[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 15/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 03152700.0

[45] 授权公告日 2007 年 2 月 28 日

[11] 授权公告号 CN 1302407C

[22] 申请日 2003.7.8 [21] 申请号 03152700.0

[30] 优先权

[32] 2002. 7. 8 [33] JP [31] 198719/02

[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 峰村淳

[56] 参考文献

CN1256599A 2000.6.14

US4786790A 1988.11.22

CN1326654A 2001.12.12

WO0075883A1 2000.12.14

审查员 尹 杰

[74] 专利代理机构 北京市柳沈律师事务所

代理人 邸万奎 黄小临

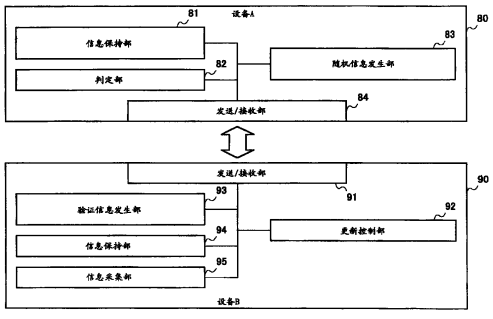
权利要求书 4 页 说明书 11 页 附图 5 页

[54] 发明名称

设备验证系统

[57] 摘要

一种设备验证系统，能够安全可靠地对没有安全区域的设备实体进行验证。 在该系统中，存储装置(10)验证便携式电话(20)。 在该系统中，存储装置(10)在安全区域保持密钥(12)，便携式电话保持序号(21)，并根据序号和用户提供的识别信息产生密钥，存储装置(10)对其中保持的密钥(12)与便携式电话(20)中产生的密钥之间的一致性作出判定，来验证便携式电话(20)。 在验证处理中，可以限制保存在存储设备(10)中的数据仅对特定的便携式电话使用。



1、一种设备验证系统，其中第一设备验证第二设备，其中所述第一设备包括:

向/从所述第二设备发送和接收信息的发送/接收部;

在安全区域保持第一验证信息的第一信息保持部；以及

对验证作出判定的判定器，

所述第二设备包括:

向/从所述第一设备发送和接收信息的发送/接收部;

保持作为所述第二设备的特定信息的第二验证信息的第二信息保持部;

从所述第二设备的外部采集第三验证信息的信息采集器；以及

根据所述第二验证信息和所述第三验证信息产生第四验证信息、并通过所述发送/接收部向所述第一设备输出所述第四验证信息的验证信息发生器，

其中所述判定器对所述第一验证信息和所述第四验证信息之间的一致性作出判定以验证所述第二设备。

2、根据权利要求 1 的设备验证系统，其中所述第二验证信息在进行第一次验证的时候是所述第二设备的特定信息。

3、根据权利要求 2 的设备验证系统，其中在进行第二次及其随后的验证的时候，所述第二验证信息是所述第一设备中产生的随机信息。

4、根据权利要求 3 的设备验证系统，其中在执行验证处理时更新所述第二验证信息，并且根据所述第二验证信息的更新，更新所述第一设备的所述第一信息保持部中保持的所述第一验证信息。

5、根据权利要求 1 的设备验证系统，其中当所述第一设备不保持所述第一验证信息时，执行与所述第一设备相互验证的设备从所述第二设备采集所述第四验证信息，并且在所述第一设备设置所述第一验证信息作为初始设置。

6、根据权利要求 1 的设备验证系统，其中所述第三验证信息保持在执行与所述第一设备相互验证的设备中，并且在验证处理中将其从该设备提供到所述第二设备。

7、一种设备验证方法，其中第一设备验证第二设备，其中所述第一设备在安全区域保持第一验证信息，

保持作为所述第二设备的特定信息的第二验证信息的所述第二设备根据

所述第二验证信息和从所述第二设备的外部提供的第三验证信息产生第四验证信息，和

所述第一设备对所述第一验证信息和所述第四验证信息之间的一致性作出判定，以验证所述第二设备。

8、如权利要求 7 所述的设备验证方法，还包括:

向所述第一设备请求随机信息的发布的步骤;

用所述第四验证信息加密从所述第一设备接收到的该随机信息，以输出到所述第一设备的步骤；和

所述第一设备对以第一验证信息解码所述加密的随机信息的结果与所述随机信息进行比较，来对第一验证信息和第四验证信息之间的一致性作出判定的步骤。

9、一种在具有第一设备以及被所述第一设备验证的第二设备的设备验证系统中的所述第二设备，包括:

向/从所述第一设备发送和接收信息的发送/接收部;

保持作为所述第二设备的特定信息的第二验证信息的信息保持部;

从所述第二设备的外部采集第三验证信息的信息采集器;

根据所述第二验证信息和所述第三验证信息产生第四验证信息、并通过所述发送/接收部向所述第一设备输出所述第四验证信息的验证信息发生器。

10、根据权利要求 9 的第二设备，其中所述发送/接收部接收来自所述第一设备的随机信号，并且所述验证信息发生器用所述第四验证信息加密所述随机信息，以通过所述发送/接收部发送给所述第一设备。

11、根据权利要求 9 的第二设备，其中所述发送/接收部接收来自所述第一设备的随机信息，并且所述验证信息发生器用所述随机信息加密所述第四验证信息，以通过所述发送/接收部发送给所述第一设备。

12、根据权利要求 9 的第二设备，进一步包括:

控制验证处理所需的信息的更新的更新控制部，

其中从所述第一设备的验证成功后，代替所述第二验证信息，所述更新控制部在所述信息保持部中存储随机信息作为新的第二验证信息，根据所述第三验证信息和该随机信息产生密钥信息，该密钥信息是新的验证信息，并通过所述发送/接收部使所述第一设备保持该密钥信息。

13、根据权利要求 10 的第二设备，进一步包括:

控制验证处理所需的信息的更新的更新控制部，

其中从所述第一设备的验证成功后，代替所述第二验证信息，所述更新控制部在所述信息保持部中存储随机信息作为新的第二验证信息，根据所述第三验证信息和该随机信息产生密钥信息，该密钥信息是新的验证信息，并通过所述发送/接收部使所述第一设备保持该密钥信息。

14、根据权利要求 11 的第二设备，进一步包括:

控制验证处理所需的信息的更新的更新控制部，

其中从所述第一设备的验证成功后，代替所述第二验证信息，所述更新控制部在所述信息保持部中存储随机信息作为新的第二验证信息，根据所述第三验证信息和该随机信息产生密钥信息，该密钥信息是新的验证信息，并通过所述发送/接收部使所述第一设备保持该密钥信息。

15、一种在具有验证第二设备的第一设备、以及将第四验证信息输出到所述第一设备的所述第二设备的设备验证系统中的所述第一设备，包括:

向/从所述第二设备发送和接收信息的发送/接收部;

在安全区域保持第一验证信息的信息保持部；以及

对根据作为所述第二设备的特定信息的第二验证信息和从所述第二设备的外部所采集的第三验证信息所产生、并通过所述发送/接收部从所述第二设备接收的第四验证信息与所述第一验证信息的一致性作出判定的判定器，

其中，所述判定器对所述第一验证信息和所述第四验证信息之间的一致性作出判定，以验证所述第二设备。

16、根据权利要求 15 的第一设备，进一步包括:

随机信息发生器，产生随机信息，以通过所述发送/接收部发送给所述第二设备，

其中，所述判定器用所述第一验证信息解码所述发送/接收部中接收的信息，对解码信息和所述随机信息的一致性做判定。

17、根据权利要求 15 的第一设备，进一步包括:

随机信息发生器，产生随机信息，以通过所述发送/接收部发送给所述第二设备，

其中，所述判定器用随机信息解码所述发送/接收部中接收的信息，对解码信息和所述第一验证信息的一致性做判定。

18、根据权利要求 15 的第一设备，其中:

在所述第二设备的验证成功后，代替所述第一验证信息，所述信息保持部保持在所述发送/接收部中接收的密钥信息，作为新的第一验证信息，该密钥信息是新验证信息。

19、根据权利要求 16 的第一设备，其中：

在所述第二设备的验证成功后，代替所述第一验证信息，所述信息保持部保持在所述发送/接收部中接收的密钥信息，作为新的第一验证信息，该密钥信息是新验证信息。

20、根据权利要求 17 的第一设备，其中：

在所述第二设备的验证成功后，代替所述第一验证信息，信息保持部保持在所述发送/接收部中接收的密钥信息，作为新的第一验证信息，该密钥信息是新验证信息。

设备验证系统

技术领域

本发明涉及一种在设备之间执行验证的设备验证系统及其验证方法、实现该方法的设备、以及用于规定该设备的操作的计算机程序，尤其是，能对不具备保存验证密钥的安全区域的设备进行外部验证。

背景技术

实体验证通常用来确认正在通讯的当事方的身份，或者确认请求连接到提供文件共享服务的计算机的用户是否是给予了访问权的合法用户。

实体验证的方案有很多。在其中的询问/应答方案中，例如，两个有关的当事方，A和B，秘密地具有对称的秘钥，其中一个当事方A产生随机数（询问）以供给另一方B，然后B使用与A对称的密钥将该随机数加密，从而将得到的数值（应答）返回给A。A使用该对称密钥解码该应答、以及如果应答与询问之间不矛盾，则确认B是合法的当事方。

近些年，借助存储装置执行相互验证处理的写/读控制微计算机得到发展并出现在市场上，其中存储装置具有用于加密处理的集成CPU或者协同处理器。微处理器具有控制存储装置的写/读的集成控制器，在配备微计算机的装置中，微处理器与插入该设备中的存储装置执行相互验证。

近期，研究出一种方案，该方案能将存储装置插入能上因特网的移动电话，并能在存储装置中存入其内容：例如，通过便携式电话从业务服务器上获得的音乐、图象以及游戏软件。

这种情况下，为了保证存储在存储装置中的数据仅在下载数据的便携式电话中使用，就产生了指定能够使用存储装置的便携式电话的想法。因为移动电信运营商限制向被征收信息服务费的承包商的便携式电话的内容传送服务，由此，将运营商从竞争者中区别开来，以增加承包者的数量。

利用装在便携式电话上的用于实体验证的存储装置，可以限制特定便携式电话的存储装置的使用，而且当便携式电话不是目标时，拒绝对该便携式电话的应答。

可以用上面嵌入有 IC 芯片的存储装置或者安全装置例如 IC 卡来秘密地保持对称密钥。然而，没有安全区域的便携式电话不能秘密地保持对称密钥。

进一步，把微计算机合并入与用存储装置执行相互验证处理的便携式电话，将带来如下问题：将在小型化和变薄方面损害便携式电话，并且成本将增长。

发明内容

本发明的目的是提供一种设备验证系统，能够安全可靠地对不带有安全区域的设备进行实体验证，进一步提供一种验证方法、实现该方法的设备、以及规定操作的计算机程序。

本发明的上述目的通过以下方式达到：从第二设备的验证信息（第二验证信息）以及例如用户输入的验证信息（第三验证信息）中产生新的验证信息（第四验证信息），并对新的验证信息和第一设备中的安全区域带有的验证信息（第一验证信息）的一致性作出判断。

根据本发明的一个方面，在设备验证系统中第一设备验证第二设备，第一设备具有发送/接收部、第一信息保持部、判定器，发送/接收部用来向/从第二设备发送和接收信息，第一信息保持部在安全区域保持第一验证信息，判定器对验证作出决定；第二设备具有发送/接收部、第二信息保持部、信息采集器、验证信息发生器、判定器，发送/接收部用来向/从第一设备发送和接收信息，第二信息保持部在安全区域保持作为第二设备的特定信息的第二验证信息，信息采集器从第二设备的外面采集第三验证信息，验证信息发生器从第二验证信息和第三验证信息中产生第四验证信息并通过发送/接收部向第一设备输出第四验证信息，判定器判断在第一验证信息和第四验证信息之间的一致性从而验证第二设备。

根据本发明的另一方面，在设备验证方法中第一设备验证第二设备，第一设备在安全区域保持第一验证信息，保持作为第二设备的特定信息的第二验证信息的第二设备产生第四验证信息，第四验证信息由第二验证信息和从第二设备的外面提供的第三验证信息产生，第一设备对第一验证信息和第四验证信息之间的一致性作出判断来验证第二设备。

根据本发明的再一方面，一种在具有第一设备以及被第一设备验证的第二设备的设备验证系统中的第二设备具有发送/接收部、信息保持部、信息采

集器以及验证信息发生器；发送/接收部用来向/从第一设备发送和接收信息，信息保持部保持作为第二设备的特定信息的第二验证信息，信息采集器从第二设备的外面采集第三验证信息，验证信息发生器从第二验证信息和第三验证信息中产生第四验证信息并通过发送/接收部向第一设备输出第四验证信息。

根据本发明的又一方面，一种在具有验证第二设备的第一设备、以及将第四验证信息输出到第一设备的第二设备的设备验证系统中的第一设备具有发送/接收部、信息保持部、判定器；发送/接收部用来向/从第二设备发送和接收信息，信息保持部在安全区域保持第一验证信息，判定器对根据作为第二设备的特定信息的第二验证信息和从第二设备的外部所采集的第三验证信息所产生、并通过发送/接收部从第二设备接收的第四验证信息与第一验证信息的一致性作出判定。

根据本发明的再一方面，集成在要被第一设备验证的第二设备中的计算机程序指定计算机执行如下过程：从第二设备保持的第二验证信息以及从第二设备的外面采集的第三验证信息而产生第四验证信息，向第一设备请求随机信息的发布，用第四验证信息加密从第一设备接收到的随机信息并向第一设备输出。

附图说明

本发明的上述以及其他目的和特征从下述的说明和相应的附图将更清楚，其中一个实施例通过举例的方式解释，其中：

图 1 是本发明的一个实施例的设备验证系统的构成图 ；

图 2 是本发明的一个实施例的设备验证系统的初始设置程序图；

图 3 是本发明的一个实施例的设备验证系统中的存储设备的结构示例图；

图 4 是本发明的一个实施例的设备验证系统中的便携式电话的结构示例图；

图 5 是本发明的一个实施例的设备验证系统中的相互验证程序的图。

具体实施方式

在本发明的设备验证系统中，设备 A 根据询问(challenge)/应答机制验

证设备 B。

如图 1 所示，设备 A80 具有发送/接收部 84、信息保持部 81、判定部 82 以及随机信息发生部 83；发送/接收部 84 向/从设备 B90 发送和接收信息，信息保持部 81 在安全区域保持第一验证信息，判定部 82 对发送/接收部 84

接收到的验证信息（第四验证信息）与第一验证信息之间的一致性作出判定，随机信息发生部 83 产生随机信息例如随机数。同时，设备 B90 具有发送/接收部 91、非安全信息保持部 94、信息采集部 95、验证信息发生部 93 以及更新控制部 92；发送/接收部 91 向/从设备 A80 发送和接收信息，非安全信息保持部 94 保持第二验证信息，信息采集部 95 从设备 B90 外面采集第三信息，验证信息发生部 93 从第二验证信息和第三验证信息中产生用于验证的信息（第四验证信息），并且通过发送/接收部 91 向设备 B80 输出第四验证信息，更新控制部 92 更新信息保持部 94 中保持的第二验证信息。

在该系统中，将要被验证的设备 B 90 在验证信息发生部 93 中产生信息（第四验证信息）用于验证，该信息从信息保持部 94 保持的第二验证信息和信息采集部 95 从设备 B90 外面采集到的第三验证信息中产生。当产生第四验证信息时，设备 B90 请求设备 A80 发出随机信息。

一旦收到请求，设备 A80 就在随机信息发生部 83 中产生随机信息例如随机数并向设备 B90 输出。

设备 B90 用第四验证信息加密从设备 A80 接收到的随机信息，并向设备 A80 输出。

在设备 A80 中，判定部 82 用信息保持部 81 保持的第一验证信息解码从设备 B90 接收到的信息，校验解码信息与设备 B90 提供的随机信息是否匹配，并对第一验证信息与第四验证信息的一致性作出决定，而且如果达到一致，则证实设备 B90。

当验证成功时，则在设备 B90 中，更新控制部 92 通知信息保持部 94 保持从设备 A80 接收到的随机信息作为用于随后验证的第二验证信息。进一步，作为新验证信息的密钥信息由随机信息和第三验证信息产生，并通过发送/接收部 91 向设备 A80 输出。设备 A80 在安全的信息保持部 81 中保持作为用于随后的验证的第一验证信息的密钥信息。

此外，在该系统中，设备 B90 可随意地验证设备 A80。

以下将介绍实施例，其中进行验证的设备 A 是存储设备，将要被验证的设备 B 是便携式电话。在设备验证系统中，存储装置和便携式电话根据询问/应答机制执行相互验证。在询问/应答机制中，普通密钥由用户输入的验证信息和便携式电话中存储的数据动态地产生。

图 2 解释了其中的程序，当新存储装置 10 插入便携式电话 20 中时，最

初发布存储装置 10 的业务服务器 30 为存储装置 10 设置询问/应答机制中的密钥 12。

例如，如图 3 所示，存储装置 10 具有存储从业务服务器 30 上下载的内容的存储器 41（其由例如闪存构成）、以及控制存储器 41 中的数据写/读的抗干扰存储控制器 42。存储控制器 42 具有 CPU43、RAM44、ROM45、内部非易失存储器 46、加密协同处理器 47、输入/输出部（I/O）48 以及 I/O 49；其中，CPU 43 用来控制存储装置 10 的操作，RAM44 在 CPU 43 的工作区域中使用，ROM 45 存储 CPU 43 的特定操作程序，抗干扰的内部非易失存储器 46 由例如，EEPROM 构成，加密协同处理器 47 执行计算处理，例如按 CPU 43 指令的加密处理，输入/输出部（I/O）48 与便携式电话 20 进行数据通讯，I/O 49 带有存储器 41。

例如，如图 4 所示，便携式电话 20 具有存储装置插槽 51、无线通讯部 57、CPU 52、ROM 53、EEPROM 54、液晶显示（LCD）器 55、语音处理部 60 以及用于开关 61 的密钥控制部 62；其中，存储装置插槽 51 用于插入存储装置 10，无线通讯部 57 与业务服务器 30 通过天线 56 进行通讯，CPU52 控制便携式电话 20 的操作，ROM53 存储用来指定 CPU52 的操作的程序，写入 EEPROM 54 中的数据用来产生询问/应答机制中的密钥，语音处理部 60 用于麦克风 58 和扬声器 59。

业务服务器 30 是，例如，执行内容分配服务的服务提供器的官方站点。被业务提供者操作的业务服务器 30 与电信运营商的运营商网关（GW）31 相连，运营商网关（GW）确保与业务服务器 30 相接的便携式电话 20 电话号码的真实性。换句话，只有与业务提供者签订协议的便携式电话才能够进入官方站点业务服务器 30。

在图 2 中，运行业务服务器 30 的业务提供者将业务服务器 30 的公共密钥和存储装置的私人密钥 13 发给存储器 10，存储装置的私人密钥 13 存储在抗干扰的内部非易失存储器 46 中。

在便携式电话 20 中，序号 21 存储在 EEPROM54 中，指定了相互验证的操作的应用程序 22 存储在 ROM 53 中。

当存储装置 10 插入便携式电话 20 的存储装置插槽 51 中时，存储装置 10 和便携式电话 20 执行相互验证。当存储装置 10 没有设置相互验证的信息时，便携式电话 20 与业务服务器 30 相连，为存储装置 10 初始设置相互

验证的信息的过程根据下面的程序执行。

①业务提供者向存储装置 10 发命令。

②用户将未设置相互验证信息的存储装置 10 插入便携式电话 20 中。

③便携式电话 20 的应用程序 22 通过运营商网关 31 与业务服务器 30 相连，并请求存储装置 10 与业务服务器 30 之间的相互验证。

④业务服务器 30 发送指示询问命令（随机数）的 Getchallenge（动态信息发布命令）。命令绕过便携式电话 20 直接发送到存储装置 10 中。根据该命令，存储装置 10 产生询问（随机数）并发送到业务服务器 30。业务服务器 30 用服务器密钥加密该随机数来产生应答，发送该应答和指示服务器对存储装置 10 验证的 External Authenticate（外部验证命令）。存储装置 10 用服务器公共密钥 11 解码该加密的随机数，如果应答与询问之间没有矛盾，则确认业务服务器 30 为一个合法方。存储装置 10 和业务服务器 30 从反方向执行同样的程序，从而该业务服务器 30 确认存储装置 10。这时，使用了存储装置 10 的密钥 30。当完成相互验证后，业务服务器 30 和存储装置 10 建立起其间使用安全信息的秘密通讯途径。

⑤业务服务器 30 通知应用程序产生一个密钥。

⑥一旦接到通知，应用程序 22 指示用户通过液晶显示（LCD）屏 55 输入识别信息。

⑦当用户输入识别信息后，应用程序 22 利用序号 21 和识别信息产生密钥并且发送到业务服务器 30。

⑧业务服务器 30 将从便携式电话 20 得到的密钥发送到存储装置 10。一旦接收到密钥信息，存储装置 10 就将信息存储到抗干扰内部非易失存储器 46 中。

这样，为存储装置 10 设置密钥 12 作为初始设置。因为密钥 12 从便携式电话 20 的序号 21 和用户想出的识别信息中产生，因此即使第三方知道存储在便携式电话 20 的序号 21，但也不能产生与密钥 12 相同的密钥。

以下将介绍当设置密钥 12 的存储装置 10 插入便携式电话 20 中时，执行存储装置 10 和便携式电话 20 之间相互验证的程序。

如图 5 所示：

①用户将存储装置 10 插到便携式电话 20 中。

②应用程序 22 输出指令，让用户通过液晶显示（LCD）屏 55 输入识别

信息。

③当用户输入该识别信息时，应用程序 22 根据序号 21 和识别信息产生密钥。

④应用程序 22 向存储装置 10 发出 Getchallenge 命令。一旦接收到该命令，存储装置 10 就为该询问产生随机数并向应用程序 22 输出，应用程序 22 获得该随机数。

⑤应用程序 22 利用在③中产生的密钥为该询问加密已获得的随机数。

⑥应用程序 22 向存储装置 10 发出 External Authenticate，并且把在⑤中加密的询问的随机数向存储装置 10 提供。

⑦存储装置 10 为使用密钥 12 的询问校验该加密的随机数。校验是一个使用密钥 12 进行解码的处理，并对经解码得到的信息（用于询问的随机数）和用于产生并保存在存储装置 10 中的询问的随机数之间的一致性作出决定（原则上，判断是否达到匹配）。当达到一致（匹配）时，验证成功。验证成功后，允许便携式电话 20 的接入。另外，至于“匹配”，一致性判断和匹配判断的公知方法是宽泛的，包括当在上、下以及中间位数上的任意位数实现匹配（甚至并未达到全部匹配时），以及对于以决定为目标的所有位都匹配时，确定达到一致性。

进一步，存储装置 10 以及便携式电话 20 双方互换，便携式电话 20 产生并加密随机数。便携式电话 20 向存储装置 10 发送该加密随机数，并且存储装置 10 用保持的密钥解码该随机数并发送回便携式电话 20。

⑧当外部验证在⑦中成功后，应用程序 22 把在④中获得的询问的随机数 23 存储在 EEPROM54 中。在其后的相互验证将使用随机数 23 而不是序号 21。

⑨应用程序 22 根据存储在 EEPROM54 中的随机数 23 和识别信息产生密钥，以写到存储装置 10 中。因为密钥信息从被验证方发送，因此存储装置 10 接收该密钥信息并保存到抗干扰内部非易失存储器 46 中。密钥 12 用在下一个相互验证中。

如果存储装置 10 在⑦中外部验证失败，则存储装置 10 拒绝从便携式电话 20 的接入并停止操作。

以这种方式，在设备验证系统中，密钥是用储存在便携式电话 20 中的信息以及用户输入的识别信息来动态地产生的，初始设置后，存储设备 10

与便携式电话 20 之间的相互验证在脱机状态用密钥执行。因此，因为密钥没有存储在不带安全区域的便携式电话 20 中，可以阻止非法从便携式电话 20 中读出密钥信息。

进一步，因为在第一相互验证中使用了利用特定于便携式电话 20 的信息的密钥，因此能够使用存储装置 10 的设备就被局限于有特定信息的便携式电话 20。

进一步，在第二以及随后的相互验证过程中，因为使用的密钥是根据上次相互验证中的询问的随机数和用户设定的识别信息产生的，因此密钥在每次相互验证中变化，并且用来产生便携式电话中装载的密钥的数字在每次相互验证中变化。因此，即使遭受到拷贝攻击以致于在便携式电话 20 与存储设备 10 之间交换的信息被盗，也无需担心识别信息被解码，进一步，即使当便携式电话 20 中的数字被盗，也没有什么危险。据此，可很安全，防欺诈。

此外，如果是下述情形：存储装置 10 和便携式电话 20 执行相互（即双向）验证时，则仅当存储设备 10 验证便携式电话 20 时可以进行单向验证。

进一步，如果是下述情形，即当序号用作便携式电话 20 的特定信息时，可以使用电话号码。

进一步，如果是下述情形，即便携式电话 20 借用密钥加密由存储设备 10 提供的随机数时，可以进行相反操作，即便携式电话 20 用随机数加密该密钥从而提供给存储设备 10。在这种情形中，因为存储设备 10 知道这个随机数，因此存储设备 10 能够通过解码抽取这个密钥，从而与装置 10 中的密钥比较并验证便携式电话 20。

还有，存储设备 10 包括带有安全区域的存储介质例如非接触型 IC 卡、接触型 IC 卡、SD 卡、以及 MMC（多媒体卡）。

设备验证系统可以按以下修改：

（1）取代用户存储识别信息，用户在初始设置中设置及注册的识别信息保存在包括业务服务器 30 而不包括便携式电话的服务器中，当执行相互验证时，便携式电话 20 从服务器中读出该识别信息。在这种情形下，服务器保存与该便携式电话 20 的电话号码相关的识别信息设置、注册。在与存储设备 10 进行相互验证的同时，便携式电话 20 通知电话号码服务器，并采集识别信息来产生密钥。

以这种方式，因为用户不需要记住识别信息，因此能够消除由错误输入带来的验证失败。进一步，在最初设置中，代替用户设置和注册该识别信息，应用程序 22 产生识别信息发送给服务器，服务器登记该信息，于是，识别信息被保存而无需用户知道该信息，并且可以消除由于用户的非法操作而对存储设备 10 进行未经授权的访问。

（2）在初始设置中，用户将设置和已注册的识别信息保存在外部存储器，用户可携带独立于便携式电话 20 的外部存储器。在设备验证过程中，用户将外部存储器插入便携式电话 20，应用程序 22 从外部存储器中读出该验证信息以产生相互验证的密钥。用做外部存储器的例子包括非接触型 IC 卡、接触型 IC 卡、SD 卡、以及 MMC（多媒体卡）。

（3）在初始设置中，便携式电话 20 与用户保持的外部设备通讯，在外部设备中保存识别信息。在设备验证中，应用程序 22 通过便携式电话 20 与外部设备通讯，采集该识别信息来产生密钥，并执行设备验证。作为外部设备，例如便携式电话和 PDA 都可考虑，作为便携式电话 20 和外部设备之间的通讯方式，红外无线以及蓝牙都可考虑。这种情形下，当用户在便携式电话 20 附近保持外部设备以用于设备验证时，便携式电话 20 从外部设备读出该识别信息，从而执行设备验证。

（4）进一步，可以加密识别信息并保存在便携式电话 20 中，进一步保存用于分别解码在业务服务器 30 中、外部存储器或者外部设备（如在（1）至（3）所述）中的识别信息的解码密钥。

（5）代替联机状态下执行对存储设备 10 中的密钥的初始设置，存储设备 10 的发布源可以向存储设备 10 发布其中嵌入的密钥。在此情形下，用户通过电话向存储设备 10 的发布源通知便携式电话 20 的序号 21 以及识别信息，或者通过在用于释放存储设备 10 的商店指示便携式电话 20 的序号以及识别信息来申请存储设备 10 的发布。存储设备 10 的发布源从该信息产生密钥，并将其间嵌入有密钥的存储设备 10 提供给用户。

进一步，虽然实施例描述了不带安全区域的便携式电话 20 和带安全区域的存储设备 10 之间的相互验证的过程，但相互验证的目标设备并不局限于电话 20 和设备 10。

例如，本发明可应用于网络家用电器与插入各个电器的存储设备之间的相互验证。在此情形，与每个网络家用电器相连的家用服务器充当业务服务

器 30 的角色。在该系统中，如在前所述的改进（1）所示，以下这种情况是有效的，即家用服务器为每个网络家用电器集体管理识别信息，并且在与存储设备的相互验证中，每个网络家用电器从家用服务器采集各自的识别信息。

进一步，带有安全区域的设备不局限于存储设备，任何带有抗干扰（temper-resistant）区域的装置都可以。

从前面可以清楚看出，在本发明的设备验证系统以及方法中，可以安全可靠地对不带有安全区域的设备进行实体验证。

进一步，当在存储设备与便携式电话之间使用该系统和方法进行相互验证时，可以限制特定便携式电话使用保存在存储设备中的数据。

本发明不局限于上述实施例，在不偏离本发明的范围内可以作出多种变化和修改。

该申请以 2002 年 7 月 8 日提交的日本专利申请 NO.2002-198719 为基础，这里结合它的全部内容作为参考。

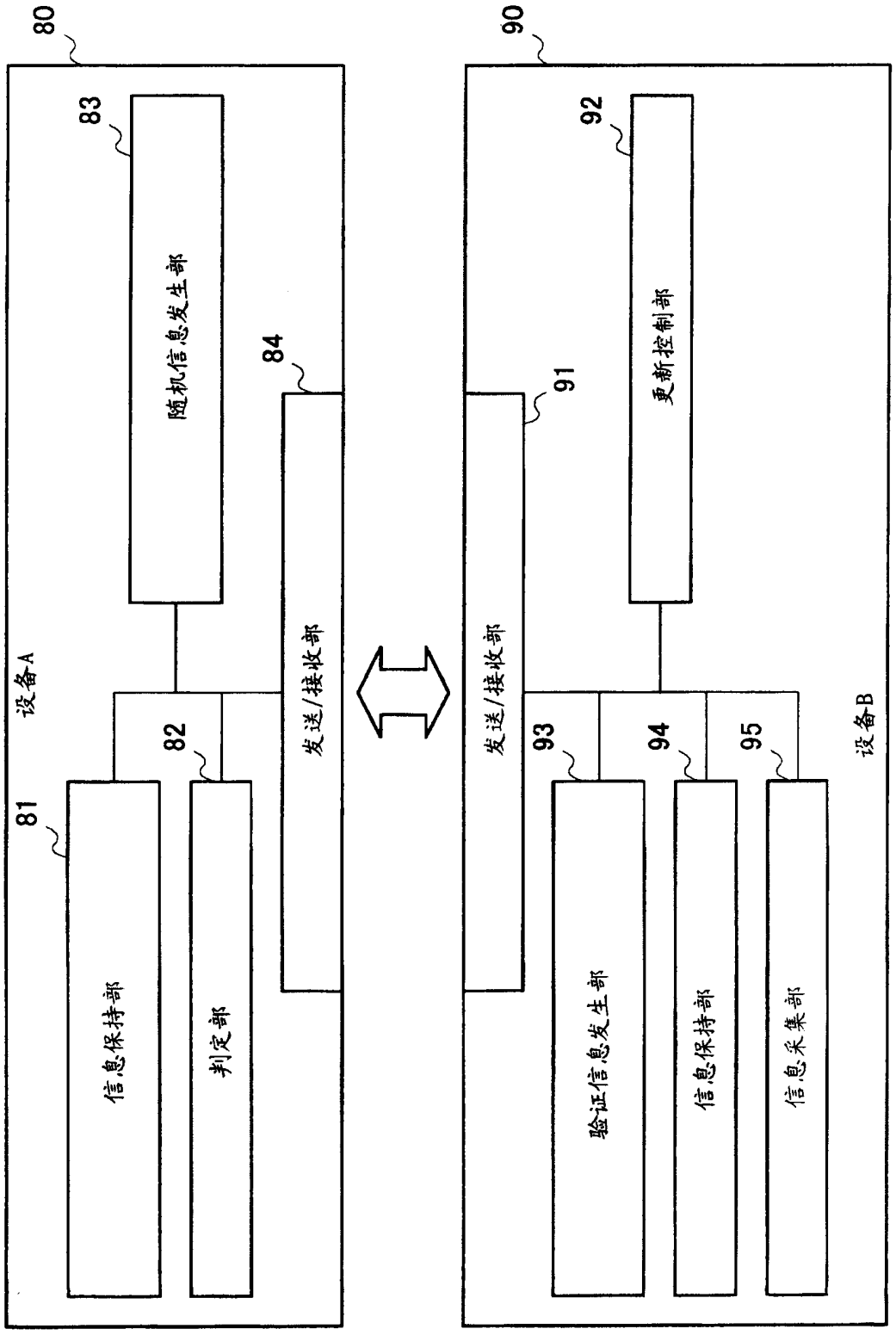

80
设备A
83
随机信息发生部
84
发送/接收部
82
判定部
81
信息保持部
90
设备B
92
更新控制部
91
发送/接收部
93
验证信息发生部
94
信息保持部
95
信息采集部

图 1

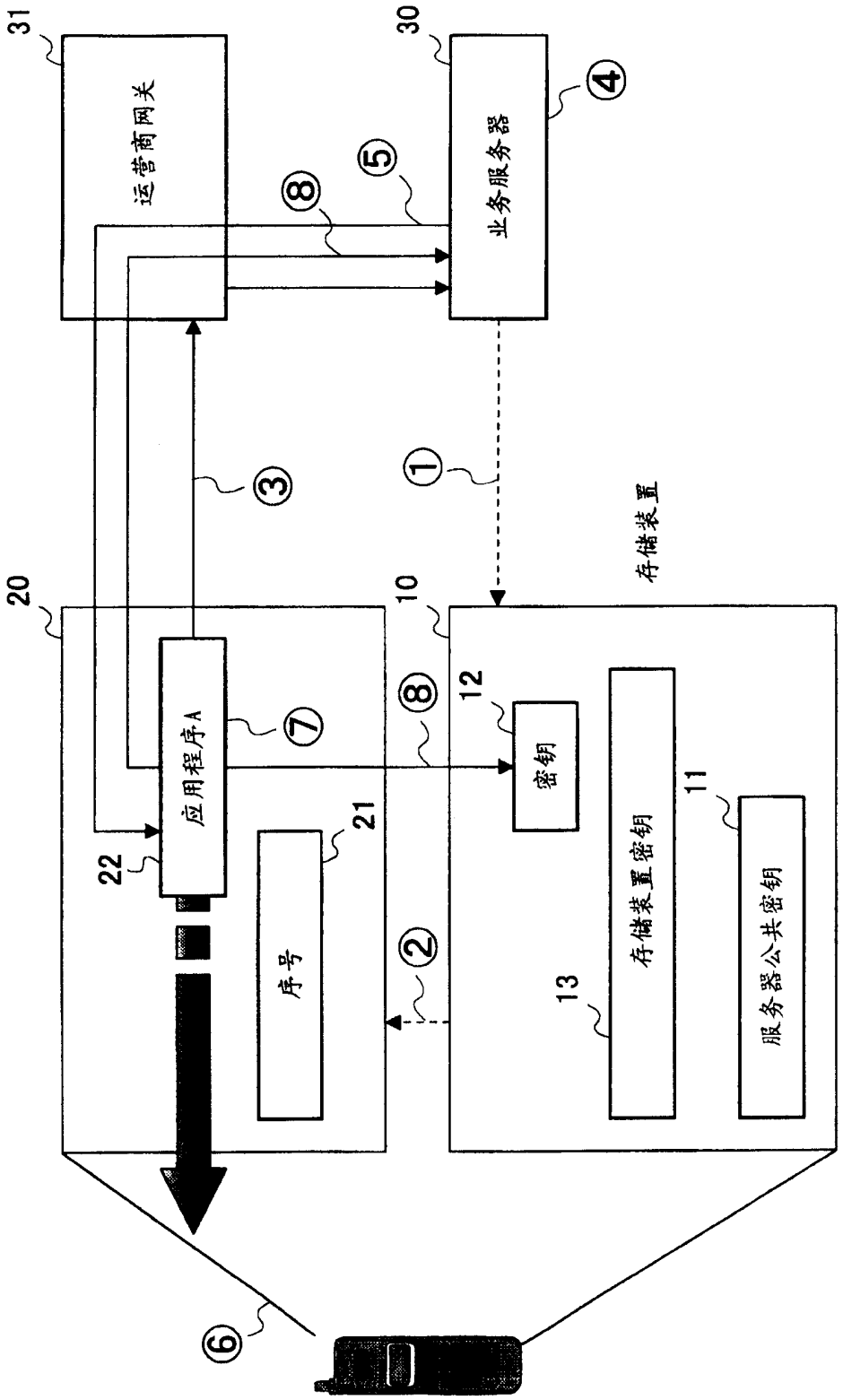

31
运营商网关
30
业务服务器
④
⑤
⑧
③
①
存储装置
20
10
应用程序A
⑦
⑧
12
密钥
22
21
序号
②
11
存储装置密钥
13
服务器公共密钥
⑥

图 2

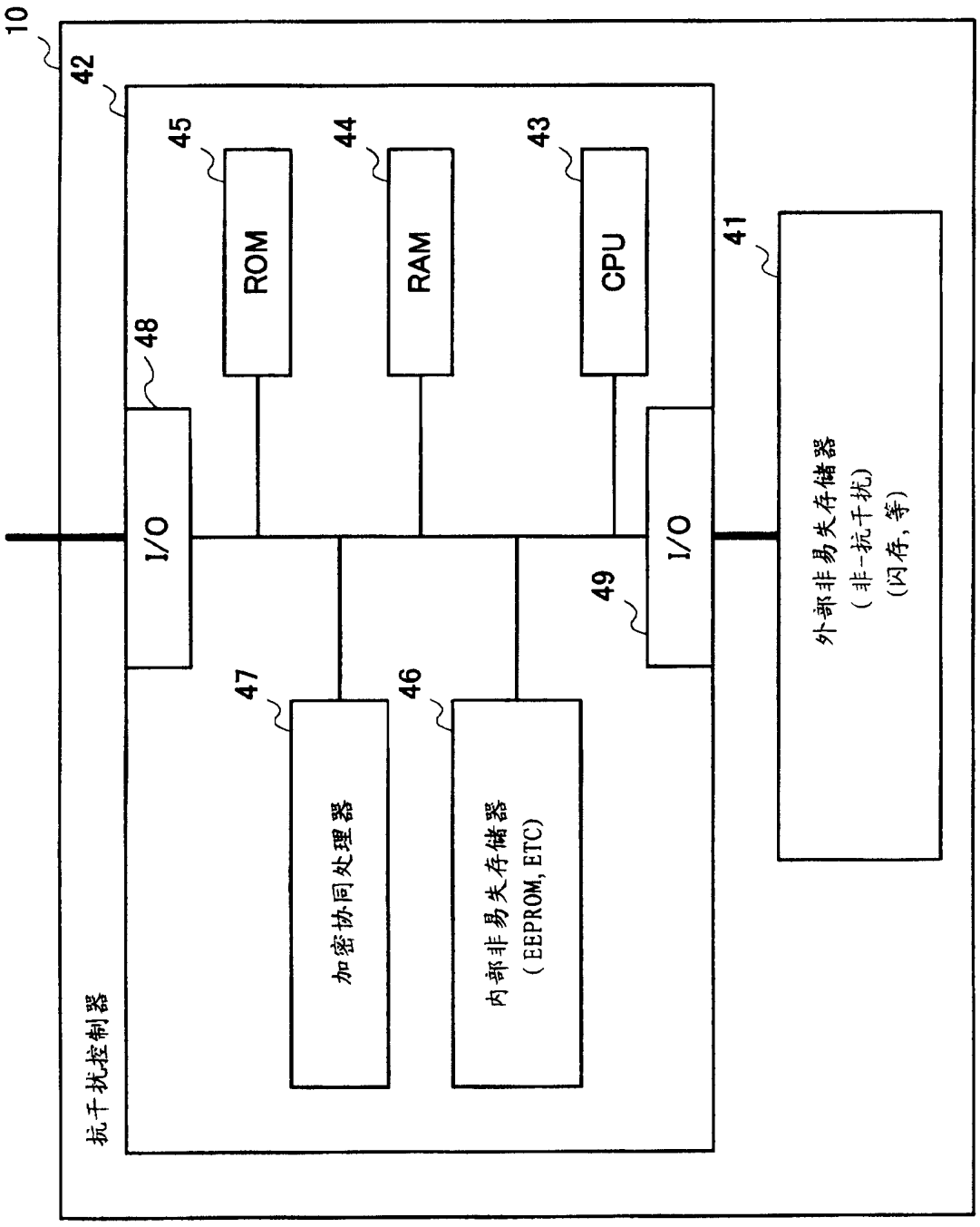

10
42
45
ROM
44
RAM
43
CPU
41
48
I/O
I/O
49
外部非易失存储器
(非-抗干扰)
(闪存,等)
47
加密协同处理器
46
内部非易失存储器
(EEPROM,ETC)
抗干扰控制器

图 3

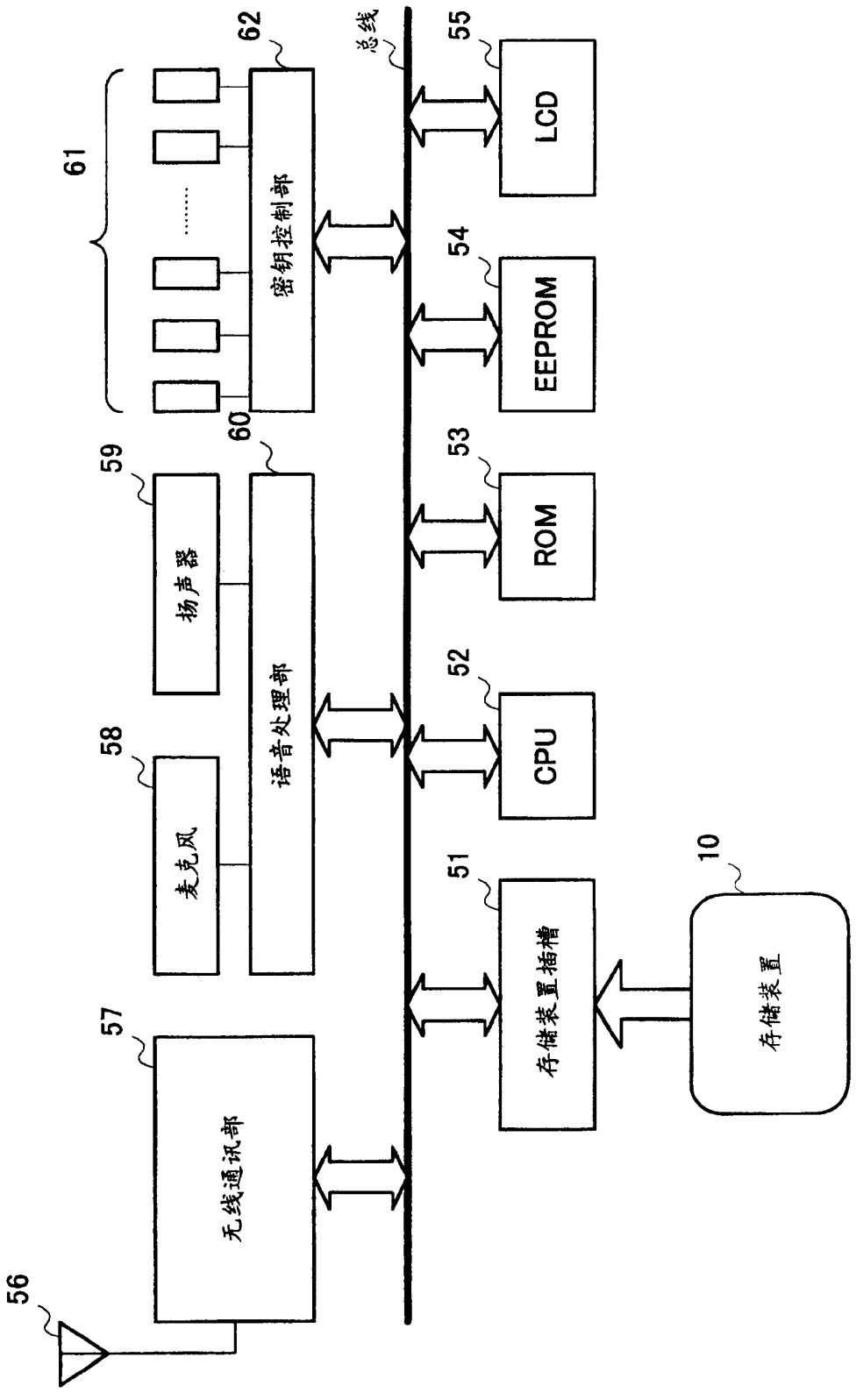

56
无线通讯部
57
麦克风
58
扬声器
59
语音处理部
60
密钥控制部
62
61
.....
总线
55
LCD
54
EEPROM
53
ROM
52
CPU
51
存储装置插槽
10
存储装置

图 4

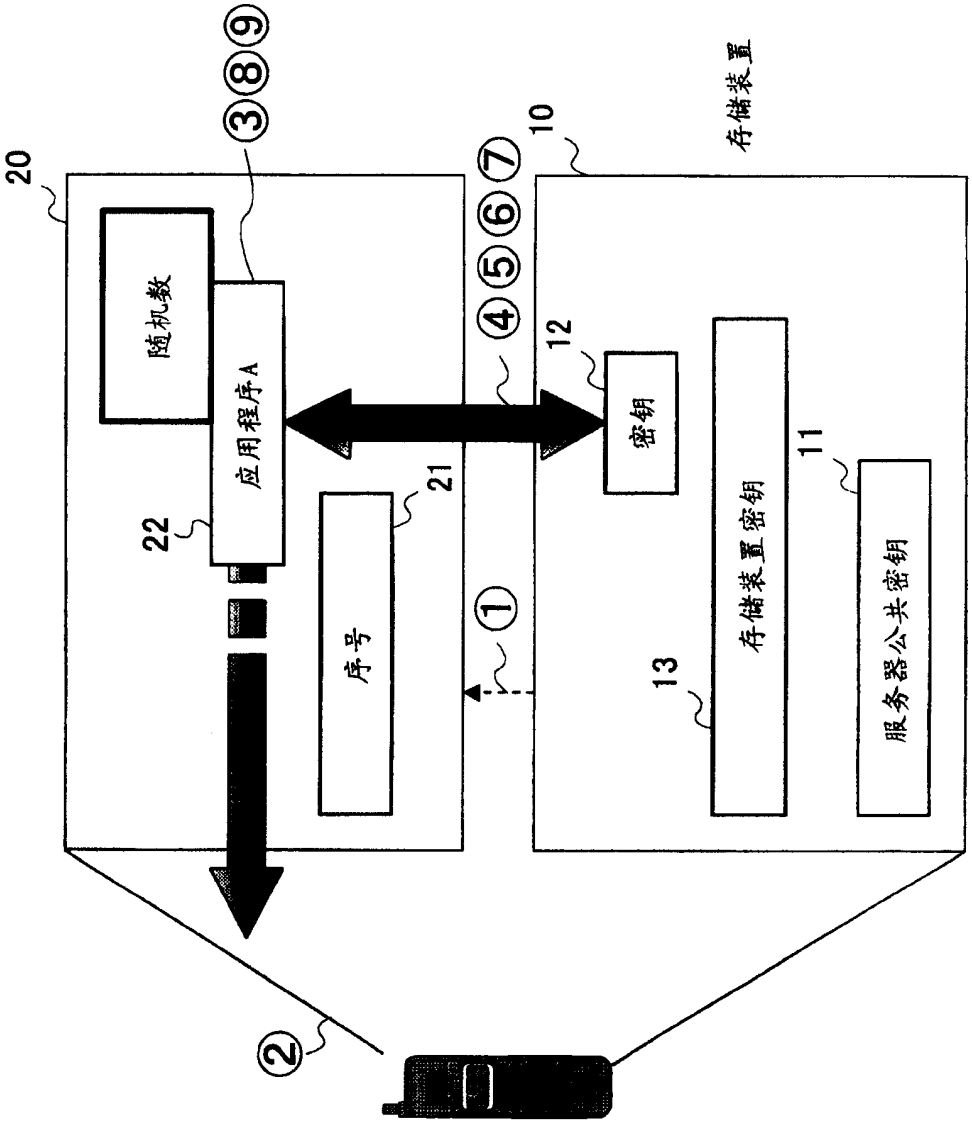

20
③⑧⑨
随机数
应用程序A
22
21
序号
①
②
④⑤⑥⑦
10
存储装置
12
密钥
13
存储装置密钥
11
服务器公共密钥

图 5