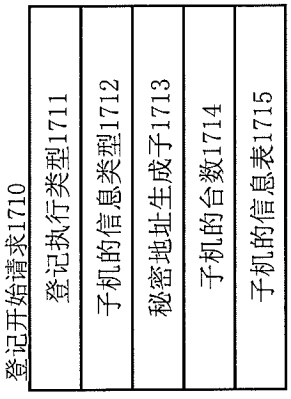

登记开始请求1710
登记执行类型1711
子机的信息类型1712
秘密地址生成子1713
子机的台数1714
子机的信息表1715

图 17

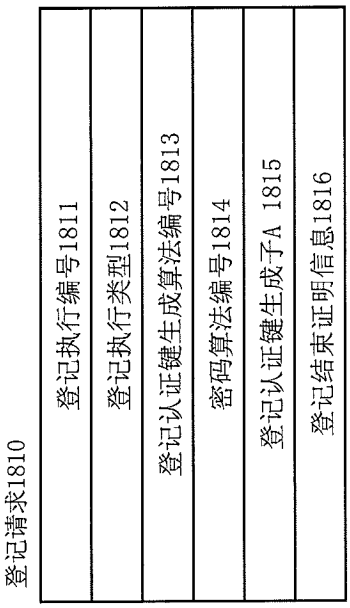

登记请求1810
登记执行编号1811
登记执行类型1812
登记认证键生成算法编号1813
密码算法编号1814
登记认证键生成子A 1815
登记结束证明信息1816

图 18

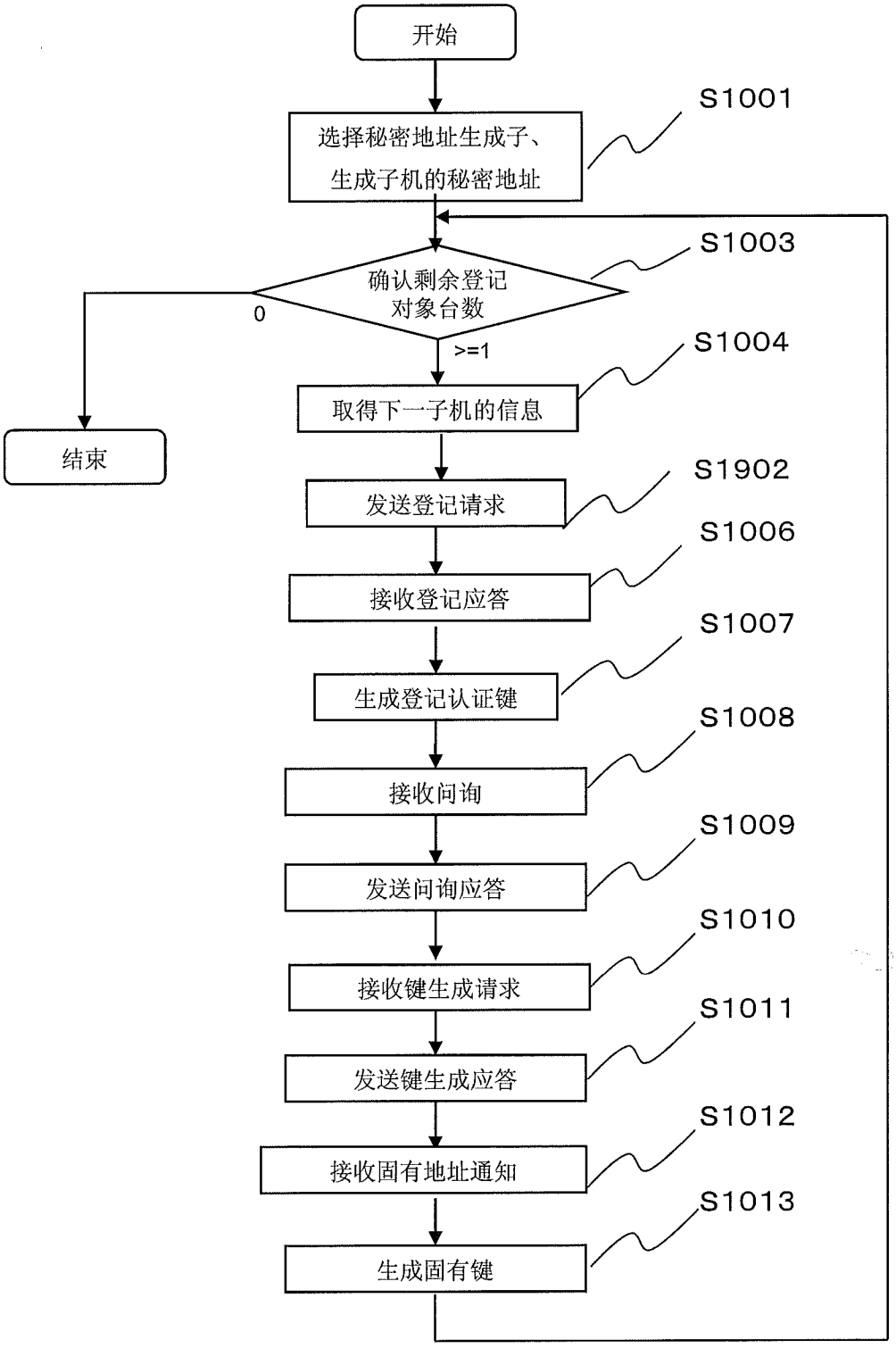

开始
S1001
选择秘密地址生成子、
生成子机的秘密地址
S1003
确认剩余登记
对象台数
0
>=1
结束
S1004
取得下一子机的信息
S1902
发送登记请求
S1006
接收登记应答
S1007
生成登记认证键
S1008
接收问询
S1009
发送问询应答
S1010
接收键生成请求
S1011
发送键生成应答
S1012
接收固有地址通知
S1013
生成固有键

图 19

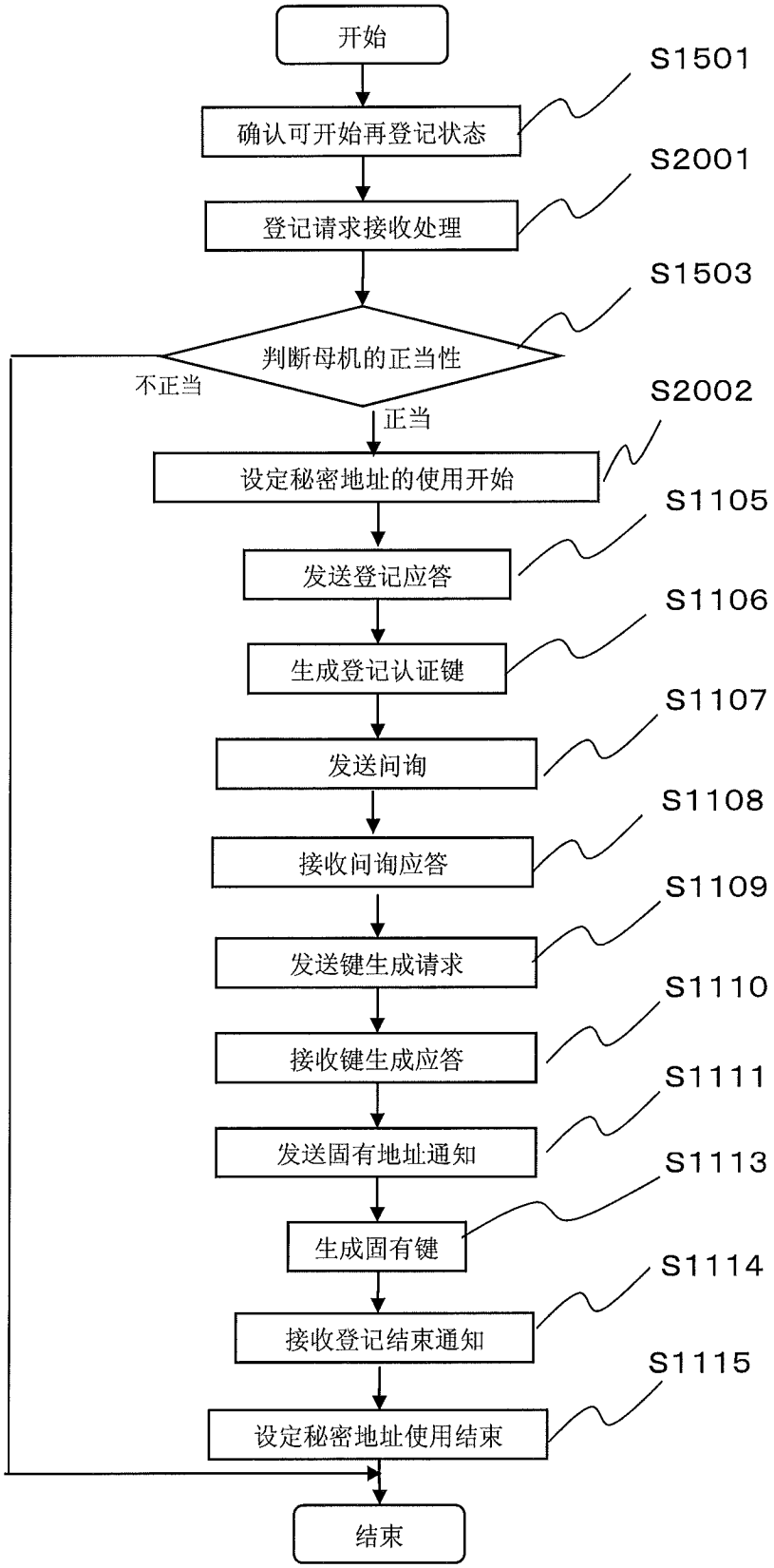

开始
S1501
确认可开始再登记状态
S2001
登记请求接收处理
S1503
判断母机的正当性
不正当
正当
S2002
设定秘密地址的使用开始
S1105
发送登记应答
S1106
生成登记认证键
S1107
发送问询
S1108
接收问询应答
S1109
发送键生成请求
S1110
接收键生成应答
S1111
发送固有地址通知
S1113
生成固有键
S1114
接收登记结束通知
S1115
设定秘密地址使用结束
结束

图 20

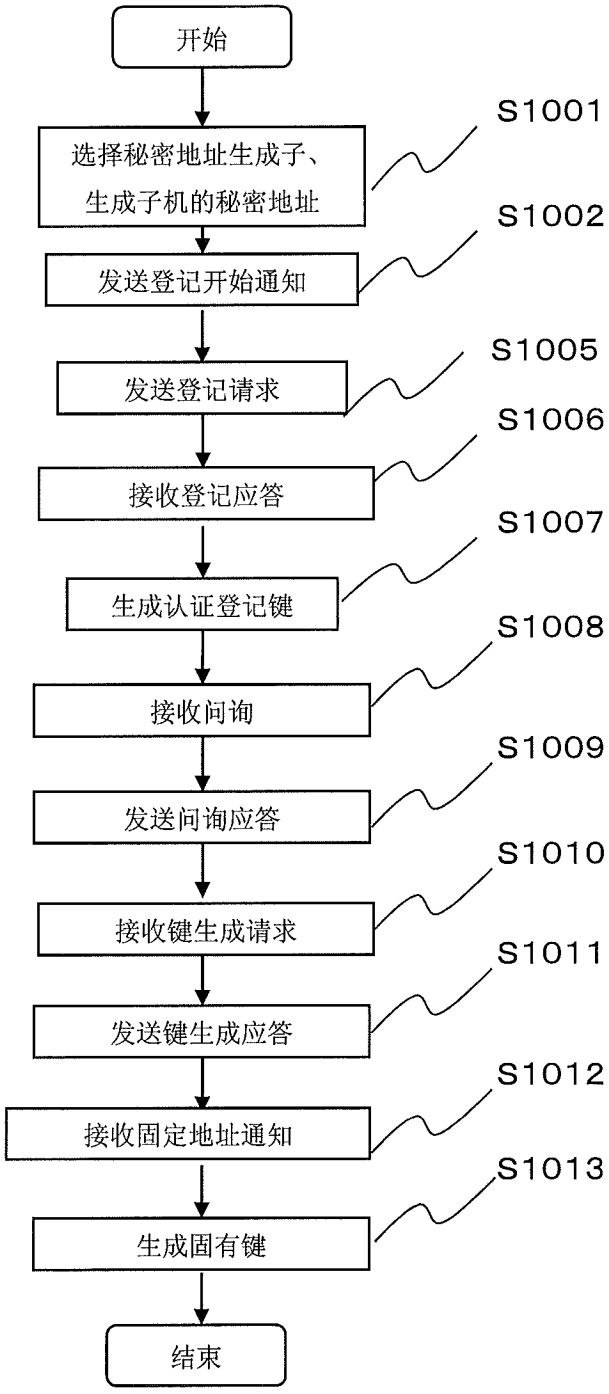

开始
选择秘密地址生成子、生成子机的秘密地址
S1001
发送登记开始通知
S1002
发送登记请求
S1005
接收登记应答
S1006
生成认证登记键
S1007
接收问询
S1008
发送问询应答
S1009
接收键生成请求
S1010
发送键生成应答
S1011
接收固定地址通知
S1012
生成固有键
S1013
结束

图 21

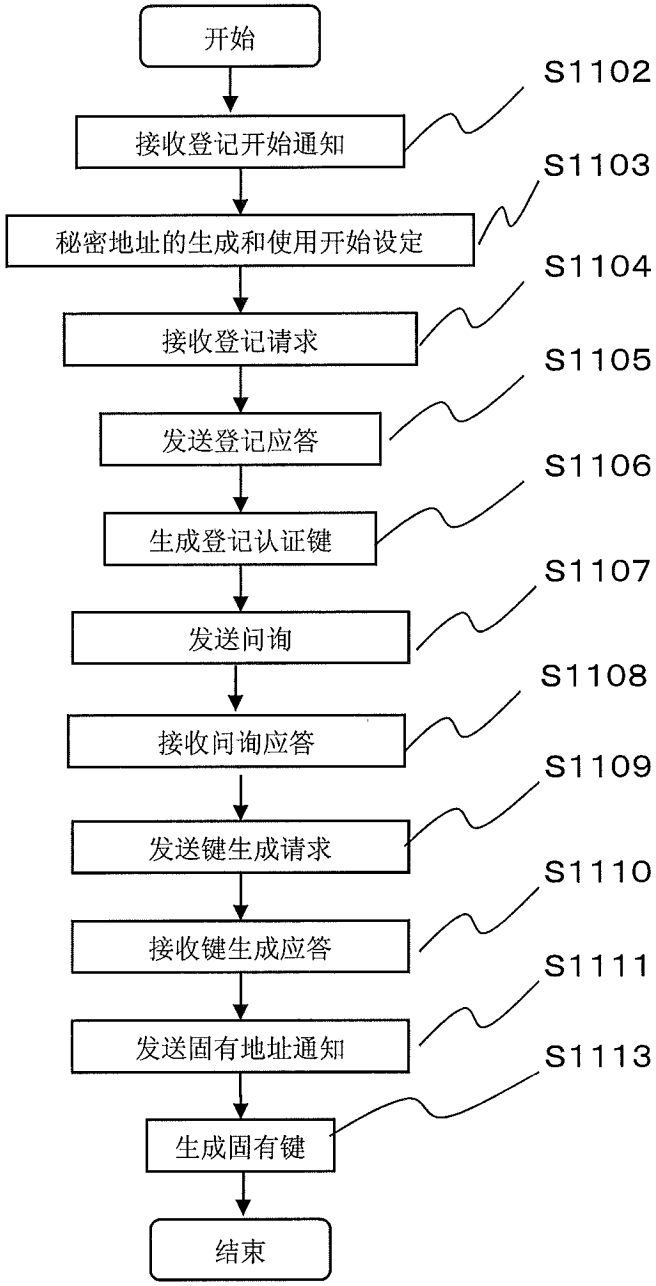

开始
S1102
接收登记开始通知
S1103
秘密地址的生成和使用开始设定
S1104
接收登记请求
S1105
发送登记应答
S1106
生成登记认证键
S1107
发送问询
S1108
接收问询应答
S1109
发送键生成请求
S1110
接收键生成应答
S1111
发送固有地址通知
S1113
生成固有键
结束

图 22

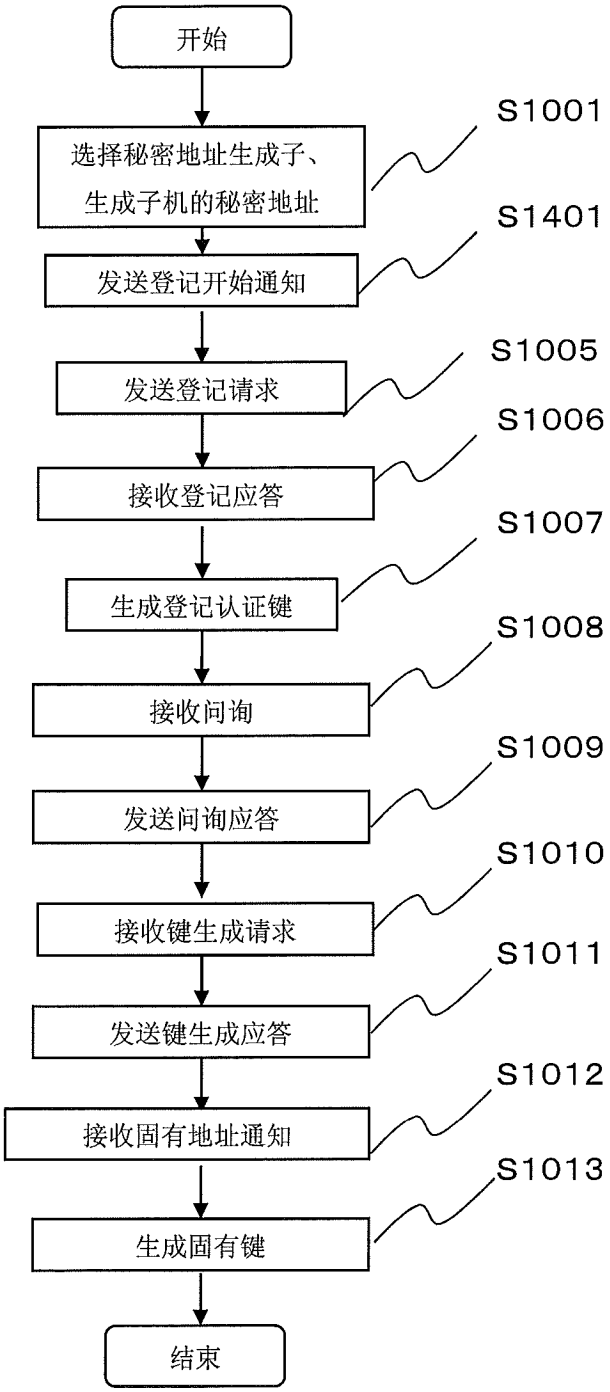

开始
选择秘密地址生成子、
生成子机的秘密地址
S1001
发送登记开始通知
S1401
发送登记请求
S1005
接收登记应答
S1006
生成登记认证键
S1007
接收问询
S1008
发送问询应答
S1009
接收键生成请求
S1010
发送键生成应答
S1011
接收固有地址通知
S1012
生成固有键
S1013
结束

图 23

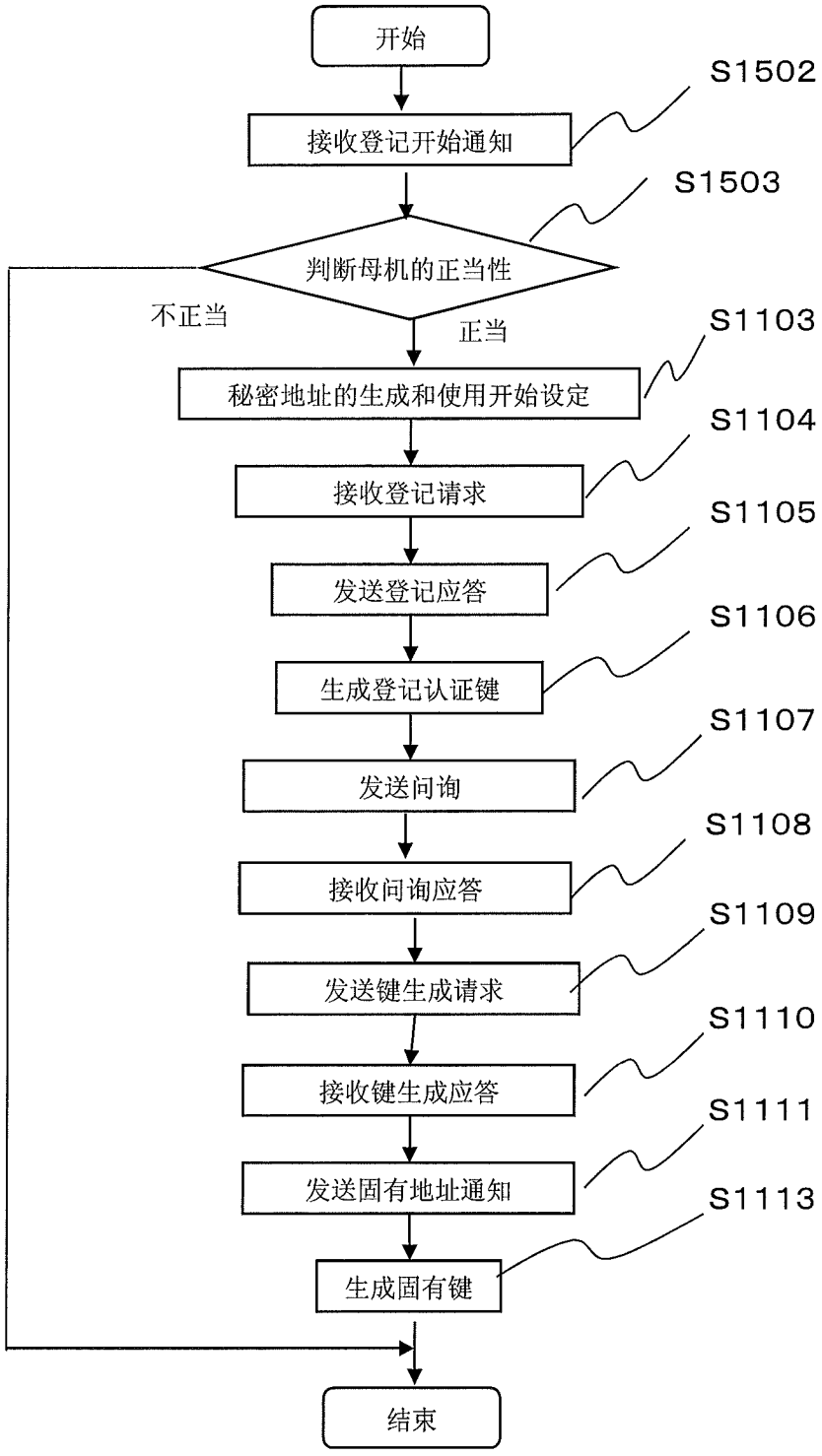

开始
S1502
接收登记开始通知
S1503
判断母机的正当性
不正当
正当
S1103
秘密地址的生成和使用开始设定
S1104
接收登记请求
S1105
发送登记应答
S1106
生成登记认证键
S1107
发送问询
S1108
接收问询应答
S1109
发送键生成请求
S1110
接收键生成应答
S1111
发送固有地址通知
S1113
生成固有键
结束

图 24

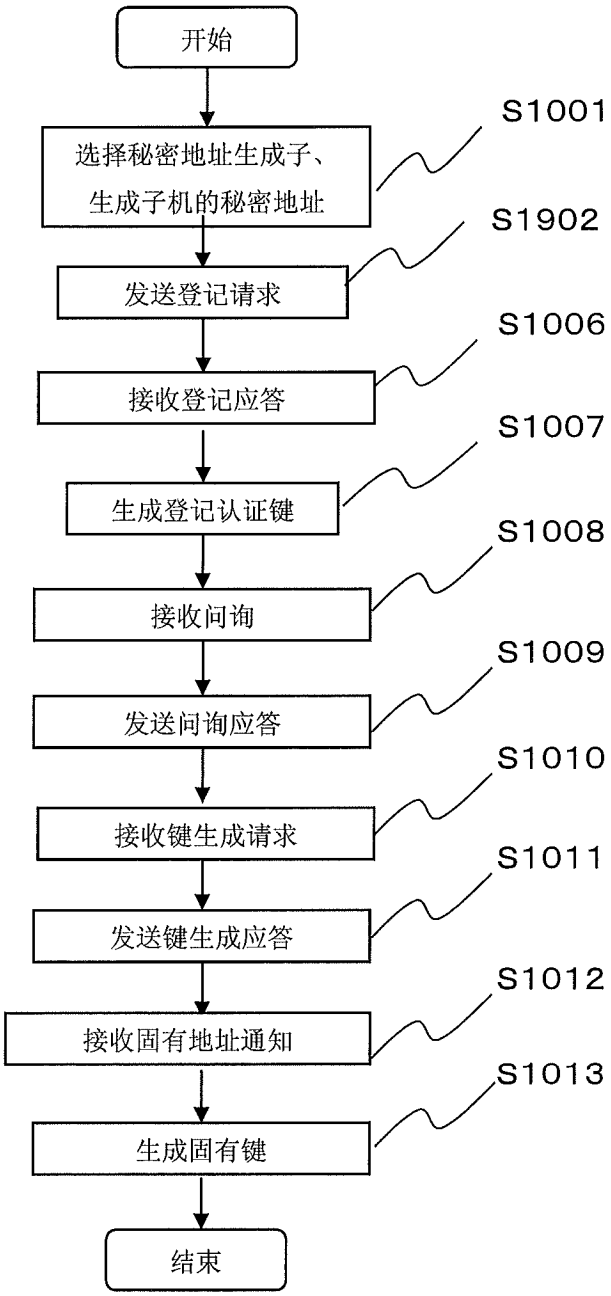

开始
选择秘密地址生成子、
生成子机的秘密地址
S1001
发送登记请求
S1902
接收登记应答
S1006
生成登记认证键
S1007
接收问询
S1008
发送问询应答
S1009
接收键生成请求
S1010
发送键生成应答
S1011
接收固有地址通知
S1012
生成固有键
S1013
结束

图 25

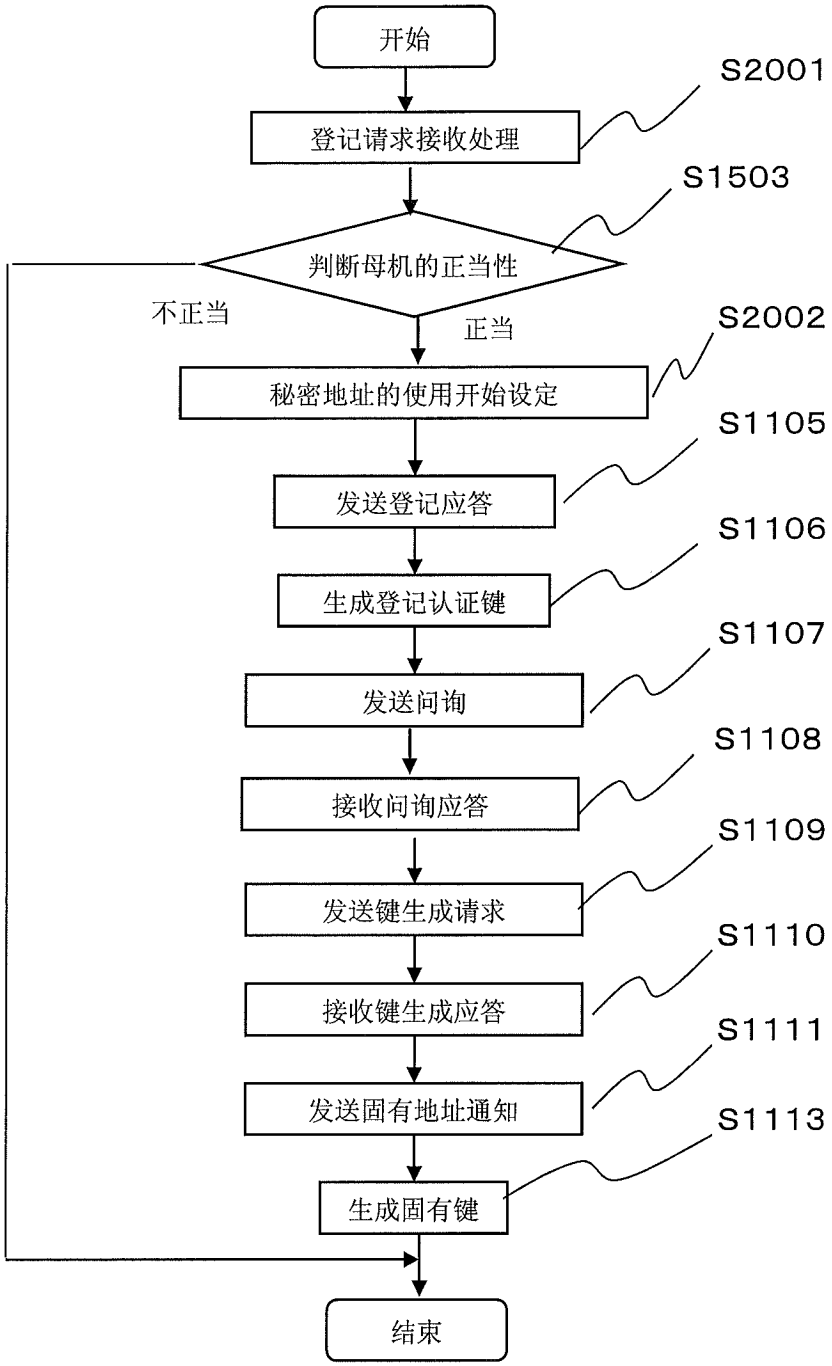

开始
S2001
登记请求接收处理
S1503
判断母机的正当性
不正当
正当
S2002
秘密地址的使用开始设定
S1105
发送登记应答
S1106
生成登记认证键
S1107
发送问询
S1108
接收问询应答
S1109
发送键生成请求
S1110
接收键生成应答
S1111
发送固有地址通知
S1113
生成固有键
结束

图 26

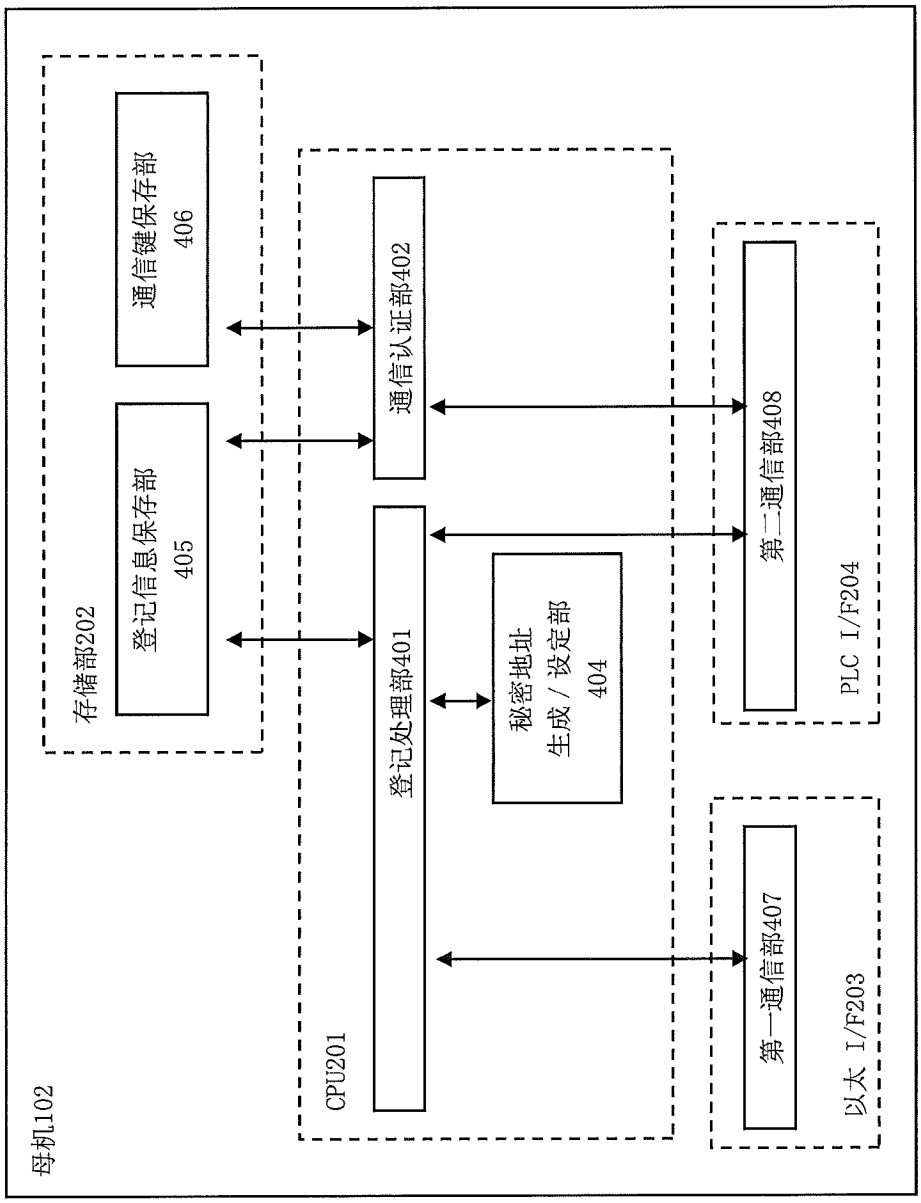

母机102
存储部202
通信键保存部
406
登记信息保存部
405
CPU201
通信认证部402
登记处理部401
秘密地址
生成 / 设定部
404
PLC I/F204
第二通信部408
以太 I/F203
第一通信部407

图 27

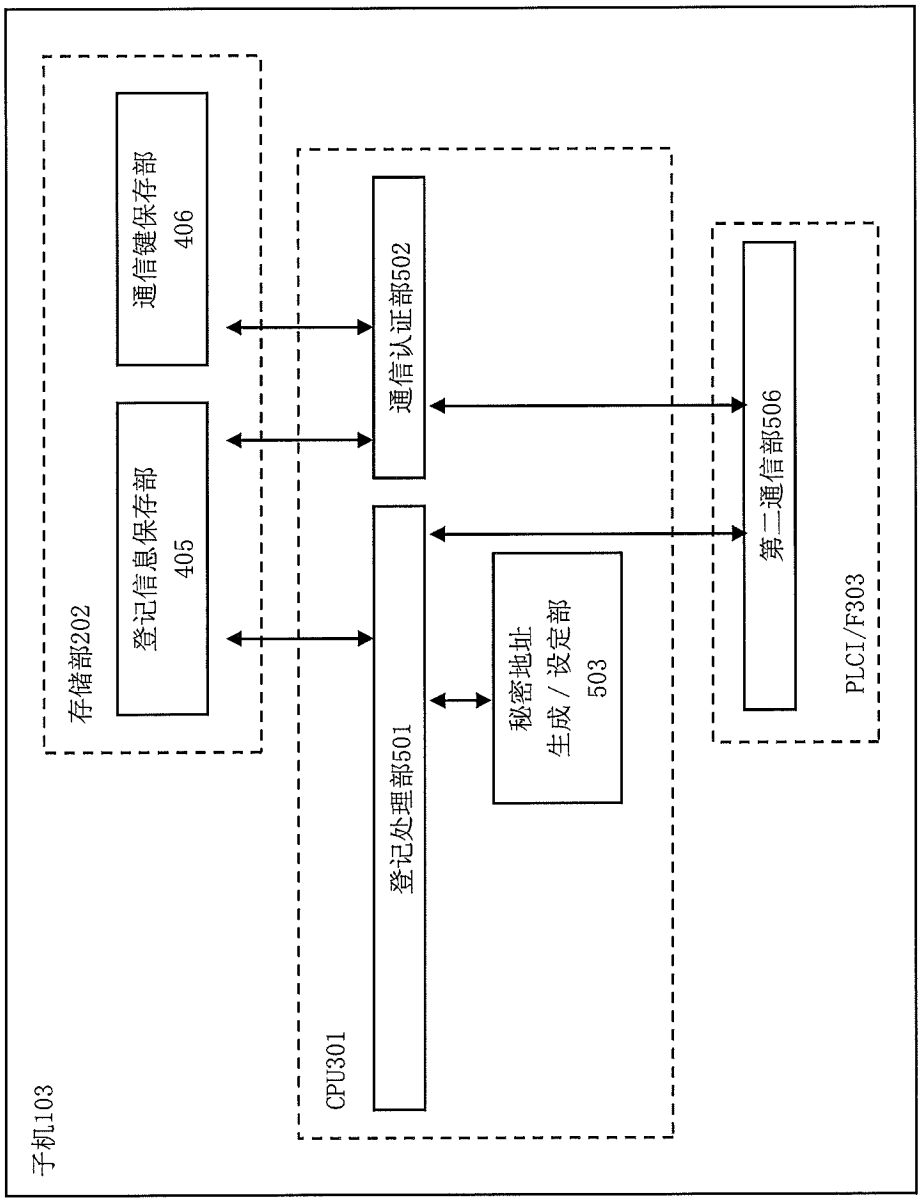

子机103
存储部202
通信键保存部
406
登记信息保存部
405
CPU301
通信认证部502
登记处理部501
秘密地址
生成 / 设定部
503
PLCI/F303
第二通信部506

图 28

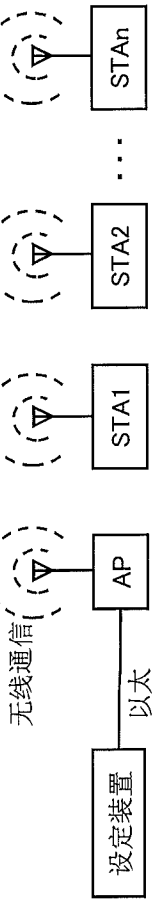

无线通信
AP
以太
设定装置
STA1
STA2
STAn

图 29

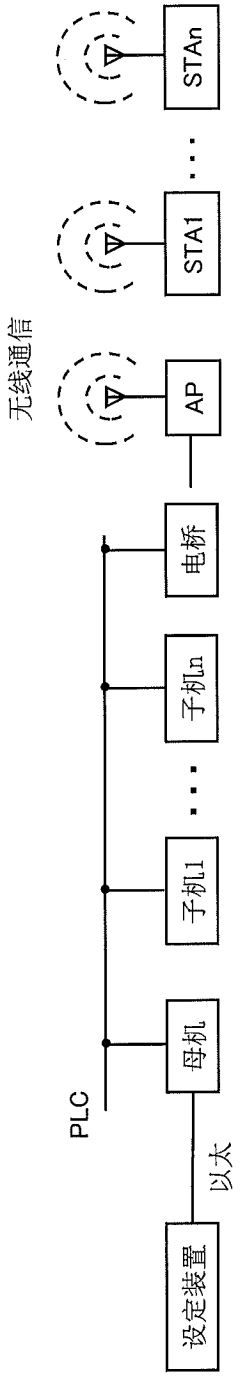

无线通信
AP
电桥
PLC
母机
以太
设定装置
子机1
子机n
STA1
STAn

图 30