

[19] 中华人民共和国国家知识产权局



[12] 发明专利说明书

专利号 ZL 03141181.9

[51] Int. Cl.

H04L 9/00 (2006.01)

H04K 1/00 (2006.01)

G06F 13/00 (2006.01)

H04B 1/38 (2006.01)

[45] 授权公告日 2006 年 9 月 20 日

[11] 授权公告号 CN 1276610C

[22] 申请日 2003.6.5 [21] 申请号 03141181.9

[30] 优先权

[32] 2002.6.5 [33] JP [31] 164808/2002

[71] 专利权人 株式会社 NTT 都科摩

地址 日本东京

共同专利权人 坂村健 越塚登

[72] 发明人 石井一彦 森谦作 青野博

本乡节之 坂村健 越塚登

审查员 刘剑波

[74] 专利代理机构 中国国际贸易促进委员会专利
商标事务所

代理人 付建军

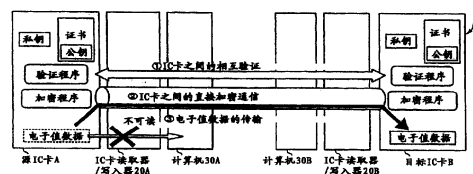
权利要求书 1 页 说明书 10 页 附图 5 页

[54] 发明名称

电子值数据通信方法及系统、IC 卡、便携终端和通信终端

[57] 摘要

本发明的目的是防止复制电子值数据本身。与传统的系统不同，在根据本发明的通信系统中，源 IC 卡 A 和目标 IC 卡 B 相互验证另一方，然后在这些 IC 卡 A、B 之间通过直接加密通信将电子值数据从 IC 卡 A 传输到 IC 卡 B，从而可以容易地防止第三方在通信路径中解密和篡改数据，并防止复制数据。



1. 一种 IC 卡，包括：

发送-接收天线；

密钥信息存储部件，用于存储其中附加有证书的公钥、私钥、以及来自目标 IC 卡的密钥信息；

程序存储部件，用于存储：验证程序，执行与目标 IC 卡进行相互验证的验证处理；以及加密通信程序，进行电子值数据的加密以及与目标 IC 卡之间的加密的电子值数据的传输；

电子值数据存储部件，用于存储非加密的电子值数据和加密的电子值数据；以及

程序执行部件，用于执行程序存储部件所存储的程序；

其中，配置程序执行部件以通过执行基于公钥和密钥信息的验证程序、以及当获得证实目标 IC 卡为合法方的验证结果时执行加密通信程序，来实施电子值数据的加密以及使用发送-接收天线来执行加密的电子值数据到目标 IC 卡的发送和从目标 IC 卡接收加密的电子值数据。

电子值数据通信方法及系统、 IC 卡、便携终端和通信终端

技术领域

本发明涉及与电子值数据传输有关的电子值数据通信方法、通信系统、IC 卡、便携终端和通信终端。这里的电子值数据代表例如电子票据、电子货币、电子礼物证书等。通信终端包括具有通信功能的便携终端（例如蜂窝电话、PHS、PDA、膝上个人计算机等）和信息处理设备（例如 POS 终端、台式个人计算机、服务器、主计算机等）。

背景技术

在使用 IC 卡的电子值数据的传统电子值流通中，在每一张 IC 卡中存储有特定卡的身份证明（ID）和密钥，并且通过这些手段来保护 IC 卡中的电子值数据。利用所述密钥的程序也存储在 IC 卡中，并且，即使 IC 卡的持有者也无法读出所述密钥，而仅能够使用 IC 卡中的程序。另一方面，为了保证 IC 卡的灵活性，IC 卡中的程序仅仅具备使用所述密钥进行认证和一般的加密功能，而读和写其中的电子值数据则由与 IC 卡读取器/写入器相连的计算机中的程序执行。但是，第三方可以解密和更改计算机中的程序，并由此涉及诸如在计算机上篡改所读取的电子值数据、将其复制到另一张 IC 卡中等等的的不公正行为。

其中，虽然可以通过电子签名技术在一定程度上防止篡改，但是防止电子值数据的复制非常困难。正是因为如此，采用了下述方法以便检验电子值是原物还是复制品。

例如，当第一次发行电子值数据时，电子值数据发行者的服务器验证被发行方的 IC 卡并识别被发行方的 IC 卡，以便在其中记录数据。电子值数据的传输总是通过服务器来完成，并且服务器更新和记录拥有每一个电子值数据的是哪一个 IC 卡。当电子值数据被使用时，服务

器检验该使用是否与合法的 IC 卡进行（第一种方法）。

或者，当第一次发行电子值数据时，电子值数据发行者的服务器验证被发行方的 IC 卡并识别被发行方的 IC 卡，以便在其中记录数据。对于电子值数据的传输，通过使用密钥源 IC 卡将证实该传输的签名添加到电子值数据中。每次传输数据时都添加签名，并且签名数量随之增加。当电子值数据被使用时，服务器依次检查有关所述值的传输的签名，以检验能否到达为其第一次发行该值的 IC 卡（第二种方法）。

但是，在第一种方法中，在传输电子值数据期间，IC 卡必须一直连接到服务器，并且，当其中一个 IC 卡没有配置与服务器的接口时，传输则不可行。由于服务器必须一直管理所有电子值数据的持有者，所以将极重的负载强加到服务器上。

在第二种方法中，每次传输所述值时添加签名，因此电子值数据量变得非常大。由于每一张 IC 卡的存储容量有限，重复传输将增加签名的数据量，从而导致 IC 卡的存储容量不足，并接着导致不能进一步记录电子值数据和进一步传输电子值数据。

由于检验电子值是原物还是复制品的过程涉及上述问题，因此非常期望防止复制电子值数据本身，以避免该检测过程。

为了解决上述问题完成了本发明，本发明的目的是提供一种防止复制电子值数据本身的电子值数据通信方法、通信系统、IC 卡、便携终端和通信终端。

发明内容

不能阻止复制电子值数据的原因在于电子值数据可以解密状态从 IC 卡中读出。另一方面，存储在 IC 卡中的程序对外保护，以便禁止任何第三方，当然，甚至是 IC 卡的持有者读出和篡改程序，正如 IC 卡内部的数据那样。因此，本发明采用其中 IC 卡中对外保护的程序直接彼此相互验证，并在它们之间直接传输电子值数据，从而防止在通信路径中的篡改和复制。

也就是说，为了实现上述目的，根据本发明的电子值数据通信方

法为实施从存储电子值数据的 IC 卡传输电子值数据到另一 IC 卡的电子值数据通信方法，该方法包括：验证步骤，其中源 IC 卡和目标 IC 卡相互验证另一方；加密步骤，其中源 IC 卡加密所述电子值数据；传输步骤，其中源 IC 卡将加密的电子值数据传输给目标 IC 卡；以及解密步骤，其中目标 IC 卡解密所述加密的电子值数据。

根据本发明的通信系统为包括多个能够存储电子值数据并能够相互通信的 IC 卡的通信系统，其中，为了在 IC 卡之间传输电子值数据，源 IC 卡和目标 IC 卡相互验证另一方，源 IC 卡加密所述电子值数据，源 IC 卡将加密的电子值数据传输给目标 IC 卡，以及目标 IC 卡解密所述加密的电子值数据。

如上所述，在本发明中首先源 IC 卡和目标 IC 卡相互验证另一方。这使得源 IC 卡和目标 IC 卡两者确保响应者是正确的通信方，从而保证通信响应者不是伪造的 IC 卡或者没有注册的计算机。然后，源 IC 卡加密电子值数据并将所加密的电子值数据传输给目标 IC 卡。进而，目标 IC 卡解密所述加密的电子值数据，从而目标 IC 卡能够获取解密的电子值数据。

如上所述，由于加密的电子值数据直接在源 IC 卡和目标 IC 卡之间传输，因此能够防止第三方在通信路径中解密和篡改数据，并防止复制数据。

本发明也可以从涉及下述 IC 卡的发明的一方面得出。也就是说，根据本发明的 IC 卡包括：电子值数据存储部件，用于存储电子值数据；程序存储部件，用于存储通信程序，该通信程序包括执行与作为另一方的目标 IC 卡进行相互验证的验证步骤、以及加密步骤，当获得另一方为合法方的验证结果时，加密电子值数据并将加密的电子值数据传输给该另一 IC 卡；以及程序执行部件，用于执行通信程序，以将存储在电子值数据存储部件中的电子值数据传输给所述另一 IC 卡。

在该 IC 卡中，程序执行部件执行存储在程序存储部件中的通信程序。在该配置中，执行验证步骤，以便与作为另一方的目标 IC 卡进行相互验证，并且当获得另一方为合法方的验证结果时，执行加密通信

步骤，以便进行电子值数据的加密并将加密的电子值数据传输给该另一 IC 卡。该配置包括下述两种情况，即，根据本发明的 IC 卡加密电子值数据并将加密的电子值数据传输给另一 IC 卡的情况，以及所述另一 IC 卡加密电子值数据并将加密的电子值数据传输给根据本发明的 IC 卡、并且根据本发明的 IC 卡接收所述加密的电子值数据的情况。

如上所述，由于根据本发明的 IC 卡配置成直接向或从另一 IC 卡传输加密的电子值数据，因此能够容易地防止第三方在通信路径中解密和篡改数据，并防止复制数据。

也可以如此配置根据本发明的上述 IC 卡，使得通信中的另一方至少包括作为合法响应者预先注册的便携终端和信息处理设备中的一个。也就是说，本发明不仅能够应用于在 IC 卡之间传输电子值数据，而且能够应用于在 IC 卡和便携终端之间传输电子值数据、以及在 IC 卡和信息处理设备之间传输电子值数据。

如上所述，应用到 IC 卡的本发明也可以应用到便携终端，并实现类似的操作和效果。也就是说，根据本发明的便携终端包括：电子值数据存储部件，用于存储电子值数据；程序存储部件，用于存储通信程序，该通信程序包括执行与作为另一方的目标便携终端进行相互验证的验证步骤、以及加密通信步骤，当获得另一方为合法方的验证结果时，执行电子值数据的加密并将加密的电子值数据传输给该另一便携终端；以及程序执行部件，用于执行通信程序，以将存储在电子值数据存储部件中的电子值数据传输给所述另一便携终端。也可以如此配置该便携终端，使得通信中的另一方至少包括作为合法响应者预先注册的 IC 卡和信息处理设备中的一个。

如上所述，应用到 IC 卡的本发明也可以应用到通信终端，并实现类似的操作和效果。也就是说，根据本发明的通信终端包括：电子值数据存储部件，用于存储电子值数据；程序存储部件，用于存储通信程序，该通信程序包括执行与作为另一方的目标通信终端进行相互验证的验证步骤、以及加密通信步骤，当获得另一方为合法方的验证结果时，执行电子值数据的加密并将加密的电子值数据传输给该另一通

信终端；以及程序执行部件，用于执行通信程序，以将存储在电子值数据存储部件中的电子值数据传输给所述另一通信终端。也可以如此配置该通信终端，使得通信中的另一方至少包括作为合法响应者预先注册的 IC 卡、便携终端和信息处理设备中的一个。

附图说明

图 1 是根据本发明实施例的 IC 卡的配置图；

图 2A 是表示根据本发明实施例的通信系统的操作图；

图 2B 是表示传统的通信系统的操作图；

图 3 是表示在通信系统中通信过程的流程图；

图 4 是表示在验证步骤中的数据交换的图；

图 5A 是表示应用本发明的便携终端的总体配置图；

图 5B 是包含在便携终端中的 IC 芯片的配置图。

具体实施方式

下面将参照附图描述本发明的实施例。

图 1 示出根据本发明的 IC 卡 10 的结构。如图 1 所示，IC 卡 10 包括：密钥信息存储器件 12，用于存储其中附加有证书 C 的公钥 K2 和私钥 K1，以存储来自响应者的密钥信息；程序存储器件 14，用于存储通信程序；电子值数据存储器件 18，用于存储电子值数据 V；以及程序执行器件 16，用于执行上述通信程序。

作为通信程序，程序存储器件 14 存储有：验证程序 P1，执行与作为另一方的目标 IC 卡进行相互验证的验证处理；以及加密通信程序 P2，当获得另一方为合法方的验证结果时，进行电子值数据的加密并将加密的电子值数据传输给该另一 IC 卡，

当执行加密通信程序 P2 时，程序执行器件 16 使用 IC 卡 10 中内置的发送-接收天线（未示出）将加密的电子值数据传输给所述另一方并从另一方接收数据。

图 2A 示出包括与图 1 中的 IC 卡 10 结构类似的多个 IC 卡的通信

系统的结构。如图 2A 所示，当电子值数据从 IC 卡 A 传输到 IC 卡 B 时，通过用于从或向 IC 卡 A 读取或写入数据的 IC 卡读取器/写入器 20A、计算机 30A、计算机 30B、以及用于从或向 IC 卡 B 读取或写入数据的 IC 卡读取器/写入器 20B，在 IC 卡 A、B 之间传递。在该配置中，在 IC 卡 A 和 IC 卡读取器/写入器 20A 之间以及在 IC 卡 B 和 IC 卡读取器/写入器 20B 之间可以建立无线通信或通过通信电缆的有线通信。此外，也可以在 IC 卡读取器/写入器 20A 和计算机 30A 之间以及在 IC 卡读取器/写入器 20B 和计算机 30B 之间建立无线通信或通过通信电缆的有线通信。

具体细节将在下面描述，但如图 2A 所示配置通信系统 1，以便从 IC 卡 A 向 IC 卡 B 传输电子值数据，源 IC 卡 A 和目标 IC 卡 B 彼此相互验证对方，由此通过 IC 卡 A、B 之间的直接加密通信将电子值数据从 IC 卡 A 传输到 IC 卡 B。

传统上，如图 2B 所示，源 IC 卡 A 使用计算机 30A 进行验证，电子值数据通过加密通信从 IC 卡 A 传输到计算机 30A，并由计算机 30A 对该加密的电子值数据再次解密。然后，在计算机 30A、30B 之间进行验证，从而电子值数据通过加密通信计算机 30A 传输到计算机 30B，并且计算机 30B 再次解密所述电子值数据。进一步，计算机 30B 与目标 IC 卡 B 进行验证，从而电子值数据通过加密通信从计算机 30B 传输到 IC 卡 B，并由 IC 卡 B 最终解密该电子值数据，由此实现电子值数据从 IC 卡 A 到 IC 卡 B 的传输。当在计算机 30A、30B 中解密时存在电子值数据没有加密的可能性，由此可能被第三方解密、篡改和复制。

与此相反，如图 2A 配置的通信系统 1 在源 IC 卡和目标 IC 卡之间实现直接传输加密的电子值数据，从而能够容易地防止第三方在通信路径中解密和篡改数据，并防止复制数据。

下面将参照图 3 和 4 描述本实施例中进行的操作。

在图 3 的验证步骤 S1，源 IC 卡 A 和目标 IC 卡 B 相互验证对方。

下面详细描述相互验证的处理过程。在该处理过程的描述中，将

IC 卡 A 简单表示为“A”，IC 卡 B 简单表示为“B”。

(1) A 首先将其证书 A 发送给 B (图 4 中所示的消息①)。假定证书 A 包含公钥 A，并且证书授权局证实公钥 A 是 IC 卡 A 的真实公钥。

(2) 对此进行响应，B 检查证书 A，以确信证书 A 中的 A 的公钥为正确的密钥。

(3) 然后，B 生成随机数 B 并使用 A 的公钥对其进行加密。

(4) 接着，B 将其证书 B、以及使用 A 的公钥加密过的随机数 B 发送给 A (图 4 中所示的消息②)。假定证书 B 包含公钥 B，并证实公钥 B 是 IC 卡 B 的真实公钥。

(5) A 检查证书 B，以确信证书 B 中的 B 的公钥为正确的密钥。

(6) 使用其自己的密钥，A 对加密的随机数 B 进行解密。

(7) 然后，A 生成随机数 A 并使用 B 的公钥对其进行加密。

(8) 接着，A 将使用 B 的公钥加密的随机数 A 发送给 B (图 4 中所示的消息③)。

(9) A 使用共用密钥 (common-key) 生成函数从随机数 A 和随机数 B 生成共用密钥 k_{AB} 。B 也使用共用密钥生成函数从随机数 A 和随机数 B 生成共用密钥 k_{AB} 。A 和 B 的共用密钥应该彼此相等，这是因为将相同的随机数代入相同的生成函数。

(10) B 使用共用密钥 k_{AB} 和消息①、②、③执行消息验证码生成函数的计算，从而生成消息验证码 (MAC)。MAC 是用于证明消息被正确发送和接收的码 (数字值)。

(11) B 将在前一步骤 (10) 中生成的 MAC 发送给 A (图 4 中所示的消息④)。

(12) A 使用共用密钥 k_{AB} 和消息①、②、③执行消息验证码生成函数的计算。其结果应该等于在前一步骤 (11) 中发送的 MAC。当它们彼此相等时，可以确认以下 5 点。

1) MAC 相等这一事实证明另一方知道 k_{AB} 和消息①、②、③。

2) 另一方知道 k_{AB} 这一事实证明另一方知道随机数 A 和随机数

B.

3) 由于使用公钥 B 对随机数 A 进行加密并发送, 所以除了其自身 A 之外只有 B 知道。

4) 因此, 可以证明通信中的另一方是 B。

5) 证明为 B 的响应者也知道消息①、②、③。因此, 到此为止所交换的消息肯定是来自 B 的消息, 并且所发送的消息也一定被正确地传递给 B。

(13) A 从前一步骤 (12) 确认响应者是 B、以及到此为止消息被正确地发送到 B 和从 B 接收。

(14) A 使用共用密钥 k_{AB} 和消息①、②、③、④执行消息验证码生成函数的计算, 以生成 MAC。MAC 是用于证明消息被正确发送和接收的码 (数字值)。

(15) A 将在前一步骤 (14) 中生成的 MAC 发送给 B (图 4 中所示的消息⑤)。

(16) B 使用共用密钥 k_{AB} 和消息①、②、③、④执行消息验证码生成函数的计算。其结果应该与在前一步骤 (15) 中所接收的 MAC 相同。如果它们相等, 与在步骤 (12) 中相同的证明方法证实响应者是合法的 A、以及到此为止消息被正确地发送到 A 和从 A 接收。

如上所述, A 和 B 确信可以相互验证对方。图 4 中所示的 $MAC_{k_{AB}}$ 表示使用共用密钥 k_{AB} 生成消息验证码 (MAC: Message Authentication Code, 消息验证码) 的函数。

在图 3 的下一步骤加密步骤 S2 中, 源 IC 卡 A 加密电子值数据。这里, 加密方法不限于任何具体的加密技术, 而是可以采用从多种事先与目标 IC 卡 B 约定好的加密方法中选择的任意一种方法。图 1 的 IC 卡中的加密程序 P2 既不包括复制命令, 也不包括数据读出命令, 从而防止 IC 卡中的程序被篡改, 由此任何人都不能复制电子值数据和读出电子值数据。

在下一步骤传输步骤 S3 中, 源 IC 卡 A 将加密的电子值数据传输

到目标 IC 卡 B。由于该原因，加密的电子值数据直接在源 IC 卡 A 和目标 IC 卡 B 之间传输，从而容易地防止第三方在通信路径中解密和篡改数据，并防止复制数据。

在下一步骤解密步骤 S4 中，源 IC 卡 B 对加密的电子值数据进行解密。从而使得目标 IC 卡 B 获得解密的电子值数据。

如上所述，通过既没有复制命令、也没有数据读出命令的 IC 卡中的防止篡改（falsification-proof）程序，电子值数据通过加密通信在源 IC 卡和目标 IC 卡之间传输，可以容易地防止第三方在通信路径中解密和篡改数据，并防止复制数据。

与 IC 卡相同，本发明也可以应用到便携终端（比如蜂窝电话、PHS、PDA、膝上计算机等）。在该应用中，与另一方进行的通信功能可以利用便携终端的功能实现，并且便携终端在结构上例如可以由包含 IC 芯片 50 的便携终端 40 构成，如图 5A 所示，IC 芯片 50 用于执行验证、加密、以及电子值数据和其它数据的存储等功能。

在该配置中，IC 芯片 50 可以类似于图 1 中 IC 卡 10 的结构来构建，如图 5B 所示。但是，由于通信功能借助于便携终端的功能实现，IC 芯片 50 不必配置与通信有关（包括天线）的结构，因此，IC 芯片 50 的尺寸可以压缩的足够小以包含在便携终端 40 中。与 IC 卡 10 一样，该 IC 芯片 50 不允许从外部篡改数据和程序。

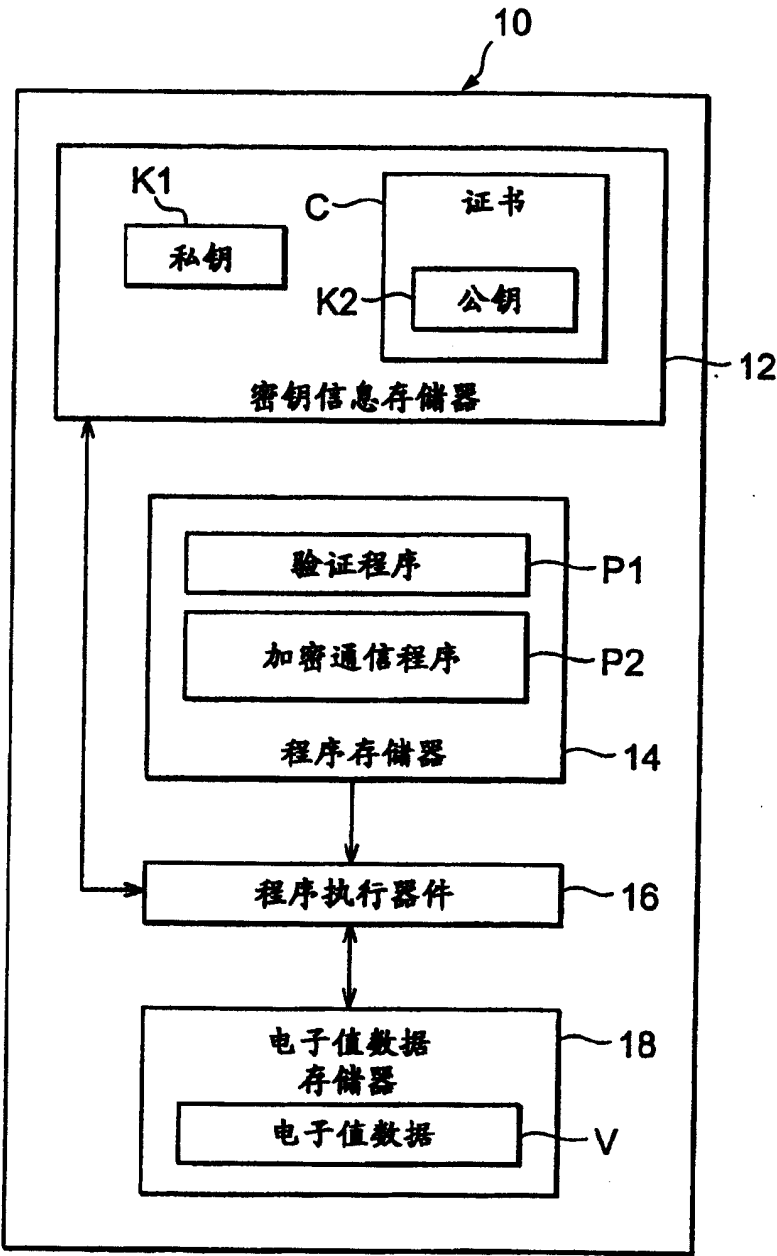
通过类似于上述 IC 卡之间的直接加密通信，电子值数据可以在包含此 IC 芯片 50 的便携终端 40 之间传输，从而可以容易地防止第三方在通信路径中解密和篡改数据，并防止复制数据。

在本发明中，可以采用将上述 IC 芯片 50 内置于信息处理设备（例如，POS 终端、台式个人计算机、服务器、主计算机等）的结构。

本发明不仅可以应用于 IC 卡之间的电子值数据传输和便携终端之间的电子值数据传输，而且可以应用到 IC 卡、便携终端、以及预先注册为合法通信终端的信息处理设备之间的电子值数据传输，并实现类似的操作和效果。

如上所述，本发明达到了防止第三方在通信路径中解密和窜改数据并防止复制数据的效果，这是由于加密的电子值数据是在源 IC 卡和目标 IC 卡之间直接进行传输。

图1



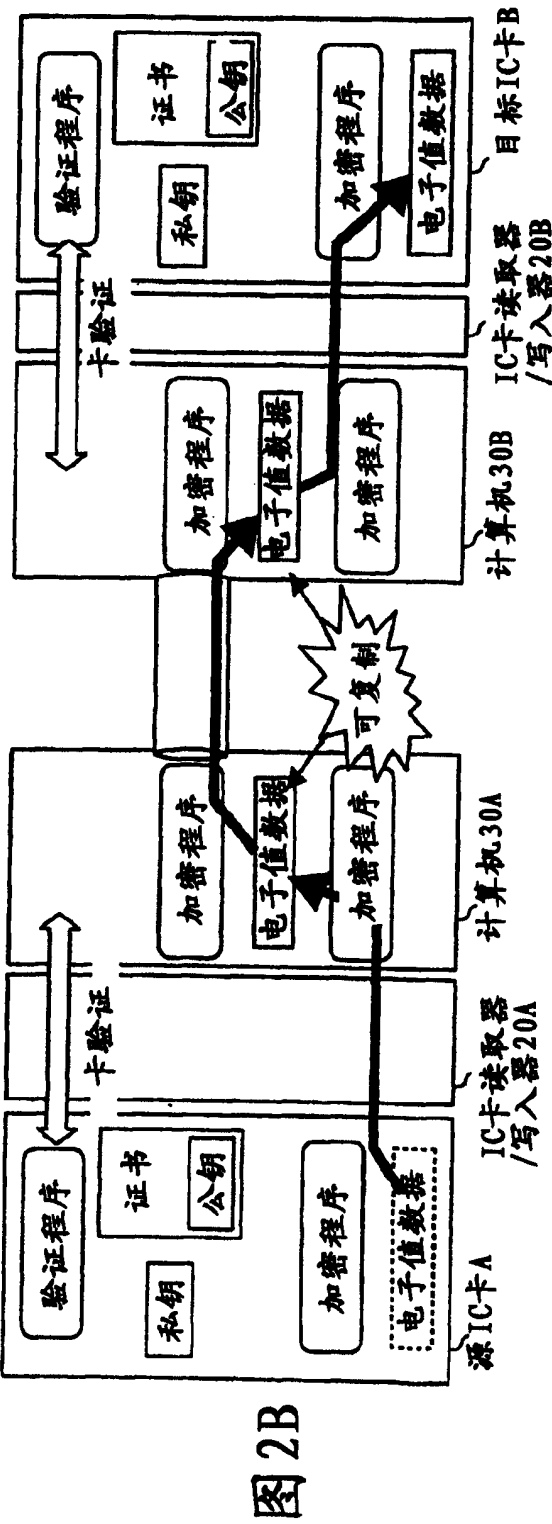
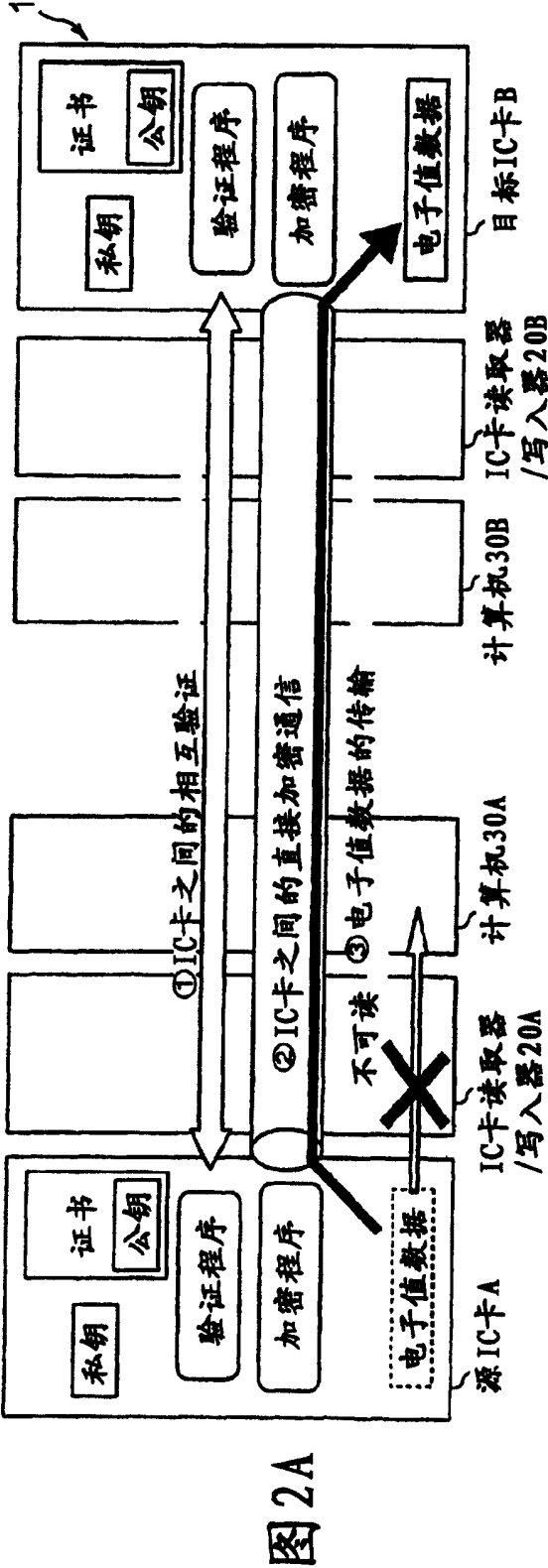


图 3

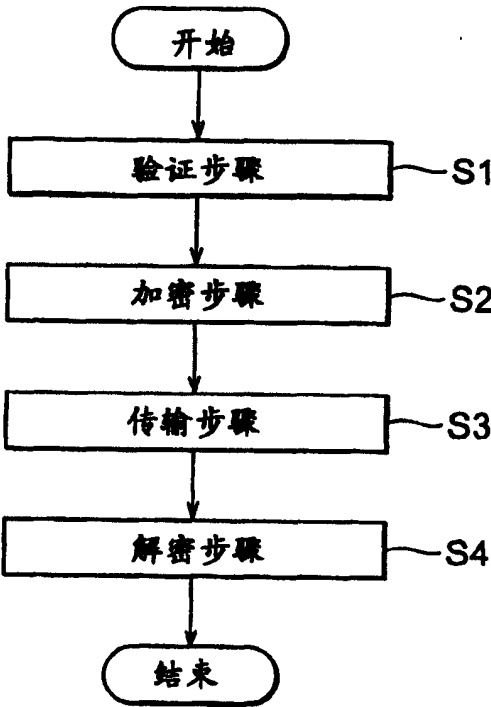


图 4

