[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G07F 7/10
H04L 9/32

[12] 发明专利说明书

专利号 ZL 02812765.X

[45] 授权公告日 2005 年 10 月 5 日

[11] 授权公告号 CN 1221928C

[22] 申请日 2002.6.7 [21] 申请号 02812765.X
[30] 优先权
[32] 2001.6.26 [33] FR [31] 01/08586
[86] 国际申请 PCT/FR2002/001956 2002.6.7
[87] 国际公布 WO2003/001464 法 2003.1.3
[85] 进入国家阶段日期 2003.12.25
[71] 专利权人 法国电讯
地址 法国巴黎
[72] 发明人 戴维·阿迪蒂 雅克·比尔热
亨利·吉尔贝 马克·吉罗
让-克洛德·帕耶
审查员 杨勤之

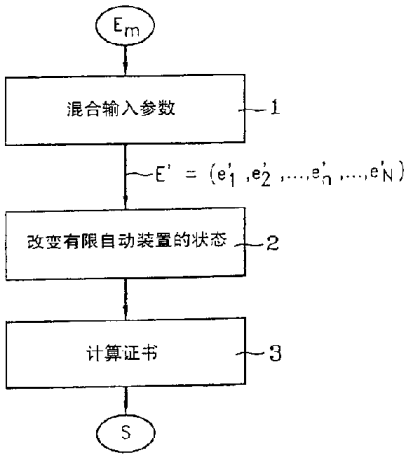
[74] 专利代理机构 永新专利商标代理有限公司
代理人 蹇 炜

权利要求书 4 页 说明书 15 页 附图 3 页

[54] 发明名称 保护电子芯片免受欺骗的加密方法

[57] 摘要

本发明涉及一种保护电子芯片免受欺骗的方法以及包含电子芯片的器件，该器件适合于保护该电子芯片免受欺骗。该方法包括：-混合(1)这些输入参数(E_m)中的一些或全部参数以便提供一个输出数据项 $E'=(e'_1, e'_2, \ldots, e'_n, \ldots, e'_N)$；将一个有限状态自动装置的状态从旧状态改变(2)为新状态，该新状态是该数据项($e'_1, e'_2, \ldots, e'_n, \ldots, e'_N$)的函数，以及借助一种以该自动装置的至少一个状态作为输入参数的输出功能来计算(3)一份证书(S)。该器件包括：混合装置，有限状态自动装置，以及，用于计算一份证书(S)的输出装置。



ISSN1008-4274

1、一种在应用程序（25）与电子芯片之间的交易中保护该电子芯片免受欺骗的加密方法，该方法包括根据该电子芯片中的输入参数（E_m）来计算一份证书（S），该方法的特征是，还包括：

借助一项混合功能来混合（1）这些输入参数（E_m）中的一些或全部参数，并提供一个混合功能输出数据项$E' = (e'_1, e'_2, ..., e'_n, ..., e'_N)$，

根据至少取决于该旧状态以及位序列（$e'_1, e'_2, ..., e'_n, ..., e'_N$）中的一个值的功能，将一个有限状态自动装置的状态从旧状态改变（2）为新状态，以及

借助一项输出功能来计算（3）该证书（S），其中该输出功能以该自动装置的至少一个状态作为一个输入参数。

2、如权利要求1的方法，其中输入参数（E_m）之一是一个存储在该芯片（23）的被保护存储器区域内的密钥K。

3、如权利要求1的方法，其中第一输入参数包括该芯片（23）固有的数据（D）。

4、如权利要求3的方法，其中第二输入参数是该芯片（23）的存储器区域内的上述数据（D）的地址。

5、如权利要求1的方法，其中这些输入参数（E_m）之一包括该芯片（23）外部的、并在执行该方法之前提供给该芯片（23）的数据（D′）。

6、如权利要求1的方法，其中这些输入参数（E_m）之一是该芯片（23）外部的、并在执行该方法之前提供给该芯片（23）的一个数据项元素（R）。

7、如权利要求1的方法，其中这些输入参数（E_m）之一包括该芯片

（23）固有的、并在执行该方法之前提供给外部实体的一个数据项元素（R′）。

8、如权利要求6或权利要求7的方法，其中该数据项元素（R, R'）是偶然选择的一个值。

9、如权利要求6或权利要求7的方法，其中该数据项元素（R, R'）是计数器的一个值。

10、如权利要求6或权利要求7的方法，其中该数据项元素（R, R'）是一个日期及一天中的时间。

11、如权利要求1的方法，其中该混合功能是这些输入参数（E_m）的线性功能。

12、如权利要求11的方法，其中该混合功能产生这些输入参数（E_m）中一些或全部参数的一个标量积。

13、如权利要求1的方法，其中该自动装置将这些输入参数（E_m）中的一些或全部参数作为输入。

14、如权利要求1的方法，其中该输出功能是一种以该自动装置的新状态作为一个输入参数的恒等功能。

15、如权利要求1的方法，其中该输出功能是一种以该自动装置的新状态作为一个输入参数的截断功能。

16、如权利要求1的方法，适用于该应用程序鉴别该芯片，其中该应用程序（25）将由该电子芯片计算（27）的证书（S）与它采用与该电子芯片（23）相同的方法计算（28）的一份证书（S′）加以比较。

17、如权利要求1的方法，适用于该芯片鉴别该应用程序，其中该电子芯片（23）将它计算（27）的证书（S）与该应用程序（25）采用相同的方法计算（28）的一份证书（S′）加以比较。

18、一种使用一份证书在芯片与应用程序之间交换一个密钥的方法，其特征为，该证书采用根据权利要求1至15中任何一项的方法来获得。

19、一种芯片与应用程序使用一份证书来进行加密的方法，其特征为，该证书采用根据权利要求1至15中任何一项的方法来获得。

20、一种使用一份证书来为一些或全部输入参数（E_m）进行电子签名的方法，其特征为，该证书采用根据权利要求1至15中任何一项的的方法、并考虑这些输入参数（E_m）来获得。

21、一种使用一份证书作为一个伪随机位序列的方法，其特征为，该证书采用根据权利要求1至15中任何一项的方法来获得。

22、一个器件（24），包括电子芯片（23）以及用于执行加密方法的装置，该方法在应用程序（25）与该电子芯片的交易中根据该电子芯片中的输入参数（E_m）计算（27）一份证书（S）来保护该电子芯片免受欺骗，该器件的特征是，包括：

混合装置，用于混合这些输入参数（E_m）中的一些或全部参数，以便提供由上述混合过程产生的一个输出数据项$E' =(e'_1, e'_2, ..., e'_n, ..., e'_N)$，

有限状态自动装置，用于根据一项功能从旧状态改变为新状态，该功能至少取决于该旧状态以及位序列（$e'_1, e'_2, ..., e'_n, ..., e'_N$）中的一个值，以及

输出装置，用于根据包括该自动装置的至少一个状态在内的输入参数

来计算该证书（S）。

23、如权利要求22的器件（24），其中该混合装置包括一个线性反馈移位寄存器，输入参数位被连续送入该寄存器，而且该寄存器影响该寄存器的初始化以及/或者这些反馈位的值，以便混合这些输入参数（E_m）中的一些或全部参数并在该寄存器输出端提供数据项$E' = (e'_1, e'_2, ..., e'_n, ..., e'_N)$。

24、如权利要求22的器件（24），其中该混合装置包括一个非线性反馈移位寄存器，输入参数位被连续送入该寄存器，而且该寄存器影响该寄存器的初始化以及/或者这些反馈位的值，以便混合这些输入参数（E_m）中的一些或全部参数并在该寄存器输出端提供数据项$E' = (e'_1, e'_2, ..., e'_n, ..., e'_N)$。

25、如根据权利要求22的器件（24），其中该自动装置包括一个布尔电路。

26、如根据权利要求22的器件（24），其中该自动装置包括一个或多个存储器的输出与地址输入之间的一个回路。

27、一张预付卡，包含根据权利要求22至26中任何一项的器件。

28、一张票券，包含根据权利要求22至26中任何一项的器件。

29、一个用于公共服务的访问终端，包含根据权利要求22至26中任何一项的器件。

30、一个电子支付终端，包含根据权利要求22至26中任何一项的器件。

保护电子芯片免受欺骗的加密方法

技术领域

本发明涉及密码术领域。特别是，本发明涉及一种用来在电子芯片与应用程序之间的交易中保护该芯片免受欺骗的加密方法。本发明还涉及一种器件，该器件包含电子芯片并适用于实现一种用来保护电子芯片免受欺骗的加密方法。

本发明非常有利于用来保护基于微处理器的或硬连线的逻辑集成电路芯片免受欺骗，特别是组合到各种不同交易所用的预付卡中的芯片，这些交易包括从一部投币式电话打电话、为出自一台自动售货机的货品付款、在一部汽车停放收费表上付一次停车费、或者为某项服务付费，譬如公共交通或政府提供的基础设施设备（收费处、博物馆、图书馆等等）。

背景技术

目前，预付卡很容易受各种类型欺骗的攻击。第一种类型的欺骗是该卡的非授权复制，这通常被称为“仿制”。第二类型的欺骗是修改附属于某张卡的数据，特别是存储在该卡内的存款数。密码术被用来抵御这些类型的欺骗，它首先借助数字签名来鉴别该卡与/或数据，然后，在合适情况下通过加密使该数据成为保密数据。密码术使用两个实体：检验器以及要被检验的对象，而且密码术既可以是对称的，也可以是不对称的。如果它是对称的，那么这两个实体共享完全相同的信息，特别是共享密钥。如果它是不对称的，那么这两个实体中的一个具有一对密钥，其中一个是保密的，另一个是公开的；不存在共享的密钥。在许多使用预付卡的系统中只

使用对称密码术，因为不对称密码术目前仍然是既慢又费钱。需要开发的第一批对称密码鉴别机制最终为每张卡计算一份不同的证书、将该证书存储到该卡的存储器、在一次交易中读出该证书并通过向支持该交易的网络的应用程序进行询问来加以检验，在该交易中，已经分配的证书或者已被存储、或者每次进行计算。这些机制没有提供足够的保护，因为该证书可能被盗用、复制以及欺骗性重放。为抵御仿制，被动的卡鉴别机制已被能够格外保证该数据完整性的主动的机制所取代。

主动鉴别机制的一般原理如下：在一次鉴别操作时，该电子芯片与该应用程序计算一份证书，该证书是将一项功能（function）应用到根据每次鉴别所确定的一列参数的结果；这列参数可以包括一个数据项元素（die），即在每次鉴别时由该应用程序确定的一个数据项加上包含在该电子芯片内的一个数据项，这列参数还包括一个该电子芯片与该应用程序均知晓的密钥。如果由该电子芯片计算出的证书与该应用程序计算出的证书完全相同，那么该电子芯片就被认为是可信的，该电子芯片与该应用程序之间的交易就会被授权。

上述鉴别机制已广为人知，但它们中的绝大多数都需要至少相当于一个微处理器的计算能力。所以这些机制适合于微处理器卡，但很难适合于只具有更为初步的计算手段的硬连线逻辑卡。本发明涉及能够在一块硬连线逻辑卡中实现的、对称的、主动的鉴别机制。

第一种这样的机制是法国专利FR 89/09734的主题。该专利中描述的方法定义了一种该应用程序知晓的、并以硬连线电路形式植入电子芯片的非线性功能。第二种这样的机制是法国专利FR 95/12144的主题。这是一种通过无条件安全主动鉴别来保护卡的方法，该鉴别的基础是对有限次数的鉴

别操作使用一种既能确保防止重放、又能确保该密钥的受控“磨损”的线性功能。

上述两种机制中的每一种都有它自己的优点与缺点。第一种机制基于这样一种（据目前的知识状况无法证明的）假设，即所用的非线性功能是保密的，对于该第一种机制，硬连线逻辑芯片的计算能力下降所导致的非常严重的制约不能提供像通常密钥算法那样宽的安全裕量，所以，所用的非线性功能的细节规范的泄漏可能代表危险。倘若鉴别操作次数不超过特定阈限，该第二种机制的优点是其安全性可以得到证实，所以不存在与泄漏所用线性功能有关的危险；但是，在该芯片使用寿命中（或者在可充值卡情况下相邻两次充值之间）对该鉴别功能使用次数必须要有严格的限定是这种解决方法固有的特点，这可能代表制约，而这种制约在一些应用程序中是难以满足的。此外，该第二种机制很难考虑对用来检验这些硬连线逻辑芯片的安全模块所作的攻击，而不是对这些芯片本身的攻击，在这种情况下，欺骗者对检验模块提供随机的响应，直到意外地获得足够数量的良好响应并且产生与他所选择的卡号相关的密钥为止。将它们的优点结合到一起的、这两类机制的组合是法国专利FR 00/03684与FR 00/04313的主题。

专利FR 89/09734描述一个硬连线的微电路卡，其中一个串行加密功能被应用到两个操作数，一个是“关键字”（譬如由该卡之外的实体提供的一个数据项元素R），另一个是该卡的“内部存储器”的“输出”（譬如依赖该应用程序的一个密钥K或者一个数据项D）。该串行加密功能由一个硬连线电路实现，该电路包括一个接收上述关键字与上述内部存储器的上述输出的逻辑运算符，随后是一个延时逻辑电路，包含一个延时装置并在保

密存储器的输出与地址输入之间形成一个回路。该逻辑运算符的输出对该保密存储器的数据输出进行运算来构成该保密存储器的新地址输入。

该方法有许多缺点。

第一缺点来源于如下事实：该关键字与该内部存储器的输出由一个简单逻辑运算符加以组合。更准确地说，该关键字的位被接连使用来构成该逻辑运算符的第一操作数，而且该内部存储器的输出的位被接连使用来构成它的第二操作数。结果，该关键字的给定位或者该内部存储器的输出的给定位对该延时逻辑电路的操作就只限于当它出现在该逻辑运算符输入端的时刻进行。

加密功能是否健全可靠部分地取决于它的扩散品质，特别是取决于该算法中影响该算法最大可能步数的输入参数的给定位。在专利FR 89/09734描述的方法中没有充分满足该扩散原理，因为每个操作数的每个位只影响一步。所以，这就可能有利于这些操作数被欺骗操纵。而且，这也可能有利于通过观察该算法的一个或多个输出来发现那些被认为仍然保密的位（譬如那些构成该密钥K的位）。

第二缺点来源于如下事实：该硬连线电路的逻辑运算符的输入参数是该关键字以及该内部存储器的输出，这妨碍了该逻辑运算符将一个内部存储器的输出与另一个内部存储器的输出加以组合。举例来说，该逻辑运算符不能将一个密钥与一个写入该芯片的应用程序数据项加以组合。所以，这可能有利于应用程序数据被欺骗性修改。

专利FR 89/09734中所述方法的其他缺点是由于使用了一个在保密存储器的数据输出与地址输入之间构成回路的、带有延时装置的延时逻辑电路。

首先，该存储器是否是一个保密存储器并不总是实质性问题。尽管存在许多利用这种存储器可能具有的缺陷（譬如与它们的非线性相关的缺陷）而对密码算法进行的攻击，但倘若详细指定这些存储器使它们不具有这些缺陷，那么它们就能够变得公开而不会整体有损于该算法的安全性。不过，尽管这不是实质性问题，但用户仍可以选择使它们维持保密以便使该算法更加安全。

其次，使用在该存储器的数据输出与地址输入之间构成回路的一个延时逻辑电路非常具有限制性。特别是，由于该存储器的大小随该输出长度（以位为单位）指数增加，所以它排除了具有很长输出的硬连线电路。举例来说，如果该输出具有4位的长度，那么该存储器的大小是64位。但是，如果该输出具有8位的长度，那么该存储器的大小是2千位，对低成本硬连线芯片而言，这是一个非常大的长度。如果该输出具有16位的长度，那么该存储器的大小就是1兆位，对任何硬连线逻辑芯片而言，这个数都过于庞大。但是，该硬连线电路输出的长度必须使一个企图意外地猜测它的值的欺骗者的成功机会小得可以忽略。如果该长度是4位，那么该欺骗者每16（即2^4）次中有一次机会，这表示在几乎所有应用程序都有太多的机会。如果该长度是8位，那么该欺骗者每256次中有一次机会，这仍然表示在大多数应用程序有太多的机会。所以，专利 FR 89/09734 中描述的方法不能同时满足一个硬连线逻辑芯片的技术限制以及大多数应用程序的安全性限制。

发明内容

本发明涉及在应用程序与电子芯片之间的交易中保护该电子芯片免受欺骗的一种加密方法，而且涉及一个器件，该器件组合了电子芯片并适

合于在这些交易中保护该电子芯片免受欺骗，该方法与该器件格外适合于硬连线逻辑芯片，而且尤其打算提供一种没有上述缺点的鉴别机制，以便使所得的鉴别机制在加密方面更加健全可靠，从而使仿制更加困难。

为此，本发明提供在应用程序与电子芯片之间的交易中保护该电子芯片免受欺骗的一种加密方法，该方法包括根据该电子芯片中的输入参数来计算一份证书，它还包括：

- 借助混合功能来混合这些输入参数中的一些或全部参数，并提供一个混合功能输出数据项$E'=(e'_1, e'_2, ..., e'_n, ..., e'_N)$，

- 按照一项功能将一个有限状态自动装置（automaton）的状态从旧状态改变到新状态，该功能至少取决于该旧状态以及该位序列（$e'_1, e'_2, ..., e'_n, ..., e'_N$）中的一个值，以及

- 借助输出功能来计算该证书，该功能以该自动装置的至少一个状态作为一个输入参数。

本发明还提供一个器件，该器件包括电子芯片以及执行一种加密方法的装置，该方法根据该电子芯片中的输入参数来计算一份证书以便在应用程序与该电子芯片之间的交易中保护该电子芯片免受欺骗，本发明还包括：

- 混合装置，它被用于混合这些输入参数中的一些或全部参数，以便提供一个由上述混合操作而产生的输出数据项$E'=(e'_1, e'_2, ..., e'_n, ..., e'_N)$，

-有限状态自动装置，它按照一项功能从旧状态改变到新状态，该功能至少取决于该旧状态以及该位序列（$e'_1, e'_2, ..., e'_n, ..., e'_N$）中的一个值，以及

- 输出装置，它被用于根据包含该自动装置的至少一个状态在内的输入参数来计算该证书。

所以，该方法与该器件的基础是混合功能以及一个自动装置。在实现鉴别机制的情况下，该方法与该器件的输入参数可以是密钥K、数据项元素R、应用程序数据D、地址A、标识符I等等。

该加密方法以及该器件的输入参数由该混合功能加以处理，该功能在它的输出处提供一个依赖于这些输入参数中一些或全部参数的数据项。该混合功能的输出数据项可以有效改变该有限状态自动装置的状态，该自动装置的至少一个状态（最好是该最终状态）被用来计算被称为该证书的输出值S。

因为有了该混合功能，所以一个输入参数的给定位的操作并不专门限于它在实现该方法的装置的输入端出现的时间，相反，它影响那个时刻以后的许多步骤。这满足扩散原理。

该自动装置十分有利于获得大的（16、32、甚至64位的）证书而不必存储大量的位。该自动装置不必包括能在一个存储器的数据输出与地址输入之间形成回路的一个简单延时逻辑电路。

使用根据本发明的方法与器件而获得的证书既可以被有效地用于在该应用程序与该芯片之间交换密钥或者加密在该应用程序与该芯片之间交换的数据，也可以被有效地用于鉴别该芯片或该应用程序。它也可以被认为是这些输入参数中的一些或全部参数的一个电子签名。它还可以被认为是一个伪随机位序列，而且，通过改变该输入参数中的至少一个参数，计算该证书的方法就变为一种生成伪随机位的方法。

附图说明

本发明的其他特征与优点在下面参考所附附图给出的、借助非限制性示例方法对本发明的特定实施例所作的说明过程中会变得显而易见。

图1是根据本发明的方法的一幅示意图。

图2是混合功能的一个示例的一幅示意图。

图3是有限状态自动装置的一个示例的一幅示意图。

图4是表示根据本发明的方法的用途的一幅示意图。

具体实施方式

图1示意性地表示符合保护电子芯片免受欺骗的发明的一种方法。该方法由下述功能构成。

第一功能1是混合功能，它将M个输入参数E_m（m＝1至M）中的一些或全部参数加以混合，并提供一个数据项$E'=(e'_1, e'_2, ..., e'_n, ..., e'_N)$作为输出，其中N是该输出数据项中的位数。每个输入参数E_m包含特定数量的位。该混合功能的输入数据由这些输入参数E_m中的一些或全部参数构成。

第一输入参数E_1可以是存储在该芯片中保护区内（也就是说，在该芯片中不能从外部读取或修改的一个存储器区域内）的一个密钥K。举例来说，这个存储器区域可以在一个寄存器内或者在一个存储器内。

第二输入参数E_2可以包括该芯片固有的数据D，即存储在该芯片的一个可编程存储器（RAM、PROM、EPROM或E2PROM）内的数据。这个数据可以有各种各样的类型，而且可以在该芯片的完全不同的生命阶段写入，譬如在该芯片的制造期间、在组合了该芯片的对象（卡、票券等）的制造期间、在由该发行实体使该对象个性化期间、或者在该用户使用该对象期间写入。

如果一个输入参数包含该卡固有的数据D，那么一个第三输入参数E_3可以是存储该数据D的芯片内的存储器区域或者每个存储器区域的地址。

第四输入参数E_4可以包含该芯片外部的数据D'，并在执行该加密方法

之前（譬如在与该应用程序的交易的开始时刻）提供给该芯片。

第五输入参数E_5可以是该芯片外部的一个数据项元素R，并在执行该加密方法之前（譬如在与该应用程序的交易的开始时刻）提供给该芯片。该数据项元素可以是一个随机值，即偶然选择的一个值，它应大得足以使选择两个相等值的概率非常小。另外，它可以根据由该应用程序与该电子芯片产生的一系列连续整数来确定，或者根据时间特性（通常是日期与一天的时间）来确定。最后，它可以是前面所述的选项中一些或全部选项的组合。

第六输入参数E_6可以是该芯片固有的一个数据项元素R'，并在执行该加密方法之前提供给该芯片。该数据项元素可以是一个随机值，即偶然选择的一个值，它应大得足以使选择两个相等值的概率非常小。另外，它可以根据由该电子芯片及外部实体（通常是该应用程序）产生的一系列连续整数来确定，或者根据时间特性（通常是日期与一天的时间）来确定。最后，它可以是上述选项中一些或全部选项的组合。

上述这列参数并非详尽无遗。增加参数的数量具有使该方法更加可靠的优点，但不利于简单实现。

根据这些输入参数E_m确定的、该混合功能的输入数据可以是任何类型的数学对象，譬如位、固定或可变长度的位串、整数、非整数等等。相同对象也适用于该混合功能的输出数据。但是，为了便于描述该方法起见，该输出被当作一个位序列$E' = (e'_1, e'_2, ..., e'_n, ..., e'_N)$，这实际上并不是对本发明所加的限制。

该混合功能可以是该输入数据的线性功能或者该输入数据的非线性功能。

图2所示的线性功能1的一个第一示例包括计算该输入数据的标量积。假设该输入数据包括一个由J个位构成的密钥K（$K_1, K_2, ..., K_J$）、一个数据项元素R以及一个由J位集合（$Z_1, Z_2, ..., Z_J$）构成的数据项D，那么该混合功能的输出数据项的第一位可以被定义为上述两个数据项的标量积。所以，该混合功能的输出数据项的第一位等于将一个“异或”运算符加到对 j = 1至J的所有值计算乘积$K_j \cdot Z_j$而获得的这J个位所得到的结果。在图2所示的实施例中，在一个“与”逻辑门4的输出处获得 j = 1至J的乘积$K_j \cdot Z_j$。加到对所有 j 值计算乘积$K_j \cdot Z_j$而获得的这J个位的“异或”运算符包括 j 从1到J-1的所有值的“异或”门$5_{j, j+1}$的一个集合。每个“异或”门$5_{j, j+1}$具有两个输入及一个输出。至少一个输入是“与”逻辑门4_j的输出，另一个输入是一个“异或”逻辑门$5_{j, j+1}$的输出或者一个“与”逻辑门4_j的输出。该“异或”门$5_{j, j+1}$的输出e′给出了该混合功能的输出数据项的第一位的值。

为了获得该输出数据项的第二位，对密钥K进行一个或多个位置的旋转运算。这会将密钥K转换为一个数据项K′。该混合功能的输出数据项的第二位可以被定义为数据项K′与J位集合（$Z_1, Z_2, ..., Z_J$）的标量积。该第二位在该“异或”门$5_{j, j+1}$的输出e′处出现。

所描述的用于获得该第二位的运算必须对每个位重复执行以便获得该输出数据项的后续各位。

存在许多基于上述定义的线性功能1的变化形式。特别是，能够避免K由于经过J次旋转后回到它的原始状态而使该输出数据项的位进入重复循环。如果I是需要的输出位数，那么能够使用一个I+J位的密钥K：（$K_1, K_2, ..., K_{I+J}$）。该混合功能的输出数据项的第一位可以被定义为数据项（$K_1, K_2, ..., K_J$）与（$Z_1, Z_2, ..., Z_J$）的标量积，该输出数据项的第二位可以被定义为数

据项（$K_2, K_3, ..., K_{J+1}$）与（$Z_1, Z_2, ..., Z_J$）的标量积，以此类推，直到该输出数据项的最后位，它可以被定义为向量（$K_{I+1}, K_{I+2}, ..., K_{I+J}$）与（$Z_1, Z_2, ..., Z_J$）的标量积。

这种变化形式十分有用，因为存在一个基于这些输出位的平行计算的实施例，它摆脱了在每次需要一个输出位时去除密钥K的做法。为此，需要两个特殊的I位寄存器，第一个用向量（$K_1, K_2, ..., K_I$）进行初始化，第二个用零向量（0, 0, ..., 0）进行初始化。如果$Z_1 = 0$，那么该第二寄存器的内容仍为零。如果$Z_1 = 1$，那么该第一寄存器的内容就构成该第二寄存器的新内容。在这两种情况下，该第一寄存器的新内容都是（$K_2, K_3, ..., K_{I+1}$）。该最后运算的实现方法是将位置向左进行一次移位，然后插入一个新位K_{I+1}。如果$Z_2 = 0$，那么该第二寄存器的内容不进行修改。如果$Z_2 = 1$，那么该第二寄存器的新内容就是将一个“异或”运算符应用到该第一与第二寄存器的内容所得的结果。在这两种情况下，该第一寄存器的新内容都是（$K_3, K_4, ..., K_{I+2}$），它是通过实现一次移位然后再插入新位K_{I+2}而获得的。如此继续进行。在读出J个位（$Z_1, Z_2, ..., Z_J$）之后，包含在该第二寄存器中的I个位就是该混合功能的I个输出位。

线性功能1的一个第二示例采用一个线性反馈移位寄存器，这些输入参数的位被连续加入该寄存器并影响该寄存器的原始状态以及/或者这些反馈位的值。有时采用“扰动的线性反馈移位寄存器”这种表达方式来指一个在该寄存器运行期间向其注入数据的寄存器。那么，输出值E'就可以是从这个寄存器的内容提取的一个或多个位。

非线性功能1的一个示例采用一个非线性反馈移位寄存器，这些输入参数的位被连续加入该寄存器。输出值S'可以是从这个寄存器的内容提取

的一个或多个位。

一项第二功能2包括将一个有限状态自动装置的状态从旧状态改变到新状态，而且至少考虑到该旧状态以及该位序列E'=（e'_1, e'_2, ..., e'_n, ..., e'_N）中的一个值，该值就相当于从数据项E'的所有位中所取的一个或多个位。在特殊的实施例中，这项功能还能够考虑到这些输入参数E_m中的一些或全部参数。该自动装置的初始状态可以根据E'与E_m中一些或全部值的函数来确定。

图3所示的自动装置的一个第一示例包括采用一个布尔电路，举例来说，这是一个使k+1位向量（A_1, A_2, ..., A_{k+1}）与一个k位向量（A'_1, A'_2, ..., A'_k）相关的电路，其中每个位A'_i是借助基本运算符（譬如AND(与)、OR（或）、exclusive-OR（异或）、NOT（非））由位（A_1, A_2, ..., A_{k+1}）求得，而且其中（A_1, A_2, ..., A_k）代表该自动装置的旧状态。举例来说，如果k＝8，那么该自动装置的输出就由如下方程给出：

A'_1 =（NOT A_3）AND A_2 OR e'; A'_2 = A_5 OR（(NOT A_8）AND（A_1 exclusive-OR A_4)); A'_3 = A_6 AND A_2; A'_4 = A_1 exclusive-OR A_4 exclusive-OR（NOT e'); A'_5 = A_3 OR A_7; A'_6 =（NOT A_5）AND A_1 exclusive-OR A_8; A'_7 = A_6 OR A_7; A'_8=（NOT e')

该方程中A_9＝e'，而e'是E'=（e'_1, e'_2, ..., e'_n, ..., e'_N）的位中的任意一位。

在图3的以图解方式显示的实施例中，A'_1是一个“或”门6的输出，这个门的一个第一输入是e'，一个第二输入是一个“与”门7的输出。“与”门7有一个第一输入A_2，它的第二输入被连接到输入为A_3的一个反向器8的输出。A'_2是一个“或”门9的输出，这个门的第一输入是A_5，它的第二输

入被连接到一个“与”门10的输出。“与”门10的一个第一输入被连接到一个反相器11的输出，一个第二输入被连接到一个“异或”门12的输出。反向器11的输入是A_8。“异或”门12具有一个第一输入A_1与一个第二输入A_4。一个“与”门13具有一个输出A'_3、一个第一输入A_6以及一个第二输入A_2。一个“异或”门14具有一个输出A'_4、一个第一输入A_1、一个第二输入A_4以及一个连接到输入为e'的反向器15的输出的第三输入。一个“或”门16具有一个输出A'_5、一个第一输入A_3以及一个第二输入A_7。一个“异或”门17具有一个输出A'_6、一个第一输入A_8以及一个连接到“与”门18的输出的第二输入。“与”门18具有一个第一输入A_1与一个连接到输入为A_5的反向器19的输出的第二输入。一个“或”门20具有一个输出A'_7、一个第一输入A_6以及一个第二输入A_7。一个反向器21具有一个输出A'_8，而它的输入是e'。对p从1到k的所有值，每个位A_p是一个输入为位A'_p的双稳电路的输出。

在该示例中，该自动装置具有一个k位的内部状态（$A_1, A_2, ..., A_k$），而且在每次该布尔电路的输入端出现由该内部状态及该混合功能的输出构成的一个新向量（$A_1, A_2, ..., A_k, e'$）时，该自动装置在该输出端有一个新状态（$A'_1, A'_2, ..., A'_k$）。

自动装置的一个第二示例采用由数字表格定义的位变换。举例来说，当k＝8时，能够将字节（$A_1, A_2, ..., A_8$）划分为两个4字节组（A_1, A_2, A_3, A_4）与（A_5, A_6, A_7, A_8），然后，如果输出位e'的值是0，就对每个4字节组施加变换T，如果该输出位e'的值是1，就对每个4字节组施加变换U。变换T由一张使每个4字节组值（a, b, c, d）与一个4字节组值（a', b', c', d'）相关的表格来定义。变换U也用同样方法来定义。

如果已经考虑了所有的输入值，那么该自动装置就处于特定的最终状

态（$F_1, F_2, ..., F_k$）。

第三功能3计算一份证书S，该功能被称为一种输出功能并具有包含该自动装置的至少一个状态在内的输入参数。这个最简单的实施例只考虑该自动装置的最终状态。但是，该功能也能够考虑该自动装置的早期状态。该输出功能最好是应用于该自动装置最终状态的恒等功能。换句话说，该证书S等于该k位数据项（$F_1, F_2, ..., F_k$）。在一个不同的实施例中，该输出功能是截断功能。该证书S可以由任何知道该芯片密钥的应用程序加以检验。为此，该应用程序不知道、但与计算该证书有关的数据（譬如该芯片固有的数据）必须由该芯片在发送该证书之前、同时或之后传送到该应用程序。该应用程序使用与该芯片完全相同的加密处理并采用与该芯片完全相同的输入数据，然后获得一份证书S'。该应用程序将它计算出的证书S'与该芯片计算出的证书S加以比较。如果它们相同，那么该应用程序就认为该芯片是可信的。该应用程序计算出的证书可以由该芯片加以检验以便使该芯片能够鉴别该应用程序。

图4表示根据本发明的方法在电子芯片与应用程序之间进行一次交易期间的用途。

电子芯片23被安装在一个支撑物24中，譬如一张预付卡、一张电子票券、一张银行卡等等。

应用程序25整体或部分地在一个电子芯片读卡机26中运行。如图4所示，该读卡机可以是非接触式读卡机或者是接触式读卡机。

如果该应用程序是一个鉴别应用程序，那么只要该卡进入该读卡机就会激发该读卡机并启动该应用程序。该应用程序提示该芯片提供采用根据本发明的方法来计算（27）一份证书S以便通报自己的身份。与此同时，该

应用程序采用与该芯片相同的方法及相同的输入参数来计算（28）一份证书。在这个计算之后，该芯片将它的结果提供给该应用程序，该应用程序则将它与它自己的结果加以比较。如果这些结果完全相同，那么该芯片就通过鉴别，该应用程序则向该芯片通告这一结论。这些决定性的输入参数可以在该芯片的每次使用之前确定、植入该芯片而且使该应用程序知晓。它们可以在采用特定方法鉴别该卡之后加以修改。可以修改所有这些参数或者只修改其中的一部分参数，或者，该应用程序也可以提供一个新参数，譬如一个采用随机方法或者根据一个计数器、一个时钟、一个日期等的值确定的数据项元素R。

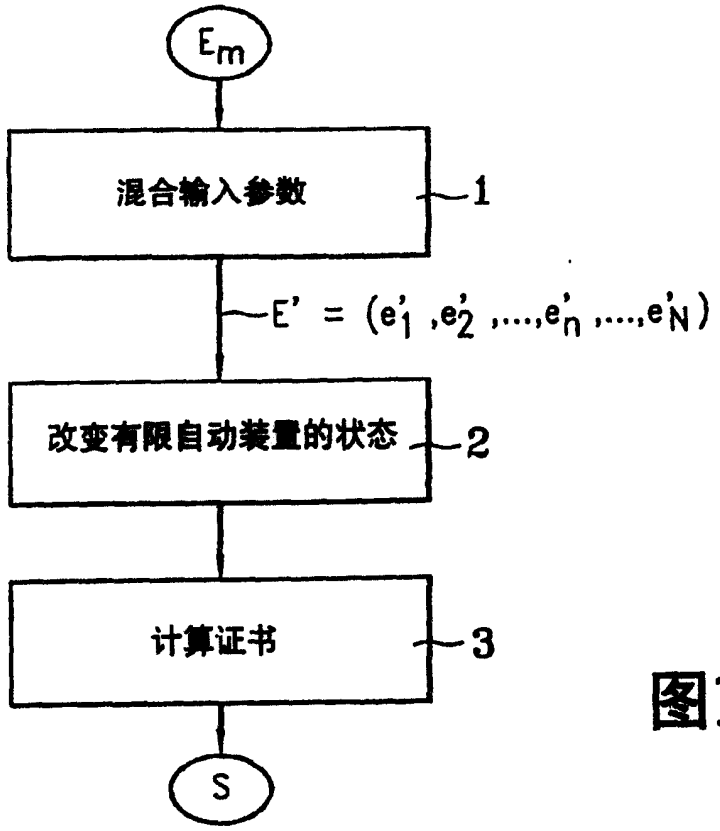


图1

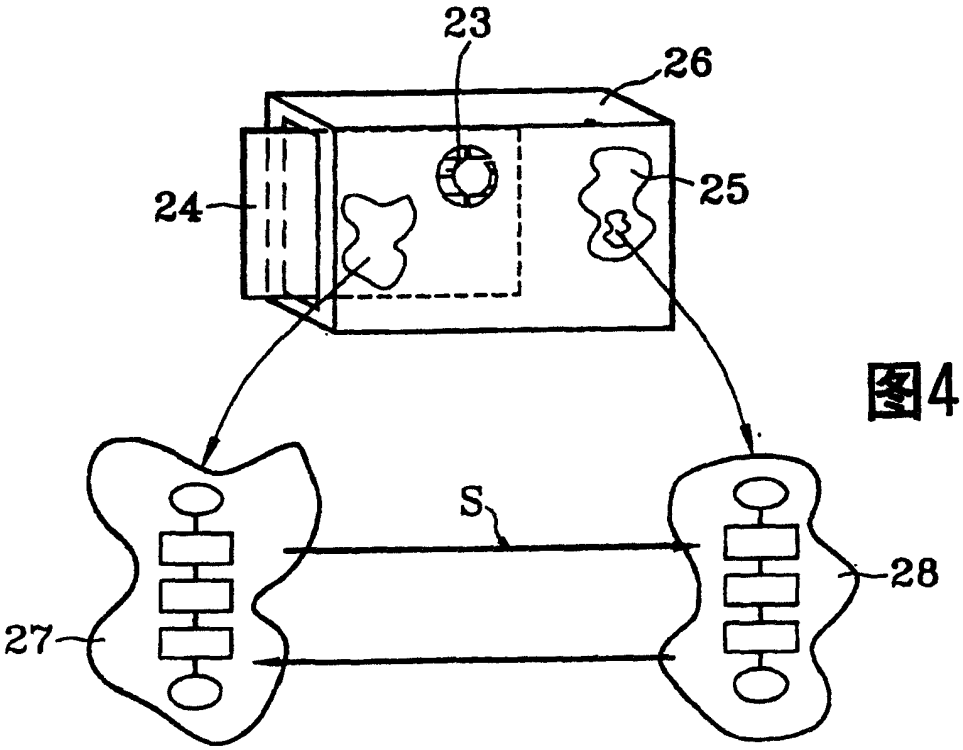
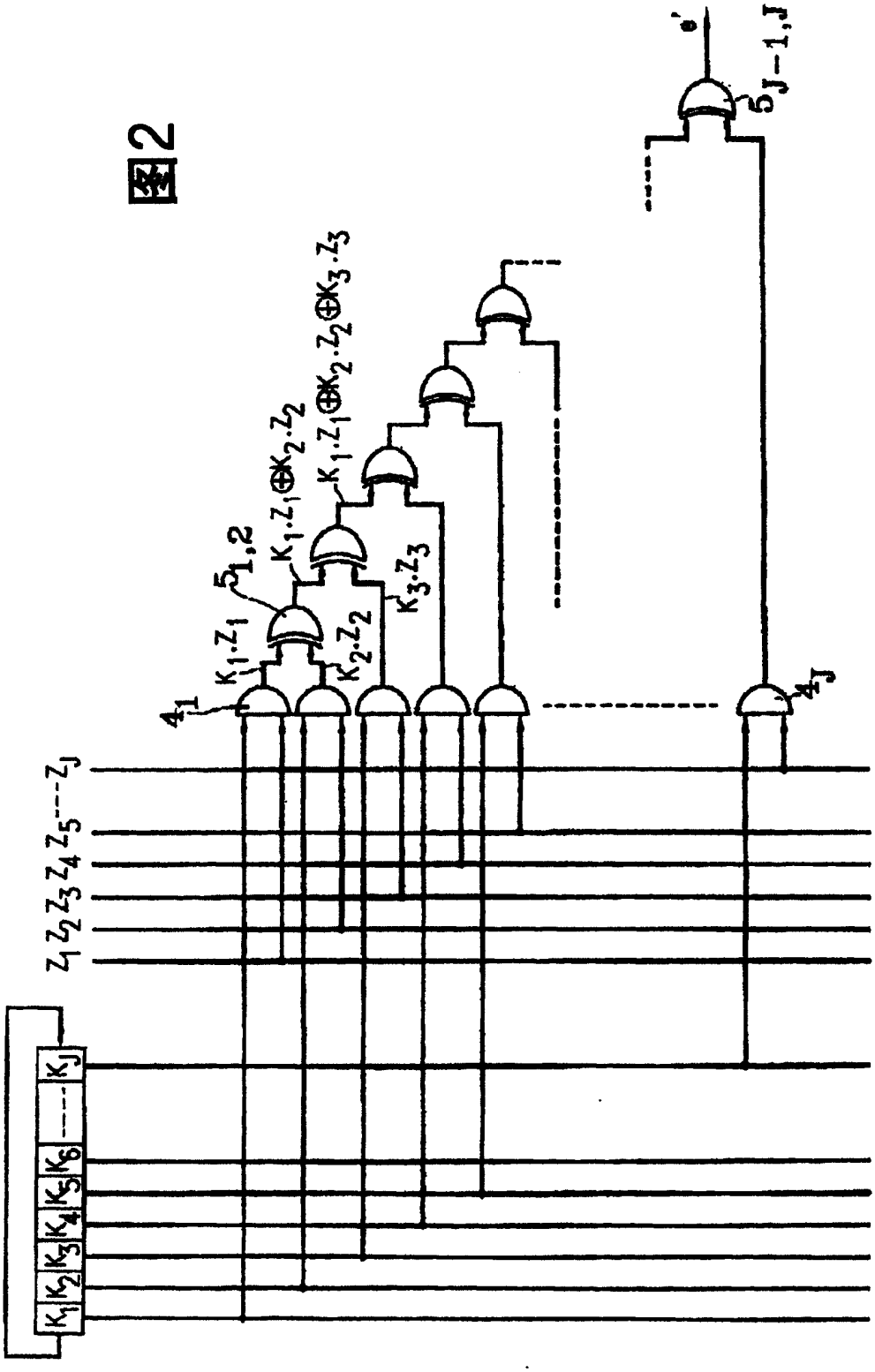


图4

图2


K1 K2 K3 K4 K5 K6 --- Kj
Z1 Z2 Z3 Z4 Z5 --- Zj
41
K1.Z1
51,2
K1.Z1⊕K2.Z2
K2.Z2
K1.Z1⊕K2.Z2⊕K3.Z3
K3.Z3
4j
5j-1,j

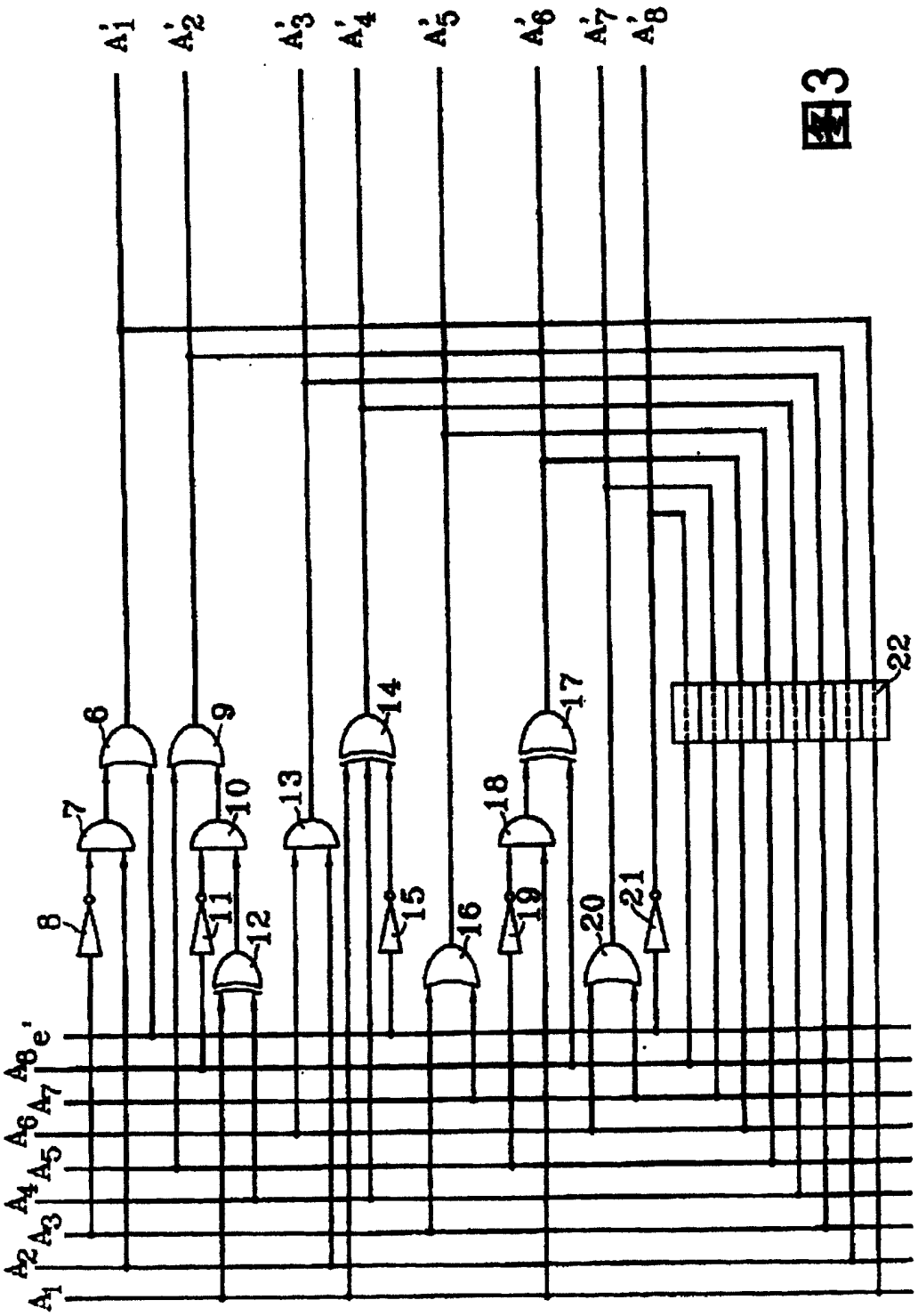

A'1
A'2
A'3
A'4
A'5
A'6
A'7
A'8
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
e'
A8
A7
A6
A5
A4
A3
A2
A1

图3