



(12) 发明专利

(10) 授权公告号 CN 103262464 B

(45) 授权公告日 2015.09.30

(21) 申请号 201180060120.5

H04L 29/06(2006.01)

(22) 申请日 2011.12.21

(56) 对比文件

(30) 优先权数据

102010055699.8 2010.12.22 DE

US 5818738 A, 1998.10.06,

(85) PCT国际申请进入国家阶段日

US 5818738 A, 1998.10.06,

2013.06.14

US 2008022121 A1, 2008.01.24,

(86) PCT国际申请的申请数据

CN 1889433 A, 2007.01.03,

PCT/EP2011/006491 2011.12.21

US 2001016908 A1, 2001.08.23,

(87) PCT国际申请的公布数据

Shinsaku Kiyomoto et al..anonymous

W02012/084241 DE 2012.06.28

attribute authentication scheme using
self-blindable certificates. 《Intelligence
and Security Informatics ISI2008》. 2008, 第
215-217页.

(73) 专利权人 德国捷德有限公司

审查员 李红玲

地址 德国慕尼黑

(72) 发明人 G. 梅斯特

(74) 专利代理机构 北京市柳沈律师事务所

11105

代理人 谢强

(51) Int. Cl.

H04L 9/08(2006.01)

H04L 9/32(2006.01)

权利要求书3页 说明书11页 附图4页

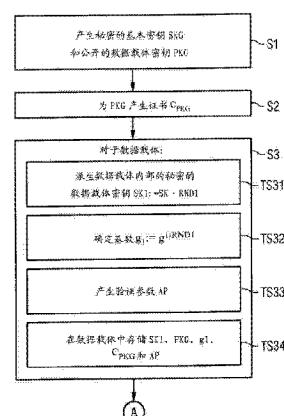
(54) 发明名称

加密方法

(57) 摘要

在一种在便携式数据载体(10)和终端设备之间的加密方法中，使用数据载体(10)的公开的数据载体密钥(PKG)和秘密的数据载体密钥(SK1)以及终端设备的公开的终端密钥(PKT)和秘密的终端密钥(SKT)。数据载体(10)使用静态的公开密钥作为公开的数据载体密钥(PKG)。数据载体(10)将从与公开的数据载体密钥(PKG)关联的秘密的基本密钥(SKG)中派生的秘密密钥用作秘密的数据载体密钥(SK1)。在本方法的范围内，所述终端设备检验与数据载体(10)关联的、与数据载体密钥不同的验证参数(AP)。

CN



1. 一种在便携式数据载体 (10) 和终端设备之间的加密方法, 其中使用所述数据载体 (10) 的公开的数据载体密钥 (PKG) 和秘密的数据载体密钥 (SK1) 以及所述终端设备的公开的终端密钥 (PK_T) 和秘密的终端密钥 (SK_T), 其中

所述数据载体 (10) 将静态的公开密钥用作公开的数据载体密钥 (PKG), 并且
将从与所述公开的数据载体密钥 (PKG) 关联的秘密的基本密钥 (SKG) 中派生的秘密的数据载体密钥 (SK1) 用作秘密的数据载体密钥 (SK1),

其特征在于, 所述终端设备检验 (TS61) 与所述数据载体 (10) 关联的、与所述数据载体密钥不同的验证参数 (AP), 其中, 所述数据载体通过所述验证参数对会话参数进行签名或加密, 使得能够由终端设备检验所述验证参数。

2. 根据权利要求 1 所述的方法, 其特征在于, 所述静态的公开密钥是公开的组密钥 (PKG)。

3. 根据权利要求 1 所述的方法, 其特征在于, 所述终端设备通过如下方式检验所述验证参数 (AP), 即, 所述终端设备解密 (TS61) 由所述数据载体 (10) 提供的、借助所述验证参数 (AP) 加密 (TS41) 的会话参数。

4. 根据权利要求 1 所述的方法, 其特征在于, 所述终端设备通过如下方式检验所述验证参数 (AP), 即, 所述终端设备校验由所述数据载体 (10) 提供的、借助所述验证参数 (AP) 数字签名的会话参数。

5. 根据权利要求 1 至 4 中任一项所述的方法, 其特征在于, 在另一次执行所述加密方法之前, 通过从所述秘密的数据载体密钥 (SK1) 中派生的、所述数据载体 (10) 的秘密的数据载体会话密钥 (SK_s) 来替代 (S10) 所述数据载体 (10) 的秘密的数据载体密钥 (SK1)。

6. 根据权利要求 1 所述的方法, 其特征在于, 借助所述数据载体 (10) 的公开的数据载体密钥 (PKG) 和秘密的数据载体密钥 (SK1) 以及所述终端设备的公开的终端密钥 (PK_T) 和秘密的终端密钥 (SK_T), 约定 (S7) 在所述数据载体 (10) 和所述终端设备之间的通信密钥 (KK)。

7. 根据权利要求 6 所述的方法, 其特征在于, 借助 Diffie-Hellman 密钥交换方法约定在所述数据载体 (10) 和所述终端设备之间的通信密钥 (KK)。

8. 根据权利要求 1 所述的方法, 其特征在于, 在使用第一随机数 (RND1) 的条件下从所述秘密的基本密钥 (SKG) 中派生 (TS31) 所述秘密的数据载体密钥 (SK1)。

9. 根据权利要求 1 所述的方法, 其特征在于, 在使用会话参数的条件下从所述秘密的数据载体密钥 (SK1) 中派生 (S9) 所述数据载体 (10) 的秘密的数据载体会话密钥 (SK_s), 其中, 提供至少一个第二随机数 (RND_s) 和 / 或所述终端设备的参数作为会话参数。

10. 根据权利要求 1 所述的方法, 其特征在于, 所述公开的数据载体密钥 (PKG) 借助以所述秘密的基本密钥 (SKG) 对规定的本原根 (g) 取幂来确定, 所述秘密的数据载体密钥 (SK1) 借助将所述秘密的基本密钥 (SKG) 与第一随机数 (RND1) 相乘来形成 (TS31), 并且第一基数值 ($g1$) 借助以所述第一随机数 (RND1) 的倒数对所述本原根 (g) 取幂来形成 (TS32)。

11. 根据权利要求 10 所述的方法, 其特征在于, 所述数据载体 (10) 的秘密的数据载体会话密钥 (SK_s) 借助将所述秘密的数据载体密钥 (SK1) 与会话参数 (RND_s) 相乘来确定 (S9), 并且会话基数 (g_s) 通过以所述会话参数 (RND_s) 的倒数对所述第一基数 ($g1$) 取幂

来形成 (S11)，其中，所述会话参数 (RND_S) 通过第二随机数和 / 或所述终端设备的参数来规定，并且其中，通过所述秘密的数据载体会话密钥 (SK_S) 替代所述秘密的数据载体密钥 (SK_1) 以及通过所述会话基数 (g_S) 替代所述第一基数 (g_1) (S10 ; S12)。

12. 根据权利要求 10 的方法，其特征在于，所述数据载体借助所述验证参数 (AP) 对所述第一基数 (g_1) 进行加密 (TS41) 或者数字签名，并且将所述第一基数以加密过或数字签名过的形式作为会话参数提供 (TS42) 给所述终端设备。

13. 根据权利要求 12 所述的方法，其特征在于，所述终端设备基于所述验证参数对加密过的第一基数 (g_1) 进行解密 (TS61) 或者对数字签名过的第一基数 (g_1) 进行校验，并且借助以所述终端设备的秘密的终端密钥 (SK_T) 对通过所述数据载体 (10) 作为会话参数提供的第一基数 (g_1) 取幂来确定 (TS62) 所述终端设备的公开的终端密钥 (PK_T)。

14. 根据权利要求 1 所述的方法，其特征在于，用作所述数据载体 (10) 的公开的数据载体密钥 (PKG) 的静态的公开密钥 (PKG) 由所述终端设备借助所述静态的公开密钥 (PKG) 的证书 (C_{PKG}) 来校验 (S8)。

15. 根据权利要求 1 所述的方法，其特征在于，所述数据载体 (10) 将对于每个会话动态产生的公开密钥替代所述静态的公开密钥用作公开的数据载体密钥 (PKG)，并且作为会话参数将从规定的本原根 (g) 派生的基数值 (g_1) 借助所述验证参数 (AP) 进行加密并且提供给所述终端设备。

16. 根据权利要求 15 所述的方法，其特征在于，对于每个会话动态地产生秘密的基本密钥 (SKG)，其中，将如下公开密钥用作动态产生的公开的数据载体密钥 (PKG)，该公开密钥借助以动态产生的所述秘密的基本密钥 (SKG) 对规定的本原根 (g) 取幂来确定，并且其中，所述秘密的数据载体密钥 (SK_1) 借助将所述秘密的基本密钥 (SKG) 与随机数 (RND_1) 相乘而形成，并且其中，所述基数值 (g_1) 借助以所述随机数 (RND_1) 的倒数对所述本原根 (g) 取幂而形成。

17. 一种便携式数据载体 (10)，包括处理器 (30)、存储器 (40 ; 50 ; 60) 和至终端设备的数据通信接口 (20 ; 20') 以及加密装置 (52)，所述加密装置构造为，在使用所述数据载体 (10) 的公开的数据载体密钥 (PKG) 和秘密的数据载体密钥 (SK_1) 以及所述终端设备的公开的终端密钥 (PK_T) 和秘密的终端密钥 (SK_T) 的条件下利用所述终端设备执行加密方法，其特征在于，所述加密装置 (52) 还构造为，借助与所述数据载体密钥不同的验证参数 (59 ; AP) 对所述方法的会话参数进行加密或数字签名。

18. 一种用于与按照权利要求 17 所述的便携式数据载体 (10) 进行数据通信的终端设备，其中，所述终端设备构造为，在使用所述数据载体 (10) 的公开的数据载体密钥 (PKG) 和秘密的数据载体密钥 (SK_1) 以及所述终端设备的公开的终端密钥 (PK_T) 和秘密的终端密钥 (SK_T) 的条件下，利用便携式数据载体 (10) 执行加密方法，其特征在于，所述终端设备构造为，检验与所述数据载体 (10) 关联的、与所述数据载体密钥不同的验证参数 (59 ; AP)。

19. 根据权利要求 18 所述的终端设备，其特征在于，所述终端设备构造为，借助按照权利要求 3 或 4 所述的方法检验所述验证参数 (59 ; AP)，并且构造为，在使用由所述数据载体 (10) 提供的、作为加密过或数字签名过的会话参数的基数 (g_1) 的条件下，结合所述终端设备的秘密的终端密钥 (SK_T) 确定所述终端设备的公开的终端密钥 (PK_T)。

20. 一种包括按照权利要求 17 所述的数据载体 (10) 以及按照权利要求 18 或 19 所述

的终端设备的系统,所述系统构造为用于执行按照权利要求1至16中任一项所述的方法。

加密方法

技术领域

[0001] 本发明涉及一种用于在便携式数据载体和终端设备之间的加密方法以及一种相应构造的数据载体和终端设备。

背景技术

[0002] 便携式数据载体、例如以电子证件形式的便携式数据载体包括具有处理器和存储器的集成电路。在存储器中存储有与数据载体的用户有关的数据。在处理器上可以执行加密应用程序，数据载体可以通过所述加密应用程序建立与终端设备的安全通信连接。此外加密装置可以支持相对于终端设备的数据载体验证，例如在边境检查等等的时候的证件的情况。

[0003] 在这样的加密方法期间在数据载体和终端设备之间准备安全的数据通信，方法是约定用于对称加密随后的数据通信的秘密的通信密钥，例如借助根据 Diffie 和 Hellman 的公知的密钥交换方法或其他合适的方法。此外通常至少终端设备校验、例如根据证书校验数据载体的真实性。

[0004] 为了执行用于约定秘密的通信密钥的方法，需要的是，终端以及数据载体分别都提供秘密密钥和公开密钥。数据载体的证书例如可以涉及其公开密钥。

[0005] 公知各种支持在便携式数据载体和终端设备之间构建安全的通信连接的方法和协议。一种在特定于会话的动态生成的密钥基础上的密钥交换方法可以附加地基于口令得到确保。秘密数据，例如PIN，生物测量的特征，例如指纹等可以用作口令。口令通常一方面存储在数据载体中并且另一方面在方法的运行过程中以合适的方式提供给终端设备。口令例如可以通过数据载体的用户借助输入装置输入到终端设备中，例如借助键盘、用于生物测量数据的传感器等等。按照另一个实施方式，口令，例如PIN，可以光学可读出地设置在数据载体上并且由终端设备相应地获取。由此确保，数据载体的合法用户同意在该方法的范围内使用数据载体，其方式为该用户输入口令或至少这样展示数据载体，使得密码可以由终端设备读出。由此可以排除不期望的数据通信，例如在无接触的路径上的数据通信。但是这样的方法不能实现数据载体和终端的相互验证。

[0006] 然而用于相对于终端设备验证数据载体或相对于数据载体验证终端设备的公知方法不能提供基于口令的方法的安全性。这些验证方法例如基于对数字证书的使用。

发明内容

[0007] 本发明要解决的技术问题是，提出一种加密方法，该加密方法考虑了现有技术的缺陷。

[0008] 上述技术问题通过具有所附权利要求的特征的方法、数据载体、终端设备和系统解决。优选实施方式和改进方案在从属权利要求中给出。

[0009] 在按照本发明在便携式数据载体和终端设备之间的加密方法中，使用数据载体的公开的数据载体密钥和秘密的数据载体密钥以及终端设备的公开的终端密钥和秘密的终

端密钥。数据载体将静态的公开密钥、特别是公开的组密钥用作公开的数据载体密钥。数据载体将与公开的数据载体密钥关联的秘密的基本密钥所派生的秘密密钥用作秘密的数据载体密钥。按照本发明，终端设备检验与数据载体关联的、与数据载体密钥不同的验证参数。

[0010] 该验证参数例如可以通过口令、数据载体的用户的生物测量特征或者通过数据载体的单独特征给出。验证参数安全地存储在数据载体中。可以在该方法的范围内以不同的方式向终端设备提供验证参数。一方面数据载体的用户可以将验证参数经过合适的输入装置输入到终端设备中，例如将 PIN 经过键盘，将生物测量特征例如经过相应的传感器进行输入。另一方面验证参数可以光学可读出地设置在数据载体上并且当数据载体合适地呈现时由终端设备读出。

[0011] 在按照本发明的方法中，不再需要在数据载体中存储秘密的基本密钥。相应地，在数据载体被攻击时秘密的基本密钥也不会被窥视。特别地，为了从秘密的基本密钥派生秘密的数据载体密钥而考虑的其他数据也不必存储在数据载体中，从而不可以根据这些在数据载体中不存在的数据从秘密的数据载体密钥推导出秘密的基本密钥。尽管如此，数据载体还保持可以通过与秘密的基本密钥对应的静态的公开的数据载体密钥来验证，例如根据涉及公开的数据载体密钥的证书，该证书可以可读出地存储在数据载体中。

[0012] 在秘密的基本密钥与对于数据载体的集合或组用作秘密的基本密钥的秘密的组密钥对应的情况下，该组的一个数据载体被揭穿对于该组的其余的数据载体来说是无害的，因为在被揭穿的数据载体中没有存储与可以危害该组的其他数据载体的安全性相关的数据。一组数据载体的其他的、没有被攻击的数据载体的秘密的数据载体密钥可以被继续使用。

[0013] 关于数据载体的用户的匿名性的顾虑(该匿名性的顾虑可以通过如下形成，即，数据载体的每次使用根据使用的静态的公开密钥与相应的用户唯一地对应)可以通过如下方式来去除，即，将公开的组密钥用作静态的公开的数据载体密钥。于是根据数据载体单独的公开的数据载体密钥来跟踪数据载体是不可能的，因为这样的数据载体密钥在数据载体中是不存在的。于是优选将公开的组密钥用作公开的数据载体密钥，该公开的组密钥不是数据载体单独的，而是对于数据载体的集合或组的所有数据载体是相同的。在此意义上，一组的全部数据载体的公开的数据载体密钥是不可区分的。由此用户的匿名性可以得到保证。

[0014] 优选地在另一次执行加密方法之前将数据载体的秘密的数据载体密钥相应地通过从秘密的数据载体密钥派生的、数据载体的秘密的数据载体会话密钥替代。也就是说，数据载体在每次执行时利用另一个秘密的数据载体密钥执行该方法。数据载体的秘密的数据载体密钥由此构造为数据载体的秘密的会话密钥。

[0015] 会话密钥在本发明的范围内始终理解为对于每个“会话”、即在此在每次执行加密方法时新确定的密钥。通常不同的会话密钥是不同的，即，在第一会话中的会话密钥的值与接下来的第二会话的该会话密钥的值是不同的。在此不可以从前面的会话密钥推导出后面使用的会话密钥或者反过来。例如终端设备的公开的终端密钥和秘密的终端密钥优选始终设置为在该意义上的会话密钥。

[0016] 根据数据载体的秘密的数据载体密钥跟踪数据载体的用户因此同样是不太可能的。数据载体的秘密的数据载体密钥虽然也可以按照另外的公知方式使用，例如在用于相

对于数据处理装置进行验证的挑战 - 响应方法中。但是通过如下, 即, 按照本发明的秘密的数据载体密钥是会话密钥, 即, 在每次采用时具有另一个值, 单单从秘密的数据载体密钥中不能推导出数据载体的身份。因此在此方面也可以保证用户的匿名性。

[0017] 通过附加使用在按照本发明的方法的范围内检验终端设备的验证参数, 可以进一步改进该方法的安全性。如果向终端设备提供正确的验证参数, 则可以假定, 数据载体处于打算执行在数据载体和终端设备之间的加密方法的合法用户手中。该方法的不打算的或不期望的执行, 例如在无接触的路径上和数据载体的用户不知晓或不同意的执行, 可以得到可靠排除。

[0018] 通过验证参数的使用与静态的公开的数据载体密钥的使用相结合可以在共同的方法中实现基于口令的方法的优点和例如根据静态的公开的数据载体密钥允许相对于终端设备基于证书地验证数据载体的这些方法的优点。以这种方式可以以极大程度节省资源、特别是计算时间。公知方法中共同的这些方法步骤、例如共同的秘密的通信密钥的约定, 按照本发明仅还执行一次。

[0019] 按照本发明的便携式数据载体包括处理器、存储器和至终端设备的数据通信接口以及加密装置。该加密装置构造为, 在使用数据载体的公开的数据载体密钥和秘密的数据载体密钥以及终端设备的公开的终端密钥和秘密的终端密钥的条件下利用终端设备执行加密方法。加密装置还构造为, 借助与数据载体密钥不同的验证参数来加密或数字地签名该方法的会话参数。

[0020] 优选地, 加密装置还构造为, 将数据载体的秘密的数据载体密钥相应地通过从秘密的数据载体密钥派生的、数据载体的秘密的数据载体会话密钥替代。以这种方式可以如上所述利用数据载体的特定于会话的秘密的数据载体密钥进行验证方法的每次执行。

[0021] 用于与按照本发明的便携式数据载体进行数据通信的按照本发明的终端设备构造为, 在使用数据载体的公开的数据载体密钥和秘密的数据载体密钥以及终端设备的公开的终端密钥和秘密的终端密钥的条件下利用便携式数据载体执行加密方法。终端密钥优选相应地构造为会话密钥。终端设备构造为, 在加密方法的范围内检验与数据载体关联的、与数据载体密钥不同的验证参数。

[0022] 终端设备构造为, 如上所述以合适的方式接收验证参数, 例如通过输入装置或光学读出装置来接收。

[0023] 验证参数的检验特别地可以通过如下进行, 即, 终端设备将由数据载体提供的加密的或数字签名的会话参数解密或校验。加密或签名在此基于验证参数。接收的验证参数的正确性可以由终端设备在该方法的执行过程中例如通过如下来检验, 即, 从会话参数派生的值、例如与数据载体达成协议的通信密钥是一致的。

[0024] 按照本发明的系统包括按照本发明的数据载体以及按照本发明的终端设备。它们分别构造为, 执行按照本发明的加密方法。

[0025] 在按照本发明的方法内借助数据载体的公开的数据载体密钥和秘密的数据载体密钥以及终端设备的公开的终端密钥和秘密的终端密钥在数据载体和终端设备之间约定通信密钥。该通信密钥然后仅提供给这两方。在该意义上该通信密钥是秘密的通信密钥。这样的密钥约定例如可以借助 Diffie-Hellman 密钥交换方法来进行。其他类似的方法同样是可以采用的。通信密钥的约定可以看作为在数据载体和终端设备之间执行的验证的形

式。只要接下来对于双方可以在数据载体和终端设备之间成功进行借助约定的通信密钥加密的数据通信，则对于一方来说另一方相应地验证成功。

[0026] 优选地，由终端设备借助公开的数据载体密钥的证书来校验数据载体的公开的数据载体密钥。为此可以将相应的证书通过数据载体以合适的方式提供给终端设备来检验。数据载体可以向终端设备例如发送证书。也可以将证书保存在数据载体的可自由读出的存储区域中。校验证书的步骤可以看作为验证方法的部分，在该部分中数据载体相对于终端设备借助证书证明自己。在公开的数据载体密钥是数据载体单独的情况下，数据载体可以通过终端设备唯一地被验证。如果作为公开的数据载体密钥使用公开的组密钥，则数据载体至少验证为与相应的组密钥对关联的组的数据载体，而不是根据数据载体单独的证书来验证，该证书在该情况下不存在。

[0027] 以相同方式，终端可以借助类似的证书相对于数据载体证明自己。

[0028] 优选地，数据载体的秘密的数据载体密钥在使用第一随机数的条件下从秘密的基本密钥派生。为此可以使用任意合适的运算，该运算尤其可以接收秘密的基本密钥以及随机数作为输入数据，并且将其处理为数据载体单独的秘密的数据载体密钥。例如可以使用数学运算，诸如相乘、取幂等。从秘密的基本密钥派生秘密的数据载体密钥例如可以在数据载体的制造期间进行，例如在个性化阶段，优选在数据载体外部进行。数据载体的秘密的数据载体密钥然后存储在数据载体中。公开的数据载体密钥和涉及该密钥的证书也可以在该阶段置入到数据载体中。但是也可以在数据载体本身中执行秘密的数据载体密钥的产生。在此，为此开始在数据载体中存储的秘密的基本密钥通过产生的秘密的数据载体密钥覆盖，并且由此不再存储在数据载体中。一旦产生了秘密的数据载体密钥，为了产生秘密的数据载体密钥而在数据载体中临时存储的随机数同样被删除。

[0029] 数据载体的、相应地在执行加密方法之后替代数据载体当前的秘密的数据载体密钥的秘密的数据载体会话密钥可以以不同方式从当前的秘密的数据载体密钥中派生出。该派生在数据载体中进行。通过从秘密的基本密钥派生初始的秘密的数据载体密钥并且从数据载体的相应当前的秘密的数据载体密钥派生数据载体的每个数据载体会话密钥的方式，间接从秘密的基本密钥派生数据载体的每个数据载体会话密钥，其中所述数据载体会话密钥然后替代当前秘密的数据载体密钥。然而不可以从数据载体的秘密的数据载体会话密钥推导出秘密的基本密钥。

[0030] 秘密的数据载体密钥通过数据载体的派生的秘密数据载体会话密钥的替代例如可以这样来进行，即，秘密的数据载体密钥通过派生的数据载体会话密钥“覆盖”，即，秘密的数据载体密钥取派生的数据载体会话密钥的值。秘密的数据载体密钥之前的值被删除。即，数据载体始终具有在按照本发明的方法中使用的“该”秘密的数据载体密钥。然而秘密的数据载体密钥的值在该方法的两次执行之间改变。数据载体由此相应地具有特定于会话的秘密的数据载体密钥。

[0031] 秘密的数据载体会话密钥从当前的秘密的数据载体密钥的派生基于会话参数进行。

[0032] 按照第一实施方式，数据载体的秘密的数据载体会话密钥在使用随机数的条件下从秘密的数据载体密钥中派生。即，随机数代表相应的会话参数。在此分别将新的随机数用于数据载体的数据载体会话密钥的每次派生。随机数可以在数据载体中产生。在派生之

后删除随机数。由此不可以从派生的数据载体会话密钥推导出为派生而使用的秘密的数据载体密钥。

[0033] 按照一个替换的实施方式,会话参数可以根据通过终端设备提供的值来确定。该值例如可以取终端设备的公开的扇区密钥的形式并且在数据载体和终端之间的验证之后提供给数据载体。在数据载体中以合适的方式考虑该扇区密钥,用于派生秘密的数据载体会话密钥。

[0034] 为了派生数据载体的秘密的数据载体会话密钥当然还可以使用多个会话参数,也就是例如随机数和终端参数。

[0035] 按照一个优选实施方式,公开的数据载体密钥借助以秘密的基本密钥对规定的本原根取幂来确定。初始的秘密的数据载体密钥在该实施方式中然后通过将秘密的基本密钥与第一随机数相乘而形成。最后,数据载体的第一基数借助以第一随机数的倒数对本原根取幂而形成。

[0036] 如果需要,然后数据载体的秘密的数据载体会话密钥借助将当前的秘密的数据载体密钥与会话参数相乘来确定。数据载体借助以会话参数的倒数对第一基数取幂来确定会话基数。会话基数的计算与为了准备加密方法的另一次执行而计算秘密的数据载体会话密钥一样进行。会话参数如上所述可以例如通过第二随机数或根据终端设备的参数来规定。数据载体的秘密的数据载体密钥然后以描述的方式通过数据载体的秘密的数据载体会话密钥替代。以相同的方式将第一基数通过会话基数替代,即,第一基数的值通过会话基数的值替代。由此也可以将数据载体的第一基数如秘密的数据载体密钥一样看作为特定于会话的。

[0037] 第一基数、即其当前的值由数据载体以规定的方式提供给终端设备。按照第一实施方式,将第一基数作为会话参数通过数据载体借助验证参数加密并且以加密的方式提供给终端设备。按照第二实施方式,数据载体可以在第一基数提供给终端设备之前借助验证参数对其进行数字签名。提供在此例如意味着发送或可自由读出地保存。

[0038] 终端设备然后借助以终端设备的秘密的终端密钥对通过数据载体提供的第一基数取幂来确定其公开的终端密钥。终端设备的秘密的终端密钥由该终端设备分别特定于会话地产生。第一基数在此由终端设备事先根据验证参数解密或校验。

[0039] 最后终端设备将如上所述确定的公开的终端密钥发送到数据载体。

[0040] 由此为约定通信密钥所需的数据在数据载体和终端设备之间交换。数据载体在其方面借助以自己的秘密密钥对接收的终端设备的公开的终端密钥的取幂来计算通信密钥。终端设备在其方面借助以终端设备自己的秘密的终端密钥对公开的数据载体密钥取幂来确定通信密钥。

[0041] 然后,或者替换地在约定通信密钥之前,终端设备也可以按照该实施方式如上所述借助为此由数据载体提供的证书来检验数据载体的公开的数据载体密钥。

[0042] 按照本发明方法的替换实施方式,数据载体不是使用静态的公开密钥作为公开的数据载体密钥而是使用对于每个会话动态产生的公开密钥。也就是说,数据载体在每次执行加密方法时使用动态产生的密钥对。在此,数据载体的公开的数据载体密钥和秘密的数据载体密钥特定于会话地在数据载体中产生。按照该实施方式,数据载体如上所述始终将从规定的本原根中派生的基数值作为会话参数提供给终端设备,该基数值事先由数据载体

借助验证参数加密过。在其他方面,第二实施方式的该方法如前面参考第一实施方式描述的那样进行。

[0043] 与设置基于口令的验证的公知加密方法不同,现在不是将任意的随机数等作为会话参数借助验证参数来加密和向终端设备提供。现在按照本发明将从本原根派生的基数用作会话参数。这具有优点,即,本原根(作为乘法子群的产生的元素)可以在数据载体中直接在随后的密钥交换方法中被考虑。数据载体内部为此不需要其他计算,也不需要与终端设备的附加的通信需求。按照现有技术,在数据载体中(和在终端设备中),必须从那里作为会话参数加密传输的随机数中借助麻烦的计算来派生合适的基数,其然后可以在密钥派生的范围内使用。除了计算,这还需要与终端设备的另外的通信需求,以交换对于派生基数值所需的另外的参数。相应地,按照第二实施方式的本方法可以在不影响安全性的情况下与公知的类似方法相比明显更有效和节省资源地执行。这特别是关于在便携式数据载体中始终短缺的资源来说是有利的。

[0044] 在数据载体中动态产生密钥对时,优选地对每个会话动态地产生秘密的基本密钥。然后,作为动态产生的公开的数据载体密钥使用借助以动态产生的秘密的基本密钥对规定的本原根取幂而确定的公开密钥。秘密的数据载体密钥最后借助将秘密的基本密钥与随机数相乘而形成。基数值借助以随机数的倒数对本原根取幂而产生。终端设备的密钥派生可以和参考第一实施方式描述的那样进行。

附图说明

[0045] 以下参考附图示例性描述本发明。其中,

[0046] 图 1 示意性示出了按照本发明的数据载体的优选实施方式,

[0047] 图 2 和图 3 示出了在图 1 的数据载体和终端设备之间按照本发明的方法的第一优选实施方式的步骤,和

[0048] 图 4 示出了图 2 和 3 的方法的用于提供特定于会话的数据载体参数的附加步骤。

具体实施方式

[0049] 参考图 1,在此作为芯片卡示出的数据载体 10 包括数据通信接口 20、20',处理器 30 以及不同的存储器 40、50 和 60。数据载体 10 也可以按照另外的构造呈现。

[0050] 数据载体 10 包括用于有接触的数据通信的接触区 20 以及用于无接触的数据通信的天线线圈 20' 作为数据通信接口 20、20'。可以设置替换的数据通信接口。还可以的是,数据载体 10 仅支持一种数据通信,也就是仅支持有接触的或无接触的数据通信。

[0051] 非易失性的、不可重写的 ROM 存储器 40 包括数据载体 10 的操作系统(OS)42,其控制数据载体 10。操作系统 42 的至少部分也可以存储在非易失性的、可重写的存储器 50 中。其例如可以作为闪存呈现。

[0052] 存储器 50 包括加密装置 52,借助该加密装置可以执行在数据载体 10 和终端设备(未示出)之间的加密方法。在此可以应用同样在存储器中存储的密钥 54、56、另一个值 57 以及数字证书 58。最后在数据载体 10 中存储验证参数 59。加密装置 52 的工作方式以及密钥 54、56 的、值 57 的、验证参数 59 的和证书 58 的在加密方法的范围内的作用将参考图 2 和 3 更详细地描述。存储器 50 可以包含其他数据,例如涉及用户的数据。

[0053] 易失性的、可重写的 RAM 存储器 60 对于数据载体 10 来说用作工作存储器。

[0054] 数据载体 10 当其例如是电子证件时可以包括其他特征(未示出)。这些特征可以可见地设置、例如印制于数据载体 10 的表面上，并且表示数据载体的用户，例如通过其姓名或照片来表示。按照下面更详细描述的一种实施方式，可以的是，验证参数 59、例如以 PIN 等形式不仅存储在数据载体 10 中，而且附加地光学可读地设置、例如印制到数据载体表面上。

[0055] 参考图 2 和 3 现在更详细描述在数据载体 10 和终端设备之间的加密方法的实施方式。在图 2 中示出了准备步骤。它们例如可以在制造数据载体 10 期间，例如在个性化阶段进行。

[0056] 在第一步骤 S1 中形成秘密的基本密钥 SKG 以及公开的数据载体密钥 PKG。秘密的基本密钥 SKG 可以构造为秘密的组密钥，其对于数据载体 10 的集合或组来说是共同的。秘密的基本密钥以及公开的数据载体密钥 PKG 是静态的，即，对于其整个寿命与数据载体 10 关联。

[0057] 公开的数据载体密钥 PKG 计算为规定的本原根 g 的取幂对规定的素数 p 取模的结果。在以下描述的计算全部应读作模素数 p，而这并不总是特别指出。两个密钥 SKG 和 PKG 形成数据载体密钥对并且是后面描述的方法的基础。

[0058] 在此要指出，全部计算，即，在本发明的范围内示出的相乘和取幂，不仅可以关于本原的模 p 剩余类群来执行，而且可以关于任意群来执行，任意群在此理解为数学结构而不可与上面提到的数据载体的组混淆，例如也可以基于椭圆曲线来执行。

[0059] 在步骤 S2 中形成证书 CPKG，其用于校验公开的数据载体密钥 PKG。

[0060] 步骤 S3 在数据载体 10 的个性化期间进行。在此数据载体 10 配备有数据载体密钥对。公开的数据载体密钥 PKG 对于数据载体 10 来说用作公开密钥。数据载体 10 的秘密的数据载体密钥 SK1 随机地、也就是在使用随机数 RND1 的条件下从秘密的基本密钥 SKG 中派生。

[0061] 以这种方式，如果秘密的基本密钥是秘密的组密钥，则该组的每个数据载体 10 配备有密钥对，其与该组的另一个数据载体的相应的密钥对由于在密钥派生时的随机分量而通过分别不同的秘密的数据载体密钥 SK1 相区别。另一方面，在 SKG 是秘密的组密钥的情况下，由于前面描述的对公开的数据载体密钥的派生，该组的所有数据载体 10 包括相同的公开的数据载体密钥 PKG。此外在该情况下数据载体的该组的全部秘密的数据载体密钥从相同的秘密的组密钥中派生。

[0062] 相反，如果秘密的基本密钥 SKG 不是组密钥，即，对于每个数据载体 10 提供单独的秘密的基本密钥，则每个数据载体 10 也包括虽静态却单独的公开的数据载体密钥 PKG。

[0063] 在子步骤 TS31 中派生数据载体单独的秘密的数据载体密钥 SK1，方法是，将秘密的基本密钥 SKG 与随机数 RND1 相乘。

[0064] 在另一个步骤 TS32 中，从本原根 g 出发，计算第一基数 g1。在此以已用于确定秘密密钥的随机数 RND1 的倒数对本原根 g 取幂： $g1 := g^{(1/RND1)}$ 。随机数 RND1 的倒数 1/RND1 在此关于模素数 p 乘法形成随机数 RND1 的乘法逆元。

[0065] 在子步骤 TS33 中产生验证参数 AP。该验证参数如后面参考图 3 描述的那样用于在加密方法的范围内的基于口令的验证。验证参数 AP 可以按照任意的、合适的形式产生或

提供,例如作为以 PIN 形式的秘密数据,作为对称加密方法(AES, TDES, DES 等等)的密钥等。同样可以将数据载体 10 后来的用户的生物测量的特征、例如指纹等作为验证参数 AP 来产生。最后也可以考虑对于数据载体 10 单独的数据载体特征作为验证参数 AP,例如 MM 特征。“MM”在此代表“可调的可用于机器的(modulierte maschinenfähiges)”(特征),即在数据载体体中置入的、秘密的机器可读材料。

[0066] 密钥 SK1 和 PKG 在子步骤 TS34 中与基数 g1、证书 C_{PKG} 和验证参数 AP 一起存储在数据载体 10 中。验证参数 AP 为此必要时合适地数字化。这例如当产生生物测量的特征作为验证参数 AP 时是适用的。在 MM 特征作为验证参数的情况下,将借助该特征机器可读地编码的“消息”再次数字地存储在数据载体 10 的存储器中。数据载体 10 如后面描述的那样需要验证参数 AP,以便由此将数据加密或数字地签名。

[0067] 必要时可以将验证参数 AP 如已经参考 MM 特征描述过的情况那样这样设置在数据载体上,使得该参数在数据载体合适地呈现给终端设备时可以由终端设备以光学的或其他方式机器地读出。于是,例如也可以将作为验证参数 AP 使用的 PIN 除了存储在数据载体 10 的存储器 50 中之外还光学可读出地设置、例如印制到数据载体 10 的数据载体本体上。在此重要的仅仅是,机器读出仅当数据载体 10 的用户打算并允许这样做时才进行,也就是例如不是未知地在无接触的路径上进行。

[0068] 随机数 RND1 不是存储在数据载体 10 中,就像秘密的基本密钥 SKG 也不存储在数据载体中那样。

[0069] 数据载体 10 由此构造为,借助其加密装置 52 利用终端设备执行加密方法,如这参考图 3 更详细描述的那样。

[0070] 在步骤 S4 中数据载体 10 向终端设备提供为了执行加密方法所需的数据(参考子步骤 TS42)。为了约定通信密钥 KK,终端设备在示出的实施方式中需要基数 g1 以及公开的组密钥 PKG。为了校验组密钥 PKG,终端设备需要相应的证书 C_{PKG} 。

[0071] 然而基数 g1 在其作为会话参数提供到终端设备之前在数据载体 10 中借助验证参数 AP 在子步骤 TS41 中加密。替换地,基数 g1 也可以借助验证参数 g1 被数字地签名。以这种方式可以简单地如后面描述的那样将基于口令的验证集成到该方法中。

[0072] 数据载体 10 可以将数据载体 10 的描述过的参数在子步骤 TS42 中发送到终端设备。也可以的是,这些值存储在数据载体 10 的可自由读出的存储区域中并且在需要时由终端设备读出。

[0073] 在步骤 S5 中外部地向终端设备提供终端设备为了检验或者验证目的所需的验证参数 AP。按照一种变型方案,验证参数可以由数据载体的用户通过输入装置输入到终端设备中。PIN 例如经由键盘等输入,指纹经由合适的传感器。替换地,数据载体的用户可以将验证参数这样合适地呈现给终端设备,使得在数据载体上设置的验证参数可以由终端设备机器地读出,例如前面描述的 MM 特征或印制在数据载体本体上的 PIN。

[0074] 在步骤 S6 中终端设备在其方面准备加密方法。在子步骤 TS61 中终端设备基于在步骤 S5 中接收的验证参数 AP 将加密的基数 $g1'$ 进行解密,以便从中获得基数 g1。在数据载体在子步骤 TS42 中向终端设备提供数字签名过的形式的基数 g1 的情况下,终端设备在子步骤 TS61 中相应地根据验证参数 AP 校验签名。

[0075] 通过终端设备对验证参数 AP 的检验和由此对数据载体 10 的用户的或者数据载体

10本身的验证,在基数 g1 由数据载体 10 在子步骤 TS41 中数字地签名了的情况下借助签名的校验在子步骤 TS61 中进行。如果该校验成功,则验证参数被认为是检验成功。

[0076] 在基数 g1 在子步骤 TS41 中由数据载体 10 借助验证参数 AP 加密了的优选替换情况下,验证参数 AP 的检验一方面在对加密过的基数 g1 进行解密的情况下进行。另一个隐含的检验步骤于是稍后在方法的运行过程中才进行,也就是通过:确定(或者没有确定)秘密的通信密钥 KK (参见步骤 S7) 的约定已经可以成功地进行。该事实可以通过如下来确定,即,基于约定的通信密钥 KK 而力求达到的、在数据载体 10 和终端设备之间的对称加密的数据通信实际上也可以执行,也就是两方具有相同的通信密钥 KK。在该时刻才表明,由终端设备在子步骤 TS61 基于在步骤 S5 中接收的验证参数 AP 解密的第一基数 g1 与数据载体 10 在子步骤 TS41 中借助在数据载体 10 中存储的验证参数 AP 加密过的基数 g1 相应。以这种方式可以防止特定攻击,例如对以验证参数形式的口令的字典攻击。

[0077] 可以设置成,紧接在此处描述的加密方法之后进行在数据载体 10 和当前的或与当前的终端设备例如经过数据通信网络相连的另外的终端设备之间的另一个验证方法。在此数据载体可以以公知方式相对于终端设备验证并且反之亦然。因为该方法也包括后面描述的密钥交换方法,例如基于公知的 Diffie-Hellman 方法的密钥交换方法,所以当前的终端设备,如果需要的话,将基数 g1 经过受保护的数据传输通道(例如经由 SSL)传送到相连的终端设备。在数据载体 10 和相应的终端设备之间的相应的验证方法然后可以如公知的那样进行。

[0078] 然后在子步骤 TS62 中,终端设备产生秘密的终端密钥 SK_T。这例如可以随机地进行。终端设备借助以自己的秘密的终端密钥对通过数据载体 10 按照描述的方式提供的基数 g1 取幂来计算该终端设备的公开的终端密钥 PK_T:

$$[0079] \quad PK_T := g1^{\wedge SK_T}.$$

[0080] 可选地,终端设备可以证实、特别是按特定的标准来检验 g1 和 / 或 PK_T。由此终端可以识别借助灵活选择的 g1 值对秘密的终端密钥 SK_T的攻击,该终端然后可以中断过程或拒绝进一步的通信。

[0081] 公开的终端密钥 PK_T通过终端设备提供、例如发送给数据载体 10。

[0082] 在下面的步骤 S7 中现在具体地约定通信密钥 KK,如已经解释的。数据载体 10 通过以自己的秘密密钥 SK1 对终端设备的公开的终端密钥 PK_T取幂来计算通信密钥 KK :

$$[0083] \quad KK_{DT} := PK_T^{\wedge SK1}$$

$$[0084] \quad = (g1^{\wedge SK_T})^{\wedge SK1} \quad (PK_T \text{ 的定义})$$

$$[0085] \quad = ((g^{\wedge (1/RND1)})^{\wedge SK_T})^{\wedge SK1} \quad (g1 \text{ 的定义})$$

$$[0086] \quad = ((g^{\wedge (1/RND1)})^{\wedge SK_T})^{\wedge (SKG*RND1)} \quad (SK1 \text{ 的定义})$$

$$[0087] \quad = (g^{\wedge ((1/RND1)*SK_T*SKG*RND1)}) \quad (\text{变形})$$

$$[0088] \quad = g^{\wedge (SK_T*SKG)}$$

[0089] 终端设备借助以终端设备的秘密的终端密钥 SK_T对公开的数据载体密钥 PKG 取幂来计算通信密钥 KK :

$$[0090] \quad KK_T := PKG^{\wedge SK_T}$$

$$[0091] \quad = (g^{\wedge SKG})^{\wedge SK_T} \quad (PKG \text{ 的定义})$$

$$[0092] \quad = g^{\wedge (SK_T*SKG)} \quad (\text{变形})$$

[0093] 也就是表明,数据载体 10 和终端设备基于分别呈现给它们的数据达到相同的结果。这如上所述仅当终端设备在子步骤 TS61 中获得与解密的结果恰好相同的基数 g1 值时才成立,该值在子步骤 TS41 中由数据载体 10 已经加密。于是,这又恰好在数据载体 10 中为了加密而考虑的验证参数 AP 与终端设备在步骤 S5 中提供的验证参数 AP 一致时才成立。换言之,恰好当基于验证参数 AP 进行的、在数据载体 10 和终端设备之间的基于口令的验证方法作为在这些方之间进行的加密方法的一部分已经能够成功地进行时才成立。

[0094] 在步骤 S8 中最后终端设备检验公开的数据载体密钥 PKG 的证书 C_{PKG} 。证书的该检验替换地也可以在步骤 S7 中约定通信密钥 KK 之前和 / 或在步骤 S6 中约定秘密的会话密钥 SK_T 之前进行。

[0095] 由此在数据载体 10 和终端设备之间的加密方法结束。

[0096] 为了可以在后面的、借助示例性描述的方法相对于同一个或另外的终端设备的另外的验证时数据载体 10 未被识别地和唯一地与用户对应,在数据载体 10 中提供特定于会话的数据载体参数。这涉及秘密的数据载体密钥 SK1 以及基数 g1。该基数 g1 如上所述在该方法的范围内传输到终端设备或以另外的方式提供给该终端设备。不变的、数据载体单独的基数 g1 由此可以用于识别数据载体 10。这也适用于数据载体 10 的秘密的数据载体密钥 SK1,只要该数据载体密钥是静态地数据载体单独的并且例如在挑战 - 响应方法的范围内被采用的话。

[0097] 下面参考图 4 描述在数据载体内部产生特定于会话的数据载体参数。

[0098] 在步骤 S9 中示出了在数据载体 10 中派生秘密的数据载体会话密钥 SK_s 。为此,在数据载体 10 中提供随机数 RNS_s 形式的会话参数。将当前的秘密密钥 SK1 与随机数 RNS_s 相乘,由此派生数据载体 10 的秘密的数据载体会话密钥 SK_s :

[0099] $SK_s := SK1 * RNS_s$ 。

[0100] 然后在步骤 S10 中将当前的秘密的数据载体密钥 SK1 的值通过数据载体会话密钥的值替代:

[0101] $SK1 := SK_s$ 。

[0102] 由此,数据载体 10 的秘密的数据载体密钥 SK1 是特定于会话的。根据秘密的数据载体密钥 SK1 对数据载体 10 的跟踪被排除,因为该秘密的数据载体密钥在两次执行验证方法之间以描述的方式改变。

[0103] 以相同的方式如在步骤 S11 和 S12 中所示,将基数 g1 通过会话基数 g_s 替代 ($g1 := g_s$),该会话基数事先通过如下计算得到,即,以随机数 RNS_s 的倒数对基数 g1 取幂: $g_s := g1^{\wedge} (1/RNS_s)$ 。由此数据载体 10 的基数 g1 始终是特定于会话的并且根据传输到终端设备的基数 g1 对数据载体 10 的跟踪被排除。随机数 RNS_s 然后被删除。由此也排除了对前面的会话参数的推导。

[0104] 替代随机数 RNS_s 或者除了所述随机数之外也可以使用另一个会话参数。该会话参数也可以与由终端设备提供的、例如在相对于数据载体成功验证之后提供的值有关。在数据载体内部根据通过终端设备提供的值计算相应的会话参数。这样计算的会话参数然后例如可以替代在步骤 S9 和 S11 中使用的随机数 RNS_s 而用于产生秘密的会话密钥或会话基数并且然后被删除。由此数据载体 10 对于下一个要进行的验证方法具有特定于会话的参数。

[0105] 按照优选实施方式,终端设备向数据载体 10 提供所谓的公开的扇区密钥 PK_{SEC} 。根

据该扇区密钥，数据载体 10 于是可以如后面描述的那样计算当前的会话参数。

[0106] 公开的扇区密钥 PK_{SEC} 在此是扇区密钥对 (PK_{SEC}, SK_{SEC}) 的部分，其中相应的秘密的扇区密钥 SK_{SEC} 不呈现给终端设备本身，而是仅呈现给上级布置的阻止实体 (Sperrinstanz)，不同的终端设备在不同的所谓扇区中下级布置于该阻止实体。即，阻止实体管理不同的扇区、例如不同的管理区等中的不同终端设备。对提到的扇区密钥对 (PK_{SEC}, SK_{SEC}) 的补充，数据载体 10 也可以包括相应的数据载体扇区密钥对 (PKD_{SEC}, SKD_{SEC}) ，其包括秘密的数据载体扇区密钥 SKD_{SEC} 和公开的数据载体扇区密钥 PKD_{SEC} 。后者存储在阻止实体可以访问的数据库中。提到的扇区密钥用于能够至少在扇区内部通过终端设备识别数据载体 10。该识别也可以由阻止实体出于阻止目的而考虑。

[0107] 数据载体 10 的识别根据在终端设备和数据载体 10 之间约定的值 I_{SEC} 进行。该值通过如下被计算，即，终端设备向数据载体 10 提供其公开的扇区密钥 PK_{SEC} 。数据载体 10 从中借助其秘密的数据载体扇区密钥 SKD_{SEC} 派生一个值，例如就像由 Diffie-Hellman 密钥交换方法中公知的那样。然后将该值借助 Hash 函数 H 压缩并且提供给终端设备。终端设备将获得的值 I_{SEC} 与终端设备从阻止实体获得的相应的值进行比较。仅阻止实体能够根据在数据库中存储的公开的数据载体扇区密钥 PKD_{SEC} 和秘密的扇区密钥 SK_{SEC} 在其方面计算值 I_{SEC} 。因此值 I_{SEC} 是与扇区有关以及与数据载体 10 有关的。阻止实体具有在其下级布置的扇区的全部的秘密的扇区密钥。

[0108] 值 I_{SEC} 现在在数据载体 10 内部用作会话参数。即，秘密的会话密钥 SK_s 和会话基数 g_s 的计算类似于步骤 S9 和 S11，但利用 I_{SEC} 而不是 RNS_s 进行。

[0109] 此时可以设置成，在数据载体 10 中将第一基数 g_1 分开地、例如作为 g_B 存储。该基数 g_B ，如下面描述的，用于检验目的并且不被覆盖。此外可以对于每个会话 i ，即，对于每个执行的在数据载体 10 和终端设备之间的验证方法，由终端设备提供的公开的扇区密钥 $PK_{SEC,i}$ 关于会话、即会话在进行顺序中的编号 i 存储在数据载体 10 中。在此仅仅涉及公开的数据。由此如果这些数据被窥视，不会产生安全风险。这些数据按照方法当数据载体为了检验而呈现给阻止实体时仅可以由该阻止实体读出。替代公开密钥地，也可以存储认证机构的标识，例如按照 ISO/IEC7816-4 的发行者标识 (Issuer Identification)。

[0110] 因为阻止实体既可识别以来自数据库的公开的数据载体扇区密钥 PKD_{SEC} ，也可以识别所有在其下级布置的扇区的全部秘密的扇区密钥 $SK_{SEC,i}$ ，所以阻止实体能够确定在数据载体 10 和这样的扇区的终端设备之间在会话 i 中已经约定的值 $I_{SEC,i}$ 。以这种方式，阻止装置可以基于在数据载体 10 中存储的值、即基数 g_B 以及每个会话 i 的公开的扇区密钥 $PK_{SEC,i}$ ，计算并且由此证实当前在数据载体中存在的基数 g_s 。为此仅需将会话 i 的公开的扇区密钥 $PK_{SEC,i}$ 与该会话 i 的值 $I_{SEC,i}$ 关联并且最后重建当前的基数 g_s 的计算，方法是，以各个会话的值 $I_{SEC,i}$ 的乘积的倒数对值 g_B (初始的 g_1) 取幂：

[0111] $g_s := g_B^{(1/(I_{SEC,1} * I_{SEC,2} * I_{SEC,3} \dots * I_{SEC,n}))}$ 。

[0112] 以这种方式，阻止实体可以检验，数据载体 10 为了派生基数 g_s 是否实际上已经按照前面描述的方式使用了秘密的数据载体扇区密钥 SKD_{SEC} 。如果没有，则在数据载体中当前存在的基数与通过阻止实体计算的基数 g_s 不同。不具有正确的秘密的数据载体扇区密钥 SKD_{SEC} 的伪造的数据载体 10 可以由阻止实体以这种方式明确地识别并且然后在必要时进行阻止。

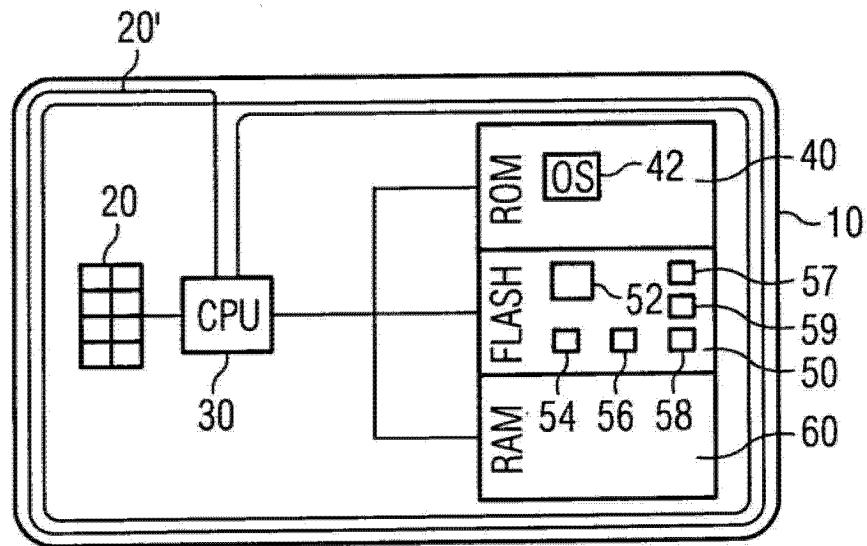


图 1

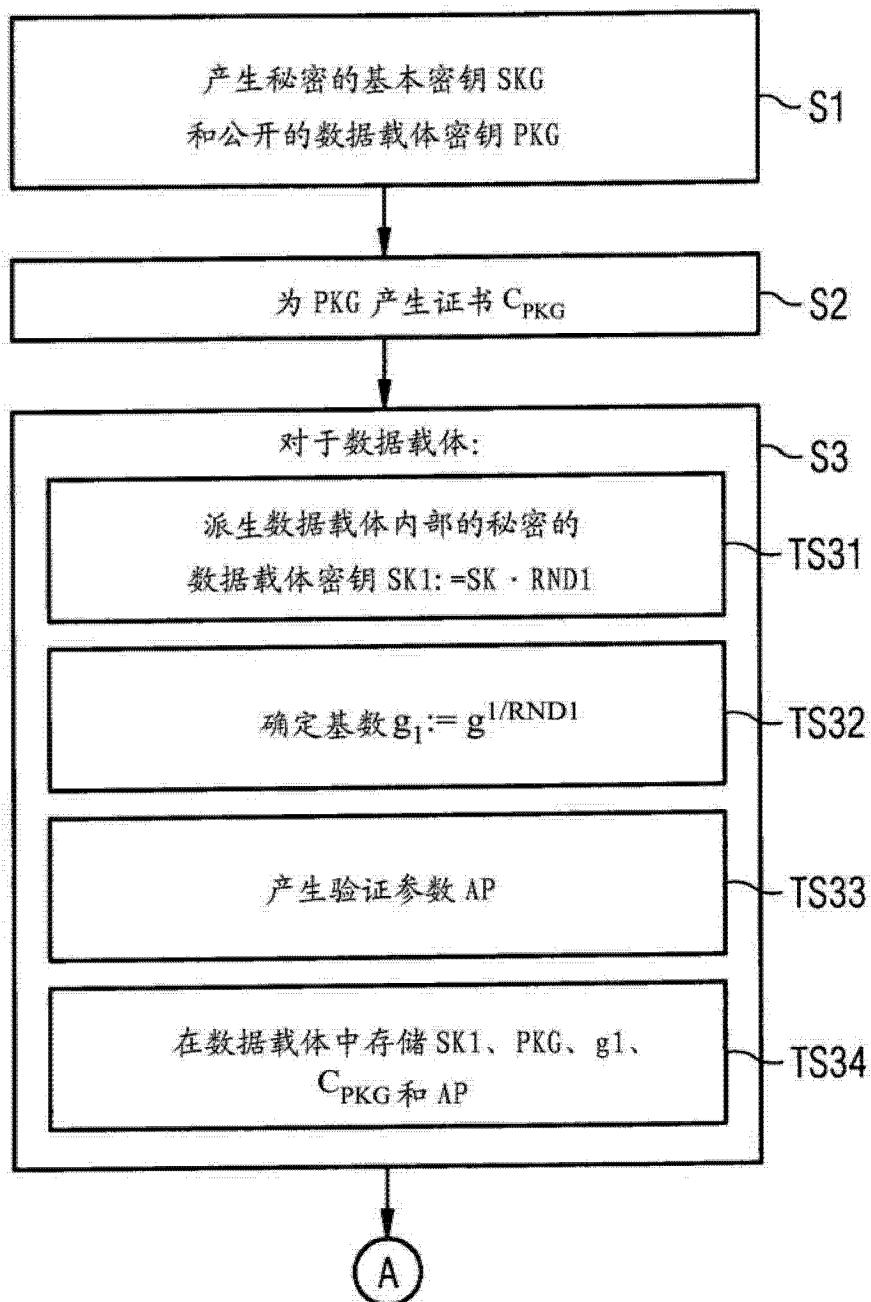


图 2

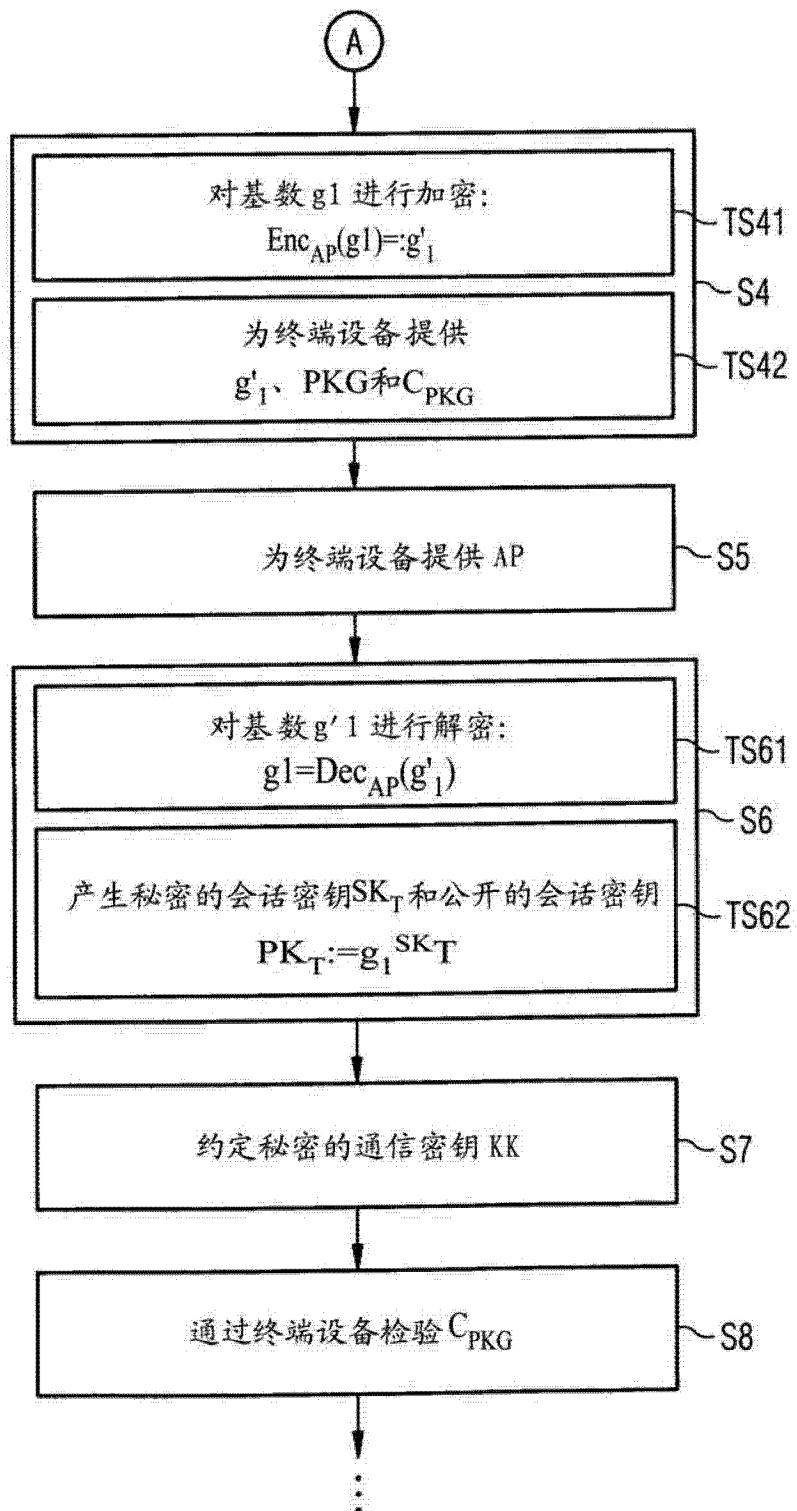


图 3

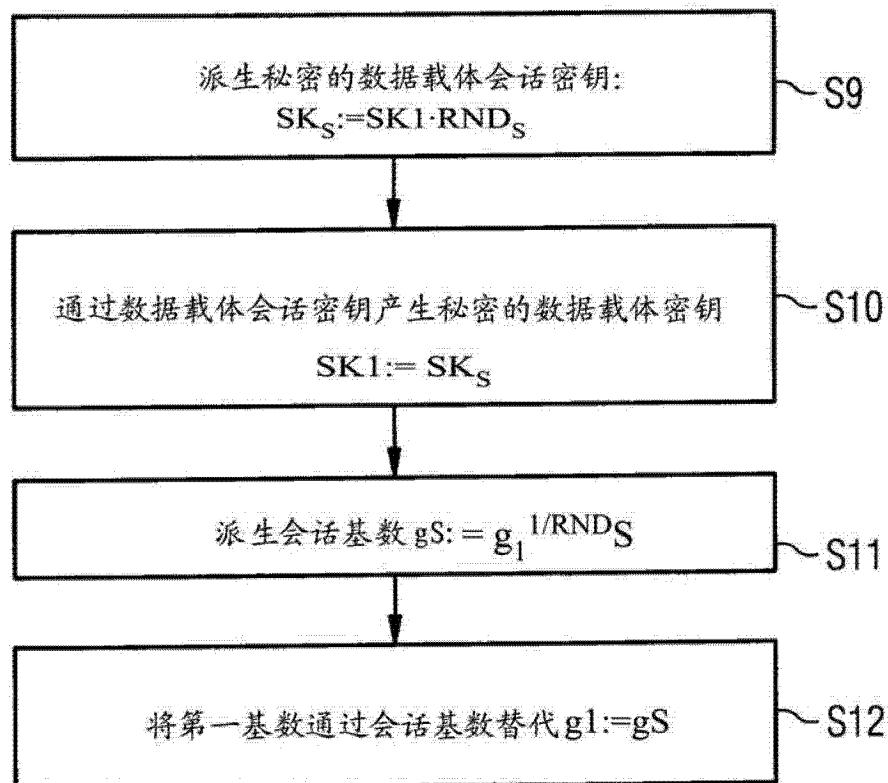


图 4