(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112042153 A
(43)申请公布日 2020.12.04

(21)申请号 201980028934.7
(22)申请日 2019.04.26
(30)优先权数据
18170044.4 2018.04.30 EP
(85)PCT国际申请进入国家阶段日
2020.10.28
(86)PCT国际申请的申请数据
PCT/EP2019/060707 2019.04.26
(87)PCT国际申请的公布数据
WO2019/211179 EN 2019.11.07
(71)申请人 默克专利有限公司
地址 德国达姆施塔特
(72)发明人 托马斯·恩德雷斯 丹尼尔·绍博
弗雷德里克·贝尔克曼
法比安·瓦尔
(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
代理人 张伟峰 夏凯
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)
G06K 9/00(2006.01)
G06K 19/08(2006.01)

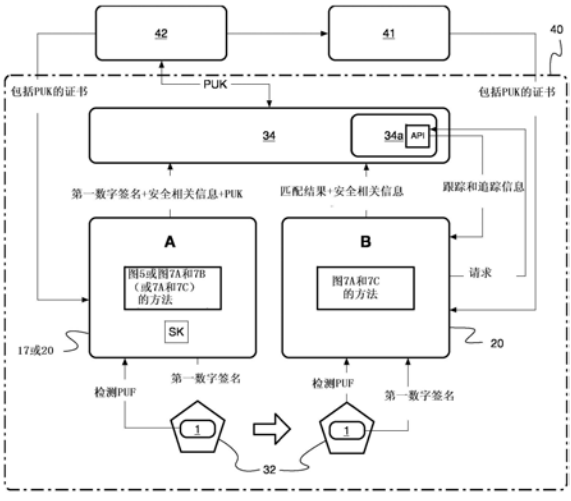
权利要求书3页 说明书27页 附图14页

(54)发明名称

复合安全标记以及用于提供和读取复合安全标记的方法和装置

(57)摘要

本发明涉及产品的防伪保护领域。具体地，本发明涉及包括物理不可克隆功能PUF的复合安全标记、包括这种复合安全标记的物理对象及其提供方法，以及用于读取标记的对应方法和读取器设备。特别地，无限制地，这种读取器设备可以与多组件安全系统，特别是防伪保护系统的组件结合使用或可以形成该组件，防伪保护系统在本文也被公开为用于防伪保护的整体安全解决方案的一部分公开。在一个实施例中，本发明涉及读取标记的方法，包括激励步骤，其中，创建根据与PUF相对应的预先确定的质询-响应认证方案的物理质询并将其应用于PUF；检测步骤，其中，检测由PUF根据质询-响应认证方案作为对质询的反应而生成的响应，并生成表示该响应的数字信号；处理步骤，其中，处理数字信号，以便通过将预先确定的密码散列函数应用于数字信号来生成响应的散列值；以及，输出步骤，其中，输出表示所生成的散列值的数据作为第一读取结果。



CN 112042153 A

1.一种用于物理对象的复合安全标记,特别是防伪产品标记,包括:

物理不可克隆的功能PUF;以及

数字签名的加密表示和/或指示能够访问所述数字签名的位置的指针的表示,其中,加密所述指针的所述表示和在所述位置可访问的所述数字签名中的至少一个;

其中,所述数字签名对散列值进行数字签名,所述散列值是将预先确定的密码散列函数应用于表示由所述PUF作为对预先确定的质询-响应认证方案的质询的反应而生成的响应的数据而得到的。

2.根据权利要求1所述的复合安全标记,其中,所述PUF包括上转换染料UCD。

3.根据前述权利要求中的任一项或多项所述的复合安全标记,其中,所述PUF包括不可克隆的物理图案或被配置为响应于所述质询而生成虚拟图案的结构。

4.根据前述权利要求中的任一项或多项所述的复合安全标记,其中,所述复合安全标记包括所述指针,并且所述指针指示到数据源的路由,所述数据源可通过通信链路访问并且所述数字签名可从所述数据源检索。

5.根据权利要求2至4中的任一项或多项所述的复合安全标记,其中,表示由所述PUF作为对用于所述UCD的预先确定的质询-响应认证方案的质询的反应而生成的响应的所述数据表示光谱条形码和/或在所述响应中发生的发光效应的特性寿命,所述光谱条形码对于所选择的离散的波长的子集具有连续或量化范围的允许光谱值。

6.根据权利要求3至5中的任何一项或多项所述的复合安全标记,其中,表示由所述PUF作为对用于所述不可克隆的物理图案或被配置为生成虚拟图案的结构的预先确定的质询-响应认证方案的质询的反应而生成的响应的所述数据分别表示所述物理图案或所述虚拟图案的至少一个公认的方面或部分。

7.一种物理对象,特别是产品,包括根据前述权利要求中的任一项或多项所述的复合安全标记。

8.一种为物理对象,特别是产品,提供复合安全标记的方法,所述方法包括:

向要标记的对象添加物理不可克隆功能PUF;

对预先确定的质询-响应认证方案的质询应用于所述PUF,以作为对所述质询的反应,来触发根据所述认证方案的响应;

检测所述响应;

将预先确定的密码散列函数应用于表示所述响应的数据以获得散列值;

用数字签名对所述散列值进行签名;以及

将所述数字签名的加密表示或指示能够访问所述数字签名的位置的指针的表示添加到要标记的所述对象,其中,所述指针的所述表示和在所述位置处可访问的所述数字签名中的至少一个被加密。

9.根据权利要求8所述的方法,其中,将所述PUF添加到要标记的对象的所述步骤包括以下一项或多项:

-将所述PUF添加到涂覆材料中以获得PUF增强的涂覆材料,并将所述PUF增强的涂覆材料应用到要标记的物理对象;

-在生产要标记的物理对象之前或同时,将PUF添加到原材料或中间材料;

-将PUF添加到加法制造过程的原材料或融合剂中,以用于生产要标记的物理对象或这

样的对象的至少一部分。

10.一种用于向物理对象,特别是产品,提供复合安全标记的装置,其中,所述装置适于执行权利要求8或9所述的方法。

11.一种利用读取器设备读取标记的方法,所述标记特别是根据权利要求1至6中任一项所述的复合安全标记,所述标记包括物理不可克隆功能PUF和第一数字签名的表示和/或指示能够访问所述第一数字签名的位置的指针的表示,所述方法包括以下步骤:

激励步骤,其中,创建根据与所述PUF对应的预先确定的质询-响应认证方案的物理质询并将其应用于PUF;

检测步骤,其中,检测所述PUF根据所述质询-响应认证方案作为对所述质询的反应而生成的响应,并生成表示所述响应的数字信号;

处理步骤,其中,处理所述数字信号,以便通过将预先确定的密码散列函数应用于所述数字信号来生成所述响应的第一散列值;

获取步骤,包括通过以下步骤访问所述第一数字签名以从其中恢复使用其签名的第二散列值:

-基于预先确定的解密方案,读取和解密所述标记中的所述第一数字签名的所述表示,或者

□-读取所述标记中的所述指针的所述表示,并从所述指针指示的所述位置获取并验证所述第一数字签名,包括分别根据所述解密方案对所述第一数字签名或所述指针的所述表示进行解密;以及

输出步骤,包括输出包括以下一个或多个的第一读取结果:

-所述第一散列值的表示和所述第二散列值的表示,

□-和/或匹配输出,所述匹配输出指示根据至少一个预先确定的匹配标准,所述第一散列值是否与所述第二散列值匹配,或者

□-输出,所述输出指示读取失败。

12.根据权利要求11所述的方法,其中,在所述处理步骤中,生成所述数字信号使得所述数字信号表示所述响应的至少一个PUF特定的区别属性,所述区别属性在检测到所述响应的环境条件的变化下至少基本上是不变的。

13.根据权利要求11或12所述的方法,其中,所述输出步骤包括对包含所生成的第一散列值的数据进行数字签名,并输出所得到的数字签名作为所述读取结果的一部分。

14.一种利用读取器设备读取标记的方法,所述标记特别是根据权利要求1至6中的任一项所述的复合安全标记,所述标记包括第一数字签名的加密表示和指示能够访问第二数字签名的位置的指针的表示两者,所述方法包括:

获取步骤,包括:

-通过基于预先确定的解密方案读取并且解密所述标记中的所述第一数字签名的表示并通过对于其进行验证,来访问所述第一数字签名,所述第一数字签名包括使用其签名的第一散列值;以及

-通过读取所述指针的所述表示并从所述指针指示的所述位置获取包括使用其签名的第二散列值的所述第二数字签名来访问所述第二数字签名,包括分别基于所述预先确定的解密方案解密获取的数字签名或所述指针的所述表示,并验证所述第二数字签名;

输出步骤,包括输出包括以下一个或多个的第一读取结果:

-所述第一散列值的表示和所述第二散列值的表示,

-匹配输出,所述匹配输出指示根据至少一个预先确定的匹配标准,所述第一散列值是否与所述第二散列值匹配;

-输出,所述输出指示读取失败。

15.根据权利要求14所述的方法,其中,所述获取步骤进一步包括:从标记获取另一数字签名或指示能够访问关于所述标记的特定的另一数字签名的来源的指针;以及

所述输出步骤进一步包括输出获取的另一数字签名的表示作为第二读取结果。

16.根据权利要求14或15所述的方法,进一步包括存储步骤,其中,将所述第一读取结果存储到第一区块链的区块中或第一无区块分布式分类账的一个或多个节点中。

17.根据权利要求16所述的方法,其中:

所述存储步骤进一步包括:分别将所述第二读取结果存储在与所述第一区块链分开的第二区块链的区块中,或存储在与所述第一无区块分布式分类账分开的第二无区块分布式分类账的一个或多个节点中;以及

存储所述第一读取结果包括分别将表示所述第一散列值的数据存储到所述第一区块链的区块中或所述第一无区块分布式分类账的一个或多个节点中。

18.根据权利要求17所述的方法,其中:

(a)如果所述存储步骤与区块链有关,则:

将表示所述第一散列值的所述数据存储到所述第一区块链的区块中进一步包括:将逻辑上将所述第一区块链的所述区块映射到所述第二区块链的对应区块的跨区块链指针存储到所述第一区块链的所述区块中;以及

将表示所述第二散列值的所述数据存储在所述第二区块链的区块中进一步包括:将逻辑上将所述第二区块链的所述区块映射到所述第一区块链的对应区块的跨区块链指针存储到所述第二区块链的所述区块中;以及

(b)如果所述存储步骤与无区块分布式分类账有关,则:

将所述散列值中的至少一个散列值存储到所述第一无区块分布式分类账的节点中包括:将跨分类账指针存储到所述第一无区块分布式分类账的所述节点中,所述跨分类账指针在逻辑上将所述第一无区块分布式分类账的所述节点映射到所述第二无区块分布式分类账的对应节点;以及

将补充信息存储到所述第二无区块分布式分类账的节点中包括:将跨分类账指针存储到所述第二无区块分布式分类账的所述节点中,所述跨分类账指针在逻辑上将所述第二无区块分布式分类账的所述节点映射到所述第一无区块分布式分类账的对应节点。

19.一种用于读取标记的读取器设备,其中,所述读取器设备适于执行权利要求11至13中任一项的方法和/或权利要求14至18中任一项的方法。

20.一种包括指令的计算机程序,所述指令当在根据权利要求19的读取器设备的一个或多个处理器上执行时,使所述读取器设备执行根据权利要求11至13中的任一项所述的方法和/或根据权利要求14至18中的任一项所述的方法。

复合安全标记以及用于提供和读取复合安全标记的方法和装置

技术领域

[0001] 本发明涉及产品的追踪与防伪保护的领域。具体地，本发明涉及包括物理不可克隆功能PUF的复合安全标记、包括这种复合安全标记的物理对象及提供复合安全标记的方法以及用于读取标记的对应方法和读取器设备。特别地，没有限制地，这种读取器设备可以与多组件安全系统，特别是防伪保护和/或跟踪系统的组件结合使用或可以形成多组件安全系统的组件，特别是防伪保护和/或跟踪系统的组件，该多组件安全系统在此也公开为用于防伪保护和安全产品跟踪的整体安全解决方案的一部分。

背景技术

[0002] 在许多行业中，产品伪造是一个重大问题，其不仅显著影响原始产品制造商的收入，而且甚至可能严重威胁伪造产品(即假产品)的消费者或操作者的健康甚至生命。此类安全相关产品类别尤其包括汽车和飞机的零件、建筑物或其他基础设施的建筑的组件、食品以及甚至医疗设备和药品。

[0003] 此外，在广泛的不同行业中，商品和物理对象的可追溯性是关键要求。这尤其适用于物流和供应链基础设施以及高度监管/结构化的工作流程环境。示例是由诸如FDA(美国食品和药物管理局)等官方监管者控制，和/或例如根据GMP(良好制造规范)、GLP(良好实验室规范)、GCP(良好临床规范)或DIN ISO或类似的其他标准和规则颁发合格证书的行业工作地点。这些受监管的环境中的每一个都特别需要审计追踪和可审计技术。另一个示例是诸如工业备件的高价值产品的可追溯性，以便证明这些零件在二级市场中的真实性和预期用途。

[0004] 为了限制伪造并特别解决此类安全问题，以及此外提供供应链和工作流程完整性，包括对工作流程和供应链中的产品进行识别和认证，各个行业已开发出许多不同的保护措施和标识方案。广泛使用的保护措施包括在产品上添加所谓的安全特征，该特征很难假冒。例如，全息图、光学可变油墨、安全线和嵌入的磁性颗粒是伪造者难以复制的已知安全特征。虽然这些安全特征的一些是“明显的”，即可以被产品的用户容易地看到或以其它方式识别，但是其他安全特征是“隐蔽的”，即它们是隐藏的并且只能通过使用诸如UV光源、光谱仪、显微镜或磁场检测器或甚至更复杂的法医设备的特定设备来检测。隐蔽的安全特征的示例特别是使用发光油墨或仅在电磁光谱的红外部分中可见而在其可见部分中不可见的油墨、特定的材料组合物和磁性颜料进行的打印。

[0005] 一组特定的安全特征，特别是在密码学中使用的特征，被称为“物理不可克隆功能”(PUF)。PUF有时也称为“物理上不可克隆功能”或“物理随机功能”。PUF是体现在物理结构中的物理实体，并且即使对于具有对PUF的物理访问的攻击者，也是易于评估但难以预测的。PUF取决于其物理微观结构的独特性，该物理微结构通常包括随机组件，该随机组件已经固有地存在于物理实体中，或者在其制造期间被明确地引入到物理实体中或在物理实体中生成，并且其基本上是不可控制且不可预测的。因此，即使通过确切相同的制造过程生产

的PUF至少在其随机组件上也不同,并且因此可以区分。尽管在大多数情况下,PUF是隐蔽特征,但这不是限制,并且明显的PUF也是可能的。此外,PUF对于使能物理对象的被动(即,没有主动广播)标识是理想的。

[0006] 特别地,利用在给定过程相关容差内在芯片上生产的微结构的最小的不可避免的变化,PUF结合其在集成电路中的实现而被人熟知,并且尤其已知用于从中推导密码密钥,例如在用于智能卡的芯片或其他安全相关芯片中。此类芯片相关PUF的解释和应用的示例在以下文章中被公开:"Background on Physical Unclonable Functions(PUFs)(在于物理不可克隆功能(PUF)的背景)",弗吉尼亚理工学院,电气和计算机工程系,2011年),该文章可在以超链接:http://rijndael.ece.vt.edu/puf/background.html在互联网中获得。

[0007] 但是,还已知其他类型的PUF,诸如用作用于造钞票的基底的纸张中纤维的随机分布,其中,纤维的分布和定向可以通过特定的检测器检测,并用作钞票的安全特征。为了评估PUF,使用了所谓的质询-响应认证方案。"质询"是对PUF施加的物理激励,"响应"是其对激励的反应。该响应取决于物理微结构的不可控制和不可预测的性质,并且因此可以用于认证PUF,并且也可以认证PUF构成其一部分的物理对象。特定的质询及其相应的响应共同形成了所谓的"质询-响应对"(CRP)。

[0008] 非对称密码学,有时也称为"公共密钥密码术"或"公共/私有密钥密码学",是基于使用密钥对的密码系统的已知技术,其中,每对密钥包括公共密钥和私有密钥。公共密钥可以广泛传播,并且通常甚至公开获得,而私有密钥是保密的,并且通常只有其所有者或持有者才能知道。非对称密码学实现以下两者:(i)认证,基是当使用公共密钥验证成对私有密钥的持有者是否通过利用他的私有密钥对其签名而发起了特定信息(例如,包含该信息的消息或存储的数据)的认证,以及(ii)借助于加密的信息(例如,消息或存储的数据)的保护,从而只有成对私有密钥的所有者/持有者才能解密其他人利用公共密钥加密的消息。

[0009] 最近,已经开发了区块链技术,其中,区块链是包含多个数据区块的分布式数据库形式的公共分类账,并且维护不断增长的数据记录列表,并且通过密码手段加固以防篡改和修订。区块链技术的突出的应用是用于互联网中货币交易的虚拟比特币。例如,以太坊(Ethereum)项目提供了另一个已知的区块链平台。本质上,可以将区块链描述为用于记下各方之间交易的去中心化协议,该协议透明地捕获并存储对其分布式数据库的任何修改,并"永久地"保存它们,即只要区块链存在。将信息存储到区块链中涉及对要存储在区块链的区块中的信息进行数字签名。此外,维护区块链涉及称为"区块链采矿"的过程,其中,作为区块链基础设施的一部分的所谓的"矿工"验证并密封每个区块,使得其中包含的信息被"永远地"保存,而区块不再能被修改。

[0010] 另一种新的分类账技术以"Tangle"的名称被已知,它是无区块化且无许可的分布式分类账架构,该架构是可扩展的、轻量级的,并在分散式对等系统中提供一致。使用Tangle作为技术基础的突出的相关技术称为"IOTA",其是物联网的交易结算和数据完整性层。

发明内容

[0011] 本发明的目的是提供一种改进的方法,该方法有效地保护物理对象以防伪造和篡改,同时允许在其授权检查的过程中有效地识别和认证该物理对象。

[0012] 通过所附独立权利要求的教导提供了对该问题的解决方案。从属权利要求的教导提供了本发明的各种优选实施例。

[0013] 此外，本文提出了整个安全解决方案，包括作为不同方面的各种装置和方法，其可以形成用于有效跟踪和保护物理对象以防伪造和篡改的完整安全解决方案的一部分。

[0014] 本文提供的安全解决方案的第一方面涉及用于物理对象的复合安全标记，特别是防伪复合安全标记。复合安全标记包括物理不可克隆功能PUF和数字签名的加密表示和/或指示可以访问所述数字签名的位置的指针的表示，其中，指针的所述表示和在该位置处可访问的所述数字签名中的至少一个被加密。数字签名对预先确定的密码散列函数应用于表示由PUF作为对预先确定的质询-响应认证方案的质询的反应而生成的响应的数据而得到的散列值进行数据签名。

[0015] 如本文所用，术语“物理对象”是指任何种类的物理对象，尤其是指任何种类的人造或产品或天然对象，例如蔬菜或一片天然原材料。此外，如本文所使用的，术语“物理对象”还可以指可以对其应用复合安全标记的人或动物。物理对象本身可以包括多个部分，例如消费品及其包装。

[0016] 如本文中所使用的，术语“复合安全标记”是指包括至少两个不同的单独标记作为其组成部分的物理实体(因此称为“复合物”)，适于应用于物理对象或在物理对象上或中创建，并且在应用到物理对象上或在物理对象上或之中创建后仍可访问，以便对其进行评估。在根据安全解决方案的上述第一方面的复合安全标记中，第一组件是PUF，并且第二组件是数字签名的加密表示或指示可以访问所述数字签名的位置的指针的表示，其中，指针的所述表示和在位置处可访问的所述数字签名中的至少一个被加密。特别地，复合安全标记的两个或更多个组件可以位于物理对象的同一基底或部分上或内。替选地，组件的子集或所有组件可以位于物理对象的分开的基底或其他部分上或内。加密可以特别地基于已知的对称或非对称加密方案，例如，根据众所周知的AES(对称)或RSA(非对称)密码方案。

[0017] 如本文所使用的，术语“数字签名”是指一个或多个数字值的集合，该确认数字数据的发送者或发起者的身份以及后者的完整性。为了创建数字签名，借助于应用适当的密码散列函数从要保护的数据中生成散列值。然后例如基于RSA密码系统，用非对称密码系统的私有密钥(有时也称为“安全密钥”)对该散列值加密，其中，私有密钥通常仅对发送者/发起者是已知的。通常，数字签名包括数字数据本身以及由发送者/发起者从其导出的散列值。然后，接收者可以将相同的密码散列函数应用于接收到的数字数据，使用与所述私有密钥相对应的公共密钥来解密数字签名中包括的散列值，并将来自数字签名的解密后的散列值与通过将密码散列函数应用于接收到的数字数据来生成的散列值进行比较。如果散列值两者匹配，则这指示该数字信息尚未被修改，并且因此其性未受到损害。此外，借助于非对称密码系统确认数字数据的发送者/发起者的真实性，这可以确保使用公共密钥的加密仅在加密的信息是在使用与该公共密钥在数学上成对的私有密钥加密的时才起作用。数字签名的表示可以特别地使用RFID发送器或一维或多维条形码(诸如QR码或DATAMATRIX码)或简单地作为多位数字来实现。

[0018] 如本文所用，术语“密码散列函数”是指特定类型的散列函数，即将任意大小的数据映射到固定大小的比特串(散列值)的数学函数或算法，该散列函数被设计为也是单向函数，即易于在每个输入上计算但在给定随机输入的图像的情况下难以求逆的函数。优选地，

密码散列函数是所谓的抗碰撞散列函数，即被设计为使得难以找到两个不同的数据集d1和d2以使得hash(d1)＝hash(d2)的散列函数。此类散列函数的突出示例是：SHA族的散列函数，例如SHA-3函数；或，BLAKE族的散列函数，例如BLAKE2函数。特别地，可以使用所谓的“可证明安全的密码散列函数”。这些是散列函数，可以在数学上证明其某个足够的安全级别。在本安全解决方案中，通过以下事实进一步提高了密码散列函数的安全：读取如本文所公开的包括PUF的标记，特别是复合安全标记，在特定的位置和时间进行，其中，带有标记的物理对象实际上在该位置和时间存在。这可以用于提高可以达到的绝对安全级别，或允许使用与较小数据集一起工作的密码散列函数，例如，较短的数据串作为输入和/或输出，同时仍提供给定的所需安全级别。

[0019] 如本文所使用的，“指示可以访问所述数字签名的位置的指针”可以特别地是指向本地或远程数据库或可以访问(例如下载)数字签名的服务器地址或因特网地址(例如超链接或类似内容)的指针。可以特别地使用RFID发射机或诸如作为其表示的QR承载码或DATAMATRIX码的一维或多维条形码来实现该指针。

[0020] 根据本安全解决方案的第一方面的复合安全标记可以被第一方(例如，产品形式的物理对象的发起者)使用，以保护可以向其应用标记的组件(即至少相应的PUF及其响应的相应数字签名)的任何物理对象。特别地，标记优选地应用到物理对象上，使得在不破坏标记或标记的至少部分的情况下，标记不能再次与对象分离。

[0021] PUF本质上已经是“不可克隆的”，并因此提供了第一安全级别，即作为确认标记的真实性并因此确认物理对象的真实性的手段。但是，通过将PUF与数字签名相结合，可以进一步将此第一安全级别增强到更高的第二安全级别，该数字签名对于从由PUF对关于PUF的预先确定的质询-响应方案的质询的响应中导出的散列值进行密码签名。以此方式，类似于用于电子文档的数字签名，创建用于物理对象的数字签名以用于保护这样的对象，特别是防止伪造。数字签名的表示和/或指示可以访问所述数字签名的位置的指针的表示的加密增加了另一安全级别，即第三安全级别，因为在读取数字签名之前相应的表示首先需要被解密，这需要了解加密方案和正确的加密密钥。

[0022] 为了验证物理对象各自起源的真实性，接收物理对象的第二方将根据此质询-响应方案的质询应用于物理对象的标记的PUF，并且应用相同的密码散列函数以从表示接收自PUF的响应的数据生成相应的第一散列值。可以通过解密数字签名的加密表示或指针的加密表示，如适用的，并且使用其相关的公共密钥解密由此恢复的数字签名，来导出数字签名中包含的第二散列值。然后可以比较第一和第二散列值。如果它们匹配，则这指示物理对象是真实的，并且复合安全标记尚未被篡改。否则，即，如果它们不匹配，则这指示自发起者将复合安全标记应用于物理对象以来，可能已发生某种欺诈。

[0023] 因此，复合安全标记提供附加的安全级别，从而提供了一种保护物理对象以防伪造和篡改的改进方式。此外，因为PUF对根据质询-响应方案的质询的响应产生数字数据，例如，数据串，所以复合安全标记可用于保护可对其应用此标记的任何物理对象，即使对象本身未提供任何数字数据。

[0024] 在下文中，描述了复合安全标记的优选实施例，其可以彼此任意组合或与本文描述的解决方案的其他方面任意组合，除非这种组合被明确地排除、不一致或在技术上是不可能的。

[0025] 根据第一优选实施方案,PUF包括上转换染料(UCD),优选多种不同的转换染料。UCD是染料,它显示出光子上转换(UC)效应的染料,其是两个或更多个光子的顺序吸收导致发射比激发波长短的波长的光的过程。它是反斯托克斯型发射。这种过程的典型示例是将红外光转换为荧光可见光。通过其可以发生上转换的材料通常包含周期系统的d区块和f区块元素的离子。这些离子的例子是Ln3+、Ti2+、Ni2+、Mo3+、Re4+和Os4+等。这样的材料通常包括振动离子光谱展宽的相对低的部分,因此在电磁光谱的非常窄的波段中显示荧光。使用各种上转换物质的各种不同组合(即混合),可以生成大量可区分的单个光谱。

[0026] 例如,假定在400nm至800nm的光谱区域内的20nm的光谱分辨率为,则如果检测仅限于光谱是否在相应的20nm间隔内显示峰的二进制问题,则已经存在2^{20}种不同的可能性。换句话说,可以将二进制值“0”或“1”分配给每个间隔,这些值中的一个值指示在该间隔中存在峰,而另一个值指示不存在该峰。因此,可以由分配给所述光谱区域被划分成的20个间隔的20个二进制值形成数字串,并且因此可以由这种串表示2^{20}个,即大约10^6个不同的组合。如果替代地仅使用10nm的间隔,则数量增加到2^{40},即大约10^{11}种不同的组合。如果另外,在每个间隔中,在每个峰的情况下进一步区别,例如各个峰是更接近“全”峰还是仅接近“半”峰(参见图4(b)),那么在40个间隔的情况下,组合数甚至增加到3^{40},即大约10^{18}种组合。因此,实际上不可能创建UCD的混合使得其显示与其试图克隆的原始混合相同的光谱。

[0027] 这样,可以使用UCD创建PUF。将UCD用于PUF的优点是,它们几乎可以应用于任何物理对象,例如作为制造物理对象或其一部分的涂层或材料的组件。此外,UCD是典型的隐蔽特征,在没有复杂的设备的情况下不能容易地被识别。这可以用来进一步提高可达到的安全级别。

[0028] 根据另一优选实施例,PUF包括不可克隆的物理图案或被配置为响应于质询而生成虚拟图案的结构。在该实施方案的一个变体中,图案可以包括大量的微观粒子,该大量的微观粒子的位置和/或定向表示可以通过实际手段被检测到但不能克隆的不可控制和不可预测的物理图案。在另一个优选的变体中,被配置为生成虚拟图案的所述结构包括被配置为当被合适的光源的光照射时生成光学斑点图案的微结构。特别地,微结构可以包括多个所谓的量子点,即非常小的半导体粒子,其大小仅几纳米,使得它们的光学和电子属性不同于较大的粒子的光学和电子属性,并且如果向它们施加电或光(例如,作为质询),则它们发射出特定波长的光。在制造期间可以控制的量子点的大小、形状和材料确定这些波长,因此可以创建巨大的各种不同的发射光谱作为相关质询-响应方案的响应。在另一个优选的变体中,微结构可以包括多种棒状量子材料(量子棒),其提供与球形量子点类似的颜色转换机制和扩展的色域。量子棒的独特优点是偏振光的发射。当然,上述微结构变体的组合也是可能的。

[0029] 如本文所用,术语“光”是指电磁辐射,并且可以包括但不限于电磁光谱的可见部分中的辐射。代替或除了可见辐射之外,光例如还可以包括紫外线或红外辐射。“斑点”图案是由一组相同或类似的波长(例如,在可见光谱中)但相位不同、振幅通常也不同的许多电磁波前的相互干扰所产得的强度图案。由干扰引起的波的强度至少在空间维度上随机变化。通常,单色且充分相干的辐射,诸如激光发射,用于生成这种斑点图案。

[0030] 特别地,该微结构可以是整体的微结构,诸如显示出足够的光学粗糙度的物理对象的表面,或者它可以包括多个分开的部分,例如,在人体(其对辐射至少部分透明)内或在

物理对象的表面上呈随机分布的微观粒子。

[0031] 与UCD类似,将这种生成斑点的微结构用于PUF的优点是,如果物理对象对生成斑点图案所需的光线足够透明,则这种微结构可以应用于几乎任何物理对象,无论是在其表面上还是甚至嵌入在对象内。因为这样的微结构通常具有光的波长的量级的特性尺寸,所以它们可以被做得非常小,并且因此通常也是在没有复杂的设备的情况下不能容易地被识别的隐蔽特征。这再次提高了可达到的安全级别。

[0032] 根据另一优选实施例,PUF包括以下至少一项:(i)隐匿地嵌入隐藏信息的图像;(ii)用包含一种或多种类型的上转换染料UCD的油墨打印的图像;(iii)包含隐藏的相位编码或频率编码的信息的全息图。特别地,除了上述提到的增加可以实现的安全级别的隐蔽安全特征之外,图像各个全息图还可以另外包括或表示明显的特征,例如一维或多维条形码,诸如QR码或DATAMATRIX码,以便呈现进一步的信息。例如,这样的代码可以覆盖下面的包含隐蔽特征的图像或全息图,或者可以用包含UCD的混合的油墨打印图像。这允许包含所涵盖的安全方面和明显的安全特征或其他信息(诸如复合安全标记或产品代码的数字签名、制造商身份、生产场所信息等)的PUF的空间效率极高的实现。

[0033] 根据另一优选实施例,数字签名和/或指针的表示由以下一个或多个实现:(i)字母数字串;(ii)图形或图像表示;(iii)一维或多维条形码;(iv)传输携带数字签名或指针的表示的信号的设备,例如短距离无线芯片(诸如RFID芯片)。特别地,该实施例可以与紧接在前的实施例组合。此外,数字签名和/或指针可以分别仅由所述串、图形图像表示、条形码或信号的一部分来表示,所述串、图形图像表示、条形码或信号中的每一个可以另外表示可能是或可能不是安全相关的其他信息。

[0034] 根据另一优选实施例,复合安全标记包括所述指针,并且所述指针指示到数据源的路由,该数据源例如是互联网中的服务器,该数据源可通过数据链路(诸如到互联网或另一网络的连接)来访问,并且可以从中检索数字签名。特别是,这允许对服务器环境中多个物理对象的数字签名进行集中管理。此外,这使得对管理的数字签名的使用进行集中监视和控制,该管理的数字签名可以多种方式使用,例如,用于早期检测到欺诈尝试或供应链优化。具体地,可以将信任中心基础设施用于这种集中监视和控制。可选地,指针还可以包含或指向与产品类型、序列号有关的信息或与用复合安全标记来标记的物理对象有关的其他信息。

[0035] 根据另一优选实施例,其中,PUF包括UCD,表示由所述PUF回应针对所述UCD的预先确定的质询-响应认证方案的质询而生成的响应的所述数据表示光谱条形码和/或在所述响应中发生的发光效应的特性寿命,该光谱条形码对于所选择的离散的波长子集具有连续或量化范围的允许光谱值。这尤其允许确定和缩放可以通过使用PUF的UCD来编码的比特或其他信息单元的数量。例如,如果在光谱的每个间隔中将对应的光谱值量化为四个光谱级别中的一个光谱级别,则该光谱间隔可用于编码PUF表示的两比特的信息。在该光谱间隔中还添加发光现象效应的特性寿命的量化可以用于添加更多的信息比特。量化在允许的光谱值的连续范围内可以是优选的,因为它可以提高抵抗PUF生成的响应的失真的鲁棒性。

[0036] 根据另一优选实施例,其中,PUF包括不可克隆的物理图案或被配置为响应于质询而生成虚拟图案的结构,表示由PUF作为对所述不可克隆的物理图案或被配置为生成虚拟图案的结构的预先确定的质询-响应认证方案的质询而生成的响应的所述数据分别表示所

述物理图案或所述虚拟图案的至少一个公认的方面或部分。特别地，所述公认的方面可以涉及应用于物理图案或虚拟图案的统计量度，诸如图案的各个节点之间的平均距离、相关的方差或标准偏差或任何其他统计矩。可替选地，根据另一变体，所述图案可以例如以矩阵的方式被扫描，并因此例如通过使用区别阈值并将示出比阈值高的光强度的矩阵点表示为“1”且将具有低于阈值的光强度的所有矩阵点表示为“0”，反之亦然，而被转换成例如比特串。以这种方式，可以将图案有效地转换为表示由PUF作为对相应质询的反应而生成的响应的数据。

[0037] 根据另一优选实施例，复合安全标记包括由加法制造工艺得到的至少一个组件，并且PUF被包含在该组件中或以其它方式形成该组件的一部分。特别地，加法制造工艺可以是所谓的3D打印工艺。优选地，PUF已经在原材料中被提供，使用加法制造工艺从该原材料制造组件。以这种方式，PUF可以被引入到部件中，而无需修改加法制造工艺基于其来执行的制造数据。此外，加法制造方法所提供的极高的灵活性和复杂性允许几乎无穷无尽的各种不同PUF及其在要标记的物理对象上或内部的布置。同样，这可以用来进一步提高可以用复合安全标记实现的安全级别。

[0038] 本文提供的解决方案的第二方面涉及物理对象，特别是产品，该物理对象包括根据解决方案的第一方面，优选地根据本文所述的其实施例或变体中的任何一个或多个的复合安全标记。

[0039] 具体地，根据优选实施例，物理对象是包括用于消费或使用的一个或多个物品及其包装的产品，以及，复合安全标记的PUF被布置在用于消费或使用的物品的至少一个物品上或包含在其中，而数字签名的表示或指向其的指针被布置在包装上或包装内。因此，在该实施例中，在两个不同的基底上形成复合安全标记。这在产品本身没有足够的空间来同时携带PUF和数字签名两者的情况下尤其有利。在一个变体中，产品是药物产品，包括：例如包含液体药物的瓶子或包含作为用于消费的物品的片剂的泡罩包装；以及，围绕该瓶子或泡罩包装的作为包装的纸板箱。复合安全标记的PUF是放置在瓶子上的打印标签，其中，该标签是用包含不同UCD的秘密混合的油墨打印的。对应于PUF的数字签名可以以二维条形码(例如QR码或DATAMATRIX码)的形式被打印在包装上。

[0040] 根据另外的优选实施例，物理对象包括以下用于消费(消费品)或使用的物品中的一项或多项：药物或化妆品化合物或组合物；医疗设备；实验室设备；设备或系统的备件或组件；杀虫剂或除草剂；播种材料；涂料、油墨、油漆、染料、颜料、清漆、浸渍物质、功能添加剂；用于产品加法制造的原材料。特别地，所有这些物品的共同点是需要防伪，以便避免故障、健康威胁或其他风险。

[0041] 本文提供的解决方案的第三方面涉及一种为物理对象(特别是产品)提供复合安全标记的方法。该方法包括以下步骤：(i)向要标记的对象添加物理不可克隆功能PUF；(ii)对所述添加的PUF中的至少一个PUF应用预先确定的质询响应认证方案的质询，以作为对所述质询的响应，根据所述认证方案触发响应；检测所述响应；(iii)对表示所述响应的数据应用预先确定的密码散列函数，以获得散列值；(iv)用数字签名对所述散列值签名；以及(v)将数字签名的加密表示或指示能够在何处访问数字签名的指针的表示添加到要标记的对象，其中，指针的所述表示和在位置处可访问的所述数字签名的至少一个被加密。

[0042] 因此，向物理对象提供复合安全标记，该物理对象包括所述PUF，并且通过加密保

护其相应的数字签名或指向其指针。优选地，PUF是如上所述的PUF，作为根据本安全解决方案的第一方面，分别是其优选实施例和变体的复合安全标记的组件。因此，通过该方法生产的所生产的复合安全标记特别地对应于根据本安全解决方案的第一方面的复合安全标记。优选地，该方法进一步包括生成非对称密码系统的公共/私有密钥对，并使用该私有密钥来创建所述散列值的所述数字签名，并使所述对应的公共密钥直接或间接地可供带有复合安全标记的对象的接收者使用。

[0043] 可选地，如上所述，复合安全标记可以包括多于一个的PUF，尤其是如上所述的PUF，以及根据步骤(ii)至(v)从PUF或指向其的指针导出的多于一个的数字签名。因此，在方法的对应实施例中，可以通过下述方式来获得附加的数字签名：在步骤(ii)中将与不同质询-响应方案相对应的不同质询应用于相同的PUF(如果后者支持)，或者在步骤(i)中将两个或多个PUF添加到要标记的对象，并对这些PUF中的每个PUF执行步骤(ii)。在这两种变体中，对于响应中的每个响应，都遵循步骤(iii)至(v)，其中，对于步骤(v)，指针可以指向生成的数字签名的对应集合。这样，可以进一步提高可达到的安全级别。

[0044] 根据另一个优选的相关实施例，将一个或多个PUF添加到要标记的对象的步骤包括以下一个或多个：(a)将一个或多种PUF添加到涂覆材料中以获得PUF增强的涂覆材料，并且例如通过喷涂、涂覆、渗透、打印或涂刷将PUF增强的涂覆材料应用到要标记的物理对象；(b)在生产要标记的物理对象之前或同时，优选借助于一个或多个化学或混合过程，将一个或多个PUF添加到原材料或中间材料(诸如油墨或色料)；(c)将一个或多个PUF添加到加法制造过程(例如，3D打印过程)的原材料或融合剂中，以用于生产要标记的物理对象或此类对象的至少一部分。特别地，可以在加法制造过程之前或期间将一个或多个PUF添加到原材料或融合剂中。这允许将一个或多个PUF容易地集成到对象本身中。此外，可以进一步提高安全级别，因为当一个或多个PUF成为对象的必需组成部分时，可以有效地防止从对象中移除，特别是非破坏性地移除一个或多个PUF。

[0045] 本文提供的解决方案的第四方面涉及一种用于为物理对象，特别是产品，提供复合安全标记的装置，其中，该装置适于执行根据解决方案的第三方面，优选地根据本文所述的任何一个或多个实施例或变体的方法。因此，解决方案的第三方面的描述和优点在细节上作必要修改后适用于根据该第四方面的设备。

[0046] 本文描述的解决方案的第五方面涉及一种用读取器设备读取包括物理不可克隆功能PUF和第一数字签名的表示和/或指示可以访问第一数字签名的位置的指针的表示的标记的方法。该标记尤其可以是根据第一方面，优选地根据本文所述的其实施例中的一个或多个实施例的复合安全标记。该方法包括以下步骤：(i)激励步骤，其中，创建根据与PUF相对应的预先确定的质询-响应认证方案的物理质询并将其应用于PUF；(ii)检测步骤，其中，检测由PUF根据质询-响应认证方案作为对质询的反应而生成的响应，并且生成表示该响应的数字信号；(iii)处理步骤，其中，处理数字信号以便通过将预先确定的密码散列函数应用于数字信号来生成响应的第一散列值；(iv)获取步骤，包括通过以下步骤访问所述第一数字签名，以从中恢复用其签名的第二散列值：(a)基于预先确定的解密方案读取和解密标记中的第一数字签名的表示，或者(b)读取标记中的指针的表示，并从指针指示的位置获取并验证第一数字签名，包括根据解密方案分别对指针的表示或第一数字签名进行解密；以及(v)输出步骤，包括输出包括以下一个或多个的第一读取结果：(a)在获取步骤中恢

复的第一散列值的表示和第二散列值的表示，(b)匹配输出，该输出指示根据至少一个预先确定的匹配标准，第一散列值是否与所述第二散列值匹配，(c)指示读取失败的输出。

[0047] 如本文所使用的，术语“激励”是指根据对应于PUF的预先确定质询-响应认证方案来创建物理质询并将其应用于PUF。具体地，激励可以包括当将电磁辐射应用于对该特定辐射敏感的PUF时，例如，如果PUF是在其处可以由所述辐射触发生成响应的反斯托克斯效应的UCD，则发射电磁辐射作为根据质询-响应认证方案触发响应的质询。因此，如本文中所使用的，“激励器”是读取器设备的适于创建这种激励并将其施加到PUF的组件。

[0048] 如本文中所使用的，检测由PUF生成的响应是指，例如，通过数字信号携带的相应的数据，物理地检测由PUF作为对根据对应的质询-响应认证方案的质询的反应而生成的响应，并生成表示该响应的数字信号。因此，如本文所用，术语“PUF检测器”是指读取器设备的适于执行检测步骤的组件。特别地，PUF检测器可以包括用于响应于由激励器施加于其的质询而由PUF发射的电磁辐射的接收器。

[0049] 本文所使用的术语“解密方案”是指特定的解密方法(诸如解密算法)和与所述解密方法结合使用的对应的密码密钥的组合，以便解密使用相应的加密方法和密钥加密的信息。

[0050] 本文使用的术语“验证数字签名”是指验证数字签名的原始性的常见方法，特别是包括通过应用假定的发起者的相关公共密钥来读取数字签名，以便检查其是否是原始的，即用所述发起者的相关秘密私有密钥签名的。

[0051] 为了将预先确定的密码散列函数应用于数字信号，散列函数可以特别地作用于整个数字信号，例如，完全数字信号的数据表示，或仅作用于其区别部分，诸如例如(i)根据定义信号的开销部分和有效载荷部分的通信协议来表示的数字信号的有效载荷部分(或其区别子集)，或(ii)落入特定时间框架内(例如，落入在将质询应用到PUF之后开始检测后的定义的时间段)的此类信号的一部分。

[0052] 因此，根据该解决方案的第五方面的读取方法可以有利地用于“读取”包括对应的PUF的标记，并提供“读取”结果作为输出数据，该输出数据可以用于验证标记或者带有标记的物理对象是否已被伪造或篡改。特别地，该方法可以用于根据该解决方案的第一方面，例如根据在此描述的其实施例或变体中的任何一个或多个，来“读取”复合安全标记。因此，读取方法可以形成总体解决方案的一部分，该总体解决方案提供附加的安全级别，从而形成保护物理对象以防伪造和篡改的改进方式。此外，在数据签名本身已经在标记中表示了的情况下，即如果不需要指针通过通信链接(诸如因特网或其他网络连接)从远程位置访问它，则该方法甚至不会需要与这样的通信链路的任何连接，并且因此可以在“离线”模式下使用，例如在现场(至少暂时)没有通信链路的位置使用。但是，如果这样的通信链路可用，则可选地，还可以替代前面的“离线”模式或除了前面的“离线”模式以外，使用“在线”模式，该模式涉及指向数字签名的指针的表示并从指针指示的位置访问数字签名。

[0053] 根据优选实施例，在处理步骤中生成数字信号，使得该数字信号表示响应的至少一个PUF特定的区别属性，该区别属性在检测到响应的环境条件的变化下至少基本不变。举例来说，这种变化的环境条件可以是PUF在被读取器设备检测到期间通常暴露于的环境的光照条件、温度、气压或其他参数或属性。该实施例的优点在于，读取方法和所使用的读取器设备关于其正确读取包括对应PUF的标记的能力的增加的鲁棒性。这使得在一方面在伪

造的或篡改的标记与带有这种标记的物理对象之间以及另一方面在未被伪造或篡改的标记/对象之间实现甚至更加可靠的区分。

[0054] 根据另一优选实施例，在检测步骤中检测响应包括：检测由PUF作为反应于质询的响应而发射的电磁辐射的至少一个属性，并生成数字信号使得其表示该响应。这尤其允许无接触地无线读取包含PUF的标记。这样的读取方法和相应的读取设备可以特别有利地用于检测非常小的PUF或嵌入在标记/对象的表面下或者其中标记或带有标记的物理对象对机械或化学冲击非常敏感的PUF的响应，该机械或化学冲击通常与基于接触的读取方法一起进行。

[0055] 具体地，根据另一个且相关的实施例，在检测步骤中检测响应包括：检测响应中发生的作为由PUF发射的电磁辐射的属性的发光效应的特性寿命。因此，检测步骤可以特别地包括：在对应的PUF的激励之后在不同的后续时间点检测发光辐射，以便例如，从检测到的辐射中导出特性寿命的度量，诸如半衰期或衰减时间的其他度量。因为这种发光效应的特性寿命主要仅是材料特定的，所以它们在大量不同的环境参数下是不变的，因此特别适合于表征对应的PUF的响应，该PUF将这种效应显示为区别属性。

[0056] 根据另一个相关的优选实施例，在检测步骤中检测响应包括：检测所发射的辐射的光谱作为由PUF所发射的电磁辐射的特性。此外，在处理步骤中处理数字信号包括从数字信号中确定以下一项或多项：(i)一个或多个特性特征(例如光谱中的峰、间隙或最小值)的位置(即波长或频率或相关参数)；(ii)表征光谱的一个或多个统计量度(例如均值、中位数、方差、标准偏差或其他统计矩或量度)；(iii)光谱的一个或多个量化光谱值(例如，辐射的强度光谱内的检测到的强度的)；(iv)表示例如针对所选择的离散的波长子集的在光谱中生的允许光谱值的连续或量化范围的光谱条形码。而且，这些变体中的每一个变体可以提供该方法对检测到响应的变化的环境条件的增强的鲁棒性。

[0057] 根据另一优选实施例，输出步骤包括：对包含所生成的第一散列值的数据进行数字签名，并输出所得的数字签名作为读取结果的一部分。以这种方式，该方法可以特别地用于例如在要通过复合安全标记保护的产品的制造或调试过程期间，初始地生成由PUF作为对预先确定的质询-响应认证方案的质询的反应而生成的响应的数字签名，如本文所公开的。特别地，除了PUF之外，所生成的数字签名可以并入这种复合安全标记中。优选地，该方法(例如，输出步骤)进一步包括生成非对称密码系统的公共/私有密钥对，并使用私有密钥来创建所述散列值的所述数字签名，并使所述对应的公共密钥直接或间接地对带有复合安全标记的对象的接收者可用。

[0058] 本文描述的解决方案的第六方面涉及一种用读取器设备读取标记的方法，该标记既包括第一数字签名的加密表示又包括指示可以访问第二数字签名的位置的指针的表示。该标记特别地可以是根据第一方面，优选地根据本文所述的任何一个或多个其实施例的复合安全标记。该方法包括：

[0059] (i)获取步骤，包括：(a)通过基于预先确定的解密方案读取并且解密在标记中的其表示并通过对于其进行验证，来访问所述第一数字签名，所述第一数字签名包括使用其签名的第一散列值，以及(b)通过读取指针的表示并从指针指示的位置获取包括使用其签名的第二散列值的第二数字签名来访问第二数字签名，包括分别基于所述预先确定的解密方案解密指针的表示或所述获取的数字签名，并验证第二数字签名；

[0060] (ii)输出步骤,包括输出包括以下一个或多个的第一读取结果:(a)第一散列值的表示和第二散列值的表示,(b)匹配输出,其指示根据至少一个预先确定的匹配标准,第一散列值是否与第二散列值匹配;(c)指示读取失败的输出。

[0061] 根据该解决方案的第六方面的方法提供了验证标记或带有标记的物理对象是否已被伪造或篡改的另一方式。与第五方面的方法的情况不同,第六方面的方法不需要激励标记中的PUF,并且不需要读取PUF对激励的对应响应。相反,验证基于(i)标记本身中的第一散列值的安全表示与(ii)标记本身中不存在但只能从安全环境(例如,互联网或区块链中的安全服务器)远程访问的第二散列值的比较。如果两个散列值匹配,则有力地指示未发生篡改。为了访问两个散列密钥,需要了解解密方案。该方法具有另一优点:读取器设备不必具有激励和读取来自PUF的响应的能力。因此,如果具有用于读取第一数字签名和指针的表示的传感器(诸如相机)、用于访问由指针指示的位置的通信链路(诸如因特网或其他网络连接)以及使其执行第六方面的所述方法的一个或多个计算机程序,则即使普通个人计算机或个人通信终端(诸如智能电话、平板计算机、便携式计算机甚至台式计算机)也可以用作读取器设备。

[0062] 根据第五和第六方面的方法中的任一个或两个的优选实施例,各个方法的输出步骤还包括以一维或多维条形码的形式输出至少一部分(优选全部)读取结果。这使得能够使用现成的条形码扫描器来进一步处理由输出步骤提供的输出,这在下述情况下特别有利:读取器设备集成在自动化生产线或其他处理线中或与其互动;读取器设备的输出需要由线而不是人类用户处理的算法来进一步处理。

[0063] 根据第五和第六方面的方法中的任一个或两个的另一优选实施例,相应的方法还包括认证步骤,其中,在准许用户在成功认证的情况下进一步操作读取器设备之前,对用户进行认证。通过防止未经授权的用户成功地与读取器设备交互并因此介入本安全解决方案提供的安全链中,这可以有利地用于进一步提高解决方案的安全。此外,这可以用于获取用户身份或其他用户有关信息,这些信息可以用于增加被标记标记的物理对象(尤其是产品)沿供应链流动的透明度。在存在安全问题的情况下,该信息然后可以用于跟踪对整个解决方案所提供的安全的潜在威胁,并识别可能与此类威胁相关的位置或人员。

[0064] 根据第五和第六方面的方法中的任何一个或两个的又一个优选实施例,相应的方法还包括通信步骤,其中,至少一部分读取结果通过通信链路被传送到相对侧。特别地,该通信步骤可以适于通过有线、无线或光通信链路(诸如例如,但不限于基于无线LAN、蓝牙、蜂窝网络或经典的电话线的通信链路)来发送和接收数据。这样的通信链路可以用于各种不同的目的,包括用于向相对侧发送所获取的信息,例如在输出步骤中提供的输出,该相对侧例如可以是中央安全实例,诸如包括中央安全服务器的信任中心,该信任中心可以构成本安全解决方案的组件。

[0065] 此外,根据第五和第六方面的方法中的任何一个或两个的另一个相关实施例,所述相应的通信步骤还包括:通过通信链路捕获安全相关信息并将其发送到预先确定的相对侧。所述相对侧例如可以是在紧接在前的实施例中提到的信任中心。特别地,这种安全相关信息的发送可以随机地发生,或者可以例如被相对侧根据预先确定的触发方案触发或远程地触发。这允许远程监视读取器设备本身的安全状态和/或读取器设备所涉及的安全相关事件。例如,这种安全相关事件例如可以是根据在输出步骤中生成的输出或读取器设备提

供的其他安全相关信息，对已经被伪造或篡改的标记/对象的检测。

[0066] 具体地，根据第五和第六方面的方法中的任一个或两个的相关优选实施例，相应的安全相关信息包括以下一项或多项：(i)表征读取器设备的当前或过去位置的位置信息；(ii)表征或标识读取器设备用户的用户数据；(iii)表征通信链路的网络数据；(iv)表征由读取器设备的至少一个传感器检测到的尝试或实际行为或读取器设备的对应反应的信息(例如，如上所述)；(v)由读取器设备中提供的认证设备生成的认证信息。

[0067] 根据第五和第六方面的方法中的任一个或两个的又一个实施例，相应的方法还包括信息监视步骤，其中，在通过通信链路从相对侧接收的信号中包含的信息中检测安全事件。该步骤尤其使得能够在经授权的相对侧，例如中央安全中心向读取器设备发送包含这种安全事件的信息的情况下，将读取器设备转变为安全模式或者甚至使其去激活，以便避免读取器设备可能对整个安全系统造成的任何负面影响。例如，如果发生了任何损害行为，诸如在读取器设备上进行了未经授权的侵入或固件/软件修改，或者未经授权的人员或在未经授权的位置使用，并且已经将损害行为传送到相对侧或由相对侧以其它方式检测到该损害行为，则可能导致这种负面影响。

[0068] 根据第五和第六方面的方法中的任何一个或两个的另一优选实施例，相应的方法还包括访问监视步骤，其中，借助于一个或多个传感器来检测作为安全事件的以下中的一个或多个，作为安全事件：(i)物理侵入读取器设备的尝试或实际行为，例如打开其外壳；(ii)在本地或远程访问读取器设备的内部控制功能(例如，它的固件、操作系统或应用)的尝试或实际行为，其中，在设备的正常操作过程中，此类访问对设备的用户不可用。具体地，这种尝试的访问可以针对接管读取器设备的功能的控制或对其进行修改。因此，该实施例可以有利地用于进一步提高本安全解决方案的安全方面，并且特别是用于保护读取器设备本身和本文提出的整个解决方案以防未经授权的侵入和篡改。

[0069] 根据第五和第六方面的方法中的任何一个或两个的另一个相关的优选实施例，相应的方法还包括安全防御步骤，其中，作为对检测到安全事件的反应而执行以下安全措施中的一个或多个安全措施：(i)锁定读取器设备，以限制或防止其进一步使用；(ii)自毁读取器设备的至少一个功能部分或破坏其中存储的数据，以防止用户进一步使用或访问该设备；(iii)输出错误消息。特别地，如上所述，安全措施可以被认为是用于使读取器设备转为安全模式或使其去激活的特定措施。

[0070] 根据第五和第六方面的方法中的任何一个或两个的又一个优选实施例，相应的获取步骤还包括：从标记中获取另外的数字签名或指示来源其中可以访问关于标记的特定的另一数字签名的指针。此外，输出步骤还包括：输出所获取的另一数字签名的表示作为第二读取结果。特别地，复合安全标记可以是如本文结合本安全解决方案的第一方面(例如，根据本文所述的优选实施例及其变体)所述的标记，其中，通过标记而被标记的对象是包括一个或多个消费或使用项目及其包装的产品。该实施例使读取器设备除了响应之外还能够获取标记中包括的其他信息，该信息尤其可以是供应链信息。一方面，这既可用于(i)鉴于标记/对象是否已被伪造或篡改而进行检查，以及(ii)读取和输出附加信息，诸如供应链或其他物流信息。而且，然而，使用(i)和(ii)两者的组合可以被用来进一步增加本安全解决方案的安全方面，因为这样的附加信息，像供应链信息，可以用于追溯地标识供应链中涉及的位置或人员，可能已经发生潜在的欺诈以及潜在的相关日期或时间框架。因此，适于执行该

实施例的方法的读取器设备是双重用途或甚至多用途设备，这增加了使用的便利性并减少了读取完全的复合安全标记所需的不同设备的数量。

[0071] 根据第五和第六方面的方法中的任一个或两个的相关优选实施例，相应的第二读取结果包括以下信息中的一个或多个：(i)关于通过读取器设备获取第二数字签名的位置的位置信息；(ii)读取器设备的用户的认证信息；(iii)指示读取器设备获取第二数字签名的时间点的时间和/或日期信息；(iv)被标记所标记的对象的产品标识、序列号和/或批号；(v)被标记所标记的对象的到期日期。

[0072] 根据第五和第六方面的方法中的任何一个或两个的又一个优选实施例，相应的方法还包括存储步骤，其中，第一读取结果被存储在(第一)区块链的区块中或无区块分布式分类账的一个或多个节点中。这使得能够以非常高的数据完整性来安全、可靠地存储读取结果，使得基本上不可能操纵或擦除或以其它方式逐渐减少或丢失此类数据(例如，由于意外或故意删除或由于数据损坏)。因此，完全的阅读历史仍然可用。此外，可以在对区块链可用的访问的任何地方访问所存储的信息。这允许安全且分布式的存储和对所存储的读取结果的访问，例如用于完整性验证的目的，诸如查验如本文所述被标记有复合安全标记的产品的供应商是否实际上是产品的发起者。基于该实施例，标记的对象和标记本身所属的物理世界可以与区块链技术的力量相联系。因此，可以实现诸如产品的物理对象的来源和供应链的高度可追溯性。

[0073] 根据第五和第六方面的方法中的任一个或两个的另一相关优选实施例：(i)相应的存储步骤还包括将第二读取结果至少部分地分别存储到与第一区块链分开的第二区块链的区块中或与第一无区块分布式分类账分开的第二无区块分布式分类账的一个或多个节点；以及(ii)存储第一读取结果包括将表示第一散列值的数据分别存储到第一区块链的区块中或第一无区块分布式分类账的一个或多个节点中。这允许例如在第五方面的方法(第一和第二读取结果的一个是从读取PUF中导出的，一个是从第二数字签名中读取的)的情况下，向各自的区块链或无区块分布式分类账中存储并因此保存第一和第二读取结果，因此提供了结合前一实施例讨论的优点。将不同的区块链或无区块分布式分类账用于两个不同的读取结果进一步提供了以下优势：容易支持用于第二读取结果的现有的(第二)供应链与用于第一读取结果的附加第一供应链的组合。因此，可以容易地启用不同的访问权限，并且区块链、无区块分布式分类账的管理分别可以在不同机构的手中。特别地，该实施例可用于验证是否(i)产品的供应商实际上是其始发者以及(ii)供应链符合预期。

[0074] 根据第五和第六方面的方法中的任一个或两个的另一相关优选实施例，相应的存储步骤还包括：

[0075] (a)如果所述存储步骤与区块链有关：

[0076] 将表示第一散列值的数据存储在第一区块链的区块中还包括：将逻辑上将第一区块链的所述区块映射到第二区块链的对应区块的跨区块链指针存储到第一区块链的所述区块中；以及

[0077] 将表示所述第二散列值的数据存储在第二区块链的区块中还包括：将逻辑上将第二区块链的所述区块映射到第一区块链的对应区块的跨区块链指针存储到第二区块链的区块中；以及

[0078] (b)如果存储步骤与无区块分布式分类账有关：

[0079] 将所述散列值中的至少一个散列值存储在第一无区块分布式分类账的节点中包括:将跨分类账指针存储在第一无区块分布式分类账的节点中,所述跨分类账指针在逻辑上将所述第一无区块分布式分类账的节点映射到第二无区块分布式分类账的对应节点;以及

[0080] 将所述补充信息存储在所述第二无区块分布式分类账的节点中包括:将跨分类账指针存储在第二无区块分布式分类账的节点中针,所述跨账本指针在逻辑上将第二无区块分布式分类账的节点逻辑映射到第一无区块分布式分类账的对应节点。

[0081] 这样,两个区块链或两个无区块分布式账本分别可以通过跨区块链指针或跨分类账指针相互连接,这可以用来进一步提高本安全解决方案可实现的安全级别。特别是,这可用于跟踪在沿着供应链的不同点上篡改或伪造标记的对象的尝试。例如,该实施例允许跟踪这样的尝试的位置和/或时间点,或者在读取器设备处的强制认证的情况下,允许标识与这样的尝试有关的用户。

[0082] 本安全解决方案的第七方面涉及一种用于读取标记的读取器设备,该标记尤其包括根据本解决方案的第一方面的复合安全标记,其中,该读取器设备适于执行本安全解决方案的第五方面或第六方面或两者的方法,优选地,执行根据本文所述的它们各自的实施例和变体中的任何一个或多个的方法。因此,本文分别关于本安全解决方案的第五和第六方面所描述的内容类似地应用于根据该第七方面的读取器设备。

[0083] 具体地,适于执行第五方面的方法的读取器设备可以包括作为功能单元的:(i)被配置为执行激励步骤的激励器;(ii)被配置为执行检测步骤的PUF检测器;(iii)被配置为执行处理步骤的处理设备;(iv)被配置为执行该方法的获取步骤的获取设备;以及,(v)被配置为执行该方法的输出步骤的输出生成器。适于执行第六方面的方法的读取器设备可以包括作为功能单元的以下部分:(i)被配置为执行该方法的获取步骤的获取设备;以及(ii)被配置为执行该方法的输出步骤的输出生成器。

[0084] 根据优选实施例,读取器设备可以进一步包括以下一个或多个:(vi)被配置为执行所述认证步骤的认证设备;(vii)被配置为执行所述通信步骤的通信设备;(viii)被配置为执行所述信息监视步骤的监视设备;(ix)安全设备,其包括至少一个传感器并且被配置为执行所述访问监视步骤;(x)被配置为执行所述安全防御步骤的安全防御布置;(xi)被配置为执行所述存储步骤的区块链存储设备。优选地,组件(i)至(xi)中的两个或更多个可以被组合或集成到读取器设备的多功能组件中。例如,涉及数据的处理的所有组件都可以被组合成或实现集成多功能处理单元。

[0085] 根据另外的优选实施例,读取器设备被集成或以其它方式形成以下一个或多个的组件:手持设备,例如产品或条形码扫描设备;生产、质量控制或调试装备;生产或质量控制或调试线;飞行对象,例如无人机;机器人,例如农业机器人;农业机械。这允许将读取器设备的功能集成到具有附加或更广泛的功能的系统中,特别是以自动化或半自动化的方式。例如,在生产质量控制或调试线的情况下,读取器设备可以集成到线中,使得其自动读取沿着线运行的产品上的标记,尤其是复合安全标记,以便执行相关数据的初始捕获。然后,可以将捕获的数据存储到相关的数据库中,或者与已存储的数据进行比较,以验证生产或调试线分别生产或调试了预期的一组产品。类似地,在诸如物流中心的供应链的一个或多个节点处,这种读取器设备可以被内联地集成到标识和运输系统中,例如,输送机中,以便在

将其运送到供应链中的下一个节点之前，基于其标记自动或半自动(例如在手持设备的情况下)查验并验证产品的真实性。这同样适用于最终节点，即产品的接收者和/或最终用户。

[0086] 根据另一优选实施例，读取器设备是便携式电子通信终端。无限制地，读取器设备例如可以是智能电话或便携式计算机，例如，平板计算机。如果读取器设备适于执行本解决方案的第六方面的方法，即，当不需要读取要读取的标记中的PUF时，则这可以特别地适用。然后可以使用无论如何存在于例如用于蜂窝通信的电子通信终端中的通信能力来建立通信链路。在某些情况下，这种电子通信终端可以替代地或附加地还适于执行本解决方案的第五方面的方法。例如，如果选择了PUF使得其可以被闪光灯激励，例如如果它包含适当的UCD，则终端(例如，智能电话或平板电脑)的闪光灯可以用作被配置为执行激励步骤的激励器。此外，如果使用终端的相机可以检测到PUF作为对由闪光灯提供的激励(质询)的反应而发射的信号，则终端的相机可以用作被配置为执行检测步骤的PUF检测器。相机还可以用作认证设备，该认证设备被配置为结合处理器平台执行所述认证步骤，该处理器平台通常无论如何都存在于这种终端中。处理器平台还可以用作被配置为例如与终端的显示器或声音发生器或其他输出装置一起执行处理步骤和输出步骤的处理设备。此外，终端的通信部分可以用作被配置为执行所述通信步骤等的通信设备。

[0087] 本安全解决方案的第八方面涉及一种包括指令的计算机程序，当该执令在根据第七方面的读取器设备的一个或多个处理器上执行时，使读取器设备执行根据本安全解决方案的第五方面或第六方面或两者的方法。计算机程序可以特别地被加载或以其他方式存储在第七方面的通信终端中，从而使其适应于执行本解决方案的第五方面和第六方面的方法中的一个或两个。

[0088] 该计算机程序可以特别地以数据载体的形式实现，在该数据载体上存储有用于执行方法的一个或多个程序。如果旨在将计算机程序产品作为独立于要在其上执行一个或多个程序的处理器平台的单独产品中的单独产品进行交易，则这可能是有利的。在另一实施方式中，计算机程序产品作为文件提供在数据处理单元上，尤其是在服务器上，并且可以经由数据连接(例如，因特网或专用数据连接(诸如专有或局域网))下载。

附图说明

[0089] 在以下详细描述和附图中提供了本安全解决方案的其他优点、特征和应用，其中：

[0090] 图1示意性地示出了根据本安全解决方案的优选实施例的各种复合安全标记；

[0091] 图2示意性地示出了根据本安全解决方案的优选实施例的多部分物理对象，该对象包括瓶装消费品和相关包装，其中，该对象被标记有根据本安全解决方案的复合安全标记，该复合安全标记包括在瓶子上实现的PUF和在包装上打印的对应数字签名；

[0092] 图3示意性地示出了根据本安全解决方案的优选实施例的另一多部分物理对象，该对象包括作为消耗品的布置在泡罩包装中的一组药物片剂和用于泡罩包装的相关包装，其中，片剂中的每个片剂包含基于UCD的PUF，并且包装包含打印品，该打印品代表与PUF相对应的一组数字签名。

[0093] 图4示出了根据本安全解决方案的优选实施例的导出表示由基于UCD的PUF作为对预先确定的质询-响应认证方案的对应质询而生成的响应的数据的各种不同的方式；

[0094] 图5示出了根据本安全解决方案的优选实施例的用复合安全标记来标记物理对象

的基本方法的流程图。

[0095] 图6示意性地示出了根据本安全解决方案的优选实施例的用于执行图5的方法的装置。

[0096] 图7A和图7B示出了流程图，该流程图示出了根据本安全解决方案的优选实施例的利用读取器设备读取包括PUF的标记(诸如图1的复合安全标记)的方法的第一实施例；

[0097] 图7A和图7C示出了流程图，该流程图示出了根据本安全解决方案的优选实施例的利用读取器设备读取包括PUF的标记(诸如图1的复合安全标记)的方法的第二实施例；

[0098] 图8A和8B示出了流程图，该流程图示出了根据本安全解决方案的另一个优选实施例的、利用读取器设备读取诸如图1的复合安全标记的标记的方法，该方法不需要作为读取过程的一部分的读取PUF；

[0099] 图9示意性地示出了根据本安全解决方案的优选实施例的读取器设备。

[0100] 图10是根据本安全解决方案的优选实施例的示意图；以及

[0101] 图11示意性地示出了根据本安全解决方案的优选实施例的一组两个交叉连接的区块链沿着被标记有复合安全标记的产品的供应链的演变。

[0102] 在附图中，相同的附图标记用于本文描述的解决方案的相同或相互对应的元件。

具体实施方式

[0103] A.复合安全标记

[0104] 图1示出了根据本安全解决方案的优选实施例的用于物理对象尤其是产品的复合安全标记1的六个不同变体(a)-(f)。这些复合安全标记1中的每一个复合安全标记1都包括PUF 2和数字签名3的加密表示，该数字签名3对散列值进行数字签名，该散列值是从表示从PUF接收到的回应与预先确定的质询-响应认证方案相对应的质询的响应的数据导出的。因此，PUF 2和数字签名3是相关的并且彼此对应。数字签名3是在非对称密码系统的公共密钥/私有密钥对的私有密钥的帮助下创建的。成功解密它后，可以在非对称密码系统的对应公共密钥的帮助下对其进行读取，以便验证数字签名的真实性，并且从而验证使用它标记的物理对象的真实性。数字签名的加密可以基于任何合适的对称或非对称密码系统，例如AES或RSA。

[0105] 基于其性质，PUF 2可以被认为是唯一的(因此是“不可克隆的”)，就像它对质询的响应那样。相应地，由于密码散列函数的抗冲突的单向性质，从响应中导出的散列值也是唯一的，并且因此仅关于与该确切的PUF 2，因为实际上不可能通过将所述散列函数应用于不同的PUF的响应来具有相同的散列值，并且如果PUF也必须同时出现在相同的位置(空间和时间重合)，则更是如此。

[0106] 因此，这种复合安全标记1即使不是不可能的，也很难假冒，因此可以用来保护诸如产品和其他商品的物理对象，特别是防伪造和篡改。

[0107] 图1(a)示出了这种复合安全标记1的第一变体，其中，PUF 2被实现为复合安全标记1的表面上的区域，该区域包含已经在其材料中的UCD的混合，或其具有包含涂覆材料或油墨的一个或多个附加层，该涂覆材料或油墨包含此类UCD的混合。加密的数字签名3由二维条形码(诸如QR码)表示。

[0108] 图1(b)示出了另一变体，其中，PUF 2以大量(例如10^6个或更多个)光反射微观粒

子的随机分布的形式被实现为微结构，当用特定波长的相干激光光照亮作为质询时，光反射微观粒子借助于干涉创建特性斑点图案。可以用诸如合适的数码相机的光学传感器来检测该图案，以便生成表示响应的数据，例如作为数字图像文件。

[0109] 图1(c)示出了又一个变体，其中，PUF 2由包含隐藏的相位编码或频率编码的信息的全息图来实现。当用特定波长的相干激光光照亮作为质询时，全息图生成虚拟的全息图像，可以在一个或多个光学传感器和合适的图像处理算法的帮助下根据质询-响应认证方案从该虚拟的全息图像中提取隐藏的信息作为响应。在该变体中，数字签名3示例性地借助于RFID芯片来实现，该RFID芯片被配置为在被激活时发射表示加密的数字签名3的信号。

[0110] 图1(d)示出了又一个变体，其中，PUF 2是借助于使用包含不同类型的UCD的混合的油墨打印的图像来实现的。可选地，此外，隐藏的信息可以隐匿地嵌入在图像中。例如，可以人工创建最小的特定颜色变化，这些变化对于人眼是不可见的，但是用来编码这种信息，并且可以使用合适的光学传感器结合相应的分析算法进行检测。在该变体中，加密的数字签名3示例性地被实现为数字串。

[0111] 图1(e)示出了另一个变体，其中，PUF 2和加密的数字签名3两者借助于使用包含不同类型的UCD的混合的油墨打印的条形码图像被实现为集成组合。条形码对加密的数字签名3进行编码，而油墨材料表示PUF 2。这允许复合安全标记1的实现极为紧凑。

[0112] 图1(f)示出了另一个变体，其中，与图1(e)一样，PUF 2和加密的数字签名3两者借助于使用包含不同类型的UCD的混合的油墨打印的条形码图像被实现为集成组合。然而，与图1(e)不同，条形码不对加密的数字签名3本身进行编码。替代地，它对指针4进行编码，该指针指示在哪里可以从不是复合安全标记1本身的一部分的地方访问实际数字签名3。优选地，该指针4是例如服务器的互联网地址的表示，数字签名3可以从该互联网地址下载或以其它方式访问。在此，用所述加密系统加密数字签名3或指针4或两者。再次，这允许复合安全标记1的极其复杂的实现，并且此外允许集中管理、存储和提供多个复合安全标记1的相应数字签名3，例如关于给定制造商的特定系列产品的数字签名3。

[0113] 图2示出了根据本安全解决方案的优选实施例的多部分物理对象。该对象包括：消耗品6，诸如包含在容器尤其是瓶子5中的液体药物；以及，相关的包装7。复合安全标记1在不同的基底上被分为两部分。作为复合安全标记1的第一部分，PUF 2被放置在瓶子5上。PUF 2的类型可以是本文所述的任何类型的PUF，特别是如上面结合图1所述的。复合安全标记1的第二部分包括条形码，该条形码表示与PUF 2相对应并且被打印在包装7上的加密的数字签名3。如上所述，因为PUF 2和加密的数字签名3相互连接，因此，可以借助于识别在根据预先确定的质询-响应认证方案作为对相关质询的反应而接收到的响应中导出的散列值和包含在加密的数字签名3中并且通过加密的数字签名3进行密码保护的散列值之间的不匹配，来检测通过更换包装7或瓶子5而进行的任何伪造。

[0114] 图3示出了根据本安全解决方案的进一步的优选实施例的另一多部分物理对象。在此，要保护的产品是包含在一组泡罩包装9中的药物片剂(药丸)8。片剂中的每个片剂包含一种类型的UCD的混合，其在吞服时不会对哺乳动物，特别是对人体造成有害影响。对于所有片剂或者可替选的，甚至每个片剂的个体或其子集，UCD的混合可以相同。如图2中，包装7形成要保护的物理对象的第二部分，并带有对应于包含在片剂8中的一个或多个PUF 2的数字签名3。以这种方式，当PUF 2是消耗品本身不可分割的一部分时，与根据图2的情况

相比，安全的级别可以进一步增强，在这种情况下，仅用于消耗品的容器5正带有PUF 2。

[0115] 图4示出了导出表示由基于UCD的PUF 2作为对预先确定的质询-响应认证方案的相应质询而生成的响应的数据的各种不同的方式(a)-(c)。特别地，质询可能包括通过具有特定属性(例如具有某一波长范围或光谱，诸如电磁光谱的红外线或紫外线部分中的特定光谱组分)的电磁辐射来照射PUF 2。

[0116] 图4(a)示出了第一变体，其中，由PUF 2响应于质询发射的光的强度I的光谱I(λ)被检测为波长λ的函数。特别地，可以借助于光谱分析或者甚至简单地通过使用足够的强度阈值来识别发生光谱I(λ)的峰的所选择的波长λ_1、λ_2、λ_3、…。举例来说，但不限于，该信息然后可以由数据串F表示，该数据串F以简单的形式仅表示相应的波长λ_1、λ_2、λ_3等的值。在增强的版本中、如图4(a)右侧所示，这些波长的对应的强度值I_1、I_2和I_3等包括在F中。可替选地或附加地，光谱I(λ)的其他特性可以由F来识别和表示。数据串F特别地可以是由一系列比特组成的二进制数。此外，数据串F可以被解释为“光谱条形码”，该“光谱条形码”表示光谱I(λ)的真实特征，特别是在其如图4(a)的右侧上示出的图形表示中。在该变体中，强度值I是模拟值，即它们可以具有可以由数据串F表示的任何值。

[0117] 图4(b)示出了另一变体，其与图4(a)的变体类似，不同之处在于强度值I被量化并且可以仅采用三个可能的值中的一个，在该示例中，这三个可能的值是适当强度单位的赋范的(normed)值“0”、“1/2”和“1”。该变体可以有利地用于创建用数据串F表示光谱的特别健壮的方式，因为由于量化，所得的数据串F的量化对由测量本身的缺陷引起的检测值I的变化不太敏感。图4(a)和4(b)中所示的变体的数据串F各自形成光谱条形码的实现。

[0118] 图4(c)示出了另一变体，其中，作为对质询的响应从PUF发射的发光(优选荧光)的强度I(t,λ)被检测为时间t和波长λ的函数。确定特性寿命T＝T(λ)，其例如可以对应于波长λ的发光光的半衰期$T_{1/2}$。对应的数据串F可以再次被形成为响应的表示。特别地，数据串F可以包括特性寿命$T_i(\lambda)$和一组不同波长的相关波长λ_i，i＝1、2，…，该相关波长优选是检测到光谱I(λ)的峰的那些波长。

[0119] 尽管为了简单说明，已经使用一维数据串F作为响应的表示描述了上述示例，但是其他形式的数据表示(特别是多维形式，诸如矩阵)也是可能的。

[0120] B.为物理对象提供复合安全标记

[0121] 在图5和6中示出根据本安全解决方案的用于向物理对象提供复合安全标记的方法和示例性装置。

[0122] 具体地，图5是示出了用复合安全标记来标记物理对象的基本方法的流程图。图6示意性地示出了根据涉及加法制造过程(3-D打印)的优选实施例的用于执行图5的方法的装置17。装置17包括3-D打印机12、PUF扫描仪14、处理设备15和条形码打印机16。此外，装置17还可以包括用于原材料的容器11和用于将从供应10提供的UCD与3D打印原材料混合的装置(未画出)。可选地，这些组件10至16中的一些或全部可以集成到同一设备中。

[0123] 在该方法的第一步骤S5-1中，将PUF 2(可选地，多个不同的PUF)添加到要标记的物理对象，该物理对象可以例如是但不限于图3和4中所示的药品中的一个，或者备件、播种材料等，如上面发明内容部分中已讨论过的。在图6的装置17的情况下，物理对象通常将是可以被3D打印的固体对象。在这种情况下，步骤S5-1可以包括将一种或多种类型的UCD(优选地，UCD的秘密混合)添加到包含适于3D打印的、例如以粉末形式的原材料的容器11中。将

UCD和原材料混合，然后将所得的材料混合作为3-D打印材料提供给3-D打印机12。在3-D打印机12的帮助下，根据借助于相应设计文件传递给3-D打印机12的产品设计规范来打印产品13，例如网格形式的医疗设备。由于在打印前已将UCD混合到原材料中，因此所得到的产品13并入了这些UCD，这些UCD共同形成一个或多个PUF 2。

[0124] 在另一步骤S5-2中，将由步骤S5-1得到的产品13暴露于由PUF扫描仪14以波长的电磁辐射的形式发射的质询C，该波长分别对应于关于并入到产品13中的PUF 2的预先确定的质询-响应认证方案的波长范围。在另一个步骤S5-3(通常与步骤S5-2基本同时发生)中，PUF扫描器14检测到由并入到产品13中的PUF 2作为对质询C的反应而发射的响应R。然后将该响应转变为表示它的数据串F，例如上面结合图4所述。特别地，但不限于，如图所示，数据串F可以是二进制串。如果存在两个或更多个PUF 2，则数据串F可以特别表示所有这些PUF2的单独响应，也可以可选地将其解释为包括所有单独PUF的组合PUF的组合单个响应。

[0125] 在另一步骤S5-4中，将数据串F作为输入提供给处理设备15，该处理设备将预先确定的密码散列函数H(...)应用于数据串F，以便生成表示响应R的散列值H＝H(F)。在另一个步骤S5-5中，在处理设备15的帮助下，用诸如众所周知的RSA方案的非对称密码系统的公共/私有密钥对的私有密钥对所得的散列值H进行数字签名，以便生成包括散列值H本身及其数字签名版本S[H(F)]的数字签名。然后，在另一个步骤5-6中，用例如RSA或AES的适当的密码方案及其各自的密钥对所生成的数字签名进行加密，以获得加密的数字签名3。

[0126] 在另一个步骤S5-7a中，使用条形码打印机16，将加密的数字签名3以二维条形码(例如QR码或DATAMATRIX码)的形式打印到产品13的表面。结果，成品13现在包括PUF 2和对应的加密的数字签名(3)两者，并且因此包括根据本安全解决方案的完全的复合安全标记1。

[0127] 在替代变体中，代替步骤S5-7a，执行另一步骤S5-7b。步骤S5-7b类似于步骤S5-7a，除了代替加密的数字签名3本身之外，在产品13上仅打印指针4，该指针4指示在何处可以访问加密的数字签名3，例如在数据库或在互联网服务器处。在步骤S5-7b之前、同时或之后，执行另一个步骤S5-8，其中，由处理设备通过数据链路将在步骤S5-6中获得的加密的数字签名3存储到指针4指示的位置，以用于以后访问。根据另一相关变体(未示出)，步骤5-6包括代替数字签名或除数字签名之外对指针进行加密，并且步骤S5-7b因此包括将加密指针的表示添加到要标记的物理对象。因此，在指针可以用来访问存储在指针所指的位置处的数字签名之前，首先需要对指针进行解密，这需要了解相应的解密方案和密钥。

[0128] 在变体S5-7a和S5-7b两者中，代替或除了打印之外，可以以电子表示的形式，分别添加(可选地加密的)指针4的加密的数字签名3的表示，电子表示例如是被布置为在接收到相应的触发信号之后发射携带所述表示的信号(参见图1(c))的RFID芯片。

[0129] C.标记的读取

[0130] 现在结合相应的图7A至图9描述包括PUF的标记的读取，特别是根据本安全解决方案的第一方面的复合安全标记的读取，例如如结合图1所示和所述。

[0131] 图7A和7B一起示出了流程图(被分成经由连接器“A”连接的两个部分)，该流程图示出了利用读取器设备读取包括PUF的标记(诸如图1的复合安全标记)的方法的实施例。该方法可选地包括第一阶段，该第一阶段包括步骤S7-1至S7-7，这些步骤用于增强执行该方法的读取器设备本身的安全。

[0132] 步骤S7-1是访问监视步骤，其中，评估传感器输出，以便作为安全事件检测物理侵入读取器设备的尝试或实际行为，或者本地或远程访问读取器设备的内部控制功能(例如处理设备或通信设备)的尝试或实际行为。如果在另一个步骤S7-2中确定在步骤S7-1中检测到安全事件(S7-2;是)，则该方法执行安全防御步骤S7-5，其中，指示安全事件的错误消息在用户接口上输出和/或通过通信链路发送到相对侧，例如预先确定的信任中心。此外，读取器设备可以被锁定和/或读取器设备或至少存储在其中的数据可以被自毁，以便避免对读取器设备的数据或任何功能的未授权的访问。否则(S7-2;否)，该方法继续进行到信息监视步骤S7-3。

[0133] 在信息监视步骤S7-3中，通过通信链路从安全解决方案的中央机构(诸如提供安全服务器的信任中心)接收信号，并对信号进行评估以便检测是否通过信号中包含的信息来指示安全事件。如果在另一步骤S7-4中确定在步骤S7-3在信息中指示了安全事件(S7-4;是)，则该方法前进到并执行作为最后步骤的安全防御步骤S7-5。否则(S7-4;否)，该方法继续进行到认证步骤S7-5。

[0134] 在认证步骤S7-6中，例如，经由适当的用户接口(诸如用于输入密码的键盘或指纹传感器等)对读取器设备的用户进行认证。如果在另一个步骤S7-7中确定步骤S7-6的认证失败(S7-7;否)，则该方法返回到步骤S7-1，或者可替选地，返回到认证步骤S7-6(未示出)。否则(S7-7;是)，该方法继续进行到第二阶段，在第二阶段中读取标记，并且输出读取结果。

[0135] 该第二阶段包括激励步骤S7-8，其中，根据与包括在标记中的PUF相对应的预先确定的质询-响应方案的物理质询被创建并且被应用于PUF，该PUF可能包含例如不同UCD的混合。

[0136] 在激励步骤S7-8之后或与其同时，执行检测步骤S7-9，其中，检测由PUF作为对物理质询的反应并且根据质询-响应认证方案而生成的响应，并生成表示响应的数字信号，并且该数字信号例如可以采取光谱条形码的形式或包括光谱条形码。

[0137] 在随后的处理步骤S7-10中，处理数字信号以便通过将预先确定的密码散列函数应用于数字信号来生成响应的散列值。可选地，处理步骤可以进一步包括对所述散列值进行数字签名以便提供其(第一)数字签名。

[0138] 处理步骤S7-10之后是输出步骤S7-14，其中，例如在读取器设备的用户接口上或在读取器设备的电子或光学接口处提供的数据流或文件中输出(第一)读取结果。(第一)读取结果包括表示在处理步骤中生成的散列值的数据和/或所述(第一)数字签名的表示。因此，该方法可以用于读取包括PUF的标记，特别是复合安全标记，如本文所公开的(例如，图1中)，并且输出基于由PUF生成的响应的对应的读取结果。图7A和7B的方法对于在将用相应的复合安全标记被标记的产品发送到供应链之前，在制造场所或物流场所初始读取PUF以获得(第一)散列值和/或其数字签名是特别有用的。

[0139] 图7C(结合图7A)示出了另一种读取标记的方法的实施例，该方法特别适合于“在现场”，即在产品的供应链的一个或多个节点处使用，该方法包括：与图7A和7B的方法相同的步骤S1至S9，并且因此在图7A中再次示出了该方法的第一部分。该方法还包括与图7B的方法类似的处理步骤S7-10和附加获取步骤S7-11，该附加获取步骤S7-11包括访问所述第一数字签名以从中恢复包含在其中的第二散列值。这是通过基于预先确定的解密方案(如果有的话)读取和解密标记中第一数字签名的表示，和/或通过读取标记中相应指针的表示

并从指针所指示的位置获取第一数字签名，包括分别根据解密方案(即，取决于哪个被加密了)解密指针的表示或获取的数字签名(即，假定为这种数字签名的信息)来实现的。另外，在图7A和7C的实施例中，获取步骤还包括从标记中获取第二数字签名或指示可以例如从远程服务器访问这种第二数字签名的来源的指针。作为第二读取结果，分别从标记或所述来源读取第二数字签名。另外，匹配标志被初始化(未设置)。验证第一获取的数字签名和第二获取的数字签名两者，以确认其原始性，或者以其它方式检测伪造或其他未经授权的操纵。可以在处理步骤S7-10之前、同时或之后执行获取步骤S7-11。

[0140] 在随后的匹配步骤S7-12中，根据预先确定的比较方案比较第一和第二散列值，该比较方案可以特别是两个散列值的所有对应数字的简单相等性测试，但是其他比较方案也是可能的。如果两个散列值匹配(S7-12；是)并且验证成功，则设置匹配标志(步骤S7-13)，否则(S7-12；否)不设置匹配标志。当然，使用这种匹配标志只是确定和传送两个散列值是否匹配的许多不同的可能的实现方式中的一个。

[0141] 该方法还包括输出步骤S7-14，其中，例如在读取器设备的用户接口上或在诸如读取器设备的电子或光学接口的接口处提供的数据流或文件中输出第一和第二读取结果。特别地，第一读取结果包括以下一个或多个：(a)第一散列值的表示和第二散列值的表示，(b)指示(i)如果设置了标志则匹配以及(ii)否则不匹配的匹配输出；(c)如果读取步骤或数字签名验证中的至少一个失败，则指示读取失败的输出。第二读取结果包括所读取的(进一步的)数字签名的表示，即，用其签名的全部或一部分的信息的表示，例如作为条形码。相应地，该方法还可以用于读取包括PUF的标记，特别是复合安全标记，如本文所公开的(例如，图1)，并输出基于PUF生成的响应的对应(第一)读取结果。

[0142] 输出的读取结果可用于现场(例如，在沿着被标记的产品的供应链上的各个节点)，或者甚至最初在制作或调试场所，当对物理对象进行初始标记时的验证的目的，以便验证标记并且以便捕获其响应以用于将来使用，例如用于将其存储在数据库中以用于后续认证目的。第二读取结果可以特别地用于在沿着供应链的点处跟踪和追踪标记的产品的流动，其中，读取器设备基于图7A和7C的方法来读取标记。

[0143] 该方法还包括存储步骤S7-15，该存储步骤S7-15优选地在输出步骤S7-14之后或同时执行。在存储步骤S7-15中，将包括表示第一散列值的数据的第一读取结果存储在第一区块链的区块中，并将在获取步骤S7-11中获得的第二读取结果存储在第二分开的区块链的区块中。此外，将连接两个区块链的相关跨区块链指针存储在两个区块链中的每个区块链中，以指示区块链中的每个区块链中的区块，这些区块在它们包含在同一读取事件中创建和存储的数据的意义上彼此对应。特别是，第二区块链可能与供应链信息(诸如，时间、位置和当前读取事件的用户标识)有关。另一方面，第一区块链用于跟踪认证信息，特别是，在当前读取事件中，带有标记的物理对象是否已被成功认证为原始的(即未被伪造或篡改)。

[0144] 此外，该方法可以包括通信步骤S7-16，其中，通过通信链路向预先确定的中央服务器发送在输出步骤中输出的数据，包括匹配的输出，以及可选地还包括时间戳和/或读取事件各自的读取器设备的当前位置(其中每个可以被认为是安全相关信息)，该中央服务器例如可以形成信任中心的一部分。

[0145] 图8A和8B一起示出了流程图(被分成经由连接器“C”连接的两个部分)，该流程图示出了利用读取器设备读取诸如图1的复合安全标记的标记的另一种方法的实施例。在此，

标记需要既包括第一数字签名的加密表示和指示可以访问第二数字签名的位置的指针的表示。与图7A和7B或7C的实施例不同，该实施例不需要(尽管不排除其选择)读取PUF作为读取过程的一部分。可选地，该方法可以包括类似的第一阶段，该第一阶段包括步骤S8-1至S8-7(其对应于图7A的步骤S7-1至S7-7)，用于增强读取器设备自身的安全。

[0146] 该方法还包括获取步骤S8-8，其中，从标记中获取包括在标记中的第一数字签名，其中，第一数字签名包括使用其签名的第一散列值。此外，通过从标记中获取指示可以访问第二数字签名的来源(例如，从远程服务器)所述指针来访问关于该标记的第二数字签名。从所述来源读取第二数字签名，并且初始化匹配标志(未设置)。此外，两个数字签名都被验证。

[0147] 在随后的匹配步骤S8-9中，比较第一散列值和第二散列值，第一散列值通过获取的第一数字签名来签名并包括在第一数字签名中，第二散列值通过获取的第二数字签名来签名并包括在第二数字签名中。如果两个散列值匹配(S8-9;是)并且验证成功，则设置匹配标志(步骤S8-10)，否则(S8-9;否)不设置匹配标志。当然，使用这种匹配标志只是确定和传送两个散列值是否匹配的许多不同的可能的实现方式中的一个。

[0148] 该方法还包括输出步骤S8-11、可选的存储步骤S8-12和可选的通信步骤S8-13。这些步骤可以特别地类似于图7B的对应步骤S7-14至S7-16，使得以上结合图7A和7B的方法提供的对应说明也分别应用于步骤8-11至8-13。因此，该方法也可以用于读取标记，特别是如本文公开的复合安全标记(例如，在图1中)。再次，读取结果可以特别用于现场(例如，在沿着被标记的产品的供应链的各个节点处)的认证目的以及用于沿着供应链跟踪和追踪被标记的产品。因为图8A和8B的方法不需要读取PUF，它特别适合由包括适当传感器(诸如摄像头)的通用便携式电子通信终端(诸如智能电话或便携式计算机，例如平板计算机)的形式的读取器设备来实现以读取标记。

[0149] 图9示意性地示出了根据本发明的优选实施例的读取器设备20。特别地，读取器设备可以适于执行图7A和7B或7C的方法。举例来说，并且在没有限制的情况下，读取器设备20可以形成制造线或调试线的组件或与其结合使用，该制造线或调试线在图9中通过输送机31示出，在该输送机上物理对象32(即产品，每个都带有本文(例如图1)中公开的复合安全标记)被运输到读取器设备20或从读取器设备20运输。

[0150] 读取器设备20可以包括各种不同的组件21至30，它们通过数据总线33或任何其他适当的通信技术可通信地互连。特别地，读取器设备20包括：激励器21，该激励器21适于根据预先确定的质询-响应认证方案生成激励并将该激励施加到在输送机31上经过的产品32上的复合安全标记1；以及，相应的PUF检测器22，该PUF检测器22适于检测由标记的PUF作为对激励的反应而发射的响应。例如，如果PUF包括不同UCD的混合，则激励器21可以适于容许适当的电磁辐射，以便激励PUF中的UCD以重新发射作为标记的特定PUF的特性的电磁辐射。因此，在这种情况下，PUF检测器适于检测这种重新发射的辐射并对其进行光谱分析，以便导出例如以光谱条形码的形式的数字信号，该数字信号表示响应并且可以进一步被处理。

[0151] 此外，读取器设备20可以包括获取设备23，该获取设备23适于获取包括在标记中的第一数字签名。特别地，获取设备23可以适于执行类似于图7C的步骤S7-11的步骤。

[0152] 另外，读取器设备20可以包括通信设备24，该通信设备24适于经由通信链路与相对侧34(例如，信任中心的中央安全服务器)通信。特别地，通信链路可以被实现为无线链

路，在这种情况下，通信设备通常将包括或连接到天线24a，或者该链路可以通过诸如电气电缆或光缆的电缆被实现为非无线通信链路24b。特别地，读取器设备20可以被配置为通过通信链路发送要在输出步骤(例如，如图7B的步骤S7-14中那样)中输出的读取结果，以便通知相对侧34读取结果和/或其他信息，诸如安全相关信息(例如，读取器设备20处安全事件的发生)。

[0153] 为了进一步增加安全，读取器设备20还可以包括认证设备25，该认证设备25适于在准许访问读取器设备20和/或其进一步使用之前(诸如在图7A的步骤S7-6和步骤S7-7中)，对读取器设备20的用户进行认证。

[0154] 读取器设备20还可以包括安全设备26，该安全设备26包括一个或多个传感器，该一个或多个传感器用于检测安全事件，诸如物理侵入读取器设备20的尝试或实际行为，或者未经授权的情况下本地或远程访问读取器设备20的内部控制功能的尝试或实际行为。优选地，安全设备26与安全防御装置27交互或进一步包括安全防御布置27，以在检测到安全事件的情况下保护读取器设备20。特别地，安全防御布置27可以适于执行类似于图7A的步骤S7-5的步骤。例如，安全防御装置27可以被配置为在检测到安全事件的情况下锁定读取器设备20的用户接口，或者激活读取器设备20中包含的安全芯片的自毁，以便保护存储在其中的数据，例如包括私有密钥或其他安全相关数据，诸如认证数据。除了安全设备26之外或替代安全设备26，读取器设备20可以包括监视设备28，该监视设备28被配置为检测在通过所述通信链路从相对侧34接收到的信号中所包含的信息中指示的安全事件。例如，如果诸如信任中心的这种相对侧34了解到攻击例如沿着给定的供应链在现场分布的读取器设备20的安全和完整性的更广泛的尝试，则这种信号可用于主动触发(至少暂时地)阻止读取器设备20在现场的任何进一步使用，以防止此类攻击篡改读取器设备20。

[0155] 此外，读取器设备20包括处理设备29，该处理设备29特别地适合于例如通过在其上运行的相应软件程序来处理由PUF检测器生成的数字信号，以便通过将预先确定的密码散列函数应用于数字信号来生成PUF的响应的散列值(参见图7B或7C的步骤S7-10)。在一些实施方式中，可以由处理设备29附加地实现读取器设备20的涉及数据处理或控制的其他功能。因此，读取器设备20的其他组件21至28和30的任何处理功能的全部或部分可以被并入到处理设备29中，而不是在单独的组件中实现。

[0156] 读取器设备还可以包括适于将数据存储在一个或多个区块链中的区块链存储设备，读取器设备20可以经由所述通信链路连接到该一个或多个区块链中。特别地，所述数据可以对应于当读取器设备用于读取包括PUF的标记时生成的读取结果。尽管区块链存储设备可以被实现为读取器设备20的单独的组件或模块，但是其优选地包括在处理设备29中，如图9所示。

[0157] 输出生成器30形成读取器设备20的另一组件。其被配置为例如在用户接口或另一接口(诸如电子或光学接口)上输出表示生成的散列值作为第一读取结果的数据、获取的数字签名(诸如上面讨论(参见图7B的步骤S7-14)的第一数字签名和第二数字签名)的表示和可选的匹配输出，该匹配输出指示处理步骤(参见图7B或7C的步骤S7-10)得到的散列值和获取步骤(参见图7C的步骤S7-11)得到的散列值是否匹配(参见图7C的步骤S7-12)。

[0158] D.整体安全解决方案

[0159] 如上所述，图10和11示出了基于包括PUF的标记的使用以及在一个或多个读取器

设备上的整体安全解决方案的进一步优选方面。特别地，图10示出了基于本安全解决方案的安全系统14的基本实施例的示意性概图，该安全解决方案允许在参与供应链的接收者B处验证被复合安全标记1(例如根据图1)所标记的产品是否是原始的，并且实际上是由位于供应链上游的推测原始制造商A提供的。

[0160] 为此，制造商A配备了一种装置，该装置用于将复合安全标记1应用于随后沿着供应链运送的产品32。例如，这样的装置可以是类似于图6所示的装置的装置。可替选地，制造商A可以配备有读取器设备20，诸如图9中所示的一个，并且使用单独的装置来应用对应的复合安全标记1，该复合安全标记1携带有由读取器设备20读取的信息，该信息包括(第一)数字签名，该(第一)数字签名包括从读取复合安全标记1中的PUF中导出的(第一)散列值。因此，装置17和20分别被配置为执行图5以及图7A和7B(和/或7C)的对应方法。另外，装置17或20被配备来生成非对称密码系统的公共/私有密钥对，将私有密钥(安全密钥，SK)分别存储在装置17和20的安全存储空间中，并向位于由受信任的第三方所接纳(entertained)的信任中心中的中央安全服务器34转发公共密钥(PUK)和第一数字签名以及可选的其他安全相关信息(诸如生成第一数字签名的时间和/或位置)。因此，信任中心充当注册机构的角色，其中，一个或多个装置17和读取器设备20的特定公共密钥被注册和存储。优选地，去往和来自信任中心的任何通信都受到加密的保护，特别是为了防止“中间人攻击”。

[0161] 为了增加可用的安全级别，可以将公共密钥提供给公共密钥基础设施(PKI)的证书颁发机构，特别是提供给相关的证书颁发机构服务器42，其中，对公共密钥进行证实并将其包括在制造商A和验证机构(服务器)41可用的密码证书中。现在，供应链中配备有此处所述的读取器设备20的任何其他节点(诸如接收者B)都可以从验证机构41请求证书以将其用于检查据称源自制造商A的标记的产品的真实性。为此，接收者B处的读取器设备20运行图7A和图7B(或图7C)的方法，并且从而检测产品32的复合安全标记1上的PUF，并读取其中包含的第一数字签名，该第一数字签名包括要与从检测到的PUF的响应导出的(第一)散列值进行比较的(第二)散列值。如果两个散列值匹配，则这确认制造商A实际上是产品32的发起者，否则该产品或其标记已被伪造或以其它方式篡改。

[0162] 该比较的结果，即匹配结果和可选的其他安全相关信息(诸如检查的时间和位置和/或进行检查的读取器设备20的用户的身份)，都被转发给并存储在信任中心的中央安全服务器34上。这允许对供应链的集中监视，并尽早识别沿着供应链发生的任何伪造或篡改问题。中央安全服务器34还可被配置为基于供应链中涉及的任何读取器设备20提供的匹配结果和安全相关信息，经由数据接口API生成跟踪和追踪数据或合并跟踪和追踪数据以及使得跟踪和追踪数据可用，该跟踪和追踪数据反映沿供应链的产品32的处理。

[0163] 图11涉及本安全解决方案，特别是安全系统40的另一优选实施例，其中，使用了区块链技术，以便安全地存储和使得沿着供应链生成的认证数据可用。具体地，图11示意性地示出了根据本安全解决方案的优选实施例的、与被标有复合安全标记1的产品32的供应链平行的一组两个交叉连接的区块链的演变。特别地，图10和图11的实施例可以在单个解决方案中组合。

[0164] 图11的解决方案包括第一区块链BC-PUF，该第一区块链BC-PUF被配置为安全地存储认证信息并使认证信息可用，该认证信息特别是从检测如本文所述的相关产品32的复合安全标记1中所包含的PUF中导出的散列值，如此处所述。此外，还提供了第二区块链BC-

SCM,其被配置为安全存储供应链信息和使供应链信息可用,该供应链信息诸如产品32的序列号、产品32的复合安全标记1的读取日期和位置等。特别地,这种供应链数据可以以通过应用适当的散列函数以相关散列值从此数据生成方式或除了相关散列值从此数据生成以外被存储在第二区块链BC-SCM中。被配置为跟踪产品32沿着供应链的运动的两个区块链BC-PUF和BC-SCM具有它们相关的区块,即,由跨区块链指针链接的包含关于沿着供应链的同一查验点的数据的区块,从而提供来自和到对应区块的引用。

[0165] 在产品32的制造商A所拥有的供应链的第一节点,该产品32被标记有例如在图1中所示的那种的如本文所述的复合安全标记1。同样,如上面分别参照图6和图9所述的装置17或读取器设备20可以用于该目的。在该标记处理的过程中,复合安全标记1根据图7A和7B(或7C)的方法分别由装置17和20检测,并且生成各自的散列值。可选地,通过将该散列值与也包含在复合安全标记1中的第一数字签名提供的对应散列值进行比较来确认该散列值,然后将其作为初始PUF散列值存储在区块链BC-PUF的第一区块中作为制造商A发起的第一存储的交易#1的一部分。

[0166] 产品32的复合安全标记1还包括第二数字签名,该第二数字签名包括从关于制造商A的供应链相关数据中导出的第二散列值。该第二散列值分别使用装置17和读取器设备20从复合安全标记1中读取,并作为制造商A发起的第一交易#1的一部分存储到第二供应链BC-SCM的第一区块中,可选地连同其他供应链相关数据一起存储。这两个第一区块都包含与制造商A拥有的供应链的初始步骤相对应的数据,并且因此,在两个区块中的每个区块中,添加了指向另一个区块链中相应的对应区块的跨区块链指针,以便允许交叉引用。

[0167] 在沿着供应链的下一步骤中,产品32到达第二中间节点C,该中间节点C例如可以由物流公司拥有,该物流公司负责产品沿着供应链的进一步运输。节点C配备有另一个读取器设备20,并且因此通过在所述读取器设备20上运行图7A和7C的方法来执行产品32的与产品32的复合安全标记1相关地检查。如果该检查确认制造商A为产品32的发起者,则将确认肯定检查的相应交易#2存储到第一区块链BC-PUF的第二区块。否则,所述存储的交易#2指示检查的否定结果,因此指示分别相对于产品32及其复合安全标记1的欺诈。此外,例如在读取器设备20的用户接口上的输出发生器30可以输出警报或错误消息,或者警报或错误消息可以经由通信链路24a或24b被发送到中央信任中心34以便指示所述否定结果。

[0168] 通过添加所述先前区块的区块散列,第二区块被交叉链接至所述区块链的先前区块,即第一区块。这种进入第一区块链BC-PUF的条目以相应的结果确认了在节点C检查了产品32。初始PUF散列值经由与第一块的交叉链接保持可用。类似地,如在先前节点中一样,供应链信息是从复合安全标记1的第二数字签名以及与该节点有关的其他数据生成的,并作为交易#2存储在第二区块链BC-SCM中。同样在该第二供应链BC-SCM中,通过将所述先前区块的区块散列存储在第二区块中,第二区块被交叉链接至先前的第一区块。再次,在第二区块中的每个第二区块中添加一个跨区块链指针,以允许在它们之间进行交叉引用。

[0169] 在沿着供应链的下一步中,产品32到达第三中间节点d,例如,该第三中间节点d可能是不配备读取器设备20而是仅配备只能读取包含在产品32的复合安全标记1中第二数字签名的常规扫描器的远程物流站。与之前的节点不同,在节点d处,类似于在节点C中,只有供应链相关数据作为交易#3写入第二区块链BC-SCM的第三区块。但是,没有数据存储在第一供应链BC-PUF中,因为扫描器无法读取复合安全标记1的PUF并生成相关数据。

[0170] 最终，在沿着供应链的第四步中，产品32到达节点B，该节点B例如可能是产品32的最终目的地或本地零售商。在该节点B，使用另一个读取器设备20执行类似的过程，如在先前节点C处那样，因此，类似的条目将添加到区块链BC-PUF和BC-SCM两者的各个其他区块中。特别地，在这样的节点B或(节点C)处，也可以使用例如根据图8A和8B的、适于执行本解决方案的第六方面的方法的读取器装置。当然，作为替代，可以将图7A和7C的方法应用于节点B处。如上所述，也可以在节点d处使用图8A和8B的方法，以便提高在那里的检查水平。这具有这样的优点：不仅可以读取第二数字签名并将相应的数据写入第二区块链，而且还可以附加地执行安全检查。可选地，这可以包括以与在节点C处类似的方式将节点B的交易数据写入第一区块链。

[0171] 这两个区块链可作为自发起所述区块链以来已经发生并且已经存储的所有所述交易的安全公共分类账。此外，区块链由于无法操作它们(在实践中)而提供了极高的完整性级别，因此它们的使用进一步增强了本文呈现的整个安全解决方案的安全。特别地，存储在两个区块链中的数据可用于检查制造商A实际上是否是产品32的发起者以及供应链是否是预期的。可以在沿着供应链的配备有读取器设备20的每个节点A、C、B处进行此检查，并且因此可以检查产品32的复合安全标记1并访问存储在两个区块链中的数据。

[0172] 尽管上面已经描述了本安全解决方案的至少一个示例性实施例，但是必须注意的是，存在对其的大量变化。此外，应当理解的是，所描述的示例性实施例仅示出了能够如何实现本安全解决方案的非限制性示例，并且不旨在限制本文描述的装置和方法的范围、应用或配置。而是，前面的描述将向本领域技术人员提供用于实现该解决方案的至少一个示例性实施例的构造，其中，必须理解的是，在不偏离所附权利要求及其合法等同物所定义的主题的情况下，可以以示例性实施例的元件的功能和设备做出各种改变。

[0173] 参考符号列表

[0174] 1 复合安全标记

[0175] 2 物理不可克隆功能，PUF

[0176] 3 与PUF对应的数字签名

[0177] 4 指示可以在何处访问数字签名的指针

[0178] 5 包含消耗品的瓶

[0179] 6 消耗品，特别是液态药物物质

[0180] 7 包装

[0181] 8 药物片剂，药丸

[0182] 9 泡罩包装

[0183] 10 不同UCD的混合物的提供

[0184] 11 具有用于3D打印的原材料的容器

[0185] 12 加法制造设备，3D打印机

[0186] 13 3-D打印的物理对象/产品

[0187] 14 PUF扫描器

[0188] 15 处理设备

[0189] 16 条形码打印机

[0190] 17 用于向对象提供复合安全标记的装置

[0191] 20 读取器设备

[0192] 21 激励器

[0193] 22 PUF检测器

[0194] 23 获取设备

[0195] 24 通信设备

[0196] 24a 天线

[0197] 24b 非无线通信链接

[0198] 25 认证设备

[0199] 26 安全设备

[0200] 27 安全防御布置

[0201] 28 监视设备

[0202] 29 处理设备

[0203] 30 输出发生器

[0204] 31 生产线的输送机

[0205] 32 标记的物理对象(产品)

[0206] 33 总线

[0207] 34 中央安全服务器,信任中心

[0208] 40 安全系统

[0209] 41 验证机构服务器

[0210] 42 证书颁发机构服务器

[0211] C 根据质询-响应认证方案的质询

[0212] R 根据质询-响应认证方案的响应

[0213] F 表示PUF对质询的响应的数据(串)

[0214] H(F) 应用于F的密码散列函数,产生散列值H=H(F)

[0215] S[H(F)] 散列值H的数字签名

[0216] λ, 波长

[0217] λ_i 在响应R中发生光强度I的峰的波长

[0218] I 光强度

[0219] I_i 在波长λ_i处的光强度

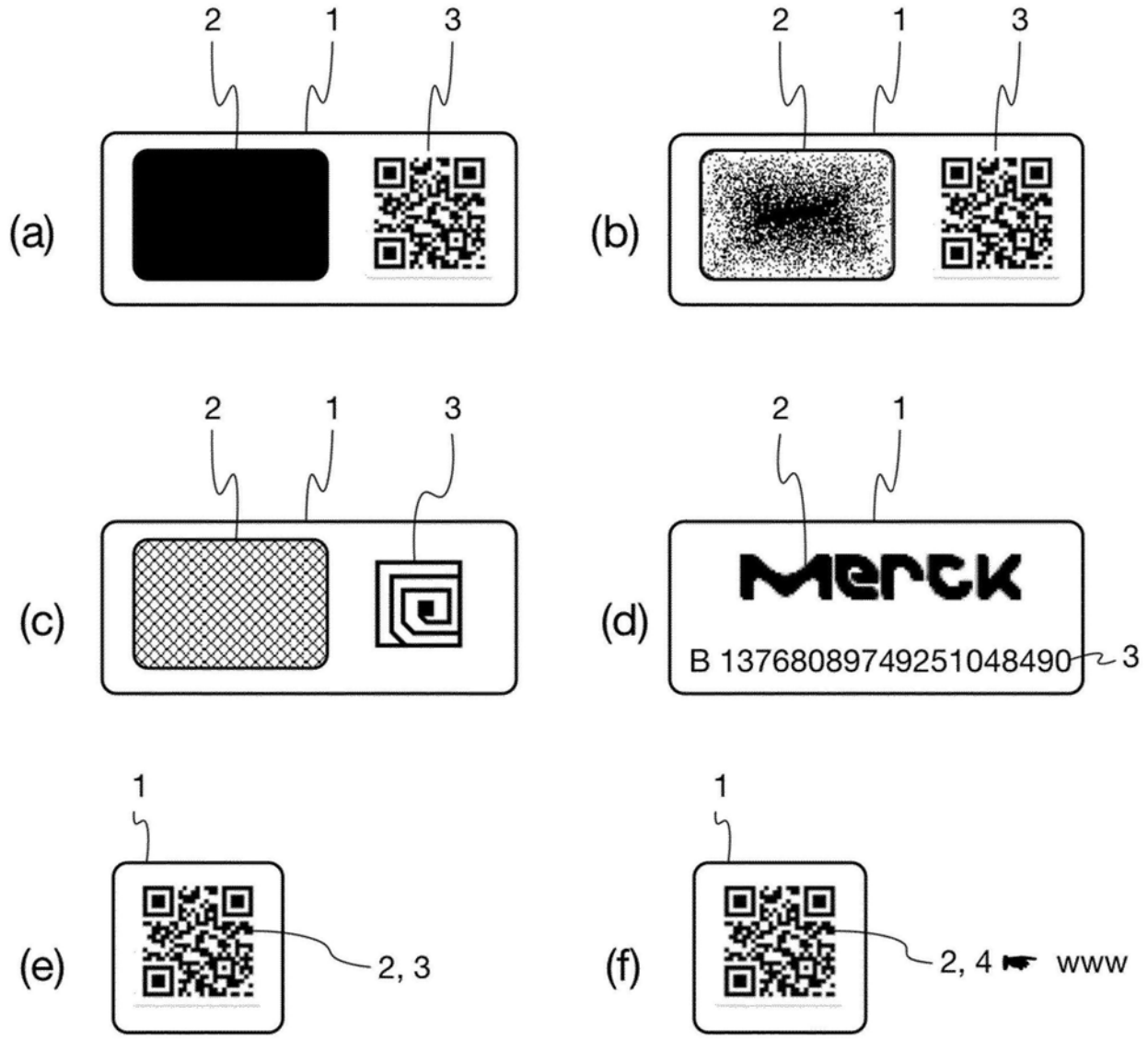


图1

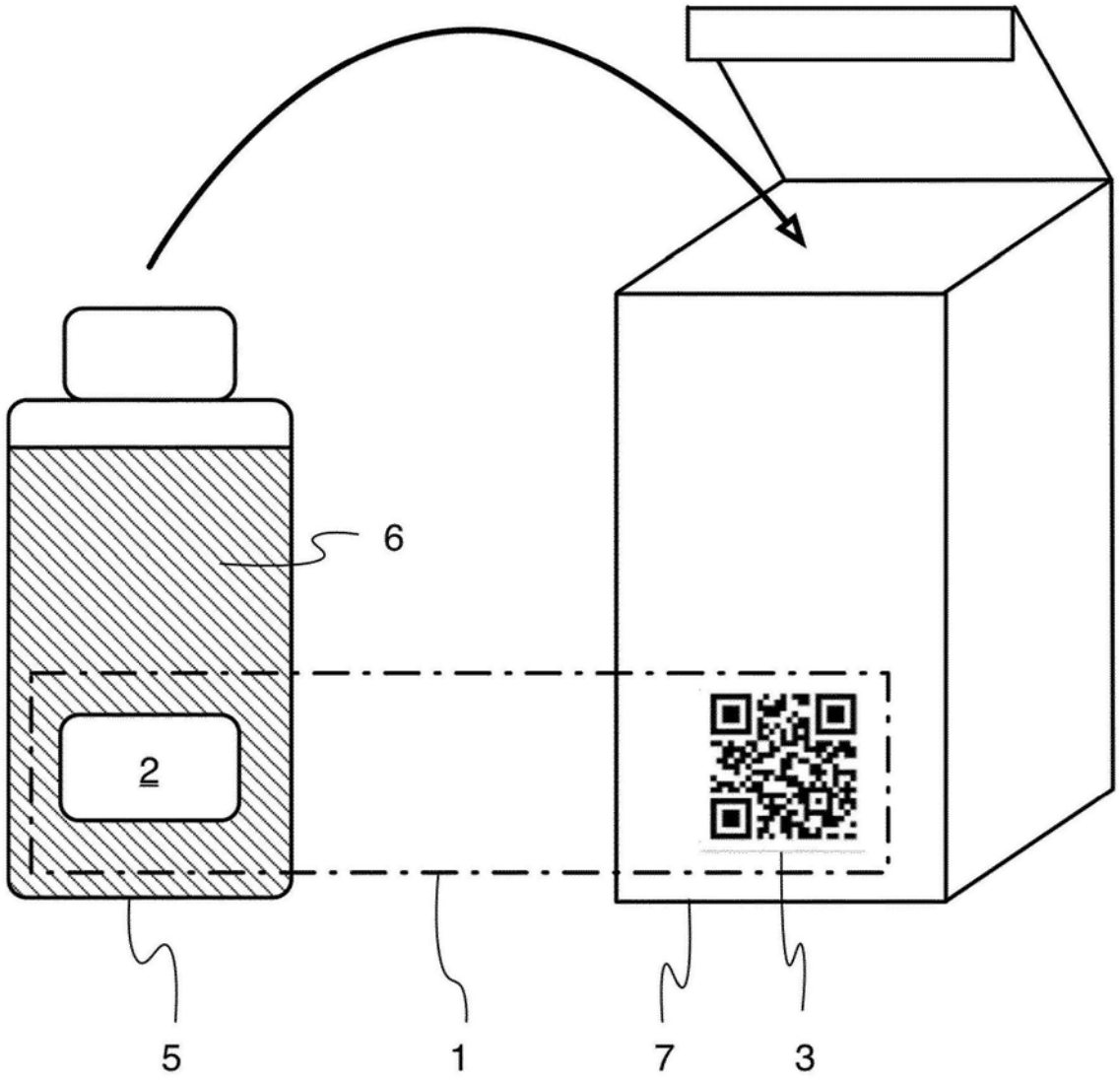


图2

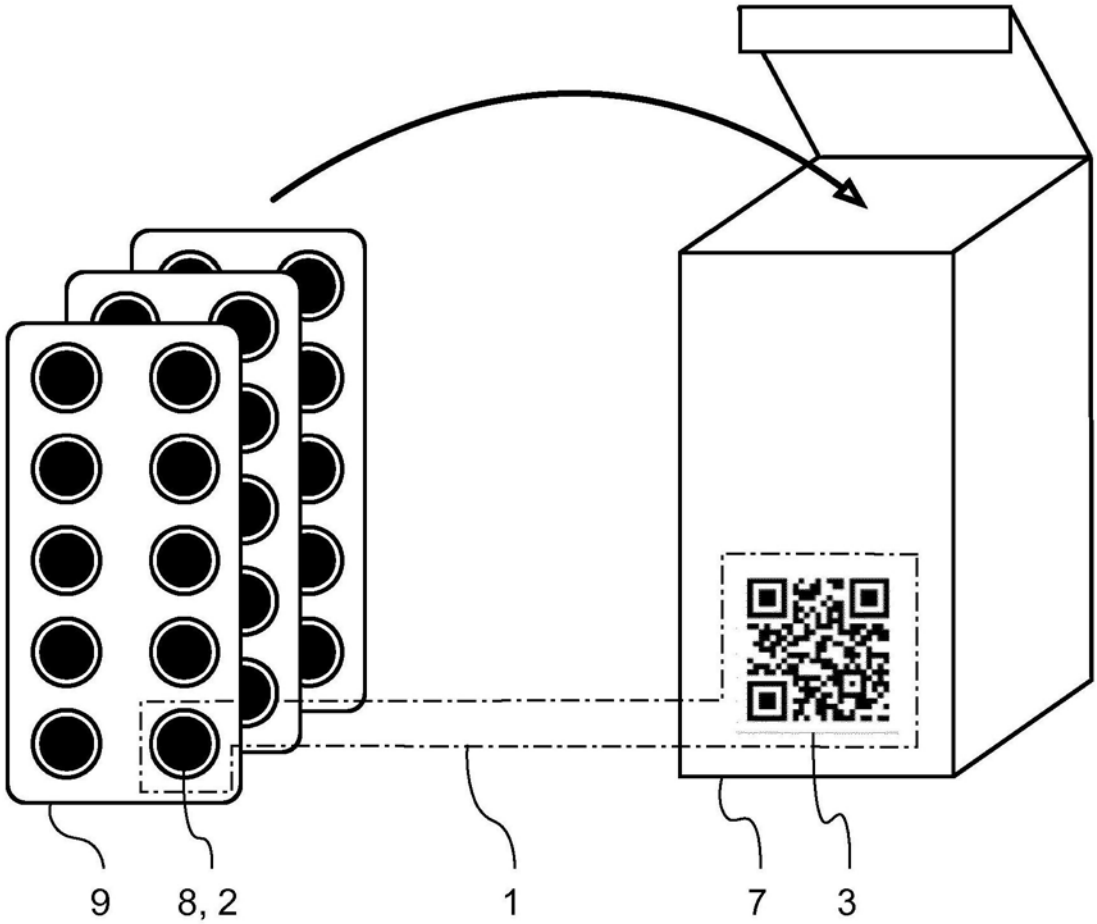


图3

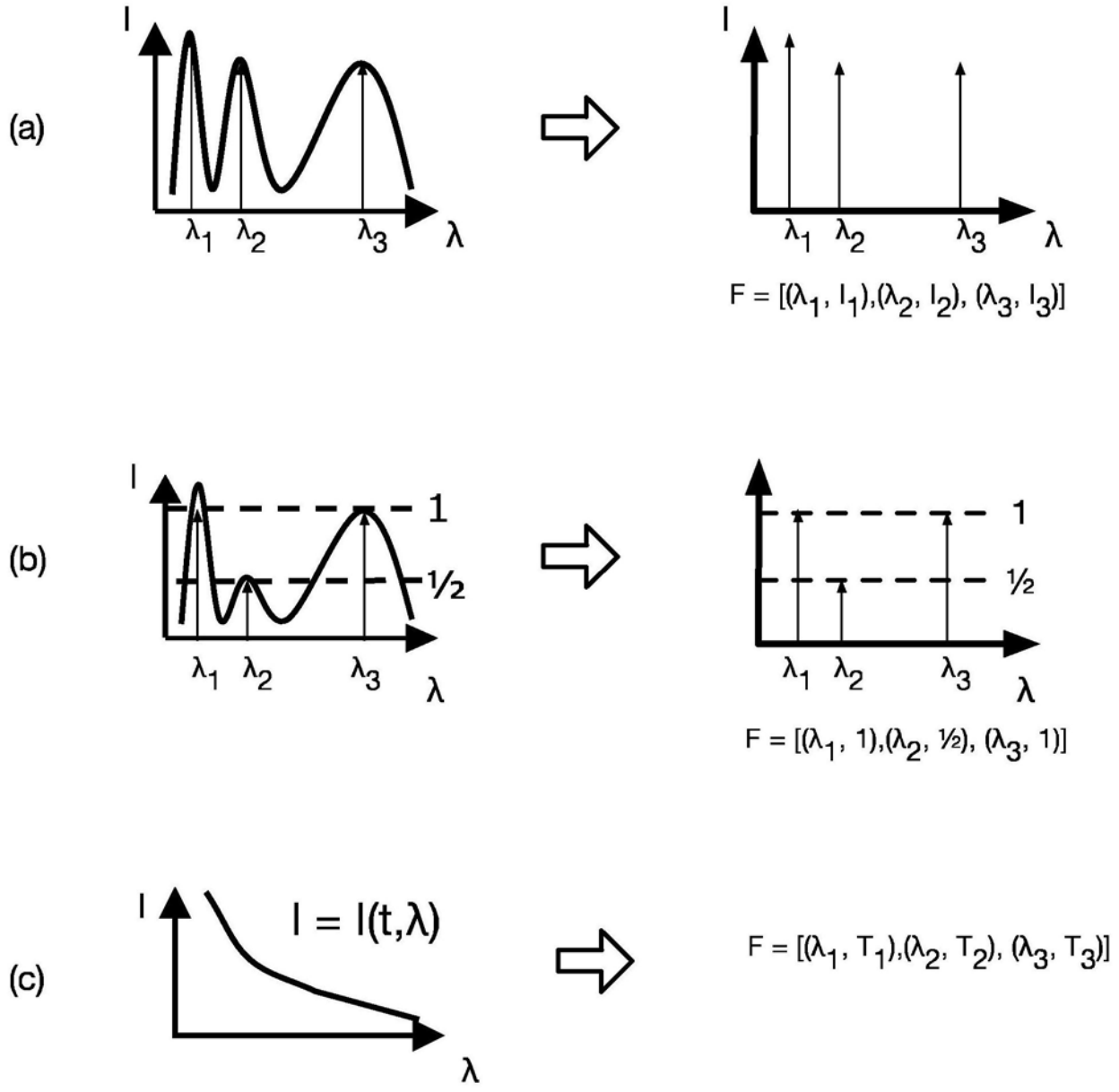

(a)
I
λ1 λ2 λ3 λ
F = [(λ1, I1),(λ2, I2), (λ3, I3)]
(b)
1
½
F = [(λ1, 1),(λ2, ½), (λ3, 1)]
(c)
I = I(t,λ)
F = [(λ1, T1),(λ2, T2), (λ3, T3)]

图4

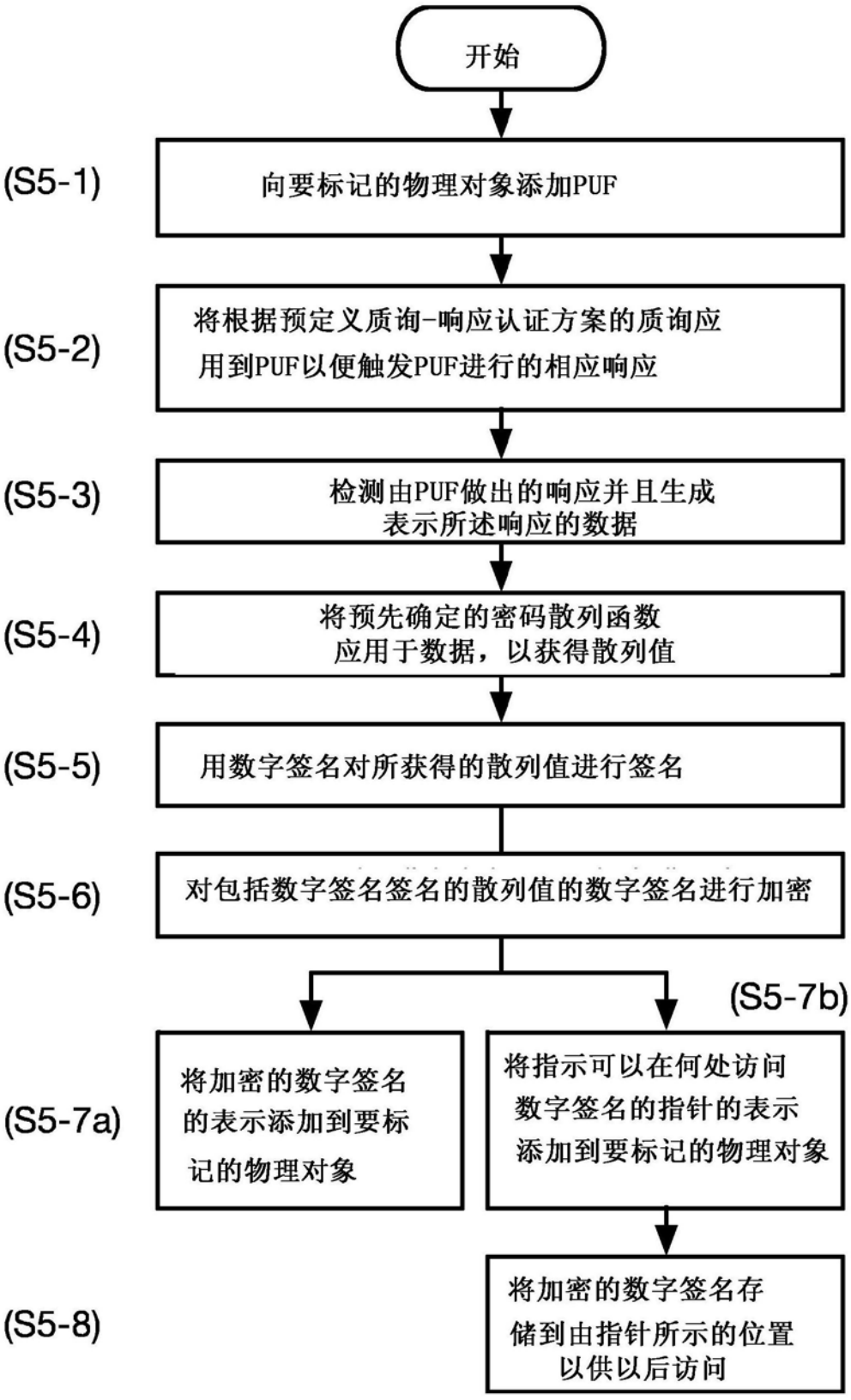

开始
(S5-1)
向要标记的物理对象添加PUF
(S5-2)
将根据预定义质询-响应认证方案的质询应用到PUF以便触发PUF进行的相应响应
(S5-3)
检测由PUF做出的响应并且生成表示所述响应的数据
(S5-4)
将预先确定的密码散列函数应用于数据，以获得散列值
(S5-5)
用数字签名对所获得的散列值进行签名
(S5-6)
对包括数字签名签名的散列值的数字签名进行加密
(S5-7a)
将加密的数字签名的表示添加到要标记的物理对象
(S5-7b)
将指示可以在何处访问数字签名的指针的表示添加到要标记的物理对象
(S5-8)
将加密的数字签名存储到由指针所示的位置以供以后访问

图5

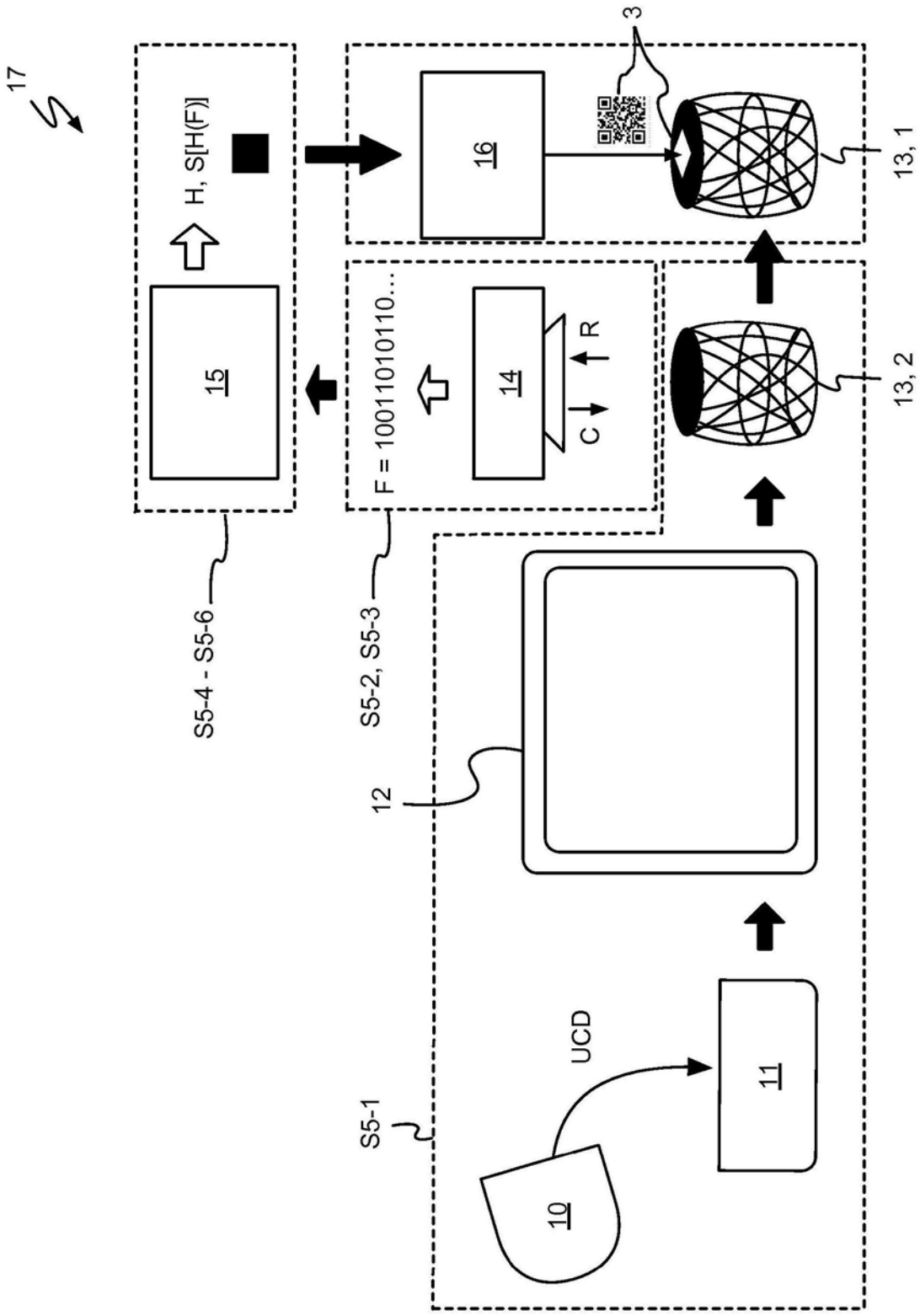

17
S
H, S[H(F)]
15
16
3
13, 1
F = 10011010110...
14
R
C
13, 2
S5-4 - S5-6
S5-2, S5-3
12
S5-1
UCD
11
10

图6

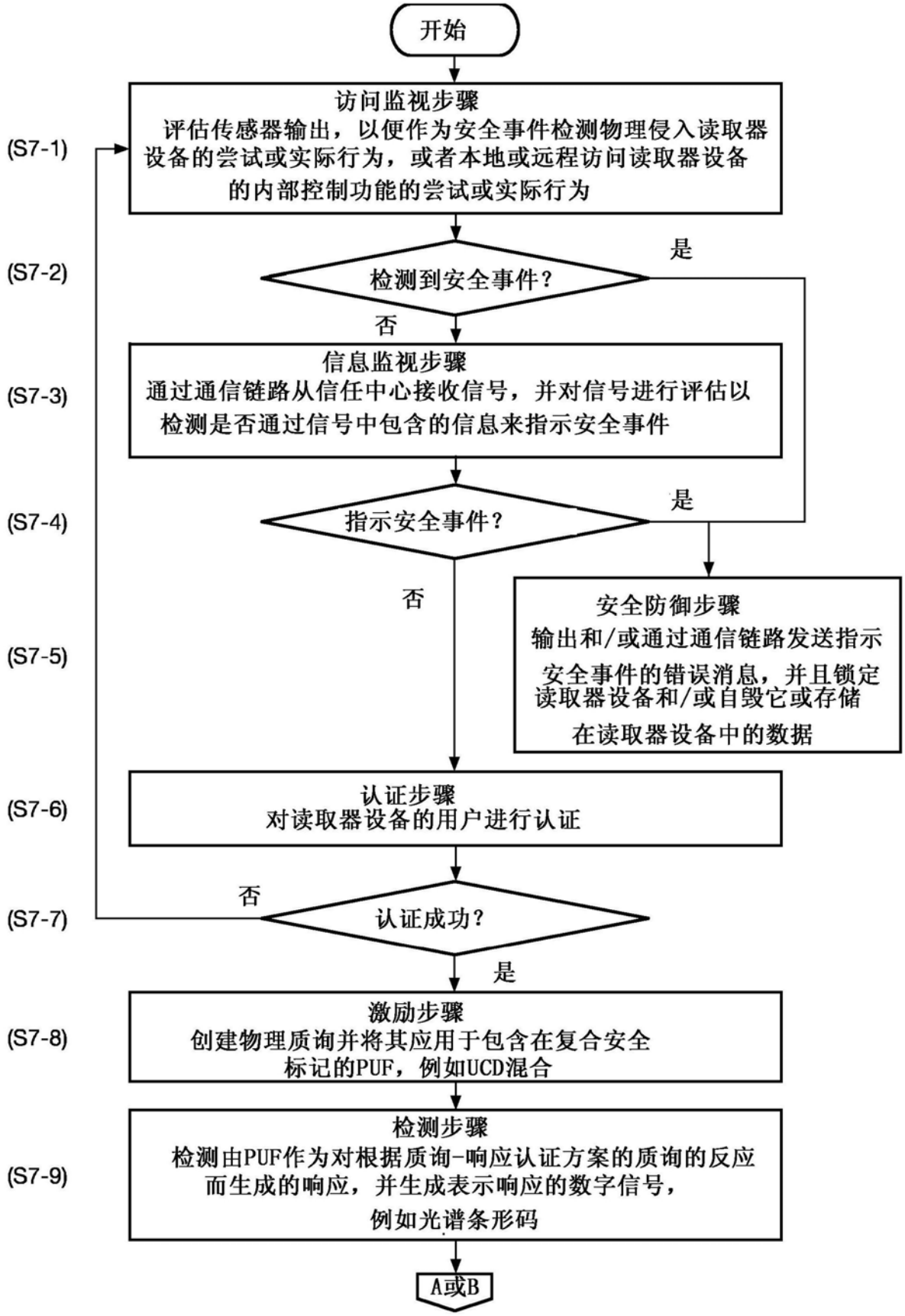

开始
访问监视步骤
评估传感器输出，以便作为安全事件检测物理侵入读取器设备的尝试或实际行为，或者本地或远程访问读取器设备的内部控制功能的尝试或实际行为
(S7-1)
检测到安全事件？
是
否
(S7-2)
信息监视步骤
通过通信链路从信任中心接收信号，并对信号进行评估以检测是否通过信号中包含的信息来指示安全事件
(S7-3)
指示安全事件？
是
否
(S7-4)
安全防御步骤
输出和/或通过通信链路发送指示安全事件的错误消息，并且锁定读取器设备和/或自毁它或存储在读取器设备中的数据
(S7-5)
认证步骤
对读取器设备的用户进行认证
(S7-6)
认证成功？
否
是
(S7-7)
激励步骤
创建物理质询并将其应用于包含在复合安全标记的PUF，例如UCD混合
(S7-8)
检测步骤
检测由PUF作为对根据质询-响应认证方案的质询的反应而生成的响应，并生成表示响应的数字信号，例如光谱条形码
(S7-9)
A或B

图7A

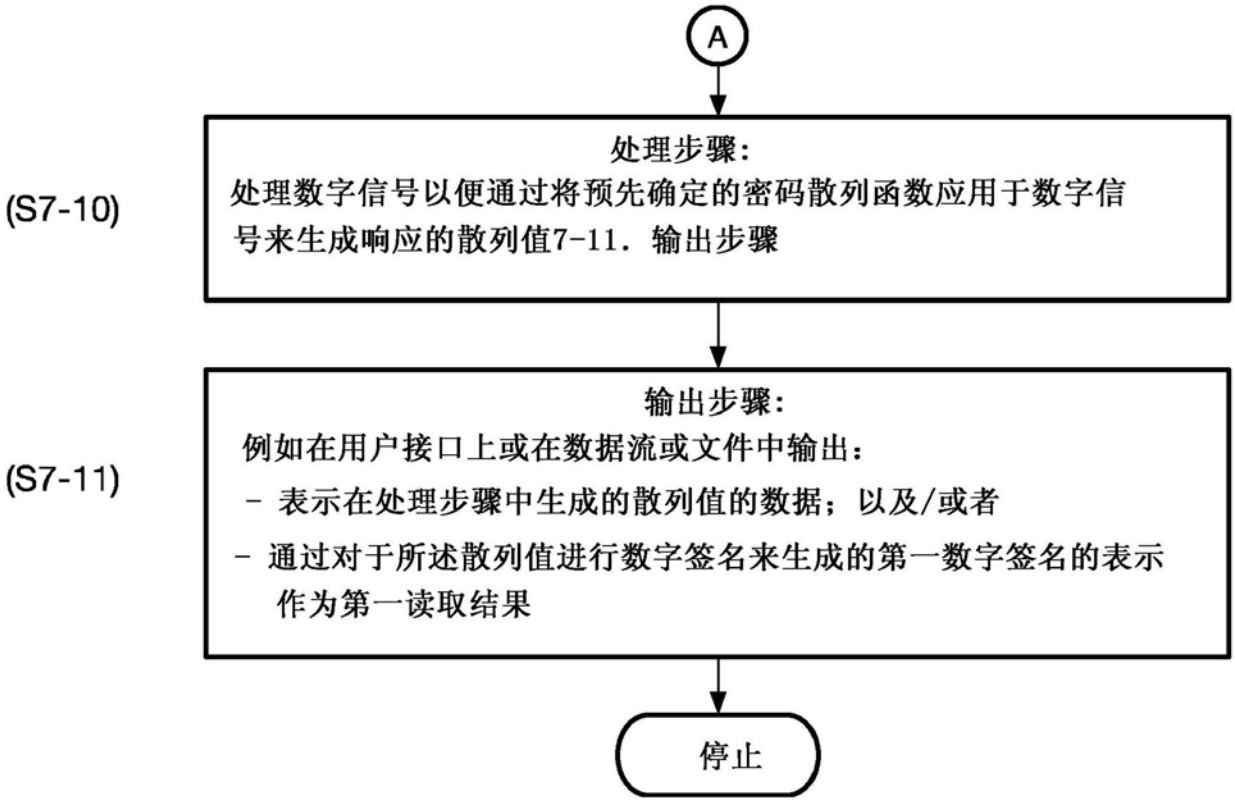

A
处理步骤：
处理数字信号以便通过将预先确定的密码散列函数应用于数字信号来生成响应的散列值7-11．输出步骤
(S7-10)
输出步骤：
例如在用户接口上或在数据流或文件中输出：
- 表示在处理步骤中生成的散列值的数据；以及/或者
- 通过对于所述散列值进行数字签名来生成的第一数字签名的表示作为第一读取结果
(S7-11)
停止

图7B

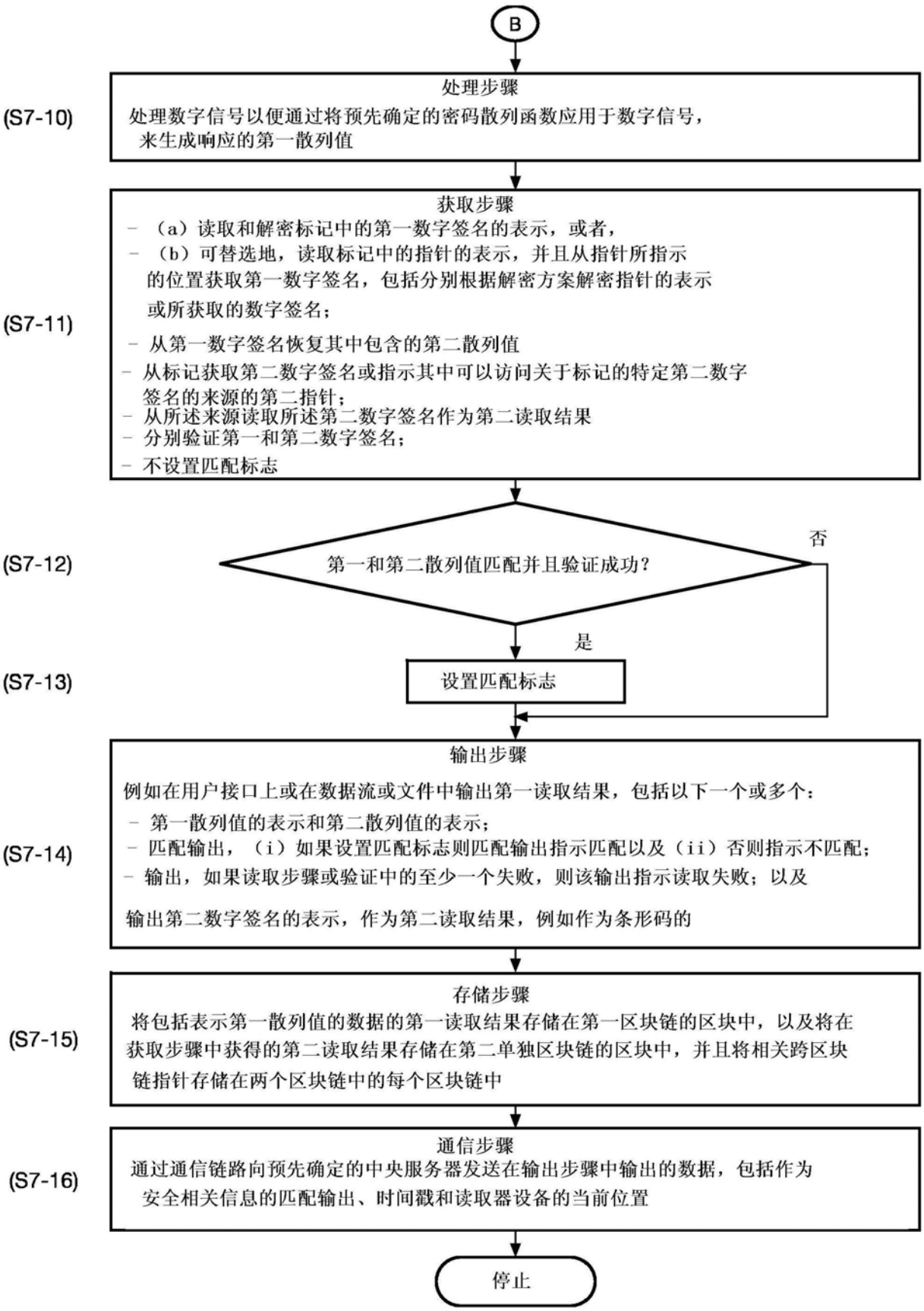

B
处理步骤
(S7-10)
处理数字信号以便通过将预先确定的密码散列函数应用于数字信号，来生成响应的第一散列值
获取步骤
(S7-11)
- （a）读取和解密标记中的第一数字签名的表示，或者，
- （b）可替选地，读取标记中的指针的表示，并且从指针所指示的位置获取第一数字签名，包括分别根据解密方案解密指针的表示或所获取的数字签名；
- 从第一数字签名恢复其中包含的第二散列值
- 从标记获取第二数字签名或指示其中可以访问关于标记的特定第二数字签名的来源的第二指针；
- 从所述来源读取所述第二数字签名作为第二读取结果
- 分别验证第一和第二数字签名；
- 不设置匹配标志
(S7-12)
第一和第二散列值匹配并且验证成功？
否
是
(S7-13)
设置匹配标志
输出步骤
(S7-14)
例如在用户接口上或在数据流或文件中输出第一读取结果，包括以下一个或多个：
- 第一散列值的表示和第二散列值的表示；
- 匹配输出，（i）如果设置匹配标志则匹配输出指示匹配以及（ii）否则指示不匹配；
- 输出，如果读取步骤或验证中的至少一个失败，则该输出指示读取失败；以及
输出第二数字签名的表示，作为第二读取结果，例如作为条形码的
存储步骤
(S7-15)
将包括表示第一散列值的数据的第一读取结果存储在第一区块链的区块中，以及将在获取步骤中获得的第二读取结果存储在第二单独区块链的区块中，并且将相关跨区块链指针存储在两个区块链中的每个区块链中
通信步骤
(S7-16)
通过通信链路向预先确定的中央服务器发送在输出步骤中输出的数据，包括作为安全相关信息的匹配输出、时间戳和读取器设备的当前位置
停止

图7C

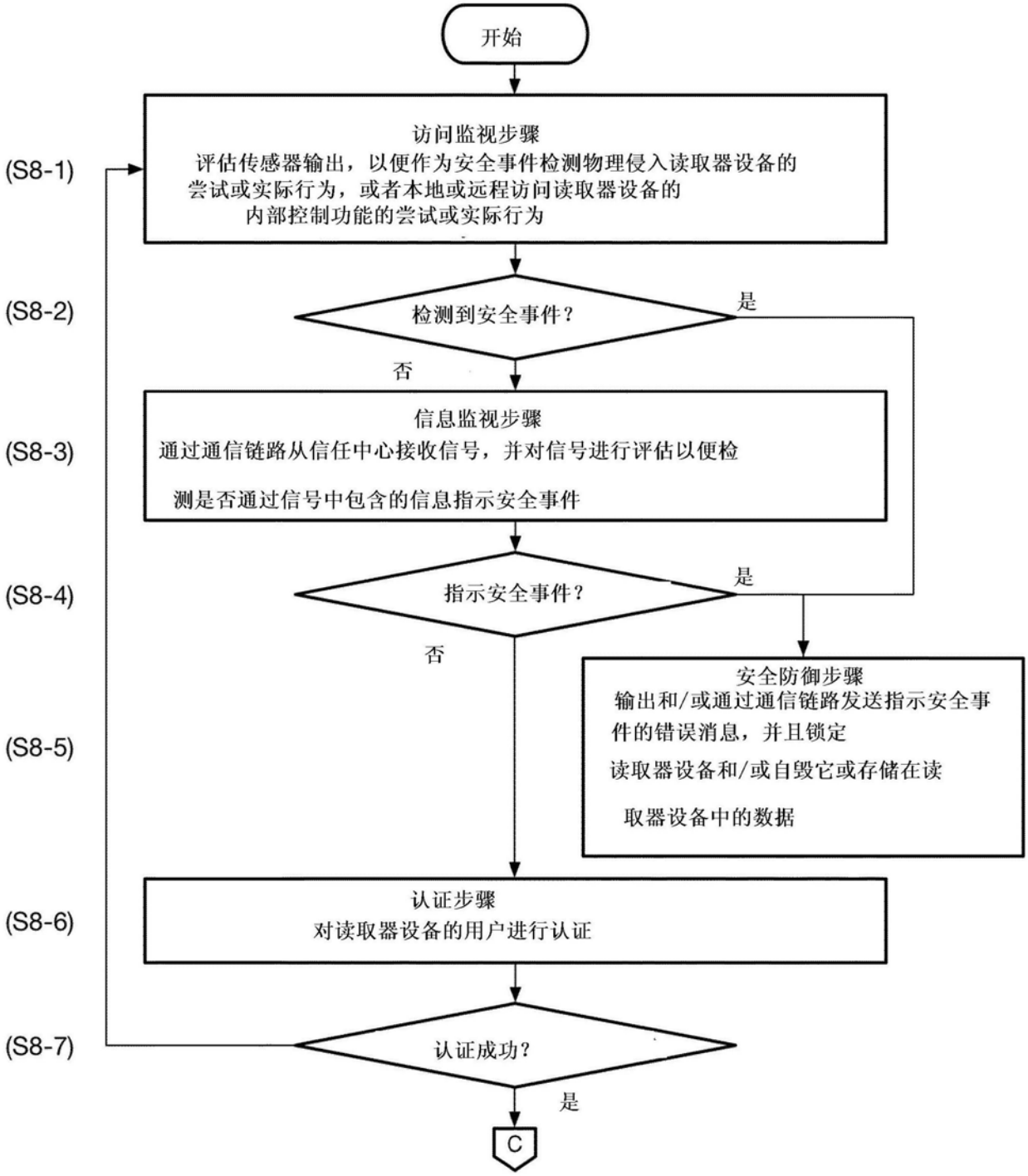

开始
(S8-1)
访问监视步骤
评估传感器输出，以便作为安全事件检测物理侵入读取器设备的尝试或实际行为，或者本地或远程访问读取器设备的内部控制功能的尝试或实际行为
(S8-2)
检测到安全事件？
是
否
(S8-3)
信息监视步骤
通过通信链路从信任中心接收信号，并对信号进行评估以便检测是否通过信号中包含的信息指示安全事件
(S8-4)
指示安全事件？
是
否
(S8-5)
安全防御步骤
输出和/或通过通信链路发送指示安全事件的错误消息，并且锁定读取器设备和/或自毁它或存储在读取器设备中的数据
(S8-6)
认证步骤
对读取器设备的用户进行认证
(S8-7)
认证成功？
是
C

图8A

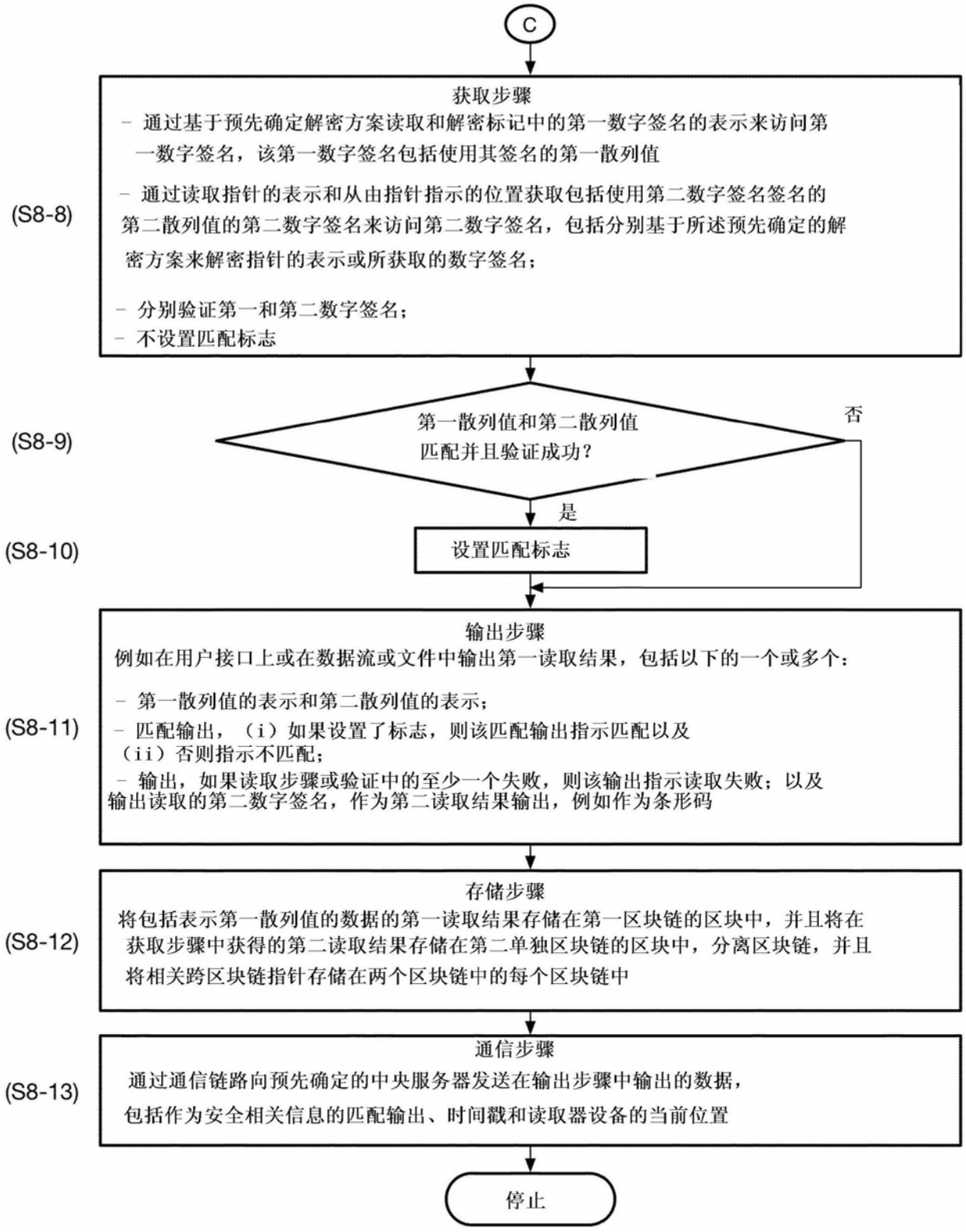

C
获取步骤
- 通过基于预先确定解密方案读取和解密标记中的第一数字签名的表示来访问第一数字签名，该第一数字签名包括使用其签名的第一散列值
- 通过读取指针的表示和从由指针指示的位置获取包括使用第二数字签名签名的第二散列值的第二数字签名来访问第二数字签名，包括分别基于所述预先确定的解密方案来解密指针的表示或所获取的数字签名；
- 分别验证第一和第二数字签名；
- 不设置匹配标志
(S8-8)
第一散列值和第二散列值匹配并且验证成功？
否
是
(S8-9)
设置匹配标志
(S8-10)
输出步骤
例如在用户接口上或在数据流或文件中输出第一读取结果，包括以下的一个或多个：
- 第一散列值的表示和第二散列值的表示；
- 匹配输出，（i）如果设置了标志，则该匹配输出指示匹配以及（ii）否则指示不匹配；
- 输出，如果读取步骤或验证中的至少一个失败，则该输出指示读取失败；以及
输出读取的第二数字签名，作为第二读取结果输出，例如作为条形码
(S8-11)
存储步骤
将包括表示第一散列值的数据的第一读取结果存储在第一区块链的区块中，并且将在获取步骤中获得的第二读取结果存储在第二单独区块链的区块中，分离区块链，并且将相关跨区块链指针存储在两个区块链中的每个区块链中
(S8-12)
通信步骤
通过通信链路向预先确定的中央服务器发送在输出步骤中输出的数据，包括作为安全相关信息的匹配输出、时间戳和读取器设备的当前位置
(S8-13)
停止

图8B

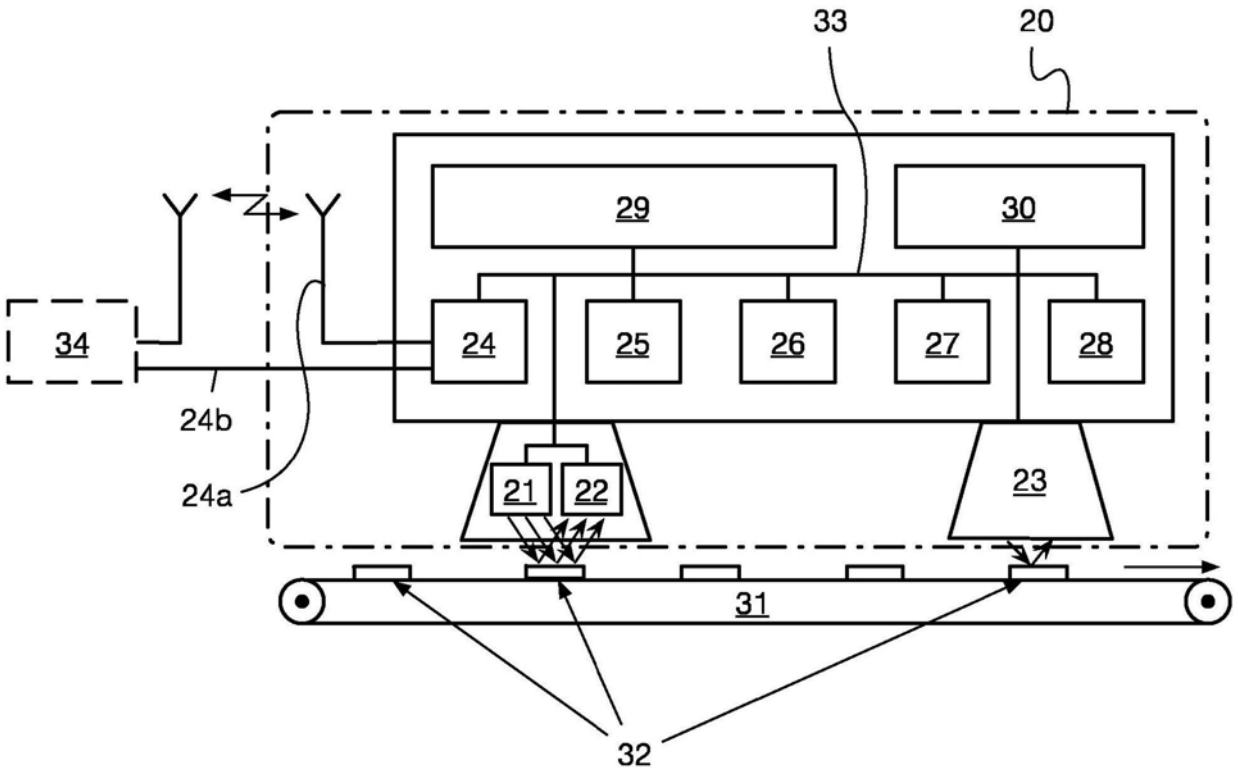


图9

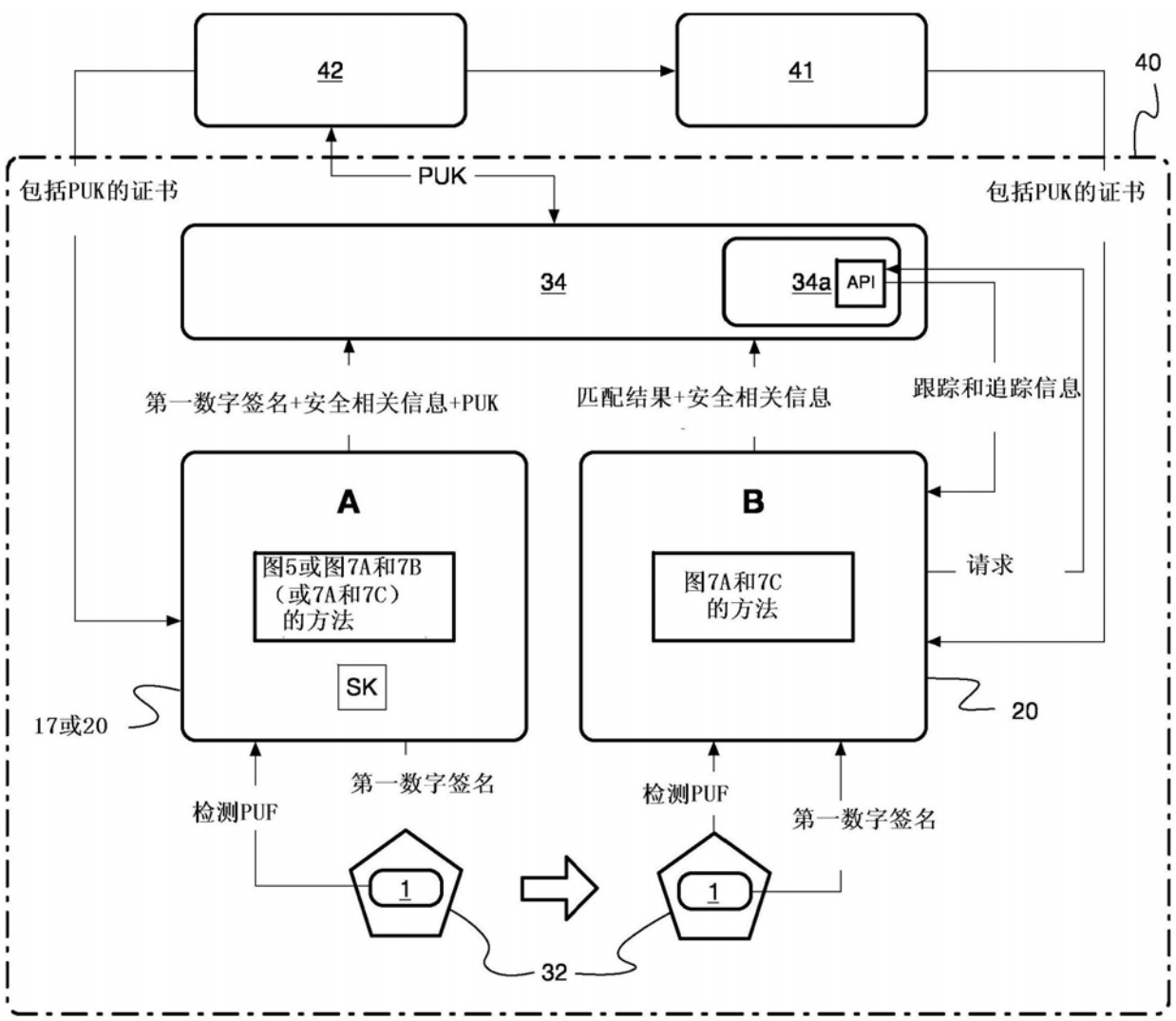

42
41
40
包括PUK的证书
PUK
包括PUK的证书
34
34a
API
第一数字签名+安全相关信息+PUK
匹配结果+安全相关信息
跟踪和追踪信息
A
图5或图7A和7B
（或7A和7C）
的方法
SK
B
图7A和7C
的方法
请求
17或20
20
检测PUF
第一数字签名
检测PUF
第一数字签名
1
1
32

图10

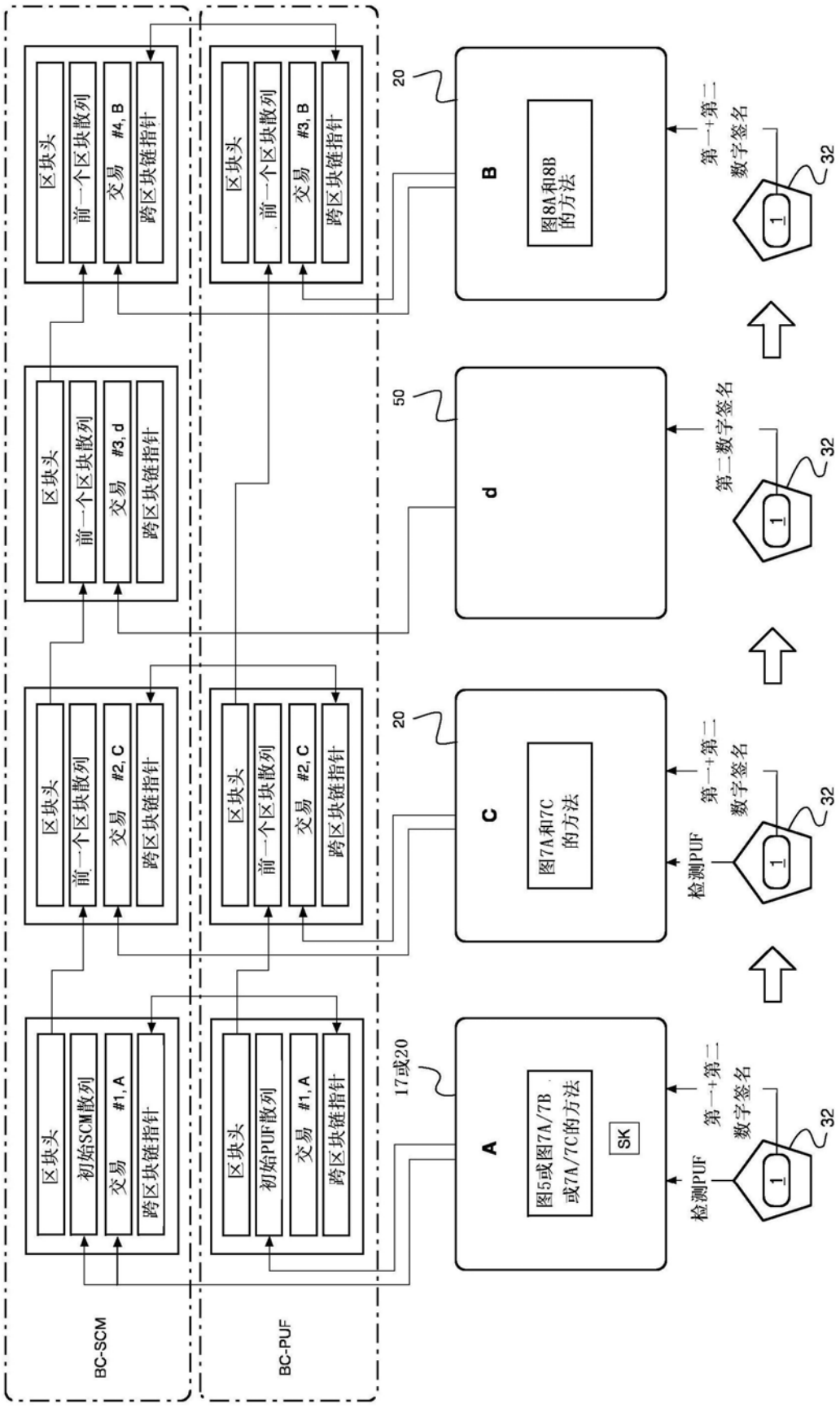

区块头
初始SCM散列
交易 #1, A
跨区块链指针
区块头
前一个区块散列
交易 #2, C
跨区块链指针
区块头
前一个区块散列
交易 #3, d
跨区块链指针
区块头
前一个区块散列
交易 #4, B
跨区块链指针
BC-SCM
区块头
初始PUF散列
交易 #1, A
跨区块链指针
区块头
前一个区块散列
交易 #2, C
跨区块链指针
区块头
前一个区块散列
交易 #3, B
跨区块链指针
BC-PUF
17或20
A
图5或图7A/7B或7A/7C的方法
SK
检测PUF
第一+第二数字签名
32
20
C
图7A和7C的方法
检测PUF
第一+第二数字签名
32
50
d
第二数字签名
32
20
B
图8A和8B的方法
第一+第二数字签名
32

图11