(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 109347642 A
(43)申请公布日 2019.02.15

(21)申请号 201811300379.2

(22)申请日 2014.08.19

(30)优先权数据
13/975,082 2013.08.23 US

(62)分案原申请数据
201480045952.3 2014.08.19

(71)申请人 高通股份有限公司
地址 美国加利福尼亚州

(72)发明人 郭旭 戴维·M·雅各布森
杨亚飞 亚当·J·德鲁
布莱恩·马克·罗森贝格

(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 杨林勳

(51)Int.Cl.
H04L 9/32(2006.01)
G06F 7/58(2006.01)

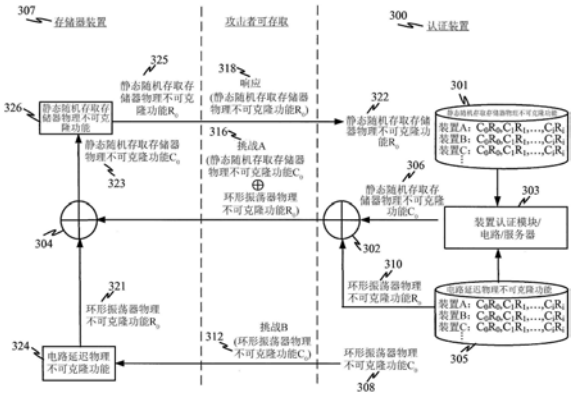
权利要求书3页 说明书13页 附图12页

(54)发明名称

一种抵抗入侵的方法、装置及机器可读存储媒体

(57)摘要

本申请涉及一种抵抗入侵的方法、装置及机器可读存储媒体。一个特征是关于通过组合静态随机存取存储器SRAM PUF及基于电路延迟的PUF(例如,环形振荡器RO PUF、仲裁器PUF等)而产生电子装置的唯一识别符。所述基于电路延迟的PUF可用于隐藏对所述SRAM PUF的挑战及/或来自所述SRAM PUF的响应,进而阻止攻击者能够克隆存储器装置的响应。



CN 109347642 A

1.一种通过认证装置操作的方法,其包括:

接收与电子装置相关联的装置识别符;

将基于电路延迟的物理不可克隆功能PUF挑战以及基于存储器单元的PUF挑战发送到所述电子装置;

从所述电子装置接收响应,所述响应包含产自所述电子装置中的基于存储器单元的PUF以及基于电路延迟的PUF的特性信息;

使用所述电子装置识别符识别所述电子装置专有的预先存储的响应;及

通过将所述预先存储的响应及接收到的所述响应进行比较而认证所述电子装置。

2.根据权利要求1所述的方法,其中所述基于存储器单元的PUF挑战以及所述基于电路延迟的PUF挑战选自先前从所述电子装置获得其响应的多个挑战。

3.根据权利要求1所述的方法,其中在所述电子装置的制造阶段或预部署阶段获得所述预先存储的响应。

4.根据权利要求1所述的方法,其中在发送所述基于电路延迟的PUF挑战以及所述基于存储器单元的PUF挑战之前接收所述装置识别符。

5.根据权利要求1所述的方法,其中与接收所述响应一起接收所述装置识别符。

6.根据权利要求1所述的方法,其中发送到所述电子装置的所述基于存储器单元的PUF挑战是被对所述基于电路延迟的PUF挑战的预先存储响应掩蔽的挑战。

7.一种认证装置,其包括:

通信接口,其用以与电子装置通信;以及

处理电路,其通信地耦合到所述通信接口,其中所述处理电路经调适以:

接收与所述电子装置相关联的装置识别符;

将基于电路延迟的物理不可克隆功能PUF挑战以及基于存储器单元的PUF挑战发送到所述电子装置;

从所述电子装置接收响应,所述响应包含产自所述电子装置中的基于存储器单元的PUF以及基于电路延迟的PUF的特性信息;

使用所述电子装置识别符识别所述电子装置专有的预先存储的响应;及

通过将所述预先存储的响应及接收到的所述响应进行比较而认证所述电子装置。

8.根据权利要求7所述的认证装置,其中所述基于存储器单元的PUF挑战以及所述基于电路延迟的PUF挑战选自先前从所述电子装置获得其响应的多个挑战。

9.根据权利要求7所述的认证装置,其中发送到所述电子装置的所述基于存储器单元的PUF挑战是被对所述基于电路延迟的PUF挑战的预先存储响应掩蔽的挑战。

10.一种认证装置,其包括:

用于接收与电子装置相关联的装置识别符的装置;

用于将基于电路延迟的物理不可克隆功能PUF挑战以及基于存储器单元的PUF挑战发送到所述电子装置的装置;

用于从所述电子装置接收响应的装置,所述响应包含产自所述电子装置中的基于存储器单元的PUF以及基于电路延迟的PUF的特性信息;

用于使用所述电子装置识别符识别所述电子装置专有的预先存储的响应的装置;

及

用于通过将所述预先存储的响应及接收到的所述响应进行比较而认证所述电子装置的装置。

11.一种具有存储在其上的一或多个指令的非暂时性机器可读存储媒体,所述一或多个指令在由至少一个处理器执行时致使所述至少一个处理器:

接收与电子装置相关联的装置识别符;

将基于电路延迟的物理不可克隆功能PUF挑战以及基于存储器单元的PUF挑战发送到所述电子装置;

从所述电子装置接收响应,所述响应包含产自所述电子装置中的基于存储器单元的PUF以及基于电路延迟的PUF的特性信息;

使用所述电子装置识别符识别所述电子装置专有的预先存储的响应;及

通过将所述预先存储的响应及接收到的所述响应进行比较而认证所述电子装置。

12.根据权利要求6所述的方法,其中通过将所述预先存储的响应及接收到的所述响应进行比较而认证所述电子装置包括:确定所述接收到的所述响应匹配于用于所述基于存储器单元的PUF挑战的预先存储的响应或者是用于所述基于存储器单元的PUF挑战的预先存储的响应的函数。

13.根据权利要求1所述的方法,其中通过将所述预先存储的响应及接收到的所述响应进行比较而认证所述电子装置包括:

根据所述基于存储器单元的PUF挑战的函数以及对所述基于电路延迟的PUF挑战的预先存储响应而获得中间挑战;以及

确定所述接收到的所述响应匹配于用于所述中间挑战的已存储响应或者是用于所述中间挑战的已存储响应的函数。

14.根据权利要求13所述的方法,其进一步包括:通过用对所述基于电路延迟的PUF挑战的所述预先存储响应对所述基于存储器单元的PUF挑战执行特有的OR运算而获得所述中间挑战。

15.根据权利要求1所述的方法,其中通过将所述预先存储的响应及接收到的所述响应进行比较而认证所述电子装置包括:

根据所述接收到的所述响应的函数以及用于所述基于电路延迟的PUF挑战的预先存储响应而获得经修改的响应;以及

确定所述经修改的响应匹配于所述基于存储器单元的PUF响应或者是所述基于存储器单元的PUF响应的函数。

16.根据权利要求15所述的方法,其进一步包括:通过用以下项中的一者来对所述接收到的所述响应执行特有的OR运算而获得所述经修改的挑战:(i)用于所述基于电路延迟的PUF挑战的预先存储的响应;或者(ii)用于所述基于电路延迟的PUF挑战的预先存储的响应的密码散列。

17.根据权利要求9所述的认证装置,其中所述处理电路经调适以通过将所述预先存储的响应及接收到的所述响应进行比较而认证所述电子装置包括所述处理电路经调适以:确定所述接收到的所述响应匹配于用于所述基于存储器单元的PUF挑战的预先存储的响应或者是用于所述基于存储器单元的PUF挑战的预先存储的响应的函数。

18.根据权利要求7所述的认证装置,其中所述处理电路经调适以通过将所述预先存储

的响应及接收到的所述响应进行比较而认证所述电子装置包括所述处理电路经调适以：

根据所述基于存储器单元的PUF挑战的函数以及对所述基于电路延迟的PUF挑战的预先存储响应而获得中间挑战；以及

确定所述接收到的所述响应匹配于用于所述中间挑战的已存储响应或者是用于所述中间挑战的已存储响应的函数。

19.根据权利要求18所述的认证装置，其中所述处理电路进一步经调适以：通过用对所述基于电路延迟的PUF挑战的所述预先存储响应对所述基于存储器单元的PUF挑战执行特有的OR运算而获得所述中间挑战。

20.根据权利要求7所述的认证装置，其中所述处理电路经调适以通过将所述预先存储的响应及接收到的所述响应进行比较而认证所述电子装置包括所述处理电路经调适以：

根据所述接收到的所述响应的函数以及用于所述基于电路延迟的PUF挑战的预先存储响应而获得经修改的响应；以及

确定所述经修改的响应匹配于所述基于存储器单元的PUF响应或者是所述基于存储器单元的PUF响应的函数。

21.根据权利要求20所述的认证装置，其中所述处理电路进一步经调适以：通过用以下项中的一者来对所述接收到的所述响应执行特有的OR运算而获得所述经修改的挑战：(i)用于所述基于电路延迟的PUF挑战的预先存储的响应；或者(ii)用于所述基于电路延迟的PUF挑战的预先存储的响应的密码散列。

一种抵抗入侵的方法、装置及机器可读存储媒体

[0001] 分案申请的相关信息

[0002] 本案是分案申请。该分案的母案是申请日为2014年8月19日、申请号为201480045952.3、发明名称为“一种抵抗入侵的方法、装置及机器可读存储媒体”的发明专利申请案。

技术领域

[0003] 本发明是关于使用物理不可克隆功能(PUF)唯一地识别存储器装置或存储器装置集成到其中的装置。

背景技术

[0004] 物理不可克隆功能(PUF)提供基于物理组件的固有变化而唯一地识别硬件装置的机制。在制造多个芯片时,复杂的半导体制造工艺引入超出设计者的控制的轻微变化。举例来说,即使两个芯片是由相同的硅晶片制成,但经设计成相同的电路径将可能在宽度上相差数纳米;硅表面中的微观差异将诱发线曲率中的几乎轻微的变化。因为这些唯一特性是不可控制的且是物理装置固有的,所以量化它们可产生固有识别符。已经基于电路延迟中的硅变化的勘测及分析而提出若干不同类型的PUF,例如基于环形振荡器的PUF、仲裁器PUF及基于路径延迟分析的PUF。

[0005] 一个PUF利用静态随机存取存储器(SRAM)的未初始化的加电状态以产生识别“指纹”。然而,SRAM PUF容易受到克隆攻击。

[0006] 因此,一般来说,需要提高当前SRAM PUF设计的安全性以抵抗克隆攻击及入侵攻击。

发明内容

[0007] 提供可被唯一地识别同时能抵抗克隆攻击的电子装置(例如,处理器、处理电路、存储器、可编程逻辑阵列、芯片、半导体、存储器等)。所述电子装置可在所述电子装置内包含充当第一物理不可克隆功能(PUF)的多个存储器单元。在一个实例中,所述第一物理不可克隆功能可使用一或多个存储器单元的未初始化的存储器单元状态作为对挑战的响应。另外,所述电子装置内的多个基于电路延迟的路径可实施第二物理不可克隆功能。在一个实例中,所述多个基于电路延迟的路径可为环形振荡器且所述第二物理不可克隆功能可接收从所述多个环形振荡器选择两个环形振荡器且使用所述两个环形振荡器之间的频率差分作出响应的挑战。

[0008] 通信接口可用来从外部服务器接收挑战。处理电路可耦合到所述通信接口、所述多个存储器单元及所述多个基于电路延迟的路径,其中所述处理电路经调适以通过使用来自第二物理不可克隆功能的第一响应进行以下操作而将所述挑战应用于第一物理不可克隆功能(a)掩蔽/暴露输入到第一物理不可克隆功能的挑战,(b)产生输入到第一物理不可克隆功能的挑战,或(c)掩蔽从第一物理不可克隆功能输出的响应。通信接口可经调适以将

来自第一物理不可克隆功能的第二响应发送所述外部服务器。另外，可将第一响应从第二物理不可克隆功能发送到外部服务器。在一个实例中，所述外部服务器可包含用于第一物理不可克隆功能的第一挑战及响应数据库及用于第二物理不可克隆功能的第二挑战及响应数据库，其中外部服务器将挑战发送到电子装置且基于所述第二响应而认证或识别电子装置。

[0009] 在一个实例中，所述挑战可包含用于第一物理不可克隆功能的第一挑战及用于第二物理不可克隆功能的第二挑战。在一个实施方案中，所述第一挑战可为由对第二挑战的预期响应掩蔽的挑战。在另一实施方案中，所述第一挑战可在所述第一物理不可克隆功能进行处理之前由来自所述第二物理不可克隆功能的第一响应修改。

[0010] 在另一实例中，所接收的挑战可由所述第二物理不可克隆功能使用以产生所述第一响应，所述第一响应随后由所述第一物理不可克隆功能用作第二挑战以产生所述第二响应。

[0011] 在又另一实例中，所述挑战可包含用于所述第一物理不可克隆功能的第一挑战及用于所述第二物理不可克隆功能的第二挑战，所述第二挑战由所述第二物理不可克隆功能使用以产生所述第一响应，所述第一响应用于掩蔽来自所述第一物理不可克隆功能的第二响应。来自所述第二物理不可克隆功能的第一响应可散列以获得中间响应。随后可使用所述中间响应掩蔽所述第二响应。

[0012] 在其它情况下，可接收所述挑战以作为以下各者中的至少一者的部分：电子装置的认证过程、电子装置的识别过程，及/或电子装置内的密钥产生过程。

[0013] 在一些实施方案中，所述电子装置可先前已接收一或多个挑战且在预部署或制造阶段期间提供(例如，到数据收集器)一或多个对应响应。

[0014] 另外，可(a)在接收挑战之前，或(b)与发送第二响应同时地将预先存储的装置识别符从电子装置发送到外部服务器，其中所述装置识别符唯一地识别电子装置。

[0015] 还提供数据收集器装置，其在电子装置的预部署或制造阶段期间获得(例如，接收或指派)与电子装置相关联的装置识别符。数据收集器装置可随后产生及发送一或多个挑战到电子装置。因此，数据收集器装置可从电子装置接收一或多个响应，所述一或多个响应包含由电子装置中的两种或更多种相异类型的物理不可克隆功能产生的特性信息。所述装置识别符、挑战及对应响应经存储以用于电子装置的后续认证。此过程可针对多个电子装置中的每一者重复。应注意，发送到电子装置的挑战可对于所有装置都相同、可针对每一电子装置随机产生，及/或可为可能的挑战的子集。

[0016] 类似地，提供认证装置，其基于来自相异类型的物理不可克隆功能的响应而认证电子装置。所述认证装置接收与电子装置相关联的装置识别符。其随后将一或多个挑战发送到电子装置。作为响应，所述认证装置从所述电子装置接收一或多个响应，所述一或多个响应包含由所述电子装置中的两种或更多种相异类型的物理不可克隆功能产生的特性信息。可使用电子装置识别符识别电子装置专有的预先存储的响应。随后可通过进行比较预先存储的响应及电子装置的所接收的一或多个响应而认证所述电子装置。所述挑战可选自先前从电子装置获得其响应的多个挑战。可已在电子装置的制造阶段或预部署阶段获得预先存储的响应。可在发送一或多个挑战之前接收所述装置识别符。可与接收所述一或多个响应一起接收所述装置识别符。

[0017] 所述挑战可包含用于第一物理不可克隆功能的第一挑战及用于第二物理不可克隆功能的第二挑战。所述第一挑战可为由对第二挑战的预期响应掩蔽的挑战。所述一或多个挑战可包含用于第一物理不可克隆功能的第一挑战及用于第二物理不可克隆功能的第二挑战，所述一或多个响应包含来自第一物理不可克隆功能的第一响应及来自第二物理不可克隆功能的第二响应，如果所述第一响应匹配对应于所述第一挑战的第一预先存储的响应且所述第二响应匹配对应于所述第二挑战的第二预先存储的响应，那么成功地认证所述电子装置。

[0018] 所述一或多个挑战包含用于第一物理不可克隆功能的第一挑战及用于第二物理不可克隆功能的第二挑战，所述一或多个响应包含来自第一物理不可克隆功能的第一响应及来自第二物理不可克隆功能的第二响应。另外，可通过使用第二响应暴露所述第一挑战而获得中间挑战。可将所接收的第一响应与和所述中间挑战相关联的预先存储的响应进行比较。

[0019] 在又另一实例中，所述一或多个挑战包含用于第二物理不可克隆功能的第一挑战，所述一或多个响应包含来自第一物理不可克隆功能的第一响应。可通过检索对应于第一挑战的预先存储的中间响应而获得中间挑战。可将所接收的第一响应与对应于所述中间挑战的预先存储的中间响应进行比较。

[0020] 在又另一实例中，所述一或多个挑战包含用于第一物理不可克隆功能的第一挑战及用于第二物理不可克隆功能的第二挑战，所述一或多个响应包含第一响应。可通过使用对应于第二挑战的预先存储的第二响应暴露第一响应而获得中间响应。将所述中间响应与和所述第一挑战相关联的预先存储的响应进行比较。

附图说明

[0021] 图1是说明基于SRAM PUF及基于电路延迟的PUF产生用于存储器装置的响应的唯一映射的示范性方式的框图。

[0022] 图2是说明使用用于存储器装置的先前获得的特性响应验证或识别特定存储器装置的示范性方式的框图，其组合SRAM PUF及基于电路延迟的PUF。

[0023] 图3是说明可如何组合SRAM PUF及电路延迟PUF以防止攻击者能够克隆存储器装置的第一实例的框图。

[0024] 图4是说明可如何组合SRAM PUF及电路延迟PUF以防止攻击者能够克隆存储器装置的第二实例的框图。

[0025] 图5是说明可如何组合SRAM PUF及电路延迟PUF以防止攻击者能够克隆存储器装置的第三实例的框图。

[0026] 图6是说明可如何组合SRAM PUF及RO PUF以防止攻击者能够克隆存储器装置的第四实例的框图。

[0027] 图7是说明根据一个实例的数据收集器装置的框图。

[0028] 图8说明在用于从电子装置获得特性信息的数据收集器装置中操作的方法。

[0029] 图9是说明经调适以基于来自每一电子装置内的多个物理不可克隆功能的响应而认证电子装置的示范性认证装置的框图。

[0030] 图10说明在用于基于来自多个物理不可克隆功能的响应而认证电子装置的认证

装置中操作的方法。

[0031] 图11是说明具有多个物理不可克隆功能的示范性电子装置的框图。

[0032] 图12说明在电子装置中操作的用于使用认证装置基于来自多个物理不可克隆功能的响应认证自身的方法。

具体实施方式

[0033] 在以下描述中，给出具体细节以提供对本发明的各种方面的彻底理解。然而，所属领域的技术人员应理解，可以在不具有这些具体细节的情况下实践所述方面。举例来说，可以框图展示电路以便避免以不必要的细节混淆所述方面。在其它情况下，可不详细展示众所周知的电路、结构和技术以便不混淆本发明的方面。

[0034] 本文中使用词“示范性”意指“充当实例、例子或说明”。本文中描述为“示范性”的任何实施方案或方面未必应解释为比本发明的其它方面优选或有利。同样，术语“方面”不要求本发明的所有方面包含所论述的特征、优点或操作模式。

[0035] 概述

[0036] 一个特征实现通过组合静态随机存取存储器(SRAM)PUF及基于电路延迟的PUF(例如，环形振荡器(RO)PUF、仲裁器PUF等)而产生唯一识别符。SRAM PUF自身可容易受到使用缺陷分析工具(例如，聚焦离子束(FIB))的克隆攻击。因此，基于电路延迟的PUF可用于隐藏对SRAM PUF的挑战及/或来自SRAM PUF的响应，进而阻止攻击者能够克隆存储器装置的响应。

[0037] 组合SRAM及基于电路延迟的物理不可克隆功能(PUF)

[0038] 物理不可克隆功能(PUF)是采用电路内的制造工艺变化来获得唯一识别符的挑战-响应机制。在一个实例中，通过电路(例如，集成电路)中的逻辑组件及互连件中的复杂统计变化来确定挑战及对应响应之间的关系。两种类型的PUF包含例如SRAM PUF及电路延迟PUF(例如，环形振荡器PUF)。

[0039] SRAM PUF利用静态随机存取存储器(SRAM)的未初始化的加电状态以产生用于存储器装置或存储器装置集成到其中的电子装置的识别“指纹”。虽然SRAM单元设计是对称的，但制造工艺偏差导致SRAM单元之间的小不对称性，从而导致启动期间的优选/偏置状态(0或1)。未初始化的SRAM单元的此偏好或偏置可用于唯一地识别存储器装置。

[0040] 然而，使用聚焦离子束(FIB)的缺陷分析攻击中的最近进步威胁着基于存储器的PUF的安全性。电路编辑攻击可使用对原始装置的相同SRAM PUF响应产生硬件克隆体。

[0041] 基于电路延迟的PUF利用振荡电路之间的由加工/制造缺陷引起的系统变化。虽然加工/制造工艺试图避免基于电路延迟的PUF中的所述变化，但在某一程度上它们始终存在且实际上可用于识别装置/芯片。在基于电路延迟的PUF的一个实例中，可同时使用多个环形振荡器且至少两个环形振荡器的输出被发送到一或多个开关(多路复用器)。挑战可充当到环形振荡器的输入(例如，挑战用以选择两个环形振荡器)且来自两个选定环形振荡器204的输出表示为第一频率及第二频率。由于所述选定环形振荡器之间的差异，它们的频率将不同(即，产生频率差分)。通过环形振荡器频率的逐对比较(例如，第一和第二频率之间的差异)而产生RO PUF输出(响应)。

[0042] 然而，实施相当大的基于电路延迟的PUF占据集成电路中的大量所需空间。

[0043] 根据一个特征，在电子装置(例如，存储器装置、半导体器件等)内组合SRAM PUF及基于电路延迟的PUF以增强SRAM PUF的安全性。

[0044] 图1是说明基于SRAM PUF及基于电路延迟的PUF(例如，环形振荡器(RO)PUF)而产生用于存储器装置的响应的唯一映射的示范性方式的框图。此框图说明询问及收集用于包括SRAM PUF 105及电路延迟PUF 122(例如，实施为环形振荡器组)的存储器装置102(例如，芯片、半导体装置等)的挑战/响应特性。

[0045] 在一个实例中，可从存储器装置102的所有或部分SRAM单元实施SRAM PUF。具体来说，SRAM PUF 105利用SRAM 106的未初始化的存储器单元104中的偏置。举例来说，在制造阶段期间，可询问未初始化的SRAM 106，使得对于每一挑战110(例如，存储器地址)，获得对应响应112(例如，逻辑0或1)。例如，对于SRAM 106内的每一存储器地址，获得与所述存储器地址相关联的存储器单元104的未初始化值/状态。对于多个挑战110，获得多个响应112。在其它方法中，可仅询问存储器地址的子集。以此方式，建构用于SRAM 106的未初始化值到地址的映射，且可将其存储在数据库114中(例如，以作为挑战及对应响应)。即，可例如在制造或质量控制过程期间建构用于每一存储器装置(芯片)的SRAM PUF挑战/响应114的数据库。举例来说，对于装置A，获得第一组挑战/响应$[C_0R_0,C_1R_1,\cdots,C_iR_i]$，对于装置B，获得第二组挑战/响应$[C_0R_0,C_1R_1,\cdots,C_iR_i]$，且对于装置C，获得第三组挑战挑战/响应$[C_0R_0,C_1R_1,\cdots,C_iR_i]$。应注意，在一些实施方案中，所有装置的挑战$[C_0,C_1,\cdots,C_i]$可相同，但响应将不同。在其它实施方案中，可随机选择每一装置的挑战$[C_0,C_1,\cdots,C_i]$，因此不同装置接收不同挑战。

[0046] 在一个实例中，电路延迟PUF 120可实施为环形振荡器(RO)PUF 122，其利用多个环形振荡器123及它们的频率偏移以产生唯一签名/响应。举例来说，对于给定挑战124(例如，两个环形振荡器输入/输出的选择)，获得对应响应(例如，两个选定环形振荡器之间的频率差异)。以此方式，获得挑战及对应响应的电路延迟PUF数据库128。

[0047] 因为SRAM 106的未初始化的存储器单元状态容易通过聚焦离子束(FIB)攻击被克隆，所以仅使用SRAM PUF 105以提供存储器装置102的唯一识别符是不安全的。然而，不同于SRAM PUF 105，电路延迟PUF 120(例如，RO PUF 122)被容易被克隆，但使用大量RO PUF是不合意的，因为它们占用芯片上的空间。因此，相对少量的环形振荡器123可与存储器装置102(例如，芯片、半导体等)上的SRAM PUF 105组合以阻止对SRAM PUF 102的克隆攻击。

[0048] 为了使挑战/响应与每一装置相关联，装置识别符108(例如，序列号、ID号等)可存储在装置102处且数据库114及128是已知的，或存储在数据库114及128处。即，每一存储器装置102的装置识别符108可经存储且与用于所述存储器装置102的对应挑战及/或响应相关联。

[0049] 图2是说明使用用于存储器装置的先前获得的特性响应验证或识别特定存储器装置的示范性方式的框图，其组合SRAM PUF及基于电路延迟的PUF(例如，环形振荡器(RO)PUF)。在操作期间，装置验证模块/电路202(例如，由验证器或认证装置/服务器实施)可使用挑战204询问存储器装置102以获得响应206，可使用SRAM PUF数据库114及电路延迟PUF数据库128的组合验证所述响应。响应206可用来验证存储器装置的身份或认证存储器装置102。应注意，此技术还可用来产生用于存储器装置的唯一识别符/签名。

[0050] 应注意，在一个实例中，存储器装置102可将其预先存储的/预先指派的装置识别符108提供给装置认证模块/电路/服务器202。装置认证模块/电路/服务器202可随后检索

先前针对所述装置识别符108存储的一或多个挑战且将它们发送204到存储器装置102。替代地，由所述电子装置与对挑战的任何响应一起提供装置识别符108(例如，其中相同挑战用于所有电子装置)。在接收到响应206之后，装置认证模块/电路/服务器202将所接收的响应206与SRAM PUF 114及电路延迟PUF 128中的对应的先前存储的响应进行比较与确定是否存在匹配。

[0051] 在此验证阶段期间，挑战204及响应206可被攻击者存取或是攻击者可存取的。因此，各种特征实现保护去往/来自存储器装置102的挑战204及/或响应206以便阻止攻击者克隆存储器装置102。

[0052] 在一个实例中，电路延迟PUF 120(例如，基于延迟的PUF)是防篡改的。虽然聚焦离子束(FIB)攻击可暴露SRAM PUF 105的存储器单元的响应，但其不提供关于电路延迟PUF 120(例如，环形振荡器)的信息。实际上，用于克隆/攻击存储器装置102的过程可具充分侵入性，其可改变电路延迟PUF 120(例如，环形振荡器)的响应，进而暴露所述攻击且导致对存储器装置102的认证/识别的失败。

[0053] 存在组合SRAM PUF 105及电路延迟PUF 120以甚至在挑战204及响应206对于攻击者是可存取时阻止攻击者克隆存储器装置102的各种方式。

[0054] 组合SRAM及RO物理不可克隆功能(PUF)以掩蔽挑战

[0055] 图3是说明可如何组合SRAM PUF 326及电路延迟PUF 324以防止攻击者能够克隆存储器装置307的第一实例的框图。在此实例中，认证装置300可包含装置认证模块/电路/服务器303、SRAM PUF数据库301及电路延迟PUF数据库305。可例如通过将多个挑战(例如，存储器地址)发送到存储器单元区且获得对应响应(例如，未初始化的存储器单元状态/值)而在制造期间产生存储器装置307的存储器单元区的SRAM PUF数据库301。类似地，可例如通过将多个挑战(例如，两个环形振荡器的选择)发送到环形振荡器且获得对应响应(例如，两个选定环形振荡器之间的频率差分)而在制造期间产生存储器装置307内的多个环形振荡器的电路延迟PUF数据库305。

[0056] 在此实例中，在装置认证模块/电路/服务器303随后尝试认证存储器装置307时，其将挑战(包括挑战A 316及挑战B 312)发送到存储器装置307。挑战A 316可包括已经通过XOR运算302组合的SRAM PUF挑战C_0 306及RO PUF响应R_0 310。因为此挑战A 316可为可由攻击者存取的，所以一个方面通过使用对应RO PUF响应R_0 310(从电路延迟PUF数据库305获得)掩蔽(例如，进行异或运算)实际SRAM PUF挑战C_0 306以产生所传输的(暴露的)挑战A 316而掩盖实际SRAM PUF挑战C_0 306。另外，还将对应于RO PUF响应R_0 310的包含RO PUF挑战C_0 308的挑战B 312从认证装置300发送到存储器装置307。

[0057] 在存储器装置307处，RO PUF挑战C_0 312用于从电路延迟PUF 324产生RO PUF响应R_0 321。挑战A 316随后与RO PUF响应R_0 321进行异或运算304以获得实际(未加密的)SRAM PUF挑战C_0 323，其可用作SRAM PUF 326的挑战。SRAM PUF 326随后产生响应SRAM PUF R_0 325。以此方式，来自存储器装置307的对认证装置300的响应可包含SRAM PUF响应R_0 318。

[0058] 在认证装置300处，所接收的响应SRAM PUF R_0 322可用于与SRAM PUF数据库301及电路延迟PUF 305中的所存储的响应进行比较且确定它们是否匹配。应注意，由于RO PUF响应R_0 310已经已知或存储在电路延迟PUF数据库305中，所以认证装置300能够使用其来用其掩蔽SRAM PUC挑战C_0 306。

[0059] 图4是说明可如何组合SRAM PUF 426及电路延迟PUF 424以防止攻击者能够克隆存储器装置407的第二实例的框图。不同于图3中的实例，在此实例中，SRAM PUF挑战C_0 406及RO PUF挑战C_0 408未加密地从装置认证模块/电路/服务器403发送到存储器装置407。在此实例中，认证装置400可包含装置认证模块/电路/服务器403、SRAM PUF数据库401及电路延迟PUF数据库405。可例如通过将多个挑战(例如，存储器地址)发送到存储器单元区且获得对应响应(例如，未初始化的存储器单元状态/值)而在制造期间产生存储器装置407的存储器单元区的SRAM PUF数据库401。类似地，可例如通过将多个挑战(例如，两个环形振荡器的选择)发送到环形振荡器且获得对应响应(例如，两个选定环形振荡器之间的频率差分)而在制造期间产生存储器装置407内的多个环形振荡器的电路延迟PUF数据库405。

[0060] 在此实例中，在装置认证模块/电路/服务器403随后尝试认证存储器装置407时，其将挑战(包括挑战A 416及挑战B 412)发送到存储器装置407。挑战A 416可包括SRAM PUF挑战C_0 406。挑战B 412包含也从认证装置400发送到存储器装置407的对应于RO PUF响应R_0 410的RO PUF挑战C_0 408。

[0061] 虽然挑战A 416可为可由攻击者存取的，但一个方面通过存储器装置407处的异或操作404而将实际SRAM PUF挑战C_0 406修改为经修改的SRAM PUF挑战C_0'423。在存储器装置407处，RO PUF挑战C_0 412用于从电路延迟PUF 424产生RO PUF响应$R_0$421。挑战A 416(即，SRAM PUF挑战C_0 406)随后与RO PUF响应R_0 421进行异或404以获得经修改的SRAM PUF挑战C_0'423，其可用作SRAM PUF 426的挑战。SRAM PUF426随后产生传回(作为响应A 418)到认证装置400的SRAM PUF响应R_0'425。以此方式，来自存储器装置407的对认证装置400的响应可包含SRAM PUF响应R_0 418。

[0062] 在此方法中，RO PUF响应R_0 421用于修改对存储器单元区426的实际挑战。因为攻击者不能够重现RO PUF响应R_0 421，所以其不知晓用于产生响应SRAM PUF响应R_0'425的经修改的SRAM PUF挑战C_0'423。

[0063] 在认证装置400处，装置认证模块/电路/服务器403可验证SRAM PUF响应R_0'422。此可例如通过使SRAM PUF挑战C_0 406与RO PUF响应R_0 420(从电路延迟PUF数据库405获得)异或402以获得经修改的SRAM PUF挑战C_0'427的本地版本而进行。经修改的SRAM PUF挑战C_0'427的本地版本可随后用于在SRAM PUF数据库401中查找对应响应且将所述响应与所接收的响应SRAM PUF响应R_0'422进行比较。

[0064] 图5是说明可如何组合SRAM PUF 526及电路延迟524PUF以防止攻击者能够克隆存储器装置的第三实例的框图。在此实例中，认证装置500可包含装置认证模块/电路/服务器503、SRAM PUF数据库501及电路延迟PUF数据库505。可例如通过将多个挑战(例如，存储器地址)发送到存储器单元区且获得对应响应(例如，未初始化的存储器单元状态/值)而在制造期间产生存储器装置507的存储器单元区的SRAM PUF数据库501。类似地，可例如通过将多个挑战(例如，两个环形振荡器的选择)发送到环形振荡器且获得对应响应(例如，两个选定环形振荡器之间的频率差分)而在制造期间产生存储器装置507内的多个环形振荡器的电路延迟PUF数据库505。

[0065] 在此实例中，在装置认证模块/电路/服务器503随后尝试认证存储器装置507时，其发送包括RO PUF挑战C_0 508的挑战512，从而具有对应的RO PUF响应R_0。

[0066] 虽然RO PUF挑战C_0 512可为可由攻击者存取的，但电路延迟PUF 524无法被攻击

者复制。在存储器装置507处，RO PUF挑战C_0 512用于从电路延迟PUF 524产生RO PUF响应R_0 521。此RO PUF响应R_0 521随后用作进入SRAM PUF 526中的SRAM PUF挑战C_0 523以获得RO PUF响应R_0 525。在替代性方法中，RO PUF响应R_0 521可用于产生挑战SRAM PUF C_0 523(例如，通过将RO PUF响应R_0 521映射或转换为存储器地址)。SRAM PUF响应R_0 518被发送到认证装置500。

[0067] 在此方法中，RO PUF响应R_0 521用于修改对SRAM PUF 526的实际挑战。因为攻击者不能够重现RO PUF响应R_0 521，所以其不知晓用于产生响应SRAM PUF响应$R_0$525的SRAM PUF挑战C_0 523。

[0068] 在认证装置500处，装置认证模块/电路/服务器503可从电路延迟PUF 505获得对应于所发送的RO PUF挑战C_0 508的RO PUF响应R_0 520。此RO PUF响应R_0 520可充当SRAM PUF挑战C_0 527。装置认证模块/电路/服务器403可验证SRAM PUF响应$R_0$422。SRAM PUF挑战C_0 527可随后用于在SRAM PUF数据库501中查找对应响应且将所述响应与所接收的响应SRAM PUF响应R_0 522进行比较。

[0069] 在图3、4及5中说明的方法中，装置认证模块/电路/服务器303、403及/或503具有对用于SRAM PUF及RO PUF两者的挑战及响应对的存取权。因此，装置认证模块/电路/服务器303、403及/或503能够验证由存储器装置307、407及507执行的操作且验证所述响应。

[0070] 组合SRAM及RO物理不可克隆功能(PUF)以掩蔽响应

[0071] 替代性方法通过使用RO PUF而保护来自存储器装置的SRAM PUF响应。

[0072] 图6是说明可如何组合SRAM PUF 626及RO PUF 624以防止攻击者能够克隆存储器装置607的第四实例的框图。在此实例中，认证装置600可包含装置认证模块/电路/服务器603、SRAM PUF数据库601及电路延迟PUF数据库605。可例如通过将多个挑战(例如，存储器地址)发送到存储器单元区且获得对应响应(例如，未初始化的存储器单元状态/值)而在制造期间产生存储器装置607的存储器单元区的SRAM PUF数据库601。类似地，可例如通过将多个挑战(例如，两个环形振荡器的选择)发送到环形振荡器且获得对应响应(例如，两个选定环形振荡器之间的频率差分)而在制造期间产生存储器装置607内的多个环形振荡器的电路延迟PUF数据库605。

[0073] 在此实例中，在装置认证模块/电路/服务器603随后尝试认证存储器装置607时，其将挑战(包括挑战A 616及挑战B 612)发送到存储器装置607。挑战A 616可包括SRAM PUF挑战C_0 606。挑战B 612包含也从认证装置600发送到存储器装置607的RO PUF挑战C_0 608。

[0074] 在存储器装置604处，RO PUF挑战C_0 612用于从电路延迟PUF 624产生RO PUF响应R_0 621。SRAM PUF挑战C_0 616由SRAM PUF 626处理以产生SRAM PUF响应$R_0$623。随后获得RO PUF响应R_0 621的散列619以作为RO PUF响应R_0'625。RO PUF响应R_0'625随后与SRAM PUF R_0 623进行异或604以获得发射回到装置认证模块/电路/服务器603的组合响应618(例如，SRAM PUF R_0异或RO PUF响应R_0')。以此方式，从SRAM PUF 626到认证装置600的SRAM PUF响应R_0 623可在传输期间受保护。

[0075] 在认证装置600处，装置认证模块/电路/服务器603可验证对应于所发送的挑战SRAM PUF C_0 606及RO PUF C_0 608的响应618。举例来说，使用电路延迟PUF数据库605，获得对应于所发送的RO PUF挑战C_0 608的RO PUF响应R_0 620。随后，装置认证模块/电路/服务器603可通过散列617RO PUF响应R_0 620且异或602所述结果与响应618以获得SRAM PUF响应R_0

627而获得SRAM PUF响应R_0 627。SRAM PUF响应R_0 627可随后用于在SRAM PUF数据库601中查找针对SRAM PUF挑战C_0 606预期的对应响应。如果响应匹配，那么存储器装置607被成功地认证或识别。

[0076] 示范性数据收集器装置及在其中操作的方法

[0077] 图7是说明根据一个实例的数据收集器装置的框图。数据收集器装置702可经调适以收集及存储唯一地表征电子装置(例如，芯片、半导体、存储器装置等)的信息。例如，在制造阶段、质量控制阶段及/或预部署阶段期间，数据收集器装置702可经调适以将挑战发送到每一电子装置且接收对每一电子装置的响应，且存储所接收的信息以供稍后用于认证/识别每一电子装置。

[0078] 数据收集器装置702可包含处理电路704、存储装置706、通信接口708及/或机器可读媒体710。通信接口708可包含发射器/接收电路718，其准许数据收集器装置702与一或多个电子装置通信(例如，有线或无线地)。

[0079] 处理电路704可包含装置识别符电路/模块722，其经调适以获得每一电子装置的唯一识别符且将此唯一识别符存储在存储装置706中的装置识别符数据库716中。处理电路704还可包含挑战产生器电路/模块720，其经调适以产生一或多个挑战且将其发出到电子装置。举例来说，所述挑战可为存储器地址(例如，对于SRAM PUF)或环形振荡器对(例如，对于RO PUF)。处理电路704还可包含SRAM PUF收集电路/模块726，其经调适以响应于所发送的一或多个挑战而收集来自电子装置中的SRAM PUF的响应。处理电路704还可包含电路延迟PUF收集电路/模块726，其经调适以响应于所发送的一或多个挑战而收集来自电子装置中的电路延迟PUF的响应。

[0080] 机器可读媒体710可包含或存储装置识别符指令730(例如，以致使处理电路从被询问的电子装置获得装置识别符)、挑战产生器指令728(例如，以致使处理电路产生/发送到被询问的电子装置的SRAM PUF及/或电路延迟PUF的随机或预先产生的挑战)、SRAM PUF收集指令732(例如，以致使处理电路收集来自被询问的电子装置的SRAM PUF的响应)，及/或电路延迟PUF收集指令734(例如，以致使处理电路收集来自被询问的电子装置的电路延迟PUF的响应)。应注意，在一个实例中，电路延迟PUF可为防篡改PUF。相比之下，已经展示SRAM PUF容易受到各种攻击(例如，聚焦离子束(FIB)攻击、电路编辑攻击等)。

[0081] 数据收集器装置702可经调适以执行图1到6中说明的步骤或功能中的一或多者。

[0082] 图8说明数据收集器装置中操作的用于从电子装置获得特性信息的方法。数据收集器装置可在预部署或制造阶段期间获得(例如，接收或指派)与电子装置相关联的装置识别符802。数据收集器装置可随后产生一或多个挑战且将其发送到电子装置804。因此，数据收集器装置可接收来自电子装置的一或多个响应，所述一或多个响应包含由电子装置中的两种或更多种相异类型的物理不可克隆功能产生的特性信息806。存储装置识别符、挑战及对应响应以用于电子装置的后续认证808。可针对多个电子装置中的每一者重复此过程。应注意，发送到电子装置的挑战可对于所有装置都相同、可针对每一电子装置随机产生，及/或可为可能的挑战的子集。

[0083] 示范性认证装置及在其中操作的方法

[0084] 图9是说明经调适以基于来自每一电子装置内的多个物理不可克隆功能的响应而认证电子装置的示范性认证装置的框图。认证装置902可经调适以询问电子装置(例如，芯

片、半导体、存储器装置等)且尝试基于装置识别符(例如,从电子装置获得)而识别电子装置,且通过执行涉及对电子装置中的SRAM PUF及电路延迟PUF的挑战的询问而认证所述电子装置。认证装置902可包含处理电路904、存储装置906、通信接口908及/或机器可读媒体910。通信接口908可包含准许认证装置902与一或多个电子装置通信(例如,有线或无线地)的发射器/接收器电路918。

[0085] 处理电路904可包含经调适以从电子装置获得唯一装置识别符的装置识别符电路/模块922。使用所获得的装置识别符,认证电路/模块936可检查装置识别符数据库916(存储装置906中)以用于与装置识别符相关联的对应挑战/响应信息。与SRAM PUF验证电路/模块924及电路延迟PUF验证电路/模块926合作的认证电路/模块936随后可将对应挑战中的一或多者发送到电子装置,且获得对所述挑战的一或多个响应。应注意,在一个实例中,电路延迟PUF可为防篡改PUF。相比之下,已经展示SRAM PUF容易受到各种攻击(例如,聚焦离子束(FIB)攻击、电路编辑攻击等)。

[0086] SRAM PUF验证电路/模块924及电路延迟PUF验证电路/模块926可使用结合挑战的所述响应分别从SRAM PUF数据库914(存储装置906中)及电路延迟PUF数据库912(存储装置906中)确定它们是否正确地匹配预期响应(即,匹配对应于数据库914及916中的挑战的响应)。如果所接收的响应匹配先前存储的对应响应,那么认证电路/模块936可得出电子装置被成功地认证的结论。此成功认证可为概率性匹配,其中只要正确地匹配阈值百分比或数目的响应,便可得出成功匹配的结论。

[0087] 机器可读媒体910可包含或存储装置识别符指令930(例如,以致使处理电路从被验证的电子装置获得装置识别符)、SRAM PUF验证指令932(例如,以致使处理电路验证来自被验证的电子装置的SRAM PUF的响应)、电路延迟PUF验证指令934(例如,以致使处理电路验证来自被验证的电子装置的电路延迟PUF的响应),及/或认证指令938,以确定SRAM PUF及电路延迟PUF验证两者是否已经成功。

[0088] 数据收集器装置902可经调适以执行图1到6中说明的步骤或功能中的一或多者。

[0089] 图10说明认证装置中操作的用于基于来自多个物理不可克隆功能的响应而认证电子装置的方法。认证装置可在后部署阶段期间获得(例如,请求或接收)与电子装置相关联的装置识别符1002。认证装置可获得一或多个挑战且将其发送到电子装置1004。例如,所述挑战可为用于所有电子装置的挑战的预定义集合。替代地,所述挑战可为使用装置识别符从数据库获得的用于电子装置的挑战的特定子集。作为发送所述一或多个挑战的结果,认证装置可从电子装置接收一或多个响应,所述一或多个响应包含由电子装置中的两种或更多种相异类型的物理不可克隆功能产生的特性信息1006。在各种实施方案中,认证装置可如参考图1、2、3、4、5及/或6所说明及描述而操作。

[0090] 装置识别符可用于识别电子装置专有的预先存储的挑战及对应响应1008。认证装置可随后通过将用于电子装置的预先存储的响应及所接收的一或多个响应进行比较而认证所述电子装置1010。在所接收的一或多个响应匹配用于电子装置的预先存储的响应时,发生成功认证。成功认证可为概率性匹配,其中只要正确地匹配阈值百分比或数目的响应,便可得出成功匹配的结论。可针对多个电子装置中的每一者重复此过程。由于每一电子装置使用物理不可克隆功能,所以即使相同挑战用于所有装置,但所述一或多个响应将是不同的。

[0091] 示范性电子装置及在其中操作的方法

[0092] 图11是说明具有多个物理不可克隆功能的示范性电子装置的框图。电子装置1102可为芯片、半导体、存储器装置等，且经调适以提供装置识别符且响应于对电子装置中的SRAM PUF及电路延迟PUF的挑战。电子装置1102可包含处理电路1104、装置识别符1116(存储装置中)、基于延迟的PUF电路1112(例如，多个振荡器环电路)、静态随机存取存储器1116(其可用作SRAM PUF)、通信接口1108及/或机器可读媒体1110。通信接口1108可包含准许电子装置1102与一或多个数据收集器及/或认证装置通信(例如，有线或无线地)的发射器/接收器电路1118。

[0093] 处理电路1104可包含装置识别符电路/模块1122，其经调适以将其唯一装置识别符1116提供到数据收集器及/或认证装置。所述处理电路还可包含SRAM PUF响应电路/模块1124及电路延迟PUF响应电路/模块1126，其经调适以获得对所接收的挑战的响应且将所述响应发送到数据收集器装置及认证装置。应注意，在一个实例中，所述电路延迟PUF可为防篡改PUF。相比之下，已经展示SRAM PUF容易受到各种攻击(例如，聚焦离子束(FIB)攻击、电路编辑攻击等)。

[0094] SRAM PUF响应电路/模块1124可将所接收的挑战发送到静态随机存取存储器1114以获得响应。例如，响应可为静态随机存取存储器1114的一或多个存储器单元的未初始化状态。类似地，电路延迟PUF响应电路/模块1126可将所接收的挑战发送到基于延迟的PUF电路1112以获得响应。

[0095] 机器可读媒体1110可包含或存储装置识别符指令1130(例如，以致使处理电路获得用于电子装置的装置识别符1116)、SRAM PUF响应指令1132(例如，以致使处理电路从电子装置的静态随机存取存储器1114获得响应)，及/或电路延迟PUF响应指令1134(例如，以致使处理电路从电子装置的电路延迟PUF获得响应)。

[0096] 电子装置1102可经调适以执行图1到6中说明的步骤或功能中的一或多者。

[0097] 图12说明在电子装置中操作的用于使用认证装置基于来自多个物理不可克隆功能的响应认证自身的方法。电子装置可能已经在预部署或制造阶段期间接收到一或多个挑战且提供了一或多个对应响应。

[0098] 电子装置使用电子装置内的多个存储器单元实施第一物理不可克隆功能1204。在一个实例中，第一物理不可克隆功能可使用一或多个存储器单元的未初始化的存储器单元状态作为对所述挑战的响应。

[0099] 电子装置还可使用电子装置内的多个基于电路延迟的路径实施第二物理不可克隆功能1206。在一个实例中，所述多个基于电路延迟的路径及/或另外防篡改。术语“防篡改”是指在尝试对其篡改以预测、确定及/或读取其响应或输出时此致使所述响应及/或输出改变的PUF的实施方案或类型。例如，物理上篡改环形振荡器或电路延迟路径类型振荡器的尝试将导致环形振荡器或电路延迟路径的响应被更改(例如，输出频率改变)。

[0100] 可从外部服务器接收挑战1208。可通过使用来自第二物理不可克隆功能的第一响应进行以下操作而将所述挑战应用于第一物理不可克隆功能：(a)掩蔽/暴露输入到第一物理不可克隆功能的挑战，(b)产生输入到第一物理不可克隆功能的挑战，或(c)掩蔽从第一物理不可克隆功能输出的响应1210。在一个实例中，所述第一挑战可识别所述多个存储器单元内的存储器地址。在另一实例中，所述挑战可从第二物理不可克隆功能中的所述多个

环形振荡器选择两个环形振荡器且使用所述两个环形振荡器之间的频率差分作出响应。可接收所述挑战以作为以下各者中的至少一者:电子装置的认证过程、电子装置的识别过程及/或电子装置内的密钥产生过程。

[0101] 来自第二物理不可克隆功能的第一响应及/或来自第一物理不可克隆功能的第二响应可随后被发送到外部服务器1212。所述外部服务器可包含用于第一物理不可克隆功能的挑战及响应的第一数据库及用于第二物理不可克隆功能的挑战及响应的第二数据库,其中外部服务器将所述挑战发送到电子装置且基于所述第二响应而认证或识别所述电子装置。

[0102] 可接收所述响应被外部服务器成功地验证的指示符1214。举例来说,在成功认证之后,电子装置可接收其已获得对网络及/或数据的存取权的指示符。

[0103] 在一个实例中,所述挑战包含用于第一物理不可克隆功能的第一挑战及用于第二物理不可克隆功能的第二挑战。举例来说,所述第一挑战可为由对第二挑战的预期响应掩蔽的挑战(如图3中所说明)。在另一情况下,可在所述第一物理不可克隆功能进行处理之前通过来自第二物理不可克隆功能的第一响应修改所述第一挑战(如图4中所说明)。

[0104] 在又另一实例中,所接收的挑战可由第二物理不可克隆功能使用以产生第一响应,所述第一响应随后由第一物理不可克隆功能用作第二挑战以产生第二响应(如图5中所说明)。

[0105] 在另一实施方案中,所述挑战可包含用于第一物理不可克隆功能的第一挑战及用于第二物理不可克隆功能的第二挑战,所述第二挑战可由第二物理不可克隆功能使用以产生第一响应,所述第一响应用于掩蔽来自第一物理不可克隆功能的第二响应(如图6中所说明)。所述方法可进一步包含:(a)散列来自第二物理不可克隆功能的第一响应以获得中间响应;和/或(b)使用中间响应掩蔽第二响应。

[0106] 在一个实例中,还可预先提供电子装置内的预先存储的装置识别符1202。其可(a)在接收所述挑战之前或(b)与发送第二响应同时地将预先存储的装置识别符从电子装置发送到外部服务器。所述装置识别符唯一地识别电子装置。

[0107] 图1到12中所说明的组件、步骤、特征及/或功能中的一或多者可以重新布置及/或组合成单个组件、步骤、特征或功能或体现在若干组件、步骤或功能中。在不脱离本发明的情况下,还可以添加额外的元件、组件、步骤及/或功能。图1到7、9及11中说明的设备、装置及/或组件可经配置以执行图8、10及12中所描述的方法、特征或步骤中的一或多者。本文中所描述的算法也可以有效地实施于软件中及/或嵌入于硬件中。

[0108] 此外,在本发明的一个方面中,图7、9及11中说明的处理电路704、904及1104可为分别经专门设计及/或硬连线以执行图8、10及12中所描述的算法、方法及/或步骤的专用处理器(例如,专用集成电路(例如,ASIC))。因此,此专用处理器(例如,ASIC)可为执行图8、10及12中所描述的算法、方法及/或步骤的装置的一个实例。

[0109] 并且,应注意,可将本发明的各方面描述为过程,所述过程被描绘为流程图、流图、结构图或框图。尽管流程图可将操作描述为连续过程,但许多操作可并行或同时执行。另外,可以重新布置操作的顺序。过程在其操作完成时终止。过程可以对应于方法、功能、程序、子例程、子程序等。当过程对应于函数时,其终止对应于函数返回到调用函数或主函数。

[0110] 此外,存储媒体可表示用于存储数据的一或多个装置,包含只读存储器(ROM)、随

机存取存储器(RAM)、磁盘存储媒体、光学存储媒体、快闪存储器装置和/或其它机器可读媒体;以及用于存储信息的处理器可读媒体和/或计算机可读媒体。术语“机器可读媒体”、“计算机可读媒体”和/或“处理器可读媒体”可包含(但不限于)非暂时性媒体(例如,便携式或固定存储装置)、光学存储装置和能够存储、含有或携载指令和/或数据的各种其它媒体。因此,本文中描述的各种方法可完全或部分地由可存储在“机器可读媒体”、“计算机可读媒体”和/或“处理器可读媒体”中且由一或多个处理器、机器和/或装置执行的指令和/或数据来实施。

[0111] 此外,本发明的方面可以由硬件、软件、固件、中间件、微码或其任何组合实施。当以软件、固件、中间件或微码实施时,用以执行必要任务的程序代码或代码段可存储在例如存储媒体或其它存储装置的机器可读媒体中。处理器可执行必要任务。代码段可以表示步骤、函数、子程序、程序、例程、子例程、模块、软件包、类,或指令、数据结构或程序语句的任意组合。代码段可以通过传递和/或接收信息、数据、自变量、参数或存储器内容而耦合到另一代码段或硬件电路。信息、自变量、参数、数据等可经由包含存储器共享、消息传递、权标传递、网络传输等任何合适的手段传递、转发或传输。

[0112] 结合本文中揭示的实例描述的各种说明性逻辑块、模块、电路、元件及/或组件可以用通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其它可编程逻辑组件、离散门或晶体管逻辑、离散硬件组件或其经设计以执行本文中描述的功能的任何组合来实施或执行。通用处理器可为微处理器,但在替代方案中,处理器可以为任何常规的理器、控制器、微控制器或状态机。处理器还可实施为计算组件的组合,例如DSP与微处理器的组合、多个微处理器的组合、一或多个微处理器与DSP核心的结合,或任何其它此类配置。

[0113] 结合本文中揭示的实例而描述的方法或算法可以处理单元、编程指令或其它方向的形式直接体现在硬件、可由处理器执行的软件模块或两者的组合中,且可含于单个装置中或跨越多个装置而分布。软件模块可驻留在RAM存储器、快闪存储器、ROM存储器、EPROM存储器、EEPROM存储器、寄存器、硬盘、可装卸磁盘、CD-ROM,或此项技术中已知的任何其它形式的存储媒体中。存储媒体可耦合到处理器,使得处理器可从存储媒体读取信息和将信息写入到存储媒体。在替代方案中,存储媒体可集成到处理器。

[0114] 所属领域的技术人员将进一步了解,结合本文所揭示的方面描述的各种说明性逻辑块、模块、电路及算法步骤可以实施为电子硬件、计算机软件或两者的组合。为清晰地说明硬件与软件的此可互换性,以上已大体就其功能性来描述了各种说明性组件、块、模块、电路和步骤。此类功能性是实施为硬件还是软件取决于具体应用及施加于整个系统的设计约束。

[0115] 本文所描述的本发明的各种特征可在不脱离本发明的情况下实施于不同系统中。应注意,本发明的前述方面仅为实例,且不应解释为限制本发明。本发明的各方面的描述既定是说明性的,且不限制权利要求书的范围。因此,本发明的教示可容易应用于其它类型的设备,且所属领域的技术人员将明白许多替代方案、修改及变化。

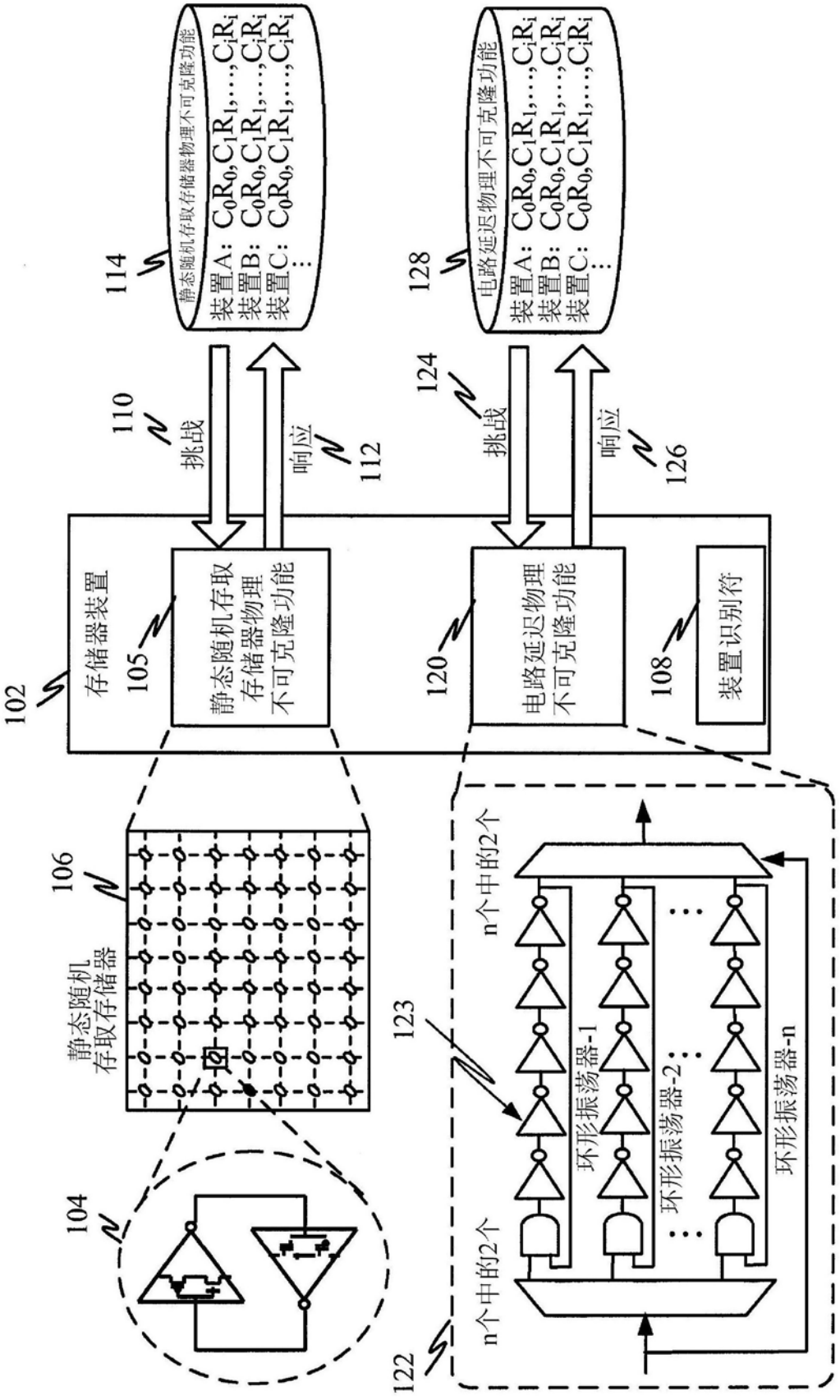

静态随机存取存储器物理不可克隆功能
装置A: C0R0,C1R1,...,CiRi
装置B: C0R0,C1R1,...,CiRi
装置C: C0R0,C1R1,...,CiRi
114
128
电路延迟物理不可克隆功能
装置A: C0R0,C1R1,...,CiRi
装置B: C0R0,C1R1,...,CiRi
装置C: C0R0,C1R1,...,CiRi
110
挑战
响应
112
124
挑战
响应
126
102
存储器装置
105
静态随机存取存储器物理不可克隆功能
120
电路延迟物理不可克隆功能
108
装置识别符
106
静态随机存取存储器
104
123
n个中的2个
环形振荡器-1
环形振荡器-2
环形振荡器-n
n个中的2个
122

图1

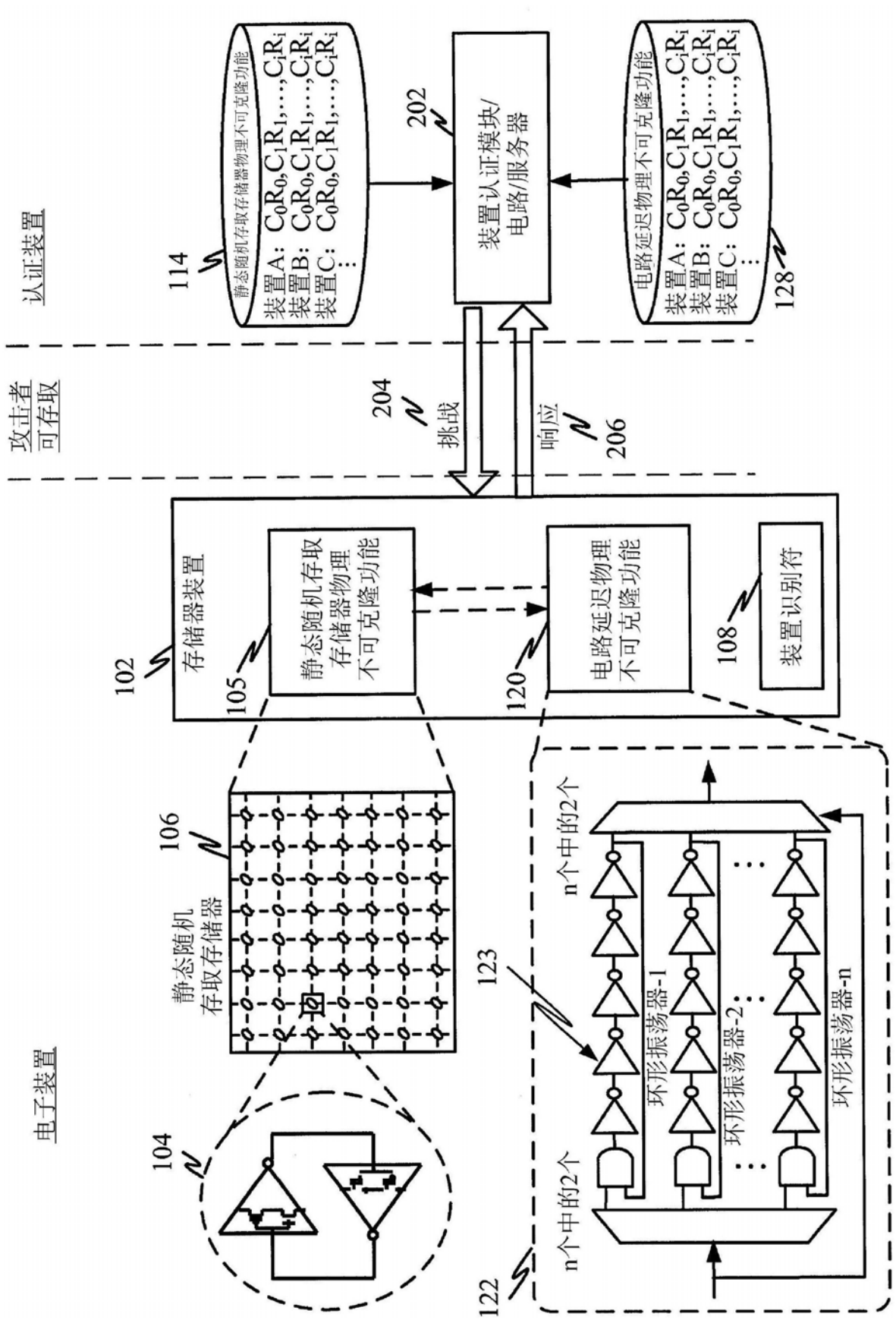

认证装置
攻击者
可存取
电子装置
静态随机存取存储器物理不可克隆功能
装置A: C0R0,C1R1,...,CiRi
装置B: C0R0,C1R1,...,CiRi
装置C: C0R0,C1R1,...,CiRi
114
202
装置认证模块/
电路/服务器
电路延迟物理不可克隆功能
装置A: C0R0,C1R1,...,CiRi
装置B: C0R0,C1R1,...,CiRi
装置C: C0R0,C1R1,...,CiRi
128
204
挑战
响应
206
102
存储器装置
105
静态随机存取存储器物理不可克隆功能
120
电路延迟物理不可克隆功能
108
装置识别符
106
静态随机存取存储器
104
123
n个中的2个
环形振荡器-1
环形振荡器-2
环形振荡器-n
n个中的2个
122

图2

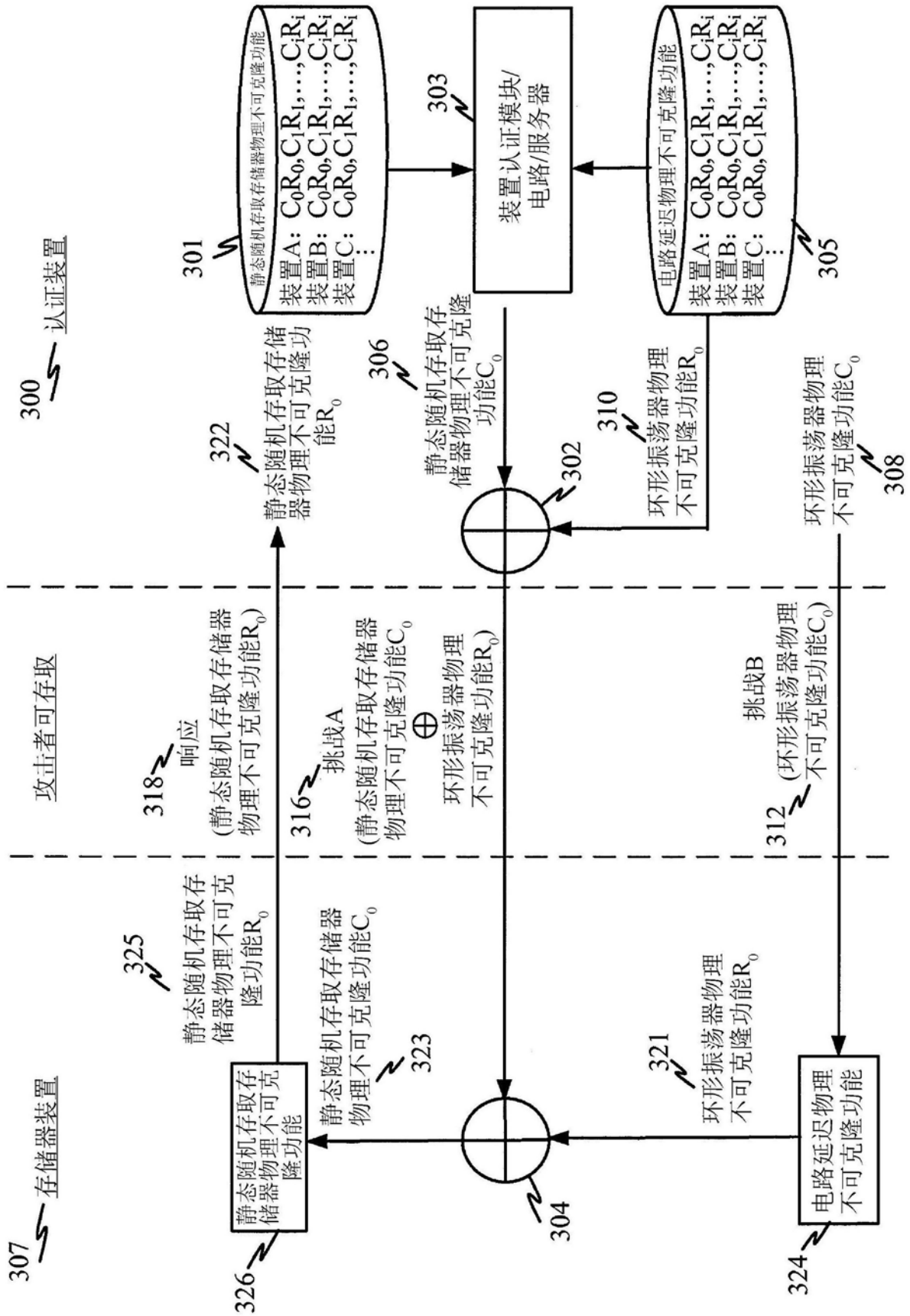

300 认证装置
307 存储器装置
攻击者可存取
静态随机存取存储器物理不可克隆功能
静态随机存取存储器物理不可克隆功能C_0
环形振荡器物理不可克隆功能R_0
电路延迟物理不可克隆功能
静态随机存取存储器物理不可克隆功能R_0
静态随机存取存储器物理不可克隆功能C_0
环形振荡器物理不可克隆功能R_0
环形振荡器物理不可克隆功能C_0
301 静态随机存取存储器物理不可克隆功能
装置A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
装置B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
装置C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
303 装置认证模块/电路/服务器
305 电路延迟物理不可克隆功能
装置A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
装置B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
装置C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
302
304
306 静态随机存取存储器物理不可克隆功能C_0
308 环形振荡器物理不可克隆功能C_0
310 环形振荡器物理不可克隆功能R_0
312 挑战B (环形振荡器物理不可克隆功能C_0)
316 挑战A (静态随机存取存储器物理不可克隆功能C_0 ⊕ 环形振荡器物理不可克隆功能R_0)
318 响应 (静态随机存取存储器物理不可克隆功能R_0)
321 环形振荡器物理不可克隆功能R_0
322 静态随机存取存储器物理不可克隆功能R_0
323 静态随机存取存储器物理不可克隆功能C_0
324 电路延迟物理不可克隆功能
325 静态随机存取存储器物理不可克隆功能R_0
326 静态随机存取存储器物理不可克隆功能

图3

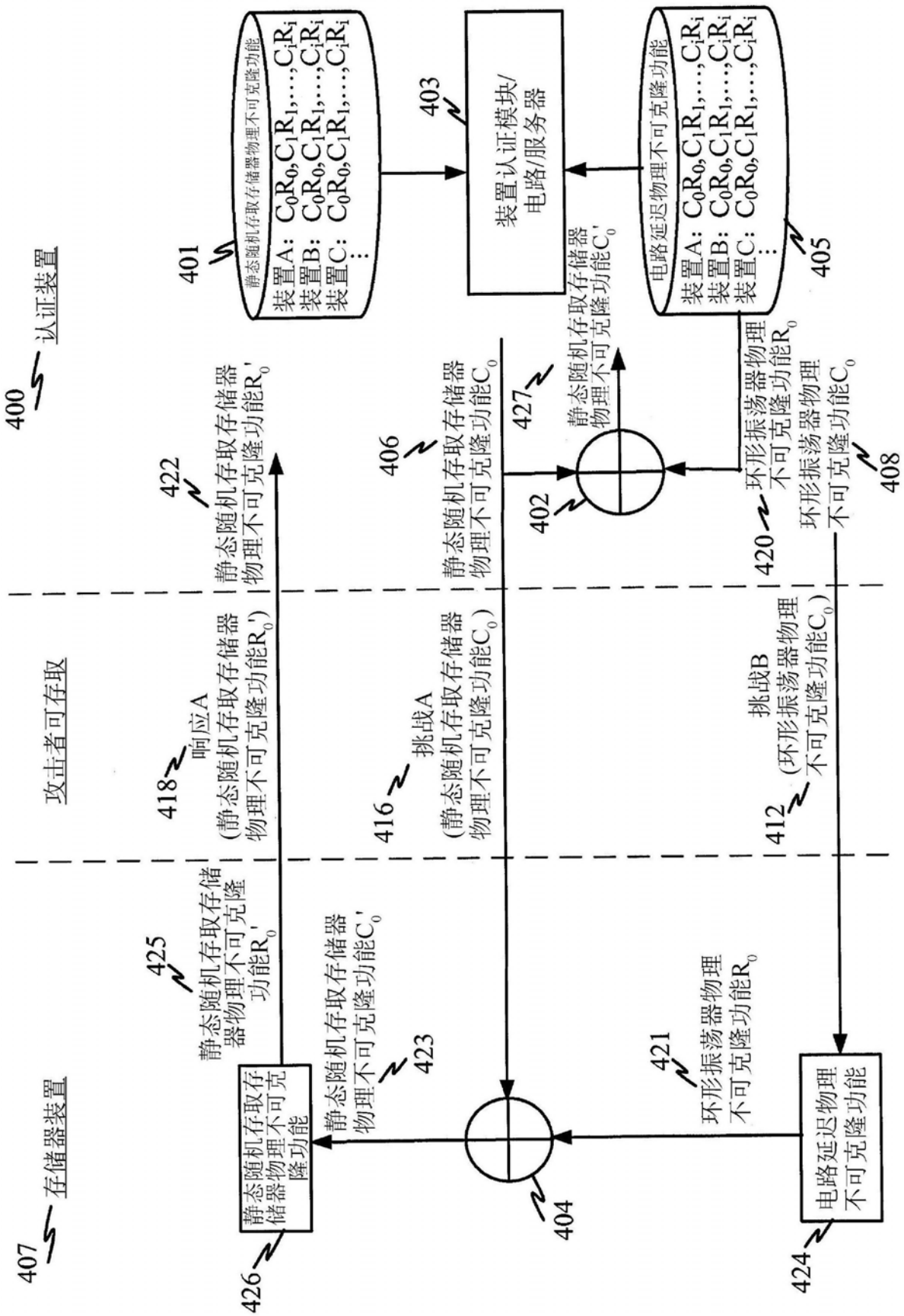

400 认证装置
401
静态随机存取存储器物理不可克隆功能
装置A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
装置B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
装置C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
403
装置认证模块/电路/服务器
405
电路延迟物理不可克隆功能
装置A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
装置B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
装置C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
攻击者可存取
407 存储器装置
422 静态随机存取存储器物理不可克隆功能R_0'
406 静态随机存取存储器物理不可克隆功能C_0
427 静态随机存取存储器物理不可克隆功能C_0'
402
420 环形振荡器物理不可克隆功能R_0
408 环形振荡器物理不可克隆功能C_0
418 响应A (静态随机存取存储器物理不可克隆功能R_0')
416 挑战A (静态随机存取存储器物理不可克隆功能C_0)
412 挑战B (环形振荡器物理不可克隆功能C_0)
425 静态随机存取存储器物理不可克隆功能R_0'
423 静态随机存取存储器物理不可克隆功能C_0'
421 环形振荡器物理不可克隆功能R_0
426 静态随机存取存储器物理不可克隆功能
404
424 电路延迟物理不可克隆功能

图4

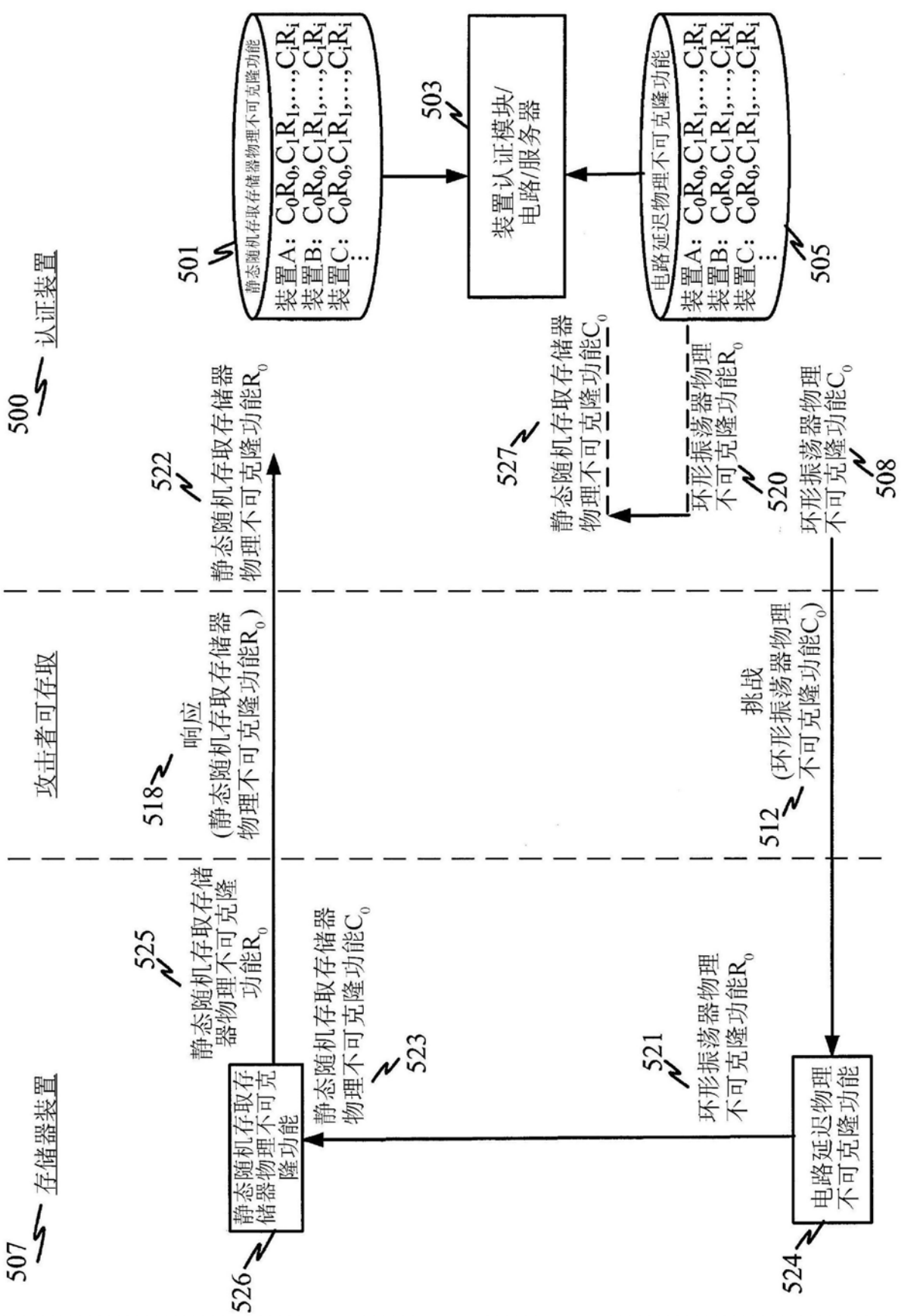

500 认证装置
501
静态随机存取存储器物理不可克隆功能
装置A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
装置B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
装置C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
503
装置认证模块/电路/服务器
505
电路延迟物理不可克隆功能
装置A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
装置B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
装置C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
522
静态随机存取存储器物理不可克隆功能R_0
527
静态随机存取存储器物理不可克隆功能C_0
环形振荡器物理不可克隆功能R_0
520
环形振荡器物理不可克隆功能C_0
508
攻击者可存取
518
响应
(静态随机存取存储器物理不可克隆功能R_0)
挑战
(环形振荡器物理不可克隆功能C_0)
512
525
静态随机存取存储器物理不可克隆功能R_0
静态随机存取存储器物理不可克隆功能C_0
523
环形振荡器物理不可克隆功能R_0
521
507 存储器装置
静态随机存取存储器物理不可克隆功能
526
电路延迟物理不可克隆功能
524

图5

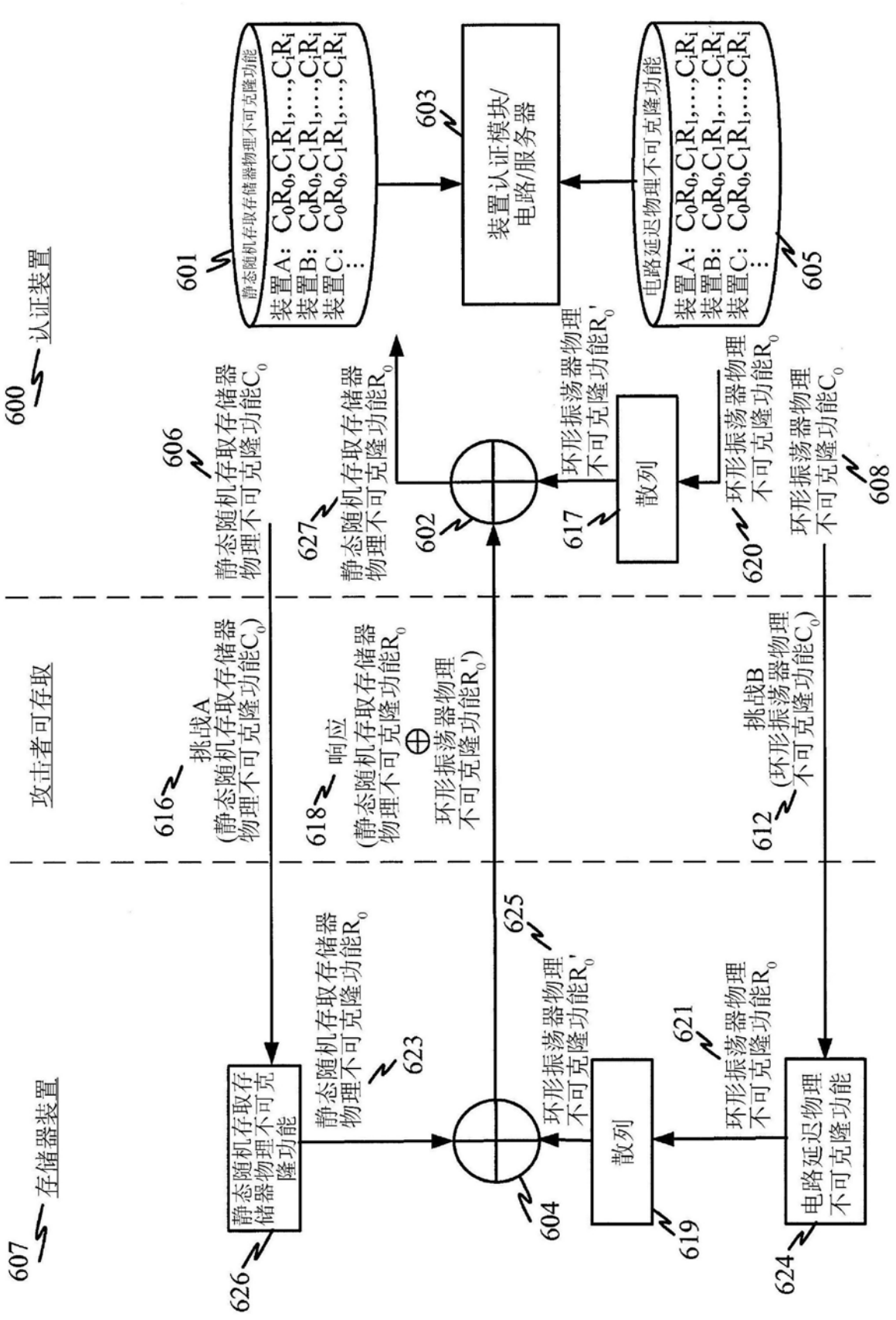

600 认证装置
601
静态随机存取存储器物理不可克隆功能
装置A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
装置B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
装置C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
603
装置认证模块/电路/服务器
605
电路延迟物理不可克隆功能
装置A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
装置B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
装置C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
606
静态随机存取存储器物理不可克隆功能C_0
627
静态随机存取存储器物理不可克隆功能R_0
602
环形振荡器物理不可克隆功能R_0'
617
散列
620
环形振荡器物理不可克隆功能R_0
608
环形振荡器物理不可克隆功能C_0
攻击者可存取
616
挑战A
(静态随机存取存储器物理不可克隆功能C_0)
618
响应
(静态随机存取存储器物理不可克隆功能R_0
⊕
环形振荡器物理不可克隆功能R_0')
612
挑战B
(环形振荡器物理不可克隆功能C_0)
607 存储器装置
静态随机存取存储器物理不可克隆功能
626
静态随机存取存储器物理不可克隆功能R_0
623
625
环形振荡器物理不可克隆功能R_0'
604
散列
619
621
环形振荡器物理不可克隆功能R_0
电路延迟物理不可克隆功能
624

图6

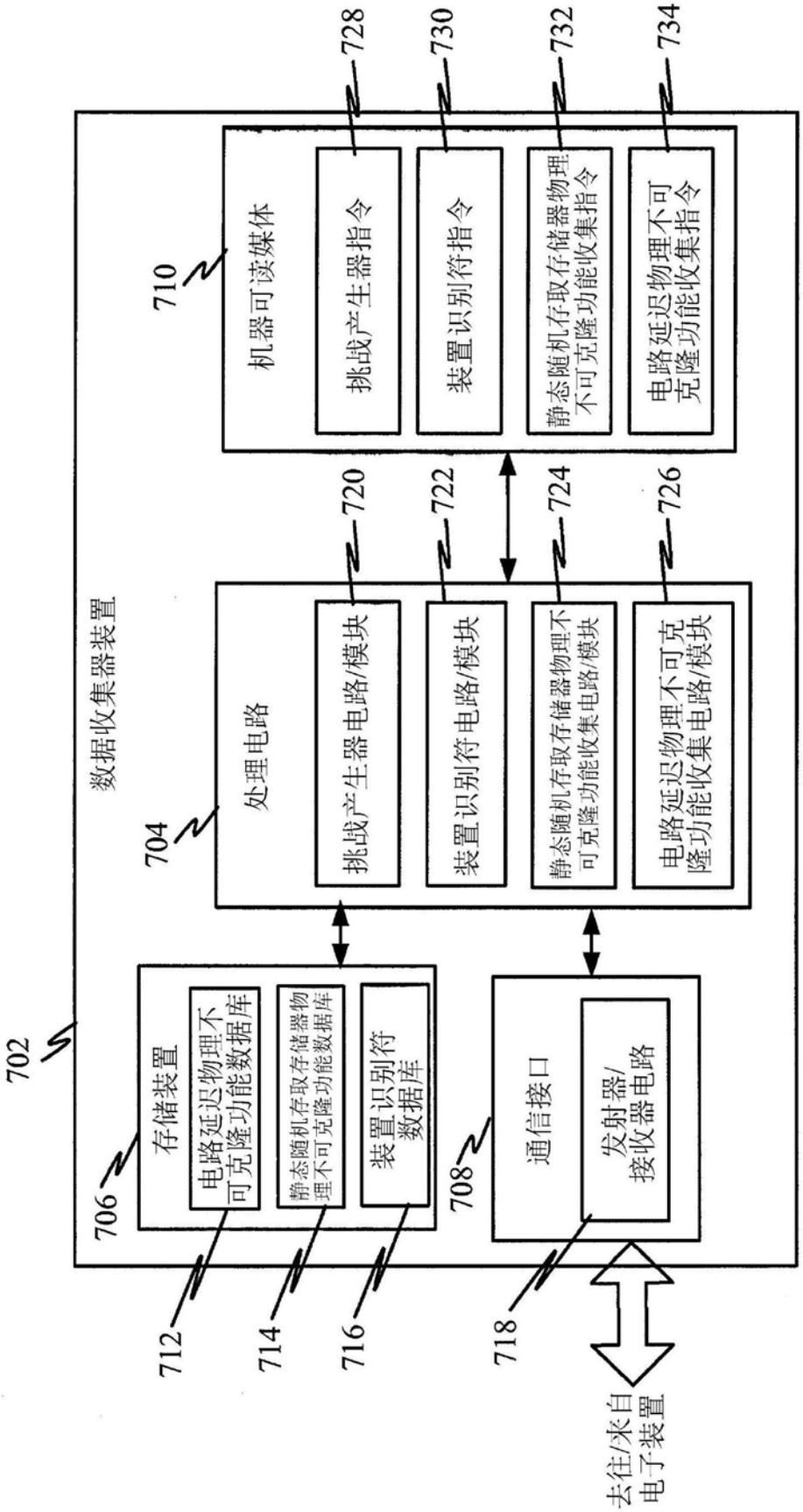

数据收集器装置
702
机器可读媒体
710
挑战产生器指令
728
装置识别符指令
730
静态随机存取存储器物理不可克隆功能收集指令
732
电路延迟物理不可克隆功能收集指令
734
处理电路
704
挑战产生器电路/模块
720
装置识别符电路/模块
722
静态随机存取存储器物理不可克隆功能收集电路/模块
724
电路延迟物理不可克隆功能收集电路/模块
726
存储装置
706
电路延迟物理不可克隆功能数据库
静态随机存取存储器物理不可克隆功能数据库
装置识别符数据库
通信接口
708
发射器/接收器电路
712
714
716
718
去往/来自电子装置

图7

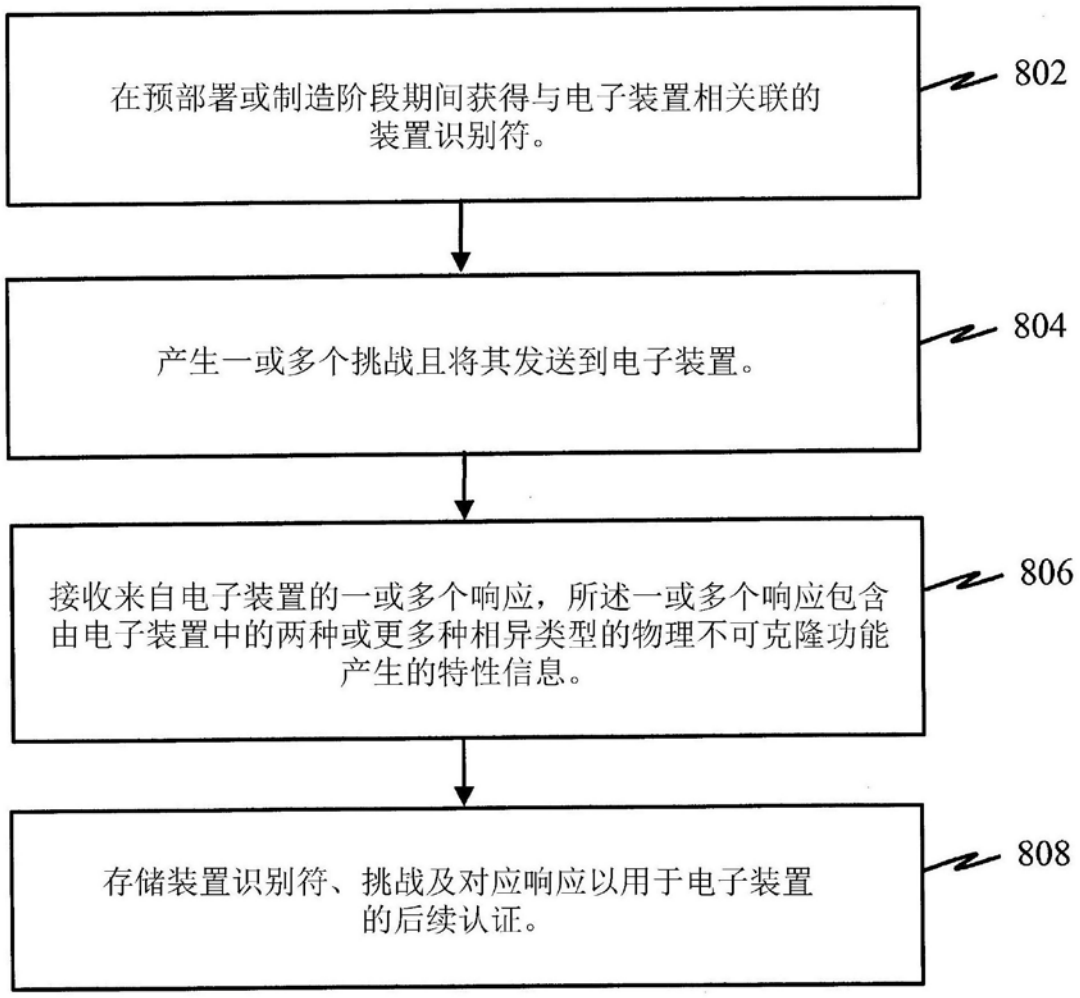

在预部署或制造阶段期间获得与电子装置相关联的装置识别符。
802
产生一或多个挑战且将其发送到电子装置。
804
接收来自电子装置的一或多个响应，所述一或多个响应包含由电子装置中的两种或更多种相异类型的物理不可克隆功能产生的特性信息。
806
存储装置识别符、挑战及对应响应以用于电子装置的后续认证。
808
在数据收集器装置上操作的方法

图8

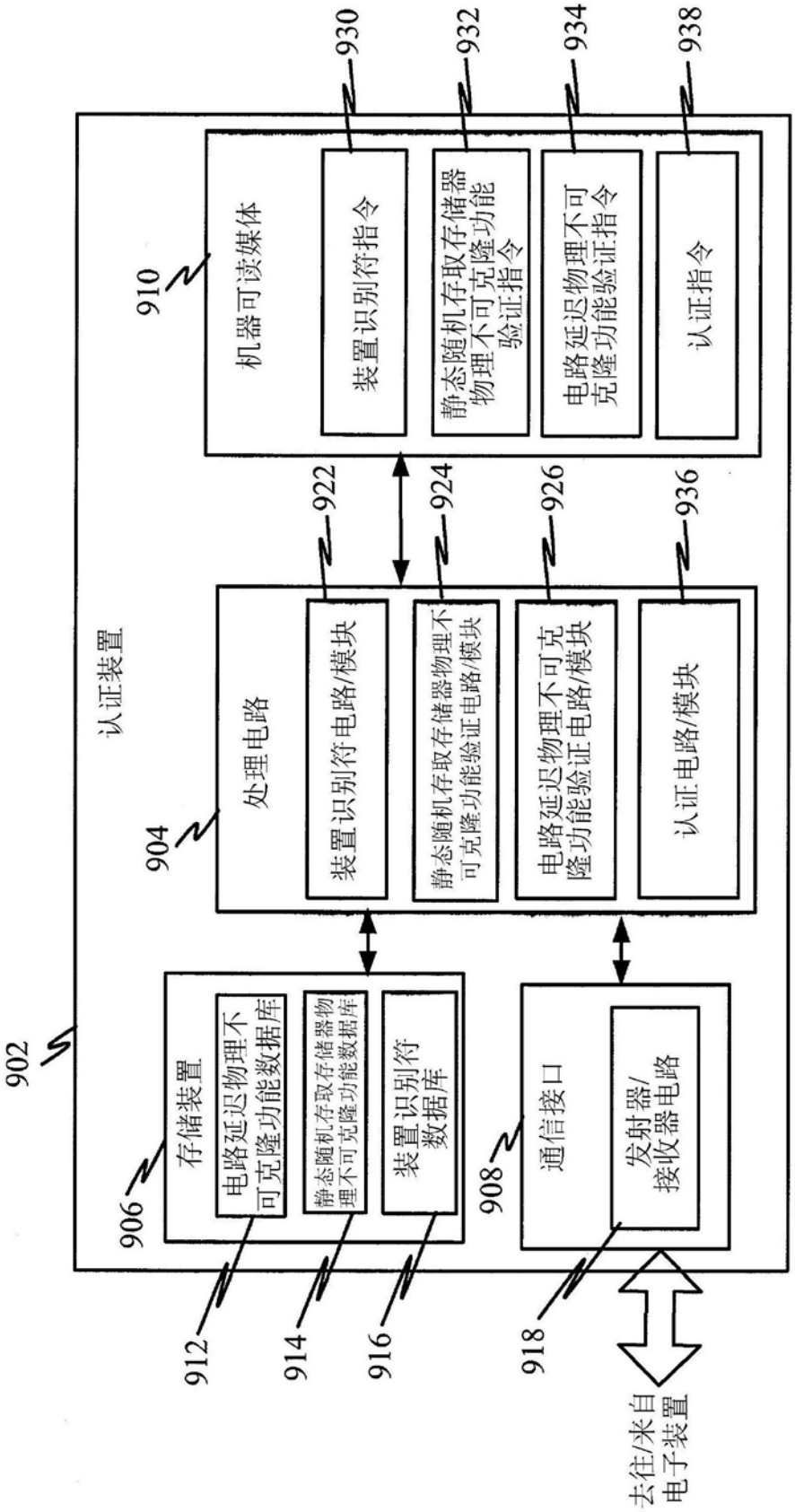
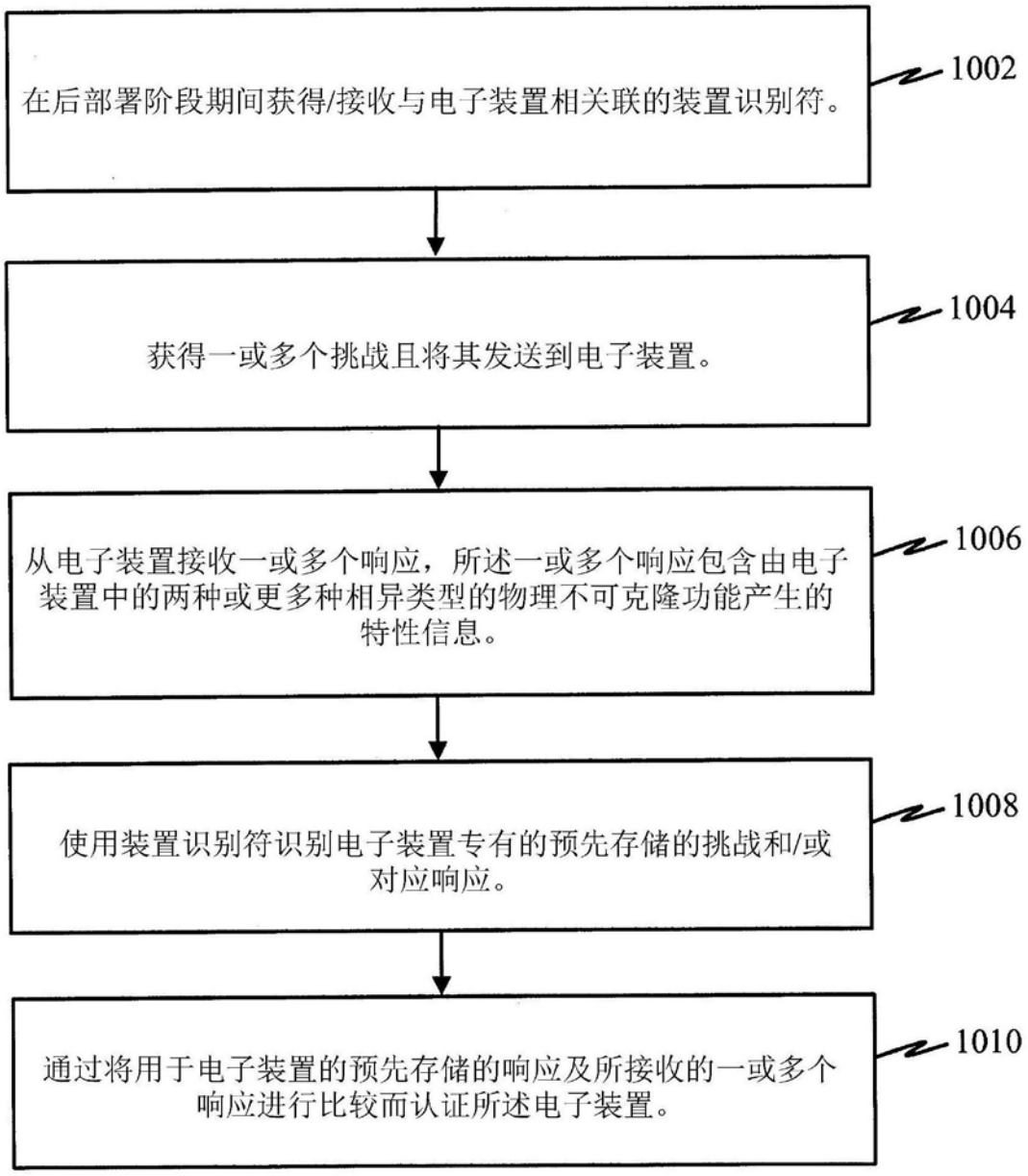

902
认证装置
904
处理电路
906
存储装置
908
通信接口
910
机器可读媒体
912
914
916
918
922
924
926
936
930
932
934
938
装置识别符电路/模块
静态随机存取存储器物理不可克隆功能验证电路/模块
电路延迟物理不可克隆功能验证电路/模块
认证电路/模块
电路延迟物理不可克隆功能数据库
静态随机存取存储器物理不可克隆功能数据库
装置识别符数据库
发射器/接收器电路
装置识别符指令
静态随机存取存储器物理不可克隆功能验证指令
电路延迟物理不可克隆功能验证指令
认证指令
去往/来自电子装置

图9



在认证装置上操作的方法

图10

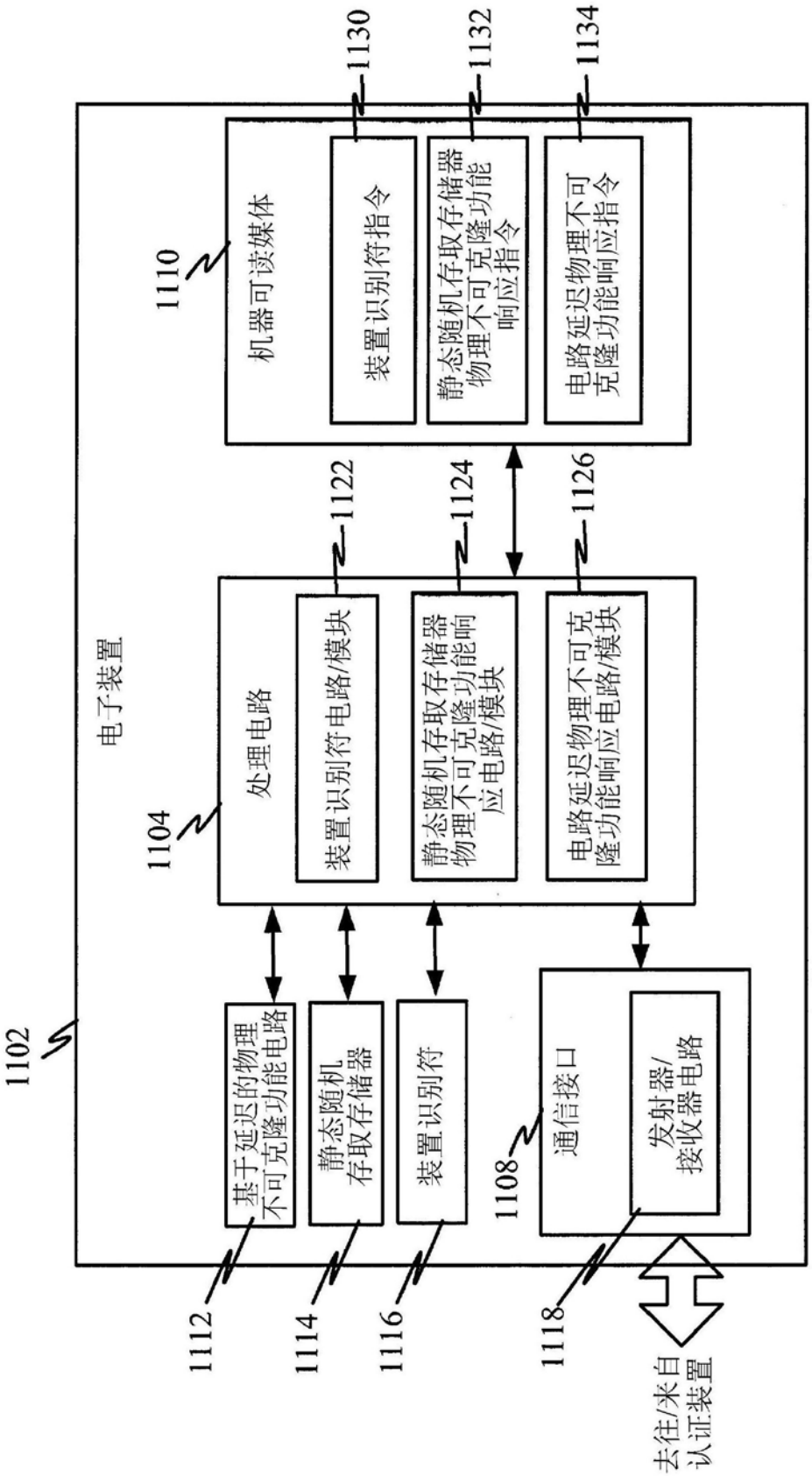

1102
电子装置
1104
处理电路
装置识别符电路/模块
静态随机存取存储器物理不可克隆功能响应电路/模块
电路延迟物理不可克隆功能响应电路/模块
1110
机器可读媒体
装置识别符指令
静态随机存取存储器物理不可克隆功能响应指令
电路延迟物理不可克隆功能响应指令
1122
1124
1126
1130
1132
1134
基于延迟的物理不可克隆功能电路
静态随机存取存储器
装置识别符
1108
通信接口
发射器/接收器电路
1112
1114
1116
1118
去往/来自认证装置

图11

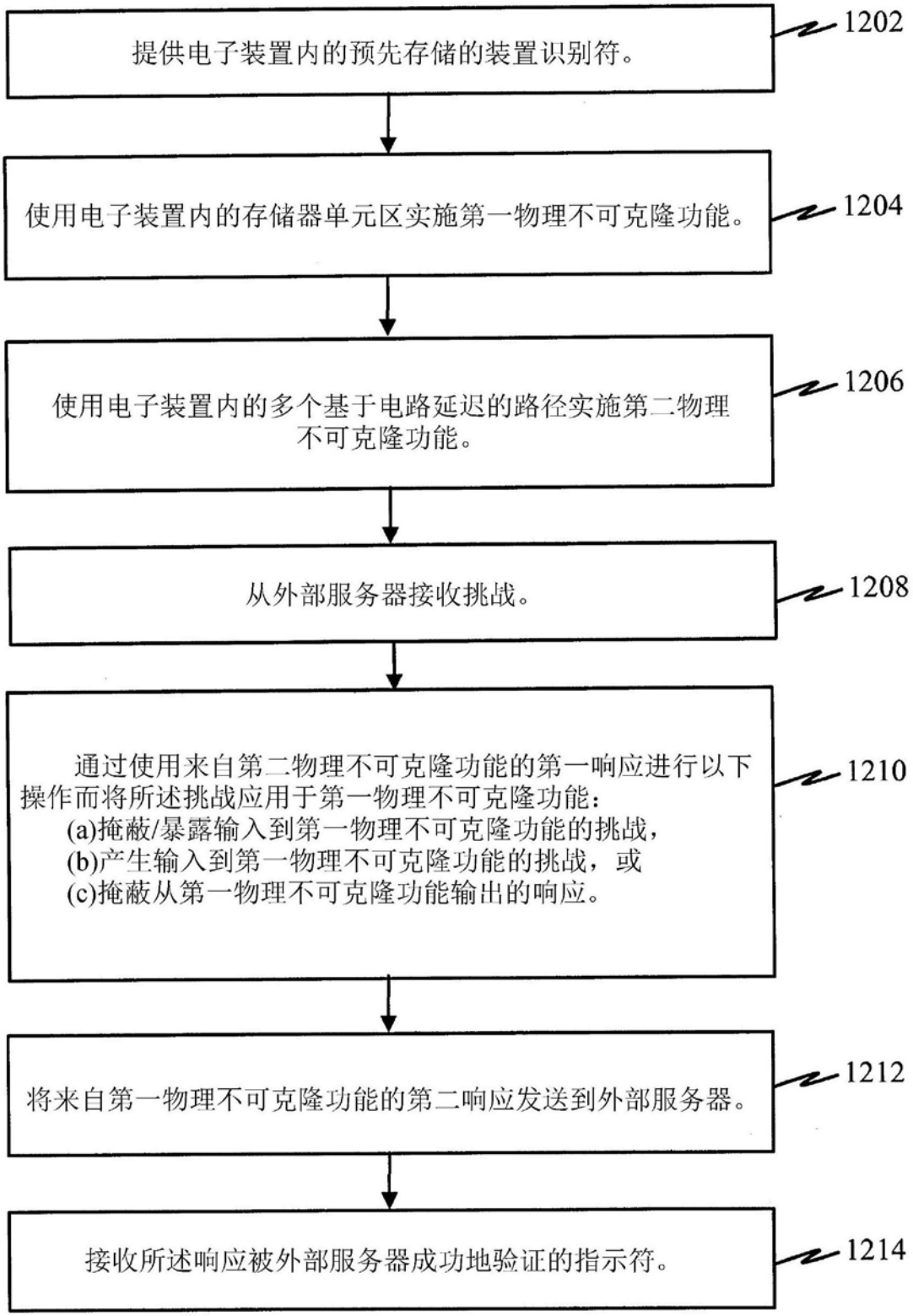

提供电子装置内的预先存储的装置识别符。
1202
使用电子装置内的存储器单元区实施第一物理不可克隆功能。
1204
使用电子装置内的多个基于电路延迟的路径实施第二物理不可克隆功能。
1206
从外部服务器接收挑战。
1208
通过使用来自第二物理不可克隆功能的第一响应进行以下操作而将所述挑战应用于第一物理不可克隆功能：
(a)掩蔽/暴露输入到第一物理不可克隆功能的挑战，
(b)产生输入到第一物理不可克隆功能的挑战，或
(c)掩蔽从第一物理不可克隆功能输出的响应。
1210
将来自第一物理不可克隆功能的第二响应发送到外部服务器。
1212
接收所述响应被外部服务器成功地验证的指示符。
1214
通过电子装置操作的方法

图12