[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G07C 11/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 200480017958.6

[45] 授权公告日 2010 年 1 月 20 日

[11] 授权公告号 CN 100583170C

[22] 申请日 2004.5.25
[21] 申请号 200480017958.6
[30] 优先权
[32] 2003. 6.25 [33] DE [31] 10328328.5
[86] 国际申请 PCT/EP2004/005581 2004.5.25
[87] 国际公布 WO2004/114173 德 2004.12.29
[85] 进入国家阶段日期 2005.12.26
[73] 专利权人 TUEV 莱茵兰控股公司
地址 德国科隆
[72] 发明人 R·维尔德 S·多泽 K·海因茨
[56] 参考文献
DE10137695A1 2003.2.13
DE19920744A1 2000.11.16
DE4109114A1 1992.9.24
US4816824A 1989.3.28
DE4341880A1 1995.6.14
CN1178949A 1998.4.15
US5367148A 1994.11.22
US6226619B1 2001.5.1
CN1226040A 1999.8.18
哈希加密方案. 黄智颖，冯新喜，张焕国. 通信技术，第 7 期. 2001
综合数字防伪方案. 蔡文望，罗平，彭小宁. 清华大学学报（自然科学版），第 43 卷第 1 期. 2003
审查员 卜冬泉
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 吴立明 张志醒

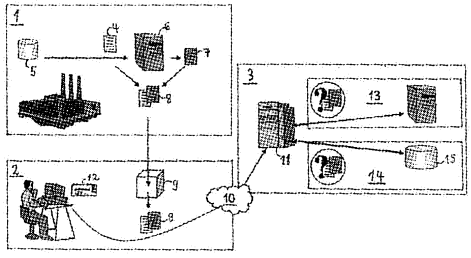
权利要求书 5 页 说明书 20 页 附图 3 页

[54] 发明名称

用于产品真实性测试的产品保护入口和方法

[57] 摘要

在根据本发明的产品保护系统中，将产品特有的标识序列(K)分配给产品件，所述产品特有的标识序列(K)借助于加密方法(F1)在应用秘密的加密序列(B)的情况下被转换为已编码的测试序列(C)。 将产品检验序列(8)安置在该产品件上或旁边，所述产品检验序列(8)包括所述已编码的测试序列(C)或由此得出的序列。 为了检查产品件的真实性，在检验询问者侧检测产品检验序列，并通过因特网(10)传送到产品保护服务器结构(11)。 在那里，借助于解密方法(F2)在应用解密序列(A)的情况下从产品检验序列(8)中得出被解密的测试序列。 检查被解密的测试序列或者由此得出的序列的真实性，并通过因特网(10)将真实性测试的结果传送到检验询问者。



1.用于借助于被安置在产品件上或旁边的产品检验序列（8）通过因特网（10）来检查所述产品件的真实性的方法，其特征在于以下步骤：

－在检验询问者侧检测所述产品检验序列（8）；

－通过所述因特网（10）将所述产品检验序列（8）传送到产品保护服务器结构（11）；

－在所述产品保护服务器结构（11）侧，借助于解密方法（F2）在应用解密序列（A）的情况下解密从所述产品检验序列（8）中得出的已编码的测试序列（C），并产生被解密的测试序列，其中，所述解密序列（A）与加密时所应用的加密序列（B）一起构成互补的密匙对，其中所述解密序列（A）是对称的加密方法的秘密密钥；

－检查所述被解密的测试序列或由此得出的序列的真实性；

－通过所述因特网（10）将所述真实性测试的结果传送到检验询问者。

2.根据权利要求 1 所述的方法，其特征在于，所述已编码的测试序列（C）作为序列段被包括在所述产品检验序列（8）中，或能通过应用哈希反函数（h_2^{-1}）从所述产品检验序列（8）的序列段中得出。

3.根据权利要求 1 或 2 之一所述的方法，其特征在于，所述被解密的测试序列代表产品特有的标识序列（K），或能通过应用哈希反函数（h_1^{-1}）被转换为产品特有的标识序列（K）。

4.根据权利要求 1 或 2 之一所述的方法，其特征在于，通过将所述被解密的测试序列或由此得出的序列与作为序列段被包括在所述产品检验序列（8）中的产品特有的标识序列（K）或由此得出的哈希序列（h_1（K））进行比较，来检查所述被解密的测试序列或由此得出的序列的真实性。

5.根据权利要求 1 或 2 之一所述的方法，其特征在于，通过检查所述被解密的测试序列或由此得出的序列是否属于事先所确定的定额，来检查所述被解密的测试序列或由此得出的序列的真实性。

6.根据权利要求 3 所述的方法，其特征在于，所述产品特有的标识序列（K）是所述产品件的序列号。

7.根据权利要求 4 所述的方法，其特征在于，所述产品特有的标识

序列（K）是所述产品件的序列号。

8.根据权利要求 1 或 2 之一所述的方法，其特征在于，在检查产品检验序列（8）的范围中测试所述检验询问者的合法性。

9.根据权利要求 1 或 2 之一所述的方法，其特征在于，在针对产品检验序列（8）进行检验询问的范围中，数据库记录项被存放在记录数据库（15）中。

10.根据权利要求 1 或 2 之一所述的方法，其特征在于，为了确定早些时候对所述产品件的产品检验序列（8）的检验询问，数据库询问在记录数据库（15）中被执行。

11. 根据权利要求 9 所述的方法，其特征在于，为了确定早些时候对所述产品件的产品检验序列（8）的检验询问，数据库询问在记录数据库（15）中被执行。

12.根据权利要求 9 所述的方法，其特征在于，将产品检验序列(8)、产品特有的标识序列（K）、已编码的测试序列（C）、被解密的测试序列或由此得出的序列中的至少一个与所述记录数据库（15）中的数据库记录项进行比较，其中，如果发现上述序列中的至少一个一致，那么所述产品件被识别为伪造品或伪造品的样本。

13.根据权利要求 10 所述的方法，其特征在于，将产品检验序列（8）、产品特有的标识序列（K）、已编码的测试序列（C）、被解密的测试序列或由此得出的序列中的至少一个与所述记录数据库（15）中的数据库记录项进行比较，其中，如果发现上述序列中的至少一个一致，那么所述产品件被识别为伪造品或伪造品的样本。

14.根据权利要求 9 所述的方法，其特征在于，检验询问的数据库记录项包括所述检验询问的日期。

15.根据权利要求 10 所述的方法，其特征在于，检验询问的数据库记录项包括所述检验询问的日期。

16.根据权利要求 9 所述的方法，其特征在于，数据库记录项包括所述检验询问者的身份。

17.根据权利要求 10 所述的方法，其特征在于，数据库记录项包括所述检验询问者的身份。

18.用于实施产品保护入口的产品保护服务器结构，该产品保护入口用于根据被安置在产品件上或旁边的产品检验序列（8）来检查所述

产品件的真实性，其特征在于：

－网页服务器模块，其通过因特网（10）能提供所述产品保护入口的网页，其中在检验询问者侧所检测的产品检验序列（8）通过所述因特网（10）被传送到所述网页服务器模块，并且其中真实性测试的结果通过所述因特网（10）被传送到所述检验询问者；

－加密模块，其借助于解密方法（F2）在应用解密序列（A）的情况下来解密从所述产品检验序列（8）中得出的已编码的测试序列（C），并产生被解密的测试序列，其中该加密模块检查被解密的测试序列或由此得出的序列的真实性，其中该加密模块借助于对称的解密方法在应用秘密的解密序列的情况下来解密所述已编码的测试序列（C），和其中所述解密序列（A）与加密时所应用的加密序列（B）构成互补的密匙对。

19.根据权利要求 18 所述的产品保护服务器结构，其特征在于，通过将所述被解密的测试序列或由此得出的序列与作为序列段被包括在所述产品检验序列（8）中的产品特有的标识序列（K）或由此得出的哈希序列（h_1（K））进行比较，所述加密模块检查所述被解密的测试序列或由此得出的序列的真实性。

20.根据权利要求 18 所述的产品保护服务器结构，其特征在于，通过检查所述被解密的测试序列或由此得出的序列是否属于事先所确定的定额，所述加密模块检查所述被解密的测试序列或由此得出的序列的真实性。

21.根据权利要求 18 至 20 之一所述的产品保护服务器结构，其特征在于记录数据库（15），其至少针对每个已经确定其真实性的产品检验序列（8）包括一个数据库记录项。

22.根据权利要求 21 所述的产品保护服务器结构，其特征在于，将产品检验序列（8）、产品特有的标识序列（K）、已编码的测试序列（C）、被解密的测试序列或由此得出的序列中的至少一个与所述记录数据库（15）中的数据库记录项进行比较，其中，如果发现上述序列中的至少一个一致，那么所述产品件被识别为伪造品或伪造品的样本。

23.用于借助于被安置在产品件上或旁边的产品检验序列（8）通过因特网（10）来检查所述产品件的真实性的设备，其具有：

－用于在检验询问者侧检测产品检验序列（8）的装置；

－用于通过因特网（10）将所述产品检验序列（8）传送到产品保护服务器结构（11）的装置；

－用于在所述产品保护服务器结构（11）侧借助于解密方法（F2）在应用解密序列（A）的情况下解密从所述产品检验序列（8）中得出的已编码的测试序列（C）并产生被解密的测试序列的装置，其中，所述解密序列（A）与加密时所应用的加密序列（B）一起构成互补的密匙对，其中所述解密序列（A）是对称的加密方法的秘密密钥；

－用于检查所述被解密的测试序列或由此得出的序列的真实性的装置；

－用于通过所述因特网（10）将所述真实性测试的结果传送到检验询问者的装置。

24.根据权利要求 22 所述的设备，其特征在于，所述已编码的测试序列（C）作为序列段被包括在所述产品检验序列（8）中，或能通过应用哈希反函数（h_2^{-1}）从所述产品检验序列（8）的序列段中得出。

25.根据权利要求 22 或 23 之一所述的设备，其特征在于，所述被解密的测试序列代表产品特有的标识序列（K），或能通过应用哈希反函数（h_1^{-1}）被转换为产品特有的标识序列（K）。

26.根据权利要求 22 或 23 之一所述的设备，其特征在于，通过将所述被解密的测试序列或由此得出的序列与作为序列段被包括在所述产品检验序列（8）中的产品特有的标识序列（K）或由此得出的哈希序列（h_1（K））进行比较，来检查所述被解密的测试序列或由此得出的序列的真实性。

27.根据权利要求 22 或 23 之一所述的设备，其特征在于，通过检查所述被解密的测试序列或由此得出的序列是否属于事先所确定的定额，来检查所述被解密的测试序列或由此得出的序列的真实性。

28.根据权利要求25 所述的设备，其特征在于，所述产品特有的标识序列（K）是所述产品件的序列号。

29.根据权利要求26 所述的设备，其特征在于，所述产品特有的标识序列（K）是所述产品件的序列号。

30.根据权利要求 23 或 24 之一所述的设备，其特征在于用于在检查产品检验序列（8）的范围中测试所述检验询问者的合法性的装置。

31.根据权利要求 23 或 24 之一所述的设备，其特征在于用于在针对产品检验序列（8）进行检验询问的范围中将数据库记录项存放在记录数据库（15）中的装置。

32.根据权利要求 23 或 24 之一所述的设备，其特征在于用于为了确定早些时候对所述产品件的产品检验序列（8）的检验询问而在记录数据库（15）中执行数据库询问的装置。

33. 根据权利要求 31 所述的设备，其特征在于用于为了确定早些时候对所述产品件的产品检验序列（8）的检验询问而在记录数据库（15）中执行数据库询问的装置。

34.根据权利要求 31 所述的设备，其特征在于用于将产品检验序列（8）、产品特有的标识序列（K）、已编码的测试序列（C）、被解密的测试序列或由此得出的序列中的至少一个与所述记录数据库（15）中的数据库记录项进行比较的装置，其中，如果发现上述序列中的至少一个一致，那么所述产品件被识别为伪造品或伪造品的样本。

35.根据权利要求 32 所述的设备，其特征在于用于将产品检验序列（8）、产品特有的标识序列（K）、已编码的测试序列（C）、被解密的测试序列或由此得出的序列中的至少一个与所述记录数据库（15）中的数据库记录项进行比较的装置，其中，如果发现上述序列中的至少一个一致，那么所述产品件被识别为伪造品或伪造品的样本。

36.根据权利要求 31 所述的设备，其特征在于，检验询问的数据库记录项包括所述检验询问的日期。

37.根据权利要求 32 所述的设备，其特征在于，检验询问的数据库记录项包括所述检验询问的日期。

38.根据权利要求 31 所述的设备，其特征在于，数据库记录项包括所述检验询问者的身份。

39.根据权利要求 32 所述的设备，其特征在于，数据库记录项包括所述检验询问者的身份。

用于产品真实性测试的产品保护入口和方法

本发明涉及一种用于测试产品的真实性或用于识别产品伪造的系统。

几乎没有一件产品免于仿造。伪造者的越来越好的技术可能性和越来越昂贵的方法导致越来越好的伪造品。消费者、但是商人也几乎不再可能一眼区分真品和伪造品。结果是该品牌制造商的销售额量下降、债务索赔和形象受损。许多品牌的传统识别特征（如标签、标牌、和包装）今天对伪造者而言不再构成障碍。因为除了产品本身以外，到现在甚至其整个包装也都被仿造。

尝试借助于专门的安全特征来抵制伪造，该安全特征要求高的技术上和资金上的花费，并且大部分只能在专用于此的企业中制造。产品或其包装或其附属单据已经在制造期间就配备了如安全线、模板（Planchette）等的安全特征，这些安全特征承载一种或多种物质，这些物质具有在视觉上或机器可测试的物理或化学特性、如荧光或磁性。全息标签也表示常用的安全特征，该全息标签显示出与观察角度相关的颜色效果，该颜色效果不能由仿制者复制，并且该全息标签可被粘贴在产品或其包装上。此外，缩微文本、纽索纹图（Guillochendruck）、潜影（Kinegramm）、转发器等等的应用属于用于提高防伪性和用于提高伪造的识别率的公知措施。

可是，所采用的安全特征根据例如法律上、医学上或也是经济上的要求分别只对于有限的产品范围有意义。工艺上花费大的措施必要时要求用于检查产品伪造的特殊的传感器和测量设备，这些设备通常是不可支配的。相反，相对伪造者的、特征的安全性所基于的技术领先消失，以便，技术领先消失得越快，安全特征的制造越有利和越简单。

从德国的公开文献 DE－OS 27 34 456 中公知了所谓的唯一卡（Unique Card）方法，其中，根据公开的信息（例如帐号和/或个人化信息）和唯一号码形成被加密的信息，其中这些信息被记录在记录载体上。在读取和检验该记录载体时，首先由被加密的信息和唯一号码再次形成公开的信息。接着，将该信息与被记录在记录载体上的公

开的信息进行比较。这种方法被用于保障 ID 卡和文档。

从公开文献 DE 28 26 469 C2 中公知一种用于保障文档的方法和设备，其中标识号码被加密地记录在该文档上，以及在检验时将从该文档中读出的被加密的标识号码进行解密，并与原来的标识号进行比较。

DE 43 41 880 A1 公开了一种针对对象的检验系统和一种用于检验对象的方法，其中在此采用例如可被构造为电子微型数据载体的模块，该模块被布置在物品/产品中或上，其中在该电子数据载体中电子地、磁性地、光学地或机械地存储标识码。

DE 199 20 744 A1 公开了一种方法，该方法研究伪造品、尤其是品牌产品的确定。在此，使最不相同的加密方法彼此结合，并且获得不可再伪造的产品。在这种情况下，给每个品牌物品提供具有系统范围内明确的符号的具体的产品芯片。

US 4,816,824 涉及扫描检查系统，其尤其是用于超市。由此使用于改善防止剽窃的在线测试成为可能。

DE 101 37 695 A1 公开了一种用于确定剽窃的方法，其中从第一特有的个性化特征与第二无规律的个性化特征的组合中获得防伪。在此，尤其是第二个性化特征也可以通过加密算法从第一个性化特征中来确定。第二个性化特征与第一个性化特征分离地被涂在各个产品上。

SI 9800026 A 的 EPO 摘要公开了一种产品安全系统，其中基本码被涂在真品上，并另外公开了秘密代码，可是该秘密代码与基本码分离地被安置在产品上。授权的用户可读出该秘密的和隐蔽安置的代码，并通过到制造商的电信连接确定该产品的真实性。

本发明所基于的任务在于，建议一种用于检查产品件的真实性的方法，该方法原则上可用于所有产品，对可检查性提出尽可能少的附加要求，并且是廉价的，以及建议一种用于实施产品保护入口的产品保护服务器结构，该产品保护入口用于根据被安置在产品件上或旁边的产品检验序列来检查所述产品件的真实性，并且建议一种用于借助于被安置在产品件上或旁边的产品检验序列通过因特网来检查所述产品件的真实性的设备。

本发明的任务通过用于借助于被安置在产品件上或旁边的产品检验序列通过因特网来检查所述产品件的真实性的方法来解决，该方法

具有以下步骤:

-在检验询问者侧检测所述产品检验序列;

-通过所述因特网将所述产品检验序列传送到产品保护服务器结构;

-在所述产品保护服务器结构侧,借助于解密方法在应用解密序列的情况下解密从所述产品检验序列中得出的已编码的测试序列,并产生被解密的测试序列,其中,所述解密序列与加密时所应用的加密序列一起构成互补的密匙对,其中所述解密序列是对称的加密方法的秘密密钥;

-检查所述被解密的测试序列或由此得出的序列的真实性;

-通过所述因特网将所述真实性测试的结果传送到检验询问者。

本发明的任务还通过用于实施产品保护入口的产品保护服务器结构来解决,该产品保护入口用于根据被安置在产品件上或旁边的产品检验序列来检查所述产品件的真实性,该产品保护服务器结构具有:

-网页服务器模块,其通过因特网能提供所述产品保护入口的网页,其中在检验询问者侧所检测的产品检验序列通过所述因特网被传送到所述网页服务器模块,并且其中真实性测试的结果通过所述因特网被传送到所述检验询问者;

-加密模块,其借助于解密方法在应用解密序列的情况下来解密从所述产品检验序列中得出的已编码的测试序列,并产生被解密的测试序列,其中该加密模块检查被解密的测试序列或由此得出的序列的真实性,其中该加密模块借助于对称的解密方法在应用秘密的解密序列的情况下来解密所述已编码的测试序列,和其中所述解密序列与加密时所应用的加密序列构成互补的密匙对。

本发明的任务此外通过用于借助于被安置在产品件上或旁边的产品检验序列通过因特网来检查所述产品件的真实性的设备来解决,该设备具有:

-用于在检验询问者侧检测产品检验序列的装置;

-用于通过因特网将所述产品检验序列传送到产品保护服务器结构的装置;

-用于在所述产品保护服务器结构侧借助于解密方法在应用解密序列的情况下解密从所述产品检验序列中得出的已编码的测试序列并

产生被解密的测试序列的装置，其中，所述解密序列与加密时所应用的加密序列一起构成互补的密匙对，其中所述解密序列是对称的加密方法的秘密密钥；

－用于检查所述被解密的测试序列或由此得出的序列的真实性的装置；

－用于通过所述因特网将所述真实性测试的结果传送到检验询问者的装置。

在根据本发明的方法中，为了产生被安置在产品件上或旁边来保证产品件的真实性的产品保护标志，首先为每个产品件确定产品特有的标识序列。这些产品特有的标识序列或由此得出的序列借助于加密方法（F1）在应用秘密的加密序列（B）的情况下来加密，其中产生已编码的测试序列。在该产品件上或旁边安置有产品检验序列，该产品检验序列包括已编码的测试序列或由此得出的序列。

为了能够区分真品与伪造品，产品的生产商可以使用秘密的加密序列（B）以及加密方法（F1），由此该生产商可以将各个产品特有的标识序列转换为已编码的测试序列，然后，将该已编码的测试序列安置在该产品件上或旁边。取代借助于物理的、测量技术的或化学的产品特征来保证产品件的真实性，在本方法中借助于加密产生的产品检验序列来识别伪造品。由此，可使用安全特征，该安全特征由于其不依赖于物理的或化学的产品特征而可被用于所有产品组。为了检查产品的真实性，不需要传感器或测量设备，而仅必须检查产品检验序列的真实性。由于取代复杂的安全特征（诸如微缩文本、纽索纹图、潜影、转发器等）而采用加密方法，所以根据本发明的方法也基本上比迄今所应用的安全特征廉价。

如果在不知道秘密的加密序列（K）的情况下从产品特有的标识序列（K）中不能产生已编码的检验序列（C），那么这是有利的。只有拥有秘密的加密序列的生产商可针对由其制造的产品件产生产品检验序列。从交易中的产品的产品检验序列中不能得出该秘密的加密序列（B）。

除了已编码的测试序列（C）或由此得出的序列以外，产品检验序列也包括产品特有的标识序列（K）。在此，产品检验序列不仅包括未被加密的标识序列（K）而且也包括已编码的测试序列（C）。因此，

通过检查产品检验序列的两个序列段的共同一致性，可以检查产品检验序列的真实性。为此，例如可以执行已编码的测试序列（C）的解密或产品特有的标识序列（K）的加密。

此外，如果产品件的序列号被用作产品特有的标识序列（K），那么这是有利的。该序列号在产品制造期间被产生，并允许将产品件分配给某一批。尤其是将序列号安置在高价值产品上是常见的实践。

为了产生根据本发明的产品检验序列，能够以不大的额外花费用被加密的检验序列来补充该序列号。

在本发明中，秘密的加密序列（B）是对称的加密方法的秘密密匙。对称的加密方法也被称作单密钥系统（Single-Key-System）或秘密密钥系统（Secret-Key-System）。为了加密产品特有的标识序列或由此得出的序列，应用秘密密匙、也即秘密的加密位串。即使加密和解密方法通常是公知的，这样产生的被加密的序列在对称的加密方法中也只能在知道该秘密密匙时再次被解密。相反地，如果利用秘密密钥解密被加密的序列提供所基于的未被加密的序列，那么该序列只能在知道该秘密密钥时才能被加密。

通常可以非常迅速地并且以少量花费不仅以硬件而且以软件来实现对称的方法。在应用对称的加密方法时的另一优点是，所应用的密钥长度和块长度一般相对短。由此，所产生的测试序列和产品检验序列相对短，以致这些序列可方便地被安置在产品件上。

如果对称的加密方法是加密方法三重 DES、IDEA、CAST－128、Blowfish、RC5、f8、Rijndael之一时，那么这是尤其有利的。

如果在加密之前借助第一哈希（Hash）方法（h_1）将产品特有的标识序列（K）转换成第一哈希序列（h_1（K）），那么这是有利的，其中已编码的测试序列（C）通过利用秘密的加密序列（B）加密第一哈希序列（h_1（K））来产生。因此，哈希方法（h_1）首先被用于产品特有的标识序列，并且这样产生的哈希序列接着被加密。通过将哈希方法附加地用于加密，可提高所有所执行的编码的安全性。因而，对于伪造者几乎不可能的是，根据已编码的测试序列（C）确定所基于的加密方法（F1）以及所基于的秘密的加密序列（B）。

此外，如果，在加密之后，已编码的测试序列（C）借助于第二哈希方法（h_2）被转换成第二哈希序列（h_2（C）），那么这是有利的，所述第二哈希序列作为产品检验序列的部分被安置在产品件上或旁边。借助于在加密之后所应用的第二哈希方法（h_2）尤其可能的是，在将很长的已编码的测试序列（C）作为产品检验序列的部分安置在产品件上或旁边之前，缩短该很长的已编码的测试序列（C）。尤其是，在应用通过大的密匙长度和块长度来表征的不对称的加密方法时，形成长的已编码的测试序列，该长的已编码的测试序列使第二哈

希方法的应用有效地出现。此外，通过第二哈希方法总共提高编码的安全性。

尤其是，如果第一或第二哈希方法是哈希方法 MD 5、SHA－1、RIPE－MD 160、MDC－2 之一，那么这是有利的。

根据本发明的防伪的产品件包括被安置在该产品件上或旁边的产品检验序列，该产品检验序列包括已编码的测试序列（C）或由此得出的序列以及产品特有的标识序列。通过借助于加密方法（F1）在应用秘密的加密序列（B）的情况下来加密产品特有的标识序列（K）或由此得出的序列，针对该产品件单独产生已编码的测试序列（C），其中秘密的加密序列（B）是对称的加密方法的秘密密钥。取代通过应用尽可能昂贵地和很难制造的安全特征，在根据本发明的产品件中借助于加密方法（F）在应用秘密的加密序列（B）的情况下来保证防伪。在待保障的产品件上制成和涂上产品检验序列只少量地引起花费和成本。

按照本发明的有利的实施方案，产品检验序列作为字母数字字符串被安置在该产品件上。例如，已编码的测试序列以及产品检验序列可作为位串来产生，其中该产品检验序列接着或者作为具有数字 0 至 9 的数字序列、或者作为 ASCII 字符的序列、或者作为任意其他的字母数字字符串来描述并被安置在产品件上。

此外，如果该产品检验序列以机器可读的形式被安置被在产品件上，那么这是有利的。例如，该产品检验序列可作为条形码（Barcode）或作为机器可读的字体被安置在产品件上。该产品检验序列也可被存储在与该产品、该产品包装或附属单据连接的磁条、存储器芯片或其他电子介质上。由于在本发明的这种实施方案中取消了键入，所以也可以处理更长的产品检验序列。

此外，如果产品检验序列以在视觉上可读的字体被安置被在该产品件上，那么这是有利的。在本发明的这种实施方案中，可通过经由键盘键入产品检验序列来检查该产品检验序列。

按照本发明的另一有利的实施方案，该产品检验序列被安置附随产品件的文档上或包装上。以这样的方式，长的产品检验序列可被附入产品，而不损害产品件。

在用于检查产品件的真实性的根据本发明的方法中，产品件的真

实性借助于被安置在该产品件上或旁边的产品检验序列通过因特网来检查。在此，在检验询问者侧检测该产品检验序列，并通过因特网将其传送到产品保护服务器结构。在产品保护服务器结构侧，从产品检验序列中得出的已编码的检验序列（C）借助于解密方法（F2）在应用解密序列（A）的情况下来解密，并产生被解密的测试序列，其中该解密序列（A）与在加密时所应用的加密序列（B）一起构成互补的密匙对，并且其中解密序列（A）是对称的加密方法的秘密密钥。该被解密的测试序列或由此得出的序列的真实性被检查，并且真实性测试的结果通过因特网被传送到检验询问者。

想要检查产品件的真实性的商人例如可以借助于其因特网浏览器将相应的产品检验序列传送到产品保护服务器结构。然后，在那里执行已编码的测试序列（C）的解密以及真实性测试。这具有以下优点，即在商人处本地不必有用于检查产品真实性的装置。传感器和测量设备（如其在现有技术的方法中被设置，用于检查物理的和化学的安全特征）在根据本发明的方法中是不必要的。因而，用于实施根据本发明的产品保护系统总共所必要的投资是最小的。由于解密不是在本地被执行、而是在产品保护服务器结构侧集中地执行，所以可选择地将秘密密钥或公匙用作解密序列（A）。

按照本发明，该解密序列（A）是对称的加密方法的秘密密匙。应用对称的加密方法具有的优点是，不仅密匙长度而且块长度是相对短的。由于对于所有检验询问集中地通过产品保护服务器结构来执行解密，所以解密序列（A）的保密可通过适当的措施来保证，例如可以通过应用防火墙、独立的密码服务器（Krypto-Server）等来保证。应用对称的方法的另一优点是，每次解密所必需的时间消耗非常小。

此外，如果该已编码的测试序列（C）作为序列段被包括在产品检验序列中或可以通过应用哈希反函数（h_2^{-1}）从产品检验序列的序列段中得出，那么这是有利的。如果，在产生产品检验序列时，已编码的测试序列（C）附加地借助于第二哈希方法（h_2）被转换成第二哈希序列（h_2（C）），那么，在产品保护服务器结构侧，哈希反函数（h_2^{-1}）必须首先被用于产品检验序列的有关的序列段，以便得到已编码的测试序列（C）。该已编码的测试序列（C）接着被解密。

此外，如果被解密的测试序列可代表产品特有的标识序列（K），

或可以通过应用哈希反函数（h_1^{-1}）被转换成产品特有的标识序列（K），那么这是有利的。如果，在产生产品检验序列时，该产品特有的标识序列（K）在加密前借助于第一哈希方法（h_1）被转换成第一哈希序列（h_1（K）），那么，在产品保护服务器结构侧，哈希反函数（h_1^{-1}）在执行解密之后被用于被解密的测试序列，以便得到产品特有的标识序列（K）。

按照本发明的另一有利的实施方案，通过将被解密的测试序列或由此得出的序列与作为序列段被包括在产品检验序列中的产品特有的标识序列（K）或由此得出的哈希序列（h_1（K））进行比较，来检查被解密的测试序列或由此得出的序列的真实性。在本发明的这个实施方案中，该产品检验序列包括所有对于确定其真实性所必需的信息。因而，该产品检验序列的真实性可以单独地根据产品检验序列自身来判定，而为此不需要额外的信息。

对此可替换地，如果通过检查被解密的测试序列或由此得出的序列是否属于事先所确定的定额（Kontingente），来检查被解密的测试序列或由此得出的序列的真实性，那么这是有利的。在本发明的这个实施方案中，事先将序列的定额分配给生产商。为了检查被解密的测试序列或由此得出的序列的真实性，确定这些序列是否在生产商之一的定额内。这具有以下优点，即在本发明的实施方案中未被加密的信息不必被包括在产品检验序列中。该产品检验序列必须仅包括被加密的信息。因此，在本发明的该实施方案中，相对短的产品检验序列就足够了。

如果在检查产品检验序列的范围中测试检验询问者的合法性，那么这是有利的。只有被授权的商人应该进行产品检验序列的询问。此外，可通过询问该检验询问者的合法性来理解所检查的产品件的来路。

按照本发明的另一有利的实施方案，在针对产品检验序列的检验询问的范围中，数据库记录项被存放在记录数据库中。由此，可建立记录数据库，该记录数据库包括所有迄今所检查的产品检验序列的数据库记录项。假设伪造者设法得到一系列真品的产品检验序列，并且将这些产品检验序列安置在其伪造的商品上。在这种情况下，加密方法将提供以下结果，即相应的产品检验序列是真的。但是，现在市场

上存在多种具有相同的产品检验序列的产品件。产品检验序列的这样的多次使用可借助于记录数据库来揭露。

如果为了确定先前对产品件的产品检验序列的检验询问而在记录数据库中执行数据库询问，那么这是有利的。假设，第一商人针对其手头的第一产品件执行检验询问，并且检查被安置在该产品件上的产品检验序列。该加密方法提供以下结果，即该产品检验序列是真的，此外这些产品检验序列的数据记录项被存放在记录数据库中。如果现在第二商人在稍后的时刻针对第二产品件执行检验询问，该第二产品件配备有相同的产品检验序列，那么可以借助于该记录数据库来确定，对这些产品检验序列先前已经由另一个商人进行了检验询问。那么，存在以下两种可能性：或者第一商人的商品是真品，而第二商人的商品是产品伪造，或者第一商人的商品是伪造品，而第二商人的商品是真品。如果多次使用被确定，那么因而进行询问的商人手头的商品或者是伪造的或者用作伪造品的样本。

总之，通过将加密方法与记录由不同的商人执行的询问进行组合来实现极为有效的保护。

如果将产品检验序列、产品特有的标识序列（K）、已编码的测试序列（C）、被解密的测试序列或由此得出的序列中的至少一个与记录数据库中的数据库记录项进行比较，那么这是有利的，其中如果发现至少一个相互一致，那么该产品件被识别为伪造品或伪造品的样本。某一产品件可利用所述的序列中的每个序列来识别，因为每个这样的序列对于各个产品件都是特有的。如果关于分别应用的序列确定多次使用，那么或者存在伪造，或者存在已用作伪造品的样本的真品。

如果检验询问的数据库记录项包括检验询问的日期，那么这是有利的。此外，如果数据库记录项包括检验询问者的身份，那么这是有利的。如果产品特有的序列的多次使用被确定，那么可借助于所参与的商人和该商人在其执行检验询问的时刻的这种信息追溯伪造产品的来路。

根据本发明的产品保护服务器结构能够实施产品保护入口，用于根据被安置在该产品件上或旁边的产品检验序列来检查该产品件的真实性。该产品保护服务器结构包括网页服务器模块，该网页服务器

模块通过因特网可提供产品保护入口的网页。在检验询问者侧检测的、用于测试生产商的产品检验序列的真实性的产品保护入口和方法通过因特网被传送到网页服务器模块，并且真实性测试的结果通过因特网被传送到检验询问者。此外，该产品保护服务器结构包括加密模块，该加密模块借助于解密方法（F2）在应用解密序列（A）的情况下解密从产品检验序列中得出的已编码的测试序列（C），并产生被解密的测试序列。在此，解密序列（A）与加密时所应用的加密序列（B）一起构成互补的密匙对。被解密的测试序列或由此得出的序列的真实性由加密模块来检查，其中加密模块借助于对称的解密方法在应用秘密的解密序列的情况下来解密该已编码的测试序列（C）。

如果产品保护服务器结构包括记录数据库，那么这是有利的，所述记录数据库至少针对每个其真实性已被确定的产品检验序列包括一个数据库记录项。借助于这样的记录数据库可以证明产品检验序列的多次应用，所述多次应用是存在产品伪造的证据。

用于产生产品保护标志的方法可借助于计算机程序产品来实施，这些计算机程序产品具有用于在计算机、数字信号处理器等上实施相应的方法步骤的装置。用于检查产品件的真实性的方法也可借助于计算机程序产品来实施，该计算机程序产品具有用于在计算机、数字信号处理器等上实施相应的方法步骤的装置。

接下来，借助于多个在附图中示出的实施例继续说明本发明。其中：

图 1 示出根据本发明的产品保护系统的图示；

图 2 示出加密和解密产品特有的标识序列 K 的示意图；

图 3 示出加密和解密产品特有的标识序列 K 的图示，其中第一哈希函数 h_1 被用于加密前的标识序列 K；

图 4 示出加密和解密产品特有的标识序列 K 的图示，其中，在加密后将第二哈希函数 h_2 用于已编码的测试序列；以及

图 5 示出通过因特网可进入的产品保护入口的实施方案。

图 1 示出关于根据本发明的产品保护系统的概况。产品的生产商 1、商人 2 以及产品保护入口 3 的提供商参与该产品保护系统。从生产商 1 方面，兴趣在于，使其用户能够检验产品真实性，以便如此保护自己不受产品伪造的损害。为了这个目的，该生产商 1 将单独的标

识序列分配给每个由其所制造的产品。每个任意的位串、数字序列或字母数字字符串可被用作标识序列。正好将各个产品的序列号用作产品特有的标识序列，所述序列号可作为生产数据 5 的部分来支配。

其次，必须在生产商的计算机结构 6 侧根据产品特有的标识序列 4 借助于秘密的加密方法来产生已编码的测试序列 7。这个已编码的测试序列 7 又可被表示为位串、测试号或者字母数字字符串。为了加密该标识序列 4，可应用所有加密方法，其中秘密的加密序列被用于进行加密。否则，偶尔发现加密序列的伪造者可能自己产生任意的产品检验序列。根据本发明，也被称为单密钥系统或秘密密钥系统的对称的加密方法可被用作加密方法。在这些方法中，秘密密匙不仅被用于进行加密也被用于进行解密。即使该加密和解密方法通常是公知的，但是利用秘密密匙来加密的序列只可借助于该秘密密匙再次被解密。

替换于对称的加密方法，不对称的加密方法也可被用于加密产品特有的标识序列。该不对称的加密方法也被称为双密匙方法或公匙方法。这样的方法以密匙对来工作，该密匙对分别包括秘密密匙以及所属的公匙。在符合今天的安全标准的公匙系统中，从公匙中以今天可支配的计算能力不能计算出私匙。因此，允许自由开放公匙。当所保密的私匙唯一地为其所有者知道并只由其所有者使用时，使用者的公匙对于所有的通信用户可自由开放。

在采用不对称的加密方法时，生产商 1 的私匙被用于加密产品特有的标识序列 4。这个密匙只可在生产商 1 的计算机系统 6 上支配，并且不允许被公开。

密钥对的所属的公共密匙被用于解密这样编码的测试序列 7，该公匙在没有特别的安全预防的情况下可被传送给所有商人和用户。尤其是，这个公匙也可通过因特网来开放。

对于每个产品件，现在不仅存在产品特有的标识序列 4，而且存在已编码的测试序列 7。为了保证产品真实性，两个序列共同作为产品检验序列 8 被安置在该产品上。产品检验序列 8 可作为位串、作为数字序列或者作为字母数字字符串被安置在产品件上或旁边。产品检验序列可例如是数字序列，该数字序列具有未被加密的序列号作为第一部分和已编码的测试号作为第二部分。但是，产品检验序列 8 不仅

包括标识序列 4 而且包括已编码的测试序列 7 不是绝对必要的。该产品检验序列 8 也可唯一地由已编码的测试序列 7 组成，其中，在这种情况下，该产品特有的标识序列 4 只有在解密产品检验序列 8 时才被得到。

例如通过印刷、压印、冲压、通过印刷包装等可以以任意的形式将产品检验序列 8 安置在产品上或旁边。产品检验序列 8 也可被印刷在包装说明书上，该包装说明书被放在产品的包装中。该产品检验序列 8 可以在视觉上可读的形式或者以机器可读的形式被安置在该产品上。在机器可读的编码中，例如可以考虑到条形码，但是磁条或者其他可磁化的介质也可用于存储产品检验序列 8。

具有被安置在其旁边或其上的产品检验序列 8 的产品以最不同的分配方式到达想要检查所得到的产品的真实性的商人 2。该商人 2 将保证，他已获得生产商 1 的真品，而没有获得由伪造者所制造的产品复制品。如果商人 2 销售伪造的产品复制品，那么他将冒在伪造品被人知道时不能继续销售的风险。所仿造的产品经常在质量上比真品差，并且就这方面而言，也将损害商人 2 的声誉。

为了检查其手头的产品 9 的真实性，商人 2 通过因特网 10 访问产品保护入口 3 的服务器结构 11。首先，商人 2 利用其标志 12 在产品保护入口处注册。为了确认用户访问合法，通常应用登陆 ID 以及密码。在商人 2 已成功验证自己身份之后，该商人 2 可以访问产品保护入口的网页，该网页从服务器结构 11 通过因特网 10 被传送到其浏览器，并且在那里被显示。在其中一个页面上，该商人可在为此所规定的输入窗口中输入其手头的商品的产品检验序列 8，由此该产品检验序列 8 通过因特网 10 被传输到服务器结构 11。

在服务器结构 11 侧，所接收到的产品检验序列 8 借助第一测试 13 和第二测试 14 来检查。该产品检验序列 8 包括已编码的测试序列 7，并且该已编码的测试序列在第一测试 13 中借助于解密方法在应用解密序列的情况下来解密。在此产生被解密的测试序列。该解密方法与在生产商 1 侧所应用的加密方法互补。

在采用对称的方法时，解密时所应用的解密序列必须与生产商 1 侧所应用的加密序列相一致。在对称的方法中，必需不仅保密加密序列而且保密解密序列。由于集中地在服务器结构 11 中执行解密，所

以可保证解密序列的保密。

如果应用不对称的方法，其中在生产商 1 侧借助于秘密的加密序列产生已编码的测试序列，那么已编码的测试序列可利用公开的解密序列、即所谓的“公匙”来解密。因此，在应用不对称的方法时，在接收机侧不必保密解密序列。这可能对项目的其他扩建阶段（Ausbaustufe）变得重要，其中产品检验不再借助于中央服务器结构、而是借助于多个分散的测试设备来执行。该解密序列接着可以作为公匙被存放在所有的测试设备上。

如果该产品检验序列不仅包括（未被加密的）标识序列而且包括已编码的测试序列作为组成部分，那么其次将被解密的测试序列与未被加密的标识序列进行比较。如果被解密的测试序列与该产品特有的标识序列相一致，该产品特有的标识序列被用作针对计算该已编码的测试序列的输出点，那么所测试的产品检验序列本身一致。然后，第一测试 13 提供以下结果，即由商人 2 所测试的产品件的产品检验序列是可信的。如果所解密的测试序列与产品特有的标识序列不一致，那么该产品检验序列是有错误的。

如果能够排除其他错误源，那么因而涉及产品伪造。这个测试结果从服务器结构 11 通过因特网 10 被传输到商人 2 的网页浏览器，并在那里被显示。

在本发明的可替换的实施方案中，该产品检验序列只由已编码的测试序列组成，而产品特有的标识序列不是该产品检验序列的组成部分。即使在这种情况下，该已编码的测试序列也首先借助于解密方法来解码，以便产生被解密的测试序列。如果在服务器结构 11 侧已知被分配给单个生产商的测试序列定额，那么可以检查这样得到的被解密的测试序列。测试在其中一个定额中是否包括该被解密的测试序列。就这方面而言，产品检验序列不必包括标识号码作为组成部分。

但是可考虑产品伪造，在该产品伪造中伪造者设法得到真品的一个或多个产品检验序列，并把这些产品检验序列安置在所伪造的产品件上。于是，所伪造的产品具有无缺陷的产品检验序列，并因此可能由第一测试 13 不被识别为伪造品。为了发现这样的产品伪造，设置第二测试 14，在所述第二测试 14 中将当前所询问的产品检验序列与所有以前所询问的产品检验序列进行比较。如果产品检验序列被复制

并被涂在所伪造的产品上，那么随着时间的推移不仅针对真品而且针对伪造品可以由分别所参与的商人执行检验询问。由此，随着时间的推移可能出现关于同一个产品检验序列的多次询问。

这样的多次询问在第二测试 14 中借助于记录数据库 15 来识别。在该记录数据库 15 中，针对每个由服务器结构 11 所处理的检验询问来存放相应的数据库记录项。为了识别检验询问，数据库记录项包括以下序列中的至少一个：产品检验序列、产品特有的标识序列、已编码的测试序列或被解密的测试序列。此外，该数据库记录项还包括已经执行检验询问的商人的 ID、以及日期并也可能包括检验询问的时间。由于装设了世界范围内使用的系统，所以在记录日期和时间时必须考虑执行询问的商人的各自的时区。该日期和时间格式必须实现各种询问的日期和时间的国际可比较性。

在第二测试 14 中，在每次商人询问时，按照对由商人所输入的产品检验序列的记录项来搜寻记录数据库 15。如果由商人所传送的产品检验序列早前已经被询问过一次，那么存在两种可能性：产品件可能是伪造品，但是也可能是真品，这些真品的产品检验序列已被用作制造所伪造的产品的样本。按照被包括在这个记录项中的、参与测试的商人的 ID 以及日期说明和时间说明，现在可以开始用于检查该商品的其他步骤。

如果产品检验序列已经通过第一测试 13，并在第二测试 14 中没有确定产品检验序列的多次使用，那么商人 2 通过因特网 10 由服务器结构 11 得到以下消息，即产品件很可能不是伪造品。可是，对此还不存在绝对的安全性，因为可能想像，伪造者已经应用了迄今还没有被测试的真品的产品检验序列。在这种情况下，只有当询问真品的产品检验序列时，该系统才会发现伪造品。

在图 2 中示意性地描述了产品特有的标识序列 K 的加密和解密。在生产商侧，产品特有的标识序列 K 借助于加密方法 F1 在应用密匙 B 的情况下来加密，其中得到已编码的测试序列 C。

在解密时，已编码的测试序列 C 借助于解密方法 F2 在应用密匙 A 的情况下来解密，其中再度得到产品特有的标识序列 K。如果，除了已编码的测试序列 C 之外，产品特有的标识序列 K 作为组成部分也被包括在产品检验序列中，那么可以将通过解密得到的标识序列与作为

产品检验序列的部分所传送的标识序列进行比较。在相互一致的情况下，涉及有效的产品检验序列，而在不一致的情况下可能存在伪造的产品检验序列。

为了进行加密和解密，可以采用所谓的对称的方法，该对称的方法也被称为单密匙系统或秘密密钥系统。在这个方法中，用于保障的加密方法 F1 或相应的秘密密匙 B 与在检验时所应用的解密方法 F2 或相应的秘密密钥 A 一致。因此，在这样的单密匙方法中，不仅必须保密由生产商用于保障的密匙 B 而且必须保密在产品保护入口侧所应用的密匙 A。

在进行加密时，仅仅在制造商侧应用秘密密匙 B，并在那里采取用于保密密匙的必要措施。例如可以在没有被连接到因特网的计算机上执行产品检验序列的产生。为了进行解密，仅仅集中地在产品保护入口的服务器结构侧必需秘密密匙 A。在服务器结构侧也可以采取用于保密在那里所采用的密匙 A 所必需的措施。如果不仅密匙 B 而且密匙 A 必须被保密，那么就这方面而言，没有困难的限制。通常可以非常快速和以少量花费不仅以硬件而且以软件来实现对称的加密方法。另一优点是，借助于对称的加密方法所产生的已编码的测试序列通常是相对短的，并且因此该产品检验序列也只由字母数字字符的相对短的序列来组成。

在对称的加密方法中，秘密密匙 B 不能从成对的未被加密的和被加密的信息的各种抽样检验中得出。对称的加密方法的另一实质特征是，被加密的信息（C）在没有秘密密匙 B 的情况下不能从未被加密的信息（K）中产生。存在一系列对称的加密方法，这些加密方法适合于用在根据本发明的产品保护方法中。一个例子是方法三重 DES，其中根据方法 DES 三次连续应用加密，其中应用两个或三个不同的密钥。在将 56 位长的密匙用于 8 字节长的密码文本块的情况下，DES 规定 8 字节长的明码文本块的加密。另一对称的加密方法是方法 IDEA，该方法以模数算法（Modulo-Arithmetik）为基础并可容易地以硬件和软件来实施。对此可替换地，也可采用对称的加密方法 CAST－128、RC5 或 f8。由 ETSI 负责地在第三代合作伙伴项目（3GPP，3rd Generation Partnership Project）的范围中来研发该方法 f8。方法 f8 是流密码（Stromchiffre），其中待加密的数据块可以具有 1

至 20000 位的长度。该待加密的数据块基于 KASUMI 块密码（块长度为 64 位）。KASUMI 又是由三菱公司所研发的 MISTY 算法的派生。另一对称的加密方法是 Rijndal 算法，其将 S－Box 用作非线性部件，并且不仅可以软件而且可以硬件来实施。

为了避免生产商必须借助于同一个私匙 B 来执行所有的加密，在采用对称的加密方法时可附加地设置所谓的密匙管理。在此，例如可以按时间顺序如此应用各种秘密密匙，以致每个单个密匙的有效性在时间上受到限制。此外，存在用于密匙管理的壳模型（Schalenmodell），其中将内部壳和外部壳的不同的密匙部件共同用于进行加密。在此，例如可以针对内部壳或外部壳的密匙部件来确定不同的有效时期。

作为对称的加密的替换方案，不对称的加密方法也可被用于加密和解密产品特有的标识序列。在生产商侧，借助于加密方法 F1 在应用密钥 B 的情况下来加密标识序列 K。在这种情况下，必须应用秘密密匙 B，因为，如果将公钥用于进行加密，那么对于每个人可能的是，对标识序列 K 产生所属的已编码的测试序列 C。为了进行解密，借助于解密方法 F2 在应用密匙 A 的情况下来解密已编码的测试序列 C。在应用也被称为双密匙或公匙系统的不对称的方法时，公匙可被用于进行解密，该公匙可使得每个人自由进入。在公匙方法中，秘密密匙 B 和公匙 A 形成互补的密匙对。在不对称的方法中，加密时所应用的秘密密匙 B 既不能根据检验时所应用的解密方法 F2、也不能根据解密时所应用的公匙 A 来确定，至少以如今可支配的计算机容量不能确定。秘密密匙 B 也不能从成对的未被加密和被加密的信息的各种抽样检验中得到。因此，该秘密密匙 B 只可供生产商使用，并且不能从公众可进入的信息中得到。不对称的加密方法的另一重要特征是，被加密的信息（C）在没有秘密密匙（B）的情况下不可从未被加密的信息（K）中得出。

作为不对称的加密方法，例如可采用方法 RSA。在 RSA 中，安全性以大数值的因数分解为基础，其中公钥和私匙取决于一对大质数（p，q）。同样，不对称的加密方法 ELGamal 也是适合的，在该方法中安全性以计算有限域上的离散对数这一难题为基础。可替换地，也可采用 DSA，该 DSA 同样以离散对数问题为基础。该不对称的加密方

法 DSA 应用多个参数，其中有其位长度近义地被称为密匙长度的质数 p、160 位长的质数 p－1 以及哈希函数 SHA。作为不对称的方法，也可采用方法 ECC（椭圆曲线加密算法（Elliptic Curve Cryptography）），其同样以计算离散对数的问题为基础。

为了提高加密的安全性，并且为了缩短长的测试序列，除了原来的加密方法以外可采用所谓的哈希方法。在图 3 中示出，如何在实际加密之前将哈希方法 h_1 用于产品特有的标识序列 K，其中产生杂乱（gehasht）的标识序列 h_1（K）。然后，这个杂乱的标识序列 h_1（K）借助于加密方法 F1 在应用密匙 B 的情况下来加密，以便这样得到已编码的测试序列 C。

在图 3 的右侧，描述了用于解密已编码的测试序列 C 的两种不同的可能性。在用（i）标明的变型中，首先，已编码的测试序列 C 借助于解密方法 F2 在应用密匙 A 的情况下来解密，其中得到杂乱的标识序列 h_1（K）。在第二步中，将哈希函数 h_1 的反函数 h_1^{-1} 用于这个杂乱的标识序列 h_1（K），以便这样得到产品特有的标识序列 K。因此，可以将这些通过解密所得到的标识序列与作为产品检验序列的部分来传送的标识序列进行比较。

在用（ii）标明的解密方法的变型中，首先，已编码的测试序列 C 同样也借助于解密函数 F2 在应用密匙 A 的情况下来解密，其中得到杂乱的标识序列 h_1（K）。此外，哈希函数 h_1 被用于作为产品检验序列的部分来传送的标识序列 K，并且在此同样也产生杂乱的标识序列 h_1（K）。可以通过比较通过解密 C 所得到的杂乱的标识序列和通过将 h_1 用于 K 所得到的杂乱的标识序列，来检查产品检验序列的真实性。借助在进行加密前所应用的哈希方法可以提高加密的安全性。

但是，可替换地或附加地，也可能首先执行加密，接着将哈希函数用于所加密的序列。这在图 4 中示出。首先，标识序列 K 借助于加密方法 F1 在应用密匙 B 的情况下来加密，其中得到已编码的测试序列 C。紧接着，将哈希函数 h_2 用于已编码的测试序列 C，以便这样得到杂乱的序列 h_2（C）。为了解密这个序列，首先，必须将哈希函数 h_2 的反函数 h_2^{-1} 用于杂乱的序列 h_2（C），以便得到已编码的测试序列 C。然后，可以借助于解密方法 F2 在应用密匙 A 的情况下将已编码的测试序列 C 转换成标识序列 K。在加密之后所应用的哈希方法尤

其适合于缩短长的测试序列。由此，包括已编码的测试序列的产品检验序列也被相应地缩短。

在图 3 中所示的、在进行加密之前所应用的哈希方法 h_1 也可以结合进行加密之后所应用的哈希方法 h_2 来应用。在解密时，在这种情况下，首先必须应用反函数 h_2^{-1}，接着解密所得到的序列，并最终必须应用反函数 h_1^{-1}。

例如，哈希函数 MD 5、SHA－1、RIPE－MD 160 可被用作哈希函数 h_1、h_2，这些方法分别提供 160 位长的哈希值。可替换于此地，可采用哈希函数 MDC－2，在该函数中哈希值的长度对应于双倍的块长度。

在图 5 中示出，可如何实施通过因特网可进入的产品保护入口。为了询问产品检验序列，商人借助于其网页浏览器 16 与产品保护入口的网页服务器 18 建立因特网连接 17。优选地建立所保障的因特网连接、例如借助于协议 SSL（安全套接字层（Secure Socket Layer））所保障的因特网连接，通过这个因特网连接该商人可以访问产品保护入口的网页。该网页服务器 18 如此被设计，以致多个商人可以同时访问。当存在到第一商人的因特网连接 17 时，第二商人可通过其网页浏览器 19 建立到网页服务器 18 的因特网连接 20。该网页服务器 18 负责整理和传送产品保护入口的网页，其中该网页例如可根据标准 HTML（超文本标记语言（Hyper Text Mark-up Language））来设计。该网页服务器 18 通过接口 21 与应用服务器 22 进行通信，在该应用服务器 22 上实施用于处理商人询问的应用。该网页服务器 18 和该应用服务器 22 是两个独立的计算机，其中这两个计算机之间的通信通过诸如 SSL 的内部协议来进行。但是，该网页服务器 18 和应用服务器 22 也可以是软件模块，该软件模块可被安装在同一个服务器计算机上。在这种情况下，两个模块之间的接口 21 可作为公共的过程接口来实现。

如果商人在相应的因特网网页输入了其 ID 和其密码，那么这些数据从网页服务器 18 通过接口 22 被转交到应用服务器 22，并在那里由负责合法性测试的过程 23 来处理。由商人所输入的产品检验序列同样也通过接口 21 到达应用服务器 22，在该应用服务器 22 上实施负责产品检验序列的测试的过程 24。该过程 24 将产品检验序列 25

传送给密码服务器 26。该密码服务器 26 是独立的计算机，该计算机可借助于防火墙与应用服务器 22 分隔开。但是，该密码服务器 26 也可作为加密模块（Kryptographiemodul）被安装在服务器计算机上，在该服务器计算机上也安装有其他的软件模块。该密码服务器 26 执行被包括在产品检验序列 25 中的已编码的测试序列的解密。在密码服务器 26 已执行了在图 2 至 4 中所示出的解密之后，该密码服务器 26 将被解密的测试序列与未被加密的标识序列 K 进行比较，该未被加密的标识序列 K 可被包括在产品检验序列 25 中。在本发明的可替换的实施方案中，密码服务器 26 将被解密的测试序列与被分配给各个商人的定额进行比较。如果确定一致，那么涉及可信的产品检验序列。

真实性测试的结果 27 被传输回过程 24。此外，针对每个由商人所输入的产品检验序列，在第二测试中检查，这些产品检验序列是否已经在早些时刻被询问了。为了执行这些测试，在应用服务器 22 上实施用于数据库询问的过程 28。该过程 28 将询问 29 传送给记录数据库 30。该记录数据库包括迄今所执行的询问的数据组，并且优选地被实施为相关的数据库，该相关的数据库可借助于询问语言 SQL（结构询问语言（Structured Query Language））来询问。该询问 29 或者包括产品检验序列、标识序列、已编码的测试序列、被解密的测试序列，或者多个这样的序列。在该记录数据库 30 中测试，是否存在对这些序列早些时候的询问。该结果 31 由记录数据库 30 传送到过程 28。如果已进行了多次询问，那么存在产品伪造的嫌疑。如果相反在记录数据库 30 中没有发现早些时候对这个产品检验序列的询问，并且所询问的产品检验序列由密码服务器 26 识别为真，那么很大可能涉及真品。

在每次询问有效的产品检验序列时，新的数据库记录项被存放在该记录数据库 30 中，该新的数据库记录项或者包括产品检验序列，或者包括标识序列，或者包括已编码的测试序列，或者包括被解密的测试序列（或多个这样的序列）。该数据库记录项附加地也可能包括进行询问的商人的 ID 以及可能包括该询问的时刻和日期。如果将来关于所询问的产品检验序列应该进行其他的询问，那么这样的多次询问可以借助于这个数据库记录项来识别。

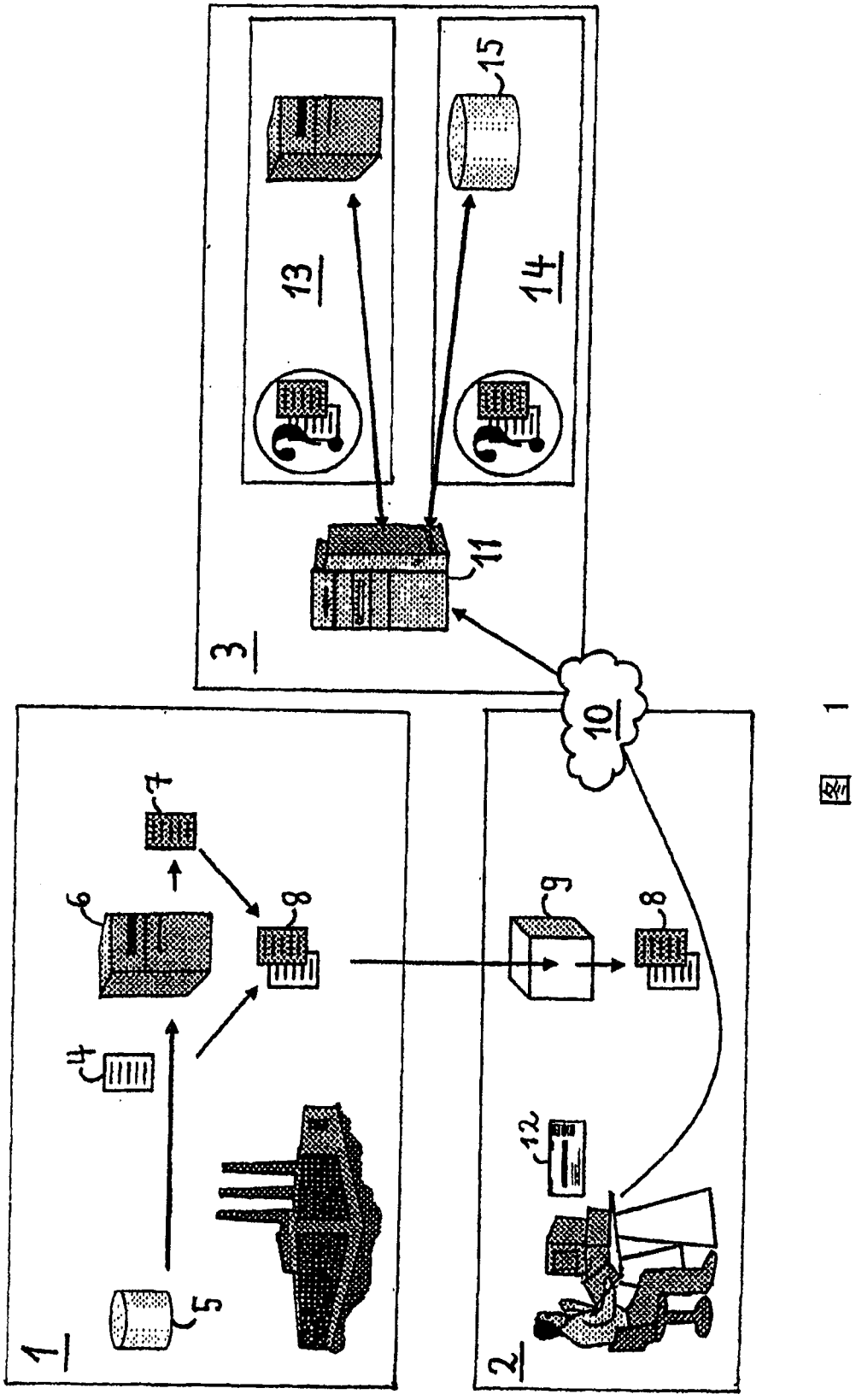


图 1

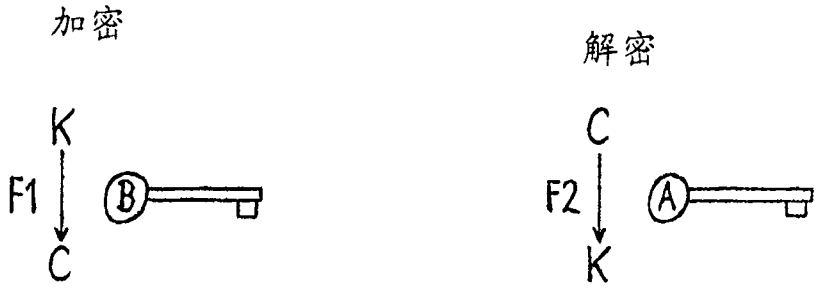

加密
K
F1
B
C
解密
C
F2
A
K

图 2

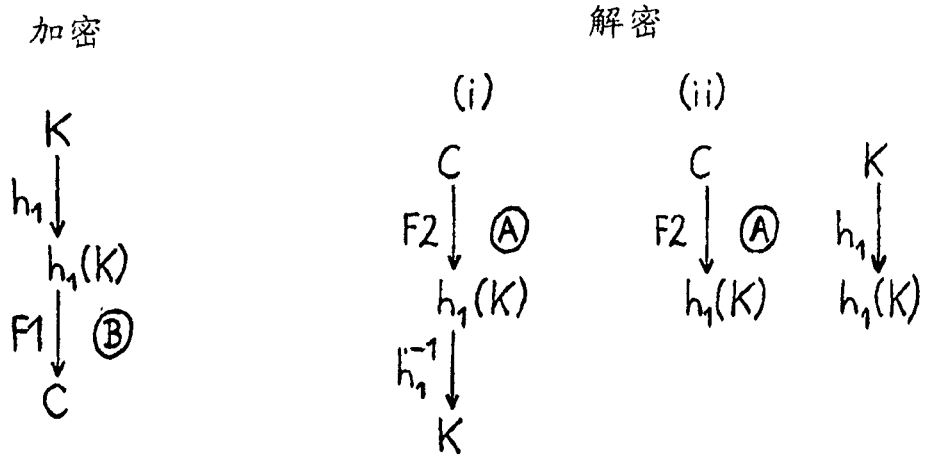

加密
K
h1
h1(K)
F1
B
C
解密
(i)
C
F2
A
h1(K)
h1-1
K
(ii)
C
F2
A
h1(K)
K
h1
h1(K)

图 3

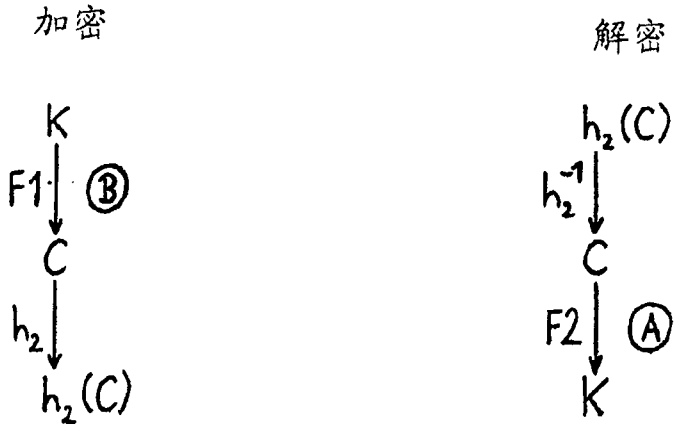

加密
K
F1
B
C
h2
h2(C)
解密
h2(C)
h2-1
C
F2
A
K

图 4

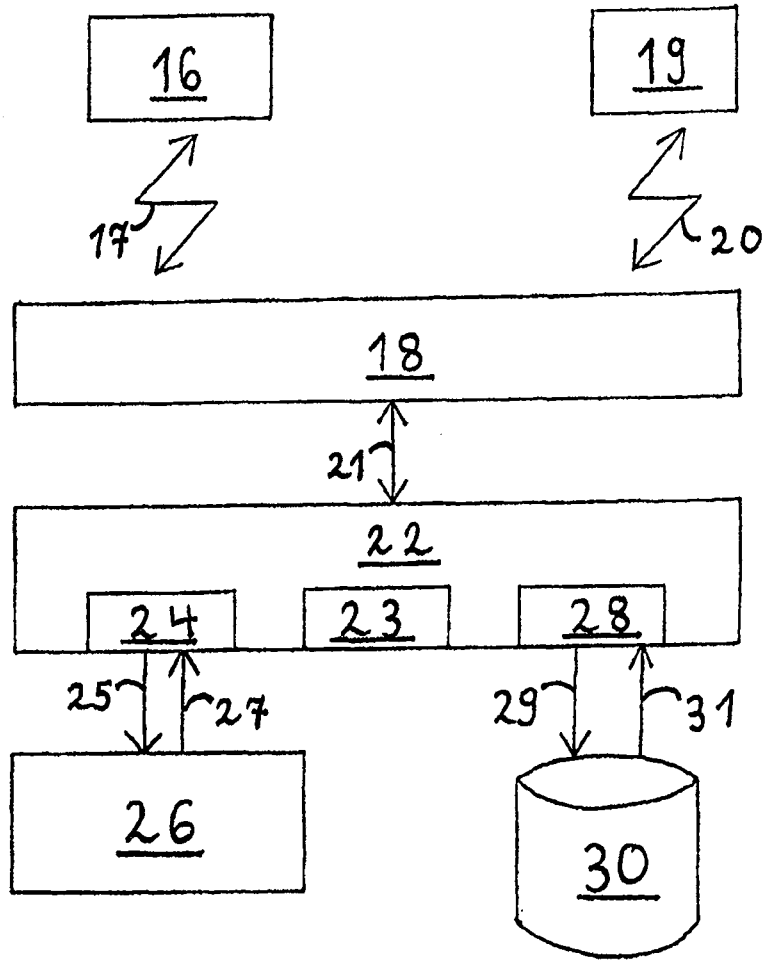


图 5