[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/08 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200780012945.3

[43] 公开日 2009 年 4 月 29 日

[11] 公开号 CN 101421971A

[22] 申请日 2007.4.5
[21] 申请号 200780012945.3
[30] 优先权
[32] 2006. 4.11 [33] EP [31] 06112483.0
[86] 国际申请 PCT/IB2007/051223 2007.4.5
[87] 国际公布 WO2007/116355 英 2007.10.18
[85] 进入国家阶段日期 2008.10.10
[71] 申请人 皇家飞利浦电子股份有限公司
地址 荷兰艾恩德霍芬
[72] 发明人 P·T·图伊尔斯
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 李亚非 谭祐祥

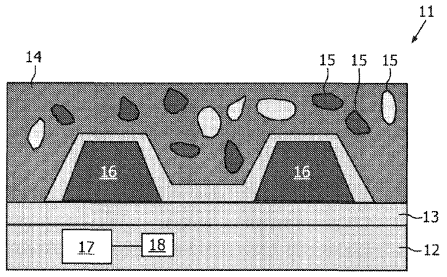
权利要求书 3 页 说明书 7 页 附图 1 页

[54] 发明名称

利用物理不可复制函数对令牌的询问响应认证

[57] 摘要

本发明涉及一种对提供可测量参数的物理令牌(14)进行认证的方法，以及一种包括提供用于认证的可测量参数的物理令牌(14)的设备(11)。 本发明的基本构思在于利用设备(11)中所包括的物理令牌(14)的特性来检测所述设备是否被篡改。 在登记阶段，测量由所述物理令牌所提供的多个物理参数的值。 这种测量值的集合被称为响应数据。 采用噪声纠正数据(也称之为帮助方数据)来以安全方式将噪声健壮性提供给所述响应数据。 于是，在认证阶段，再次测量参数值，并且采用噪所述声纠正数据来推导验证数据。 对所述验证数据与所述登记数据进行比较，并且确定所推导出的验证数据是否与所述登记数据对应。 如果对应，则认为所述物理令牌是经过认证的。



1.一种对提供可测量参数的物理令牌（14）进行认证的方法，所述方法包括以下步骤：

测量由所述物理令牌（14）提供的多个（N）所述参数的值（$R'_0, \ldots, R'_{N-1}$）；

以噪声纠正数据（$W_0, \ldots, W_{N-1}$）来处理所述测量值（$R'_0, \ldots, R'_{N-1}$），以推导验证数据（$S'_0, \ldots, S'_{N-1}$）；

对验证数据（$S'_0, \ldots, S'_{N-1}$）与登记数据（$S_0, \ldots, S_{N-1}$）进行比较，所述登记数据（$S_0, \ldots, S_{N-1}$）是根据所述噪声纠正数据以及在所述物理令牌的登记期间所测量的所述多个（N）参数的值（$R_0, \ldots, R_{N-1}$）推导出的；

确定所推导出的验证数据（$S'_0, \ldots, S'_{N-1}$）是否与所述登记数据（$S_0, \ldots, S_{N-1}$）对应，其中，如果所述验证数据与所述登记数据之间存在对应关系，则认为所述物理令牌是经过认证的。

2.如权利要求1所述的方法，其中，在物理令牌（14）的登记期间推导出所述噪声纠正数据（W）。

3.如权利要求1或2所述的方法，进一步包括以下步骤：

以密码方式保护所述验证数据（S'），其中，对所述以密码方式所保护的验证数据与以密码方式所保护的登记数据进行比较，并且如果所述受保护的验证数据与所述受保护的登记数据之间存在对应关系，则认为所述物理令牌是经过认证的。

4.如权利要求3所述的方法，其中，通过应用不可逆函数来保护所述数据。

5.如权利要求4所述的方法，其中所述不可逆函数是散列函数。

6.如权利要求4或5中的任意一项所述的方法，其中，所述以密码方式保护数据的步骤包括以下步骤：

将不可逆函数应用于所述验证数据（S'），其中，对所述不可逆函数的输出与应用于所述登记数据的所述不可逆函数的输出进行比较，并且如果所述不可逆函数的所述两个输出之间存在对应关系，则认为所述物理令牌是经过认证的。

7.如权利要求3或4中的任意一项所述的方法，其中，通过加密方

式来保护所述数据。

8.如前述权利要求中的任意一项所述的方法，进一步包括以下步骤：

在物理令牌（14）的登记期间选择所述噪声纠正数据（W），从而通过应用函数（F_G）使得$(W, S) = F_G(R)$，基于所述噪声纠正数据和所述多个（N）参数的测量值（R）来推导所述登记数据（S）。

9.如权利要求8所述的方法，进一步包括以下步骤：

将所述噪声纠正数据（W）和所述登记数据（S）存储在所述物理令牌（14）处。

10.一种设备（11），包括提供用于所述设备的认证的可测量参数的物理令牌（14），所述设备进一步包括：

用于测量由所述物理令牌（14）所提供的多个（N）所述参数的值（$R'_0, \ldots, R'_{N-1}$）的装置（16）；

用于进行以下操作的装置（17）：以噪声纠正数据（$W_0, \ldots, W_{N-1}$）来处理所述测量值（$R'_0, \ldots, R'_{N-1}$）以推导验证数据（$S'_0, \ldots, S'_{N-1}$）；对验证数据（$S'_0, \ldots, S'_{N-1}$）与登记数据（$S_0, \ldots, S_{N-1}$）进行比较，所述登记数据（$S_0, \ldots, S_{N-1}$）是根据所述噪声纠正数据以及在所述物理令牌的登记期间所测量的所述多个（N）参数的值（$R_0, \ldots, R_{N-1}$）推导出的；以及确定所推导出的验证数据（$S'_0, \ldots, S'_{N-1}$）是否与所述登记数据（$S_0, \ldots, S_{N-1}$）对应，其中，如果所述验证数据与所述登记数据之间存在对应关系，则认为所述物理令牌是经过认证的。

11.如权利要求10所述的设备（11），其中，所述用于处理的装置（17）被进一步布置为：将不可逆函数应用于所述验证数据（S'），其中，对所述不可逆函数的输出与应用于所述登记数据的所述不可逆函数的输出进行比较，并且如果所述不可逆函数的所述两个输出之间存在对应关系，则认为所述物理令牌（14）是经过认证的。

12.如权利要求7或8中的任意一项所述的设备（11），其中，所述用于处理的装置（17）被进一步布置为：在物理令牌（14）的登记期间选择所述噪声纠正数据（W），从而通过应用函数（F_G）使得$(W, S) = F_G(R)$，基于所述噪声纠正数据和所述多个（N）参数的测量值（R）来推导所述登记数据（S）。

13.如权利要求10-12中的任意一项所述的设备（11），进一步包

括:

用于存储所述噪声纠正数据(W)和所述登记数据(S)的装置(18)。

14.如权利要求 10-13 中的任意一项所述的设备(11),进一步包括:集成电路。

15.如权利要求 14 所述的设备(11),其中,所述物理令牌(14)包括:涂覆层,在所述涂覆层中,散布介电粒子(15),所述涂覆层覆盖所述集成电路。

16.一种计算机程序产品,其包括计算机可执行组件,当所述计算机可执行组件运行在所述设备所包括的处理单元(17)上时,用于使得设备(11)执行如权利要求 1-9 中的任意一项所述的步骤。

利用物理不可复制函数对令牌的询问响应认证

技术领域

本发明涉及一种对提供可测量参数的物理令牌进行认证的方法，以及一种包括提供用于认证的可测量参数的物理令牌的设备。

背景技术

物理不可复制函数（physical uncloneable function，PUF）是一种用于创建防篡改环境的结构，其中，多方可以建立共享的秘密和/或密码材料（例如加密密钥）。PUF 是一种物理令牌，对其提供输入——询问。当将询问提供给 PUF 时，其产生被称为响应的随机模拟输出。因为其复杂度及其所遵循的物理规律，令牌被认为是“不可复制的”，即，对于物理复制和/或计算式模型是不可行的。PUF 有时也被称为物理随机函数。如果 PUF 与控制函数（control fuction）组合，则实质上可以加强 PUF。在实践中，PUF 和与 PUF 不可分的算法被包括在防篡改芯片（所谓的受控 PUF（CPUF））内。以硬件、软件或它们的组合实现的算法对 PUF 的输入和输出进行管理。例如，禁止频繁询问 PUF，禁止特定类型的询问，隐藏 PUF 的物理输出，仅公开以受密码保护的数据等等。

可以将 PUF 用作密码密钥材料的生成器的原因在于，可以根据 PUF 的输出推导出比特串。这种 PUF 的示例是在随机位置包含光散射元件的 3D 光学介质。对于光学介质的输入（即询问）可以是例如照射 PUF 的激光光束的入射角，输出（即响应）是由光散射元件所创建的作为特定入射角结果的斑点图案。这种响应可以通过相机来检测，并且可以被量化为密码密钥。创建可以用作密码密钥材料的源的 PUF 的另一方式是：以介电粒子散布在其中的涂覆层来覆盖集成电路（IC）。这些粒子典型地具有不同的介电常数以及归因于制造工艺的或多或少的随机形状、尺寸和位置。传感器元件被布置在 IC 的顶部金属层，以在不同涂覆层位置对电容值进行本地化测量。在该示例中，涂覆层自身构成物理不可复制函数。作为介电粒子的随机特性的结果，所测量

的电容值促成了优秀的密钥材料。具有涂覆层形式的 PUF 的 IC 对电容进行测量，并且将电容值转换为比特串，根据所述比特串而推导密码密钥。

"Protecting Devices by Active Coating" by Dr. Reinhard Posch, Technische Universitat GRAZ, AUSTRIA, published in *Journal of Universal Computer Science, vol. 4, no. 7 (1998), 652-668, © Springer Pub. Co.,*公开了一种利用例如在智能卡中或在一些其它安全硬件设备的覆盖材料中所使用的涂覆材料的随机特性来检测设备的篡改的方法。在所公开的方法中，涂覆层被假设为具有电可测量特性（例如电阻或电容）的材料。因为材料的不可再现和随机特性，所以可以感测电可测量特性，并且可以根据所感测的值来创建密码密钥材料。篡改这种类型的涂覆层的操作导致密码密钥的改变，并且篡改操作因此毁坏所述密钥。

对集成电路（IC）的物理攻击在某种程度上引出了一个主要的安全性问题，所述程度日益增大，并且芯片制造商一般以保护性涂覆层来覆盖他们的 IC。攻击者不断开发技术来绕过芯片制造商的防范措施。这些技术范围从蚀刻到光和离子束攻击。因此，期望开发并改进用于阻止对芯片（例如 IC）的安全性攻击的方法。

发明内容

本发明的目的在于解决现有技术中的上述问题，并且提供一种用于检测设备的篡改的方式。

通过一种如权利要求 1 所述的对提供可测量参数的物理令牌进行认证的方法以及一种如权利要求 10 所述的包括提供用于认证的可测量参数的物理令牌的设备来达到该目的。

在本发明第一方面中，提供一种方法，包括以下步骤：测量由物理令牌所提供的多个所述参数的值；以噪声纠正数据处理测量值，以推导验证数据的集合。进一步地，所述方法包括以下步骤：对所述验证数据与登记数据进行比较，所述登记数据根据在物理令牌的登记期间所测量的所述多个参数的值而推导得出；确定所推导出的验证数据是否与所述登记数据对应，其中，如果所述验证数据与所述登记数据之间存在对应关系，则将所述物理令牌看作是认证的。

在本发明第二方面中，提供一种设备，该设备包括：用于测量由

物理令牌所提供的多个所述参数的值的装置；用于进行以下处理的装置：以噪声纠正数据处理测量值，以推导验证数据的集合；对所述验证数据与登记数据进行比较，所述登记数据根据所述噪声纠正数据和在物理令牌的登记期间所测量的所述多个参数的值而推导得出；确定所推导出的验证数据是否与所述登记数据对应，其中，如果所述验证数据与所述登记数据之间存在对应关系，则所述设备被认为是认证的。

本发明的基本构思在于利用设备中所包括的物理令牌的特性来检测所述设备是否被篡改。

在登记阶段，测量由所述物理令牌所提供的多个物理参数的值。例如，应该对其检测篡改的设备包括：具有传感器元件的集成电路（IC）、覆盖 IC 的涂覆层的形式的物理令牌。被布置在 IC 处的所述传感器元件被布置为：测量由所述涂覆层所提供的多个物理参数（例如在不同涂覆层位置处的电容）。因此，在涂覆层的 N 个不同位置处典型地测量电容值，这产生测量值 $R_0, R_1, \ldots, R_{N-1}$ 的集合 R。测量值的这个集合被称为响应数据。采用噪声纠正数据（也称之为帮助方数据）来以安全方式提供噪声健壮性。在登记期间所获得的响应不一定必须与在认证阶段期间所获得的（理论上相同的）响应相同。当测量物理特性（例如响应）时，总是有随机噪声出现在测量操作中，从而用于将所测量的模拟特性转换为数字数据的量化处理的结果（outcome）将对于相同物理特性的不同测量操作而不同。为了向噪声提供健壮性，在登记期间推导帮助方数据并且对其进行存储。所述帮助方数据将在认证期间被使用，以实现噪声健壮性。帮助方数据被看作是公共数据，并且仅公开可忽略的量的关于根据所述响应数据所推导出的秘密登记数据的信息。

在示例性帮助方数据方案中，经由以 $(W, S) = F_G(R)$ 的方式的某些适当函数 F_G，所述帮助方数据 W 和登记数据 S 是基于物理令牌的响应数据 R 的。函数 F_G 可以是随机化函数，其使得能够从响应数据的一个单个集合 R 生成很多对（W，S）帮助方数据 W 和登记数据 S。这允许所述登记数据 S（并且因此也允许帮助方数据 W）对于不同登记授权方（authorities）而不同。于是将所推导出的帮助方数据和登记数据存储在实现所述物理令牌的设备中。所述设备包括微处理器或具有计算能力的某些其它适当的设备，以及存储装置。优选地，但并非必须，

在存储所述登记数据之前，由所述微处理器以密码方式来保护所述登记数据。

于是，在认证阶段，测量电容值，其产生测量值 $R'_0, R'_1, \ldots, R'_{N-1}$ 的另一集合 R′。在登记阶段，选取帮助方数据，从而当将 delta-contracting 函数 G 应用于所述响应数据 $R=R_0, R_1, \ldots, R_{N-1}$ 和帮助方数据 $W=W_0, W_1, \ldots, W_{N-1}$ 时，结果等于登记数据 $S=S_0, S_1, \ldots, S_{N-1}$。delta-contracting 函数具有以下特性：其允许选取帮助方数据的适当的值，从而充分类似响应的数据的任意值产生相同输出值（即与登记数据相同的数据）。结果，如果 R′充分程度地相似于 R，则 G(R, W) = G(R′, W) = S。因此，在认证期间，噪声响应 R′连同帮助方数据 W 一起将产生验证数据 S′ = G(R′, W)，其与登记数据 S 相同。按以下方式来布置所述帮助方数据：不公开关于所述登记数据的信息。于在所述设备中以密码方式保护所述登记数据的情况下，所述设备的所述微处理器在认证阶段也以密码方式保护所述验证数据 S′。一旦在所述设备中已经以密码方式保护了所述登记数据和所述验证数据，那么就可以在所述设备外部安全地处理所得到的受保护数据。

在认证阶段，对所述验证数据 S′与所述登记数据 S 进行比较，并且确定所推导出的验证数据是否与所述登记数据对应。如果对应，则将所述物理令牌看作是认证的。

本发明有利地用于确定设备（例如集成电路）是否已经被攻击或者篡改。典型地，对所述设备的物理攻击毁坏保护性涂覆层。通过毁坏所述涂覆层（即所述设备的物理令牌），已经修改了所述涂覆层的特性，并且已经改动了在给定涂覆层位置处的涂覆层的响应。结果，在认证阶段所推导出的响应数据将不同于在所述登记数据中所推导出的所述响应数据，并且包括所述物理令牌的设备的认证操作将失败。

例如，当 IC 希望检查其是否受攻击时，其在 N 个涂覆层位置（其中，传感器被布置在各个位置以用于测量电容）执行电容值的测量，产生测量值 $R'_0, R'_1, \ldots, R'_{N-1}$。于是，在登记期间所创建的帮助方数据 $W_0, W_1, \ldots, W_{N-1}$ 用于推导验证数据 $S'_0, S'_1, \ldots, S'_{N-1}$。于是，IC 计算 $S'=S'_0 \| \ldots \| S'_{N-1}$，散列值 H（S′）（其中，‖表示数据的级联）——即登记数据——通过散列函数而以密码方式来保护。然而，应注意，可以对验证数据 S′的明文拷贝与所述登记数据 S 的明文拷贝进行比较，在

此情况下，无需采取密码保护方式。最终，IC 检查是否 H(S) = H (S′)。如果存在对应关系，则 IC 判断其尚未被攻击，而如果散列值彼此不对应，则一个或多个测量的电容值不同于在登记期间所测量的对应值。IC 于是得出结论：其已经被篡改，并且将适当地采取行动（例如进入休眠模式或简单地自我关闭）。已由给定传感器在认证期间所测量的并且关于由相同的给定传感器在登记期间所测量的值而不同的电容值极有可能暗示：IC 已经被篡改。因此，所述多个（N 个）测量电容值必须落入待认证 IC 的预定误差容限边界之内：推导 S 和 S′所采用的 delta-contracting 函数 G 越敏感，所述边界越窄。

在本发明实施例中，将不可逆函数的形式的密码函数（例如散列函数）应用于所述验证数据 S′。有利的是，应该采用登记阶段和认证阶段两者，而不公开根据在所述设备处测量的涂覆层电容值所推导出的秘密数据（即登记数据以及验证数据）。因此，在所述秘密数据待从所述设备导出的情况下，所述设备的微处理器通过使用散列函数来使得在所述登记阶段中的登记数据模糊化，产生散列值 H（S）。散列函数具有需要相对少量的处理功率的优点。在认证时，所述验证数据 S′被散列化，这产生 H（S′）。如果比较结果示出 H(S)=H(S')，则包括所述物理令牌的设备确定其尚未被攻击，并且因此其是认证的。

进一步地，通过将散列函数应用于所述秘密数据，如上所述，如果需要，则可以在所述设备外部安全地处理散列化后的登记数据 H（S）和验证数据 H（S′）。

在另一实施例中，在登记期间例如使用对称加密方式或不对称加密方式对所述登记数据 S 进行加密。有可能的是，在认证阶段也对所述验证数据 S′进行加密，并且将对应的加密后的数据集合 E_K（S）与 E_K（S′）彼此进行比较。或者，对已加密的登记数据进行解密，散列化，并且与所述验证数据的散列化拷贝进行比较。如果执行加密操作，则可以有利地重用数据。

当研读所附权利要求以及以下描述时，本发明的其它特征和优点将变得清楚。本领域技术人员应理解，可以组合本发明的不同特征，从而创建除了以下所描述的实施例之外的实施例。

附图说明

以下将参照附图给出本发明优选实施例的详细描述，其中：

图 1 示出根据本发明实施例的包括提供用于认证的可测量参数的物理令牌的设备。

具体实施方式

图 1 示出根据本发明实施例的包括提供用于认证的可测量参数的物理令牌的设备。该设备 11 包括集成电路（IC），其由半导体晶片 12、绝缘层 13 和传感器元件 16 组成。进一步地，该设备包括覆盖 IC 的涂覆层 14 的形式的物理不可复制函数（PUF）。在涂覆层 14 中，散布介电粒子 15。这些粒子典型地具有不同介电常数，并且是随机大小和形状。传感器元件 16 被布置在绝缘顶部金属层 13 处，以用于在不同涂覆位置对电容值进行本地化测量。设备 11 典型地布置有：输入，经由所述输入可以输入数据；输出，经由所述输出可以提供加密/解密（并且有可能被签署的）数据。或者，设备 11 可以接收已加密数据作为输入数据，并且输出解密后的数据。设备 11 还包括微处理器 17 或具有计算能力的某些其它适当的设备（例如 ASIC（专用集成电路）、FPGA（现场可编程门阵列）、CPLD（复杂可编程逻辑设备）等等）。微处理器例如被采用为执行密码运算，并且根据测量的电容值来推导数据集合。进一步地，设备 11 包括存储装置 18，并且微处理器典型地被布置有模数转换器（未示出），以用于将测量的模拟电容值转换为数字比特串，以用于进一步处理。当执行本发明的方法不同实施例的步骤时，微处理器典型地执行下载到设备并且存储在存储装置 18 中的适当的软件。本领域技术人员理解，关于输入和/或输出数据，存在大量组合，加密/解密所述数据，或者根据其中使用了所述设备的应用而以任何其它适当的方式对所述数据进行处理。

因此，在本发明实施例中，在设备 11 的登记期间由传感器元件 16 来测量涂覆层 14 的多个电容值 R_0、R_1、……、R_{N-1}。由设备来选取噪声纠正数据 W，并且通过应用于微处理器 17 的函数 F_G，以 $(W, S) = F_G(R)$ 的方式来推导基于噪声纠正数据 W 和涂覆层的响应数据 R（其典型地包括级联的电容值 $R_0||R_1||\ldots\ldots||R_{N-1}$）的登记数据 S。此外，微处理器将散列函数 H 应用于登记数据 S，其产生散列值 H（S）。所推导出的帮助方数据 W 和受保护的登记数据 H（S）被存储在设备的存储

器 18 中。

于是，在认证阶段，在检测到有可能篡改设备的情况下，在与在登记期间所使用的相同传感器元件 18 处测量电容值，这产生测量值 R'_0、R'_1、……、R'_{N-1} 的另一集合 R′。如上所述，在登记期间选取帮助方数据，从而当将 delta-contracting 函数 G 应用于登记响应数据 R 和帮助方数据 W 时，结果等于登记数据 S。delta-contracting 函数具有以下特性：其允许选取帮助方数据的适当的值，从而充分类似响应的数据的任意值产生相同输出值（即与登记数据相同的数据）。结果，如果在认证期间所推导出的响应数据 R′充分程度地相似于在登记期间所推导出的响应数据 R，则 G(R, W) = G(R′, W) = S。因此，如果涂覆层 14 的电容特性尚未被修改，则在认证期间，噪声响应 R′连同帮助方数据 W 一起将产生验证数据 S′ = G(R′, W)，其与登记数据 S 相同。微处理器 17 执行验证数据的散列化运算，产生 H（S′）。于是，对散列化后的验证数据与散列化后的登记数据进行比较。如果 H(S′)=H(S)，则认为设备未被篡改，并且因此可以是认证的。

虽然已经参照本发明特定示例性实施例描述了本发明，但许多改动、修改等等对于本领域技术人员将是清楚的。因此，所描述的实施例并非意欲限制所附权利要求所定义的本发明的范围。

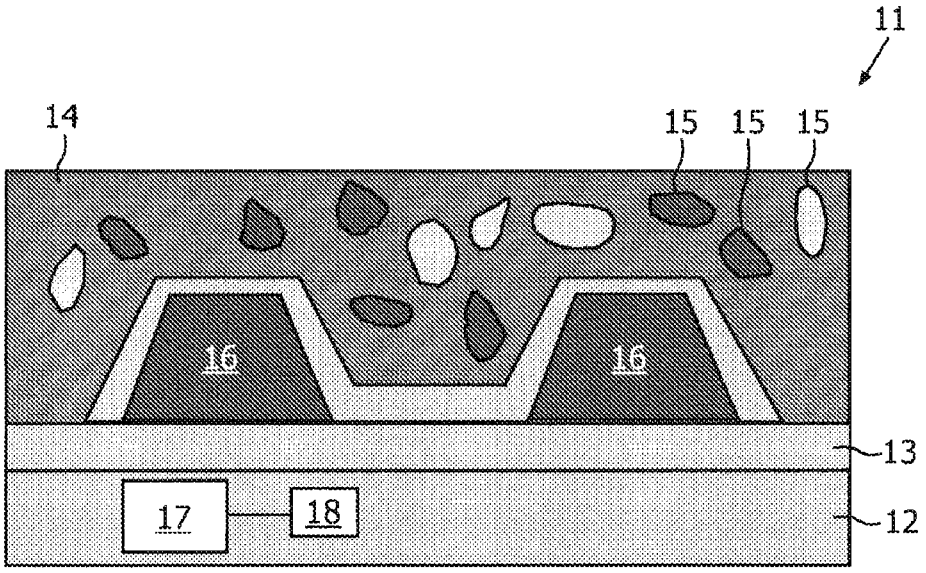


图 1