(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104704500 B
(45)授权公告日 2018.01.12

(21)申请号 201380052622.2

(22)申请日 2013.11.07

(65)同一申请的已公布的文献号
申请公布号 CN 104704500 A

(43)申请公布日 2015.06.10

(30)优先权数据
13/694,221 2012.11.08 US

(85)PCT国际申请进入国家阶段日
2015.04.08

(86)PCT国际申请的申请数据
PCT/US2013/000253 2013.11.07

(87)PCT国际申请的公布数据
WO2014/074127 EN 2014.05.15

(73)专利权人 英特尔公司
地址 美国加利福尼亚

(72)发明人 H·M·科斯拉维 D·A·李
R·斯林瓦萨拉加万

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 刘瑜 王英

(51)Int.Cl.
G06F 21/30(2006.01)

(56)对比文件
US 2009/0202068 A1,2009.08.13,
WO 2006/108181 A2,2006.10.12,
EP 2221742 A1,2010.01.22,

审查员 翟紫伶

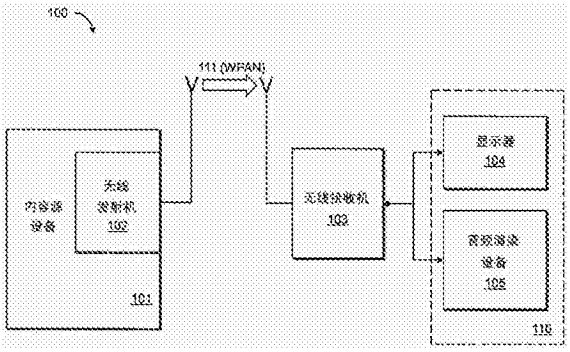
权利要求书4页 说明书13页 附图11页

(54)发明名称

用于片上系统装置中的内容保护的集成电路、无线显示系统、方法、装置、设备和介质

(57)摘要

内容处理集成电路包括片上系统(SoC),该SoC还包括处理器,用于从外部设备接收认证请求以认证是否准许SoC从外部设备接收加密的内容,并且一旦对SoC进行了认证,则接收该加密的内容。提供了认证处理器,该认证处理器耦合到所述处理器,用于当所述处理器接收到认证请求时,针对外部设备对SoC进行认证,并且生成解密密钥用于对加密的内容进行解密。提供了解密处理器,该解密处理器耦合到处理器和认证处理器,用于从认证处理器接收解密密钥,以及使用解密密钥对加密的内容进行解密。还描述了具有这种SoC的无线显示系统。还描述了在SoC中实现安全的和健壮的内容保护的方法。



CN 104704500 B

1.一种内容处理集成电路,包括:

片上系统SoC,其还包括:

处理器,用于从外部设备接收认证请求以认证是否准许所述SoC从所述外部设备接收加密的内容,以及一旦对所述SoC进行了认证,则接收所述加密的内容;

耦合到所述处理器的认证处理器,用于当所述处理器接收到所述认证请求时,针对所述外部设备对所述SoC进行认证,以及一旦对所述SoC进行了认证,生成用于对所述加密的内容进行解密的解密密钥;

以及

耦合到所述处理器和所述认证处理器的解密处理器,用于从所述认证处理器接收所述解密密钥,以及使用所述解密密钥对所述加密的内容进行解密。

2.根据权利要求1所述的内容处理集成电路,其中,所述认证处理器是与所述处理器分离的安全引擎处理器,并经由通信链路来耦合到所述处理器。

3.根据权利要求2所述的内容处理集成电路,其中,所述安全引擎处理器还包括在所述安全引擎处理器内的存储软件指令的存储器,当所述软件指令被所述安全引擎处理器执行时,实现也由所述外部设备实现的预定的内容保护协议。

4.根据权利要求3所述的内容处理集成电路,其中,所述预定的内容保护协议是高带宽数字内容保护(HDCP)协议。

5.根据权利要求1所述的内容处理集成电路,其中,所述认证处理器包括处理器寄存器,在将所生成的解密密钥直接发送给所述解密处理器之前,所述处理器寄存器存储所述解密密钥,其中不将所述解密密钥发送给所述处理器,并且不将所述解密密钥暴露给在所述处理器上运行的任何软件。

6.根据权利要求1所述的内容处理集成电路,其中,所述解密处理器与所述处理器是分离的,并经由通信链路来耦合到所述处理器,其中所述解密处理器还执行传输流解复用功能,以在对所述加密的内容进行解密之前,使所述加密的内容中的视频内容与音频内容相分离。

7.根据权利要求1所述的内容处理集成电路,其中,所述解密密钥是基于会话的密钥,其中在会话完成之后,所述基于会话的密钥失效。

8.根据权利要求1所述的内容处理集成电路,还包括:耦合到所述处理器的无线通信模块,用于从所述外部设备无线地接收所述认证请求和所述加密的内容,以及将所述认证请求和所述加密的内容传送给所述处理器,其中所述无线通信模块还耦合到所述认证处理器以在所述外部设备和所述认证处理器之间传达认证信息。

9.一种无线显示系统,包括:

内容源设备,用于生成和无线地发送加密的内容;

片上系统无线接收机,用于从所述内容源设备接收认证请求以认证是否准许所述接收机接收所述加密的内容,以及一旦对所述接收机进行了认证,则接收所述加密的内容,所述片上系统无线接收机还包括:

处理器,耦合为接收所述认证请求和所述加密的内容;

认证处理器,耦合到所述处理器以(1)在所述处理器接收到所述认证请求时,针对所述内容源设备对所述接收机进行认证,以及(2)生成用于对所述加密的内容进行解密的解密

密钥；

解密处理器，耦合为从所述认证处理器接收所述解密密钥，以及使用所述解密密钥对所述加密的内容进行解密；以及

耦合到所述接收机的内容渲染设备，用于接收和显示所述解密的内容。

10.根据权利要求9所述的无线显示系统，其中，所述认证处理器是与所述处理器分离的安全引擎处理器，并经由通信链路来耦合到所述处理器，其中所述安全引擎处理器还包括在所述安全引擎处理器内的存储软件指令的存储器，当所述软件指令被所述安全引擎处理器执行时，实现也由所述内容源设备实现的预定的内容保护协议，以对所述加密的内容进行加密。

11.根据权利要求10所述的无线显示系统，其中，所述预定的内容保护协议是高带宽数字内容保护(HDCP)协议。

12.根据权利要求9所述的无线显示系统，其中，所述认证处理器包括处理器寄存器，在将所生成的解密密钥直接发送给所述解密处理器之前，所述处理器寄存器存储所述解密密钥，其中不将所述解密密钥发送给所述处理器，并且不将所述解密密钥暴露给在所述处理器上运行的任何软件。

13.根据权利要求9所述的无线显示系统，其中，所述解密处理器与所述处理器是分离的，并且经由通信链路来耦合到所述处理器，其中所述解密处理器还执行传输流解复用功能，以在对所述加密的内容进行解密之前，使所述加密的内容中的视频内容与音频内容相分离。

14.根据权利要求9所述的无线显示系统，其中，所述解密密钥是基于会话的密钥，其中在会话完成之后，所述基于会话的密钥失效。

15.根据权利要求9所述的无线显示系统，还包括：耦合到所述处理器的无线通信模块，用于从所述内容源设备无线地接收所述认证请求和所述加密的内容，以及将所述认证请求和所述加密的内容传送给所述处理器，其中所述无线通信模块还耦合到所述认证处理器以在所述内容源设备和所述认证处理器之间传达认证信息。

16.一种在片上系统SoC媒体处理装置中提供安全的和健壮的内容保护的方法，包括：

在所述SoC媒体处理装置的处理器中，从外部设备接收认证请求以认证是否准许所述SoC媒体处理装置从所述外部设备接收加密的内容，以及一旦对所述SoC媒体处理装置进行了认证，则接收所述加密的内容；

使认证处理器(1)根据预定的内容保护协议，针对所述外部设备对所述SoC媒体处理装置进行认证，以及(2)针对根据所述预定的内容保护协议而加密的所述加密的内容，生成解密密钥；以及

一旦对所述SoC媒体处理装置进行了认证并且生成了所述解密密钥，则由所述处理器从所述外部设备接收所述加密的内容，以及向所述SoC媒体处理装置的解密处理器发送所述加密的内容，以使所述解密处理器利用直接从所述认证处理器接收的所述解密密钥对所述加密的内容进行解密。

17.根据权利要求16所述的方法，还包括：在接收到所述认证请求时，由所述处理器向所述外部设备发送所述SoC媒体处理装置的证书。

18.根据权利要求17所述的方法，还包括：

在发送所述证书之后，在所述处理器中从所述外部设备接收加密的主密钥；

向所述认证处理器发送所述加密的主密钥用于解密；

从所述认证处理器接收以随机生成的数字的形式的所述主密钥的解密的确认；以及

向所述外部设备发送所述随机生成的数字，以对所述主密钥的解密和验证进行确认。

19.根据权利要求16所述的方法，还包括：使所述认证处理器对来自所述外部设备的本地检验请求进行响应。

20.根据权利要求16所述的方法，其中，使所述认证处理器生成针对所述加密的内容的解密密钥，还包括：

从所述外部设备接收加密的会话密钥；以及

向所述认证处理器发送所述加密的会话密钥用于解密，以变成所述解密密钥。

21.根据权利要求16所述的方法，还包括：一旦对所述SoC媒体处理装置进行了认证并且在所述认证处理器中生成和存储了所述解密密钥，则使所述解密处理器经由后门密钥装载，直接从所述认证处理器接收所述解密密钥。

22.一种用于在片上系统SoC媒体处理设备中提供安全的和健壮的内容保护的装置，包括：

用于从外部设备接收认证请求以认证是否准许处理器从所述外部设备接收加密的内容，以及一旦对所述处理器进行了认证，则接收所述加密的内容的单元；

用于使与所述处理器分离的外部认证处理器(1)根据预定的数字内容保护协议，针对所述外部设备对所述处理器进行认证，以及(2)针对根据所述预定的数字内容保护协议而加密的所述加密的内容，生成解密密钥的单元；

用于一旦对所述处理器进行了认证并且生成了所述解密密钥，则从所述外部设备接收所述加密的内容，并且使与所述处理器分离的解密处理器直接从所述认证处理器接收所述解密密钥的单元；以及

用于向所述解密处理器发送所述加密的内容，以利用所述解密密钥进行解密的单元。

23.根据权利要求22所述的装置，其中，所述解密密钥是在所述外部设备处被加密的并被发送给所述处理器的解密的会话密钥。

24.根据权利要求23所述的装置，还包括：用于使所述解密处理器经由后门密钥装载，直接从所述认证处理器接收所述解密的会话密钥的单元。

25.根据权利要求22所述的装置，还包括：

用于在接收到所述认证请求时，由所述处理器向所述外部设备发送所述处理器的证书的单元；

用于在发送所述证书之后，在所述处理器中从所述外部设备接收加密的主密钥的单元；

用于由所述处理器向所述认证处理器发送所述加密的主密钥用于解密的单元；

用于从所述认证处理器接收以随机生成的数字的形式的所述主密钥的解密的确认的单元；以及

用于向所述外部设备发送所述随机生成的数字，以对所述主密钥的解密和验证进行确认的单元。

26.根据权利要求22所述的装置，还包括：用于使所述认证处理器对来自所述外部设备

的本地检验请求进行响应的单元。

27.根据权利要求22所述的装置，其中，用于使所述认证处理器生成针对所述加密的内容的解密密钥的单元，还包括：

用于从所述外部设备接收加密的会话密钥的单元；以及

用于向所述认证处理器发送所述加密的会话密钥用于解密，以变成所述解密密钥的单元。

28.一种用于在片上系统SoC媒体处理装置中提供安全的和健壮的内容保护的设备，所述设备包括：

存储器，用于存储指令；以及

处理器，耦合到所述存储器，所述指令被所述处理器执行以实现根据权利要求16-21中的任一项所述的方法。

29.一种计算机可读介质，具有指令，所述指令当由处理器执行时使得所述处理器实现根据权利要求16-21中的任一项所述的方法。

用于片上系统装置中的内容保护的集成电路、无线显示系统、方法、装置、设备和介质

技术领域

[0001] 本公开的实施例涉及安全的内容传输和显示。更具体地说，本公开的实施例涉及片上系统装置中的健壮的并且安全的内容保护的改进性实现。

背景技术

[0002] 众所周知，内容用户对媒体内容的访问正在从机会访问改变成按需访问。通常通过将按需媒体内容以及一些标准的媒体内容流式地传输到多媒体接收平台(例如，机顶盒、智能电话、计算机平板设备、膝上型计算机等等)以进行内容显示，来传送这些内容。如果多媒体内容是优质内容，则通常在向多媒体接收平台进行传输期间，以某种方式来保护该多媒体内容。例如，可以使用各种数字版权管理(DRM)和条件访问(CA)技术，来为从媒体源到多媒体接收平台的媒体内容提供保护。这些技术通常涉及内容媒体的加密。

[0003] 片上系统(SoC)设备是将电子系统的各种组件并入到单一管芯或基底的集成电路。例如，SoC集成电路可以在单一芯片上包括处理器内核、存储器、视频组件、音频组件和/或通信组件。由于它们的相对较小的尺寸，因此在很多多媒体接收平台中都使用SoC。

附图说明

[0004] 通过举例的方式来说明本公开的特征和优点，并且其并不旨在将本公开的范围限制于所示出的具体实施例。

[0005] 图1是根据本公开的示例性实施例包括无线片上系统(SoC)接收机的无线显示系统的体系结构概述。

[0006] 图2示出了根据本公开的示例性实施例包括媒体引擎、认证处理器和解密处理器的无线显示系统的无线SoC接收机的结构。

[0007] 图3示出了根据本公开的示例性实施例的无线显示系统的无线SoC接收机的认证处理器的结构。

[0008] 图4示出了根据本公开的示例性实施例的无线显示系统的无线SoC接收机的解密处理器的结构。

[0009] 图5是根据本公开的示例性实施例的无线显示系统的无线SoC接收机的媒体引擎的概述。

[0010] 图6是示出了根据本公开的示例性实施例由无线显示系统的无线SoC接收机的媒体引擎执行的用于设备认证和内容加密的过程的流程图。

[0011] 图7是示出了根据本公开的示例性实施例由无线显示系统的无线SoC接收机的认证处理器执行的用于设备认证和密钥解密的过程的流程图。

[0012] 图8示出了根据本发明的示例性实施例在无线显示系统的无线发射机(没有存储的主密钥)和无线SoC接收机之间在所述接收机的认证期间的序列和数据流。

[0013] 图9示出了根据本公开的示例性实施例在无线显示系统的无线发射机(具有存储

的主密钥)和无线SoC接收机之间在所述接收机认证期间的序列和数据流。

[0014] 图10示出了根据本公开的示例性实施例在无线显示系统的无线发射机和无线SoC接收机之间在所述无线SoC接收机的本地校验期间的序列和数据流。

[0015] 图11示出了根据本公开的示例性实施例在会话密钥交换和解密期间在无线显示系统的无线发射机和无线SoC接收机之间的序列和数据流。

具体实施方式

[0016] 在下文的描述中,为了说明起见,给出了特定的术语以便提供对本公开的实施例的透彻理解。对于本领域的技术人员来说显而易见的是,可以不需要说明书中的这些特定细节来实现这些实施例。在其它实例中,以框图形式示出了公知的电路、设备和程序,以避免对本公开的实施例造成模糊。

[0017] 图1示出了根据本公开的实施例包括实现安全的并且健壮的内容保护方案的具有发射机102的内容源设备101和无线片上系统(SoC)接收机103的无线显示系统100的整体体系结构。图2-7示出了诸如图1的SoC接收机103这样的SoC接收机集成电路的各种组件的结构和操作,并且图8-11示出了无线显示系统100的设备之间的序列和数据流。

[0018] 在无线显示系统100之前,已使用各种数字版权管理(DRM)和条件访问(CA)技术,来为从媒体源到媒体接收设备的媒体内容提供保护。高带宽数字内容保护(HDCP)是数字内容保护LLC所提供的一种这样的技术。开发该技术以防止数字音频和视频内容流经连接时对所述内容进行复制。这些连接包括数字可视接口(DVI)和高清晰度多媒体接口(HDMI)。

[0019] HDCP协议的功能中的一种是对接收设备进行认证,并在认证期间生成或者交换用于这些接收设备的解密密钥。如果将接收设备认证为被授权接收HDCP加密的内容,则相应的发射机对内容数据进行加密以防止该内容数据流向到该接收设备时被窃听。随后,接收设备使用生成的或者交换的解密密钥,对加密的内容数据进行解密。

[0020] 一种实现HDCP认证和密钥交换功能的现有方式具有在接收设备的处理器上运行的软件形式。与这种现有方式相关联的一个问题在于这些密钥是不安全的,并容易被恶意软件或间谍软件"发现"或黑客攻击。这是由于这些密钥以软件级别进行存储,并且需要能被在处理器上运行的各种软件代码和底层操作系统访问的事实,这使得可能经由恶意软件或间谍软件对这些密钥进行未被授权访问。

[0021] 图2示出了根据本公开的一个实施例的SoC接收机集成电路200的结构,其可以实现图1的无线SoC接收机103以提供安全的并且健壮的内容保护。根据本公开的一个实施例,以及如下面更详细描述的,SoC接收机集成电路200除了包括媒体引擎201之外,还包括认证处理器206和解密处理器208,其中媒体引擎201包括处理器202和存储器203。存储器203存储将要在处理器202上执行的软件代码。媒体引擎201(即,处理器202)不执行设备认证和解密密钥生成或交换功能。其也不使用解密密钥来执行内容解密操作。相反,将这些设备认证和解密密钥生成或交换功能委托给认证处理器206,将使用解密密钥的内容解密功能委托给解密处理器208。

[0022] 此外,一旦在认证处理器206中生成了解密密钥,不将该解密密钥发送给媒体引擎201的处理器202。相反,将该解密密钥存储在认证处理器206的处理器寄存器(即,寄存器207)中,并通过后门密钥装载与解密处理器208共享该解密密钥。根据本公开的实施例,后

门密钥装载技术是指两个组件或处理器通过在这两个组件或处理器之间共享的硬件级寄存器来安全地共享秘密信息的过程。在所给出的实施例中，认证处理器206和解密处理器208“共享”认证处理器206的处理器寄存器(例如，寄存器207)，其提供用于在这两个处理器之间共享秘密解密密钥的安全通道。换言之，解密处理器208有权访问认证处理器206的存储有该秘密和解密的解密密钥的处理器寄存器(例如，寄存器207)。

[0023] 上面所描述的实现的一个优点在于：通过使用认证处理器206(而不是处理器202)，在处理器202上运行的任何软件代码都不能够访问该认证过程，因此使得认证和解密密钥交换过程健壮和安全。

[0024] 上面所描述的实现的另一个优点在于：不将该解密密钥暴露给在处理器202上运行的任何软件代码(这是由于在处理器202中没有接收到该密钥)，因此避免了经由在媒体引擎202中运行的恶意软件或间谍软件被黑客攻击或访问的可能性。这为SoC接收机集成电路200以及图1的无线显示系统100提供了安全的和健壮的内容保护。下面将还结合图1到图11，更详细地描述无线显示系统100和SoC接收机集成电路200(图2)。

[0025] 贯穿该说明书，如下所述地定义下面的术语。

[0026] 术语“内容”、“媒体内容”或“多媒体内容”指代文本、音频、静态图像、动画、视频和/或交互式内容的组合。

[0027] 术语“无线”、“无线地”或“无线通信”指代在没有物理地连接的两个或更多个点之间进行信息的电子传输。

[0028] 术语“显示”指代内容渲染，其并不限于可视显示或者渲染。其可以指代视频或音频内容的显示(或者可视渲染)。其还可以指代通过扬声器或耳机来渲染音频内容。

[0029] 术语“SoC(片上系统)”指代将电子系统的各种组件合并在单一管芯或基底上的集成电路。例如，SoC可以在单一芯片上包括一个或多个处理器、存储器、微处理器、微控制器、视频组件、音频组件和/或通信组件。

[0030] 术语“处理器”指代数据处理电路，其可以是微处理器、协处理器、微控制器、微计算机、中央处理单元、现场可编程门阵列(FPGA)、可编程逻辑电路和/或基于在存储器中存储的操作指令来操纵信号(模拟信号或数字信号)的任何电路。

[0031] 术语“存储器”指代一个存储电路或多个存储电路，例如，只读存储器、随机存取存储器、易失性存储器、非易失性存储器、静态存储器、动态存储器、闪存、高速缓存和/或存储数字信息的任何电路。

[0032] 通常，用于表示指令块的示意图单元可以使用任何适当形式的机器可读指令来实现，例如，软件或固件应用、程序、函数、模块、例行程序、进程、过程、插件、小应用程序、小工具、代码段和/或其它形式，每一个这种指令可以使用任何适当的编程语言、库、应用程序接口(API)和/或其它软件开发工具来实现。例如，一些实施例可以使用Java、C++和/或其它编程语言来实现。类似地，用于表示数据或信息的示意图单元可以使用任何适当的电子布置或结构来实现，例如，寄存器、数据存储、表、记录、数组、索引、散列、映射、树、列表、图、文件(任何文件类型)、文件夹、目录、数据库和/或其它形式。

[0033] 此外，在附图中，在使用诸如实线或虚线或箭头之类的连接元素来说明两个或更多其它示意元素之间的连接、关系或关联时，缺少任何这种连接元素并不意味着暗示可能不存在连接、关系或关联。换言之，为了不对本公开造成模糊，在附图中可能没有示出元素

之间的一些连接、关系或关联。此外，为了便于说明起见，可以使用单一连接元素来表示元素之间的多个连接、关系或关联。例如，在一个连接元素表示信号、数据或指令的通信时，本领域技术人员应当理解，该元素可以表示用于实现该通信的一个或多个信号路径(例如，总线)，如可能需要的。

[0034] 参见图1，使用无线显示系统100从内容源设备101向无线显示系统100的内容渲染系统110发送内容以进行内容渲染。该内容可以是文本、音频、静态图像、动画、视频和/或交互式内容的组合。内容渲染系统110通过有线连接来连接到无线接收机103。内容渲染系统110包括显示器104和音频渲染设备105。显示器104可以是电视(TV)显示器、高清晰度TV(HDTV)显示器、计算机监视器或显示器或者投影显示器。音频渲染设备105可以是一个或多个扬声器和/或耳机(其包括头戴装置)。

[0035] 内容源设备101可以是智能电话、平板计算机、膝上型计算机、桌面型计算机、移动互联网设备、机顶盒或者能够生成或传输媒体内容的其它设备。内容源设备101可以包括内容生成器(例如，DVD播放器)，或者可以通过互联网从远程源按需地获得媒体内容。

[0036] 内容源设备101包括无线发射机102。无线发射机102用于通过无线接收机103从内容源设备101向渲染系统110发送媒体内容。无线发射机102使用相同的无线通信协议与无线接收机103进行通信。所使用的无线通信技术或协议可以是蓝牙(其还称为IEEE 802.15.1标准)、Wi-Fi(其还称为IEEE 802.11标准)、HomeRF(家庭射频标准)、红外线、ZigBee(其还称为IEEE 802.15.4标准)。包括发射机102的内容源设备101可以使用已知的方式来实现。因此，它们的结构和操作在下文将不更详细描述。

[0037] 无线接收机103可以体现在机顶盒、智能电话、智能显示器、平板计算机、膝上型计算机、桌面型计算机、移动互联网设备或者能够传输媒体内容的其它设备中。无线接收机103可以被配置为传输任何类型的媒体内容，例如，其包括电影、图片、图像、歌曲、音频和/或视频记录、和/或任何其它类型的音频、视频和/或音频和视频内容。

[0038] 根据本公开的一个实施例，无线网络111是无线个域网(WPAN)。在另一个实施例中，无线网络111是无线局域网。在另外的实施例中，无线网络111可以是有线和无线网络的组合。

[0039] 此外，无线显示系统100可以包括一个或多个中继器(在图1中没有示出)。中继器包括组合在一起的类似发射机102的发射机电路和接收机电路(类似接收机103)。其充当发射机102和接收机103之间的通信中继站。

[0040] 在图1中，无线显示系统100被示出为具有其内容源设备101，内容源设备101通过无线网络111与该系统的无线接收机103无线地通信。这实现了本公开的一个实施例。但是，显示系统100并不限于这种无线实现。例如，内容源设备101和接收机103之间的通信可以是有线网络或者有线和无线网络的组合。

[0041] 根据本公开的一个实施例，发射机102和接收机103之间发送的媒体内容是受保护的或加密的。用于这种内容保护或加密的一种协议或标准是高带宽数字内容保护(HDCP)标准。HDCP标准具有多种版本，其包括HDCP 1.0版本和HDCP 2.0版本。如上所述，HDCP是用于保护媒体内容的内容保护协议。

[0042] 在一个实施例中，HDCP内容保护协议使用根据高级加密标准(AES)的密码学技术，其中AES描述了可以对信息进行加密(译成密码)和解密(破译)的对称加密技术(其还称为

Rijndael算法)。可以在2001年11月26日发布的联邦信息处理标准出版物197(FIPS PUB 197)中找到AES的详细描述。在另一个实施例中,HDCP内容保护协议使用非对称密码学技术。

[0043] 多种操作模式可以用于AES加密和解密操作。操作模式包括电子码本(ECB)、密码块链接(CBC)、输出反馈(OFB)、计数器和密码反馈(CFB),其提供任意长度的消息的保真度。诸如计数器与密码块链接消息认证码(CCM)、Galois计数器模式(GCM)和偏移码本模式(OCB)之类的其它操作模式确保保真度和消息完整性两者。

[0044] 根据本公开的一个实施例,接收机103的SoC电路实现为在无线显示系统100中发送的内容提供了安全的并且健壮的认证和内容解密。下面还结合图2-11来进一步详细地描述接收机103的结构和操作。

[0045] 在图2中并且如上所述,根据本公开的示例性实施例,无线SoC接收机集成电路200可以实现图1的无线接收机103。如图2中所示,根据本公开的示例性实施例,无线SoC接收机集成电路200包括媒体引擎201、认证处理器206和解密处理器208。媒体引擎201包括处理器202和存储器203。处理器202充当无线SoC接收机集成电路200的主处理器,而存储器203存储在处理器202上执行的软件程序代码。存储器203可以具有能由认证处理器206和/或解密处理器208访问的存储区域。无线SoC接收机集成电路200的其它处理器可以充当协处理器、微型处理器、或者处理器202的微控制器。在一个实施例中,无线SoC接收机集成电路200的组件位于同一个基底上,或者位于同一个芯片之中。

[0046] 在一个实施例中,处理器202是类似微处理器的中央处理单元(CPU)。在另一个实施例中,处理器202是简单的数据处理单元。使用处理器间调用通信协议,来实现处理器202和类似处理器206和208的其它处理器之间的通信。可以使用已知的技术来实现处理器202的结构和功能。

[0047] 无线SoC接收机集成电路200包括通信模块205,其实现通信协议以实施无线SoC接收机集成电路200与外部设备的无线通信。实现的通信协议可以包括TCP/IP(传输控制协议/互联网协议)、UDP/IP(用户数据报协议/互联网协议)、RTSP(实时流协议)、RTP(实时传输协议)和MPEG-TS(运动图像专家组-传输流)。使用的无线通信技术可以是蓝牙、Wi-Fi、HomeRF、红外线和ZigBee。通信模块205的结构和功能可以使用已知的技术来实现。

[0048] 无线SoC接收机集成电路200还包括音频模块211和视频模块212。音频模块211用于处理音频内容数据,向外部渲染设备发送所处理的数据。视频模块212用于处理视频内容数据,并将其发送给外部渲染设备。这两个模块的结构和功能是已知的,故在下文中没有进一步详细描述。

[0049] 无线SoC接收机集成电路200中的所有模块、组件或功能块通过通信链路204连接在一起。通信链路204可以简单地称为链路204。在一个实施例中,链路204是简单的通用总线,其用于在无线SoC接收机集成电路200的所有模块或组件之间传送数据、信息和/或指令。在另一个实施例中,链路204统一地表示无线SoC接收机集成电路200的任意两个组件之间的各种专用通信链路或总线。在该情况下,无线SoC接收机集成电路200中的任何一对组件具有专用的通信链路或连接,并且链路204统一地表示它们。链路204可以使用任何已知的总线技术来实现,或者可以简单地是电子连接线。

[0050] 根据本公开的一个实施例,媒体引擎201(即,处理器202)不执行设备认证和解密

密钥生成或交换功能。其也不针对在无线SoC接收机集成电路200中接收的内容来执行内容解密操作。相反，将这些设备认证和解密密钥生成或交换功能委托给认证处理器206，将使用内容解密功能委托给解密处理器208。

[0051] 此外，一旦在认证处理器206中生成了解密密钥，并不将该解密密钥发送给媒体引擎201的处理器202(或者处理器202不能访问该解密密钥)。相反，将该解密密钥存储在处理器寄存器(即，寄存器207)中，并通过后门密钥装载仅由解密处理器208共享该解密密钥。如上所述，后门密钥装载技术是指两个组件或处理器通过在这些组件或处理器之间共享的硬件级寄存器来安全地共享秘密信息的过程。在SoC 200的实施例中，认证处理器206和解密处理器208“共享”认证处理器206的处理器寄存器(例如，寄存器207)，其提供用于在这两个处理器之间共享秘密解密密钥的安全通道。换言之，解密处理器208有权访问认证处理器206的存储有该秘密和解密的解密密钥的处理器寄存器(例如，寄存器207)。这防止了将该解密密钥暴露给在处理器202上运行的任何软件代码(这是由于处理器202并不接收该密钥)。这减小了经由在媒体引擎202中运行的恶意软件或间谍软件被黑客攻击或访问的可能性。这为SoC接收机集成电路200(以及因此为图1的无线显示系统100)提供了安全的并且健壮的内容保护。

[0052] 图3示出了根据本公开的示例性实施例的SoC集成电路中的认证处理器300的结构。认证处理器300可以实现图2的SoC集成电路200的认证处理器206。如通过图3可以看到的，认证处理器300包括安全引擎处理器301和处理器内存储器303，其中处理器内存储器303存储内容保护协议软件302，并只可被安全引擎处理器301进行访问。在一个实施例中，内容保护协议软件302实现HDCP内容保护协议。

[0053] 可以将安全引擎处理器301体现成与SoC的主处理器(例如，图2的SoC 200)相分离的安全协处理器或处理电路。在一个实施例中，安全引擎处理器301是协处理器、微控制器、微计算机、和/或基于存储器中存储的操作指令来操纵信号(模拟信号或数字信号)的任何电路。安全引擎处理器301包括随机数发生器(没有示出)和可以用于存储解密的密钥的处理器寄存器(即，图2中的寄存器207)。安全引擎处理器301的结构是已知的，故在下文中没有进一步详细描述。

[0054] 图4示出了根据本公开的示例性实施例可以实现图2的解密处理器208的解密处理器400的结构。如通过图4可以看到的，解密处理器400包括处理器硬件电路401和存储器402，其中存储器402存储在处理器硬件电路401上执行的软件程序代码403和404。软件程序代码403是传输流解复用软件程序，软件程序代码403实现内容解密功能。换言之，处理器400执行传输流解复用功能以将视频与音频内容分离和内容解密功能两者。

[0055] 处理器硬件电路401可以由任何已知的处理器或微控制器或协处理器来实现，故没有进一步详细描述。解密软件代码404是基于HDCP的解密代码，该解密操作是已知的，故下文没有进行进一步详细描述。

[0056] 图5示出了根据本公开的示例性实施例可以实现图2的媒体引擎201的媒体引擎500的结构。如图5中所示，媒体引擎500包括处理器硬件501和在处理器硬件501上运行的操作系统502。在操作系统502之上，提供有在操作系统502上运行的软件程序代码503-506。操作系统502和代码503-506存储在媒体引擎500的存储器(图5中没有示出)中。

[0057] 代码503是在认证和密钥交换期间控制媒体引擎500(即，处理器硬件501)与SoC电

路(即,图2的SoC电路200)的其它组件(例如,图2的认证处理器206)的交互和接口的认证控制代码。代码503实现HDCP协议。其可以包括HDCP库和HDCP库API(应用程序接口)。其还可以包括安全引擎处理器API和安全引擎处理器驱动程序以及HDCP处理器间调用通信协议代码。

[0058] 代码505是在解密期间控制媒体引擎500(即,处理器硬件501)与SoC电路(即,图2的SoC电路200)的其它组件(例如,图2的解密处理器208)的交互和接口的解密控制代码。图6示出了代码503和505的过程和操作,下面将对其进一步详细地描述。

[0059] 图6示出了根据本公开的示例性实施例的设备认证、密钥解密和内容解密的过程。图6中所示出的过程可以由图2的处理器202来执行,可以由图5的认证控制代码503来实现。

[0060] 该过程开始于601,其中在601处,处理器接收AKE_init(认证和密钥交换发起)消息。该AKE_init消息包括消息ID和由发射机(例如,发射机102)生成的64比特随机数r_{tx}。发射机还可以称为请求者。该随机数r_{tx}用作发射机的设备ID和认证请求。

[0061] 在602处,处理器向发射机发回证书$Cert_{rx}$。

[0062] 在603处,处理器接收加密的主密钥K_m。主密钥K_m是在发射机/请求者处生成的并使用接收机公钥$Kpub_{rx}$来加密。如上所述,利用具有RSA OAEP填充的RSA-1024来执行该加密操作。

[0063] 在604处,处理器向认证处理器(例如,图2的认证处理器206)发送r_{tx}和加密的主密钥K_m。随后,认证处理器(例如,图2的处理器206)利用具有中国余数定理格式的私钥值对主密钥K_m进行解密。使用中国余数定理计算来在认证处理器中执行这种解密。此外,在对主密钥K_m进行成功解密之后,认证处理器还计算H'值(即,H'=HMAC-SHA256(r_{tx} XOR REPEATER, K_d))。将该H'值发送给发射机,以验证该认证是否成功。处理器并不涉及到该解密和H'值的计算操作中。

[0064] 此外,在604处,处理器还向发射机发回随机数r_{tx}。该随机数r_{tx}用作接收机的设备ID和在接收机中已接收到加密的主密钥的确认。

[0065] 在605处,处理器从发射机接收该认证是否成功的确认。如果成功的话,则处理器从发射机接收本地检验命令r_n。

[0066] 在606处,处理器通过向认证处理器发送r_n,使认证处理器执行本地检验操作。认证处理器(例如,图2的认证处理器206)随后计算L'值(即,=HMAC-SHA256(r_n,k_d XOR r_{rx})。随后,通过两个处理器之间的共享存储器,将L'值发送给所述处理器。随后,将L'值发送回发射机,以便与发射机中所计算的L值进行验证。对于认证和本地检验的成功完成来说,必须在预定的时间段之内将所计算的L'值发送回发射机。当发射机发起用于本地检验的消息时,其建立看门狗定时器。来自接收机的消息应当在该指定的时间之内到达发射机。

[0067] 在607处,处理器从发射机或请求者接收加密的会话密钥。解密处理器(例如,图2的解密处理器208)使用该会话密钥,对由发射机发送的加密的内容进行解密。因此,该会话密钥是解密密钥。

[0068] 在发射机中,利用64比特伪随机数r_{iv}来生成会话密钥K_s。随后,发射机执行密钥推导以生成dkey2。随后,发射机将128会话密钥加密成$E_{dkey}(K_s)=K_s$ XOR(dkey2XORr_{rx})。随后,发射机将加密的会话密钥K_s与64比特伪随机数r_{iv}发送给接收机,并被处理器接收。

[0069] 处理器将加密的会话密钥K_s与r_{iv}传送给认证处理器,以便对会话密钥进行解密。

处理器并不涉及该会话密钥解密，并且无权访问解密的会话密钥。这防止了在处理器上运行的软件代码访问解密后的会话密钥。这为无线显示系统(例如，图1的系统100)提供了安全的和健壮的内容保护。

[0070] 在608处，处理器从发射机接收加密的内容，将其发送给解密处理器(例如，解密处理器208)，以利用经由后门密钥装载技术直接从认证处理器装载到解密处理器的解密后的会话密钥进行解密。

[0071] 在609处，处理器接收解密后的内容，并且执行其它内容处理功能。随后，处理器向外部渲染设备(例如，图1的内容渲染系统110)发送内容以用于渲染。

[0072] 图7根据本发明的示例性实施例，示出了设备认证和密钥解密的过程。图7中所示出的过程可以由无线显示系统的无线SoC接收机的认证处理器(例如，图2的认证处理器206)执行。

[0073] 该过程开始于701，在701处，认证处理器从处理器(例如，图2的处理器202)接收认证请求r_{tx}。这由存储器(例如，图2的存储器203)中存储的软件代码(例如，图5的认证控制代码503)来实现。该软件代码将认证请求r_{tx}写入到与所述处理器(例如，图2的202和206)共同共享的存储器，并且认证处理器通过AKE_init IPC调用(即，认证和密钥交换初始化处理器间调用)将r_{tx}复制到其内部存储器。

[0074] 在702处，认证处理器接收加密的主密钥K_m。如上所述，在发射机(例如，图1的发射机102)中，使用公钥$Kpub_{tx}$对主密钥K_m进行加密。

[0075] 在703处，认证处理器使用其随机数发生器，生成随机数r_{rx}。经由处理器间调用命令，将该随机数r_{rx}传送给所述处理器。

[0076] 在704处，认证处理器利用私钥$Kpriv_{rx}$，对主密钥K_m进行解密。用于对K_m进行解密的私钥值具有中国剩余定理格式。使用中国剩余定理计算，在认证处理器中执行解密。此外，认证处理器计算H'值(即，=HMAC-SHA256(r_{tx}XOR REPEATER,K_d))。发射机使用H'值来验证认证是否成功。随后，通过将H'值写入到所述处理器和认证处理器之间的共享存储器的输出负载区域，来将H'值发送回所述处理器。随后，所述处理器将H'值发送给发射机，以与发射机中计算的H值进行验证。

[0077] 在705处，认证处理器从所述处理器接收本地检验命令r_n。这通过在处理器上运行的认证控制代码来完成，其中处理器将该命令写入到所述两个处理器共享的存储器的输入负载区域中，随后认证处理器将该命令复制到其内部存储器。

[0078] 在706处，认证处理器通过计算L'值(即，=HMAC-SHA256(r_n,k_dXOR r_{rx})来执行本地检验。随后，经由两个处理器之间的共享存储器，将L'值发送给所述处理器。随后，处理器将L'值发送给发射机，以便与发射机中所计算的L值进行验证。对于认证和本地检验的成功完成，必须在预定的时间段之内将所计算的L'值发送给发射机，以使本地检验成功。

[0079] 在707处，认证处理器接收加密的会话密钥K_s和64比特伪随机数r_{iv}。

[0080] 在708处，认证处理器对会话密钥进行解密。这通过首先执行密钥推导以生成$dkey_2$来完成。随后，认证处理器将128比特会话密钥K_s解密成$E_{dkey}(K_s)$XOR($dkey_2$XORr_{rx})。认证处理器还计算K_s XOR 1c 128。随后，将解密的密钥存储在处理器寄存器中，等待经由后门密钥装载来装载到解密处理器(例如，图2的解密处理器208)中。在将解密的会话密钥装载到解密处理器之前，在所述处理器(例如，图2的处理器202)上运行的软件代码不可访问

该解密的会话密钥。

[0081] 图6-7是示出根据本发明的实施例的过程或功能的流程图。可以串行地、并行地或者按照与所描述的顺序不同的顺序来执行这些附图中示出的技术。这些技术还可以被执行一次或多次。应当理解的是，并不需要执行所描述的所有技术，可以增加另外的技术，可以使用其它技术来替代所示出的技术中的一些。

[0082] 图8根据本公开的示例性实施例，示出了在接收机的认证期间，无线发射机(例如，图1的发射机102)和无线SoC接收机(例如，图1的接收机103)之间的序列和数据流。在该例子中，发射机没有存储的用于接收机的主密钥Km。这意味着发射机和接收机彼此之间是第一次进行通信。图9根据本公开的示例性实施例，示出了在接收机的认证期间，发射机(例如，图1的发射机102)和SoC接收机(例如，图1的接收机103)之间的序列和数据流。在该例子中，发射机具有存储的用于接收机的主密钥Km。这意味着发射机和接收机彼此之间之前进行过通信。图10根据本公开的示例性实施例，示出了在无线SoC接收机的本地检验期间，发射机(例如，图1的发射机102)和SoC接收机(例如，图1的接收机103)之间的序列和数据流。本地检验指代确定接收机在发射机的预定的传输范围之内。图11根据本发明的示例性实施例，示出了在会话密钥交换和解密期间，发射机(例如，图1的发射机102)和SoC接收机(例如，图1的接收机103)之间的序列和数据流。下面将更详细描述这些序列和数据流。

[0083] 在图8中，TX代表发射机侧，并且RX代表接收机侧。箭头指示数据流方向。箭头线上面的符号指示在认证和密钥交换期间发送的数据。如通过图8可以看到的，发射机首先向接收机发送AKE_init(认证和密钥交换发起)消息以发起认证操作。该AKE_init消息包括由发射机生成的64比特随机数r_{tx}和消息ID。随机数r_{tx}作为发射机的设备ID和认证请求。

[0084] 在接收到AKE_init消息之后，接收机发送回证书$Cert_{rx}$。如上面结合图2-7所描述的，这由SoC接收机(例如，接收机200)的处理器(例如，图2的处理器202)来完成。证书$Cert_{rx}$存储在接收机的闪存中。随后，发射机使用公钥$Kpub_{dcp}$，对$Cert_{rx}$进行验证。在该时间，接收机的处理器还向认证处理器(例如，图2的认证处理器206)传送随机数r_{tx}，以开始认证和密钥交换操作。

[0085] 在发射机对$Cert_{rx}$进行验证之后，利用接收机公钥$Kpub_{rx}$来生成和加密主密钥K_m。如上所述，使用RSA-1024与RSA OAEP填充来执行该加密操作。

[0086] 随后，将主密钥K_m发送给接收机。接收机使它的认证处理器利用私钥$Kpriv_{rx}$对加密的主密钥K_m进行解密。用于对K_m进行解密的私钥值具有中国剩余定理格式。使用中国剩余定理计算，在认证处理器(例如，图2的处理器206)中执行解密。

[0087] 在接收到主密钥K_m之后，接收机还生成接收机随机数r_{rx}，并将其发送给发射机。随机数r_{rx}的生成由在接收机的认证处理器之内的随机数发生器来执行。该随机数r_{rx}作为接收机的设备ID和接收机已接收到加密的主密钥的确认。

[0088] 随后，接收机的认证处理器(例如，图2的认证处理器206)计算H'值(即，=HMAC-SHA256(r_{tx}XOR REPEATER,K_d))。随后，接收机的处理器将H'值发送给发射机。发射机计算H值，并且验证是否H=H'。如果是，则该认证是成功的，并且发射机存储主密钥K_m和E(K_m,K_h)。E(K_m,K_h)是包括主密钥K_m和接收机的私钥K_h的散列的配对信息。如果H不等于H'，则接收机的认证失败。

[0089] 参见图9，发射机已经创建了主密钥K_m，并且序列和数据流与图8的不同点在于：没

有主密钥生成。相反，有用于取回存储的配对信息$E(K_m,K_h)$与接收机ID的主密钥取回功能。

[0090] 参见图10，发射机(例如，图1的发射机102)通过生成和向接收机(例如，图1的接收机103或图2的接收机200)发送r_n，来发起本地检验。随后，认证处理器(例如，图2的认证处理器206)计算L'值(即，$=HMAC\text{-}SHA256(r_n,k_d XOR\ r_{rx})$。随后，经由两个处理器之间的共享存储器，将L'值发送给接收机的处理器(例如，图2的处理器202)。随后，将L'值发送回发射机，以便与发射机中所计算的L值进行验证。对于认证和本地检验的成功完成，必须在预定的时间段之内将所计算的L'值发送至发射机(例如，如图10中所示)。当发射机发起用于本地检验的消息时，其建立看门狗定时器。来自接收机的消息应当在该指定的时间之内到达发射机。

[0091] 在图11中，在认证和本地检验的成功完成之后，发射机(例如，图1的发射机102)开始会话密钥交换的过程。解密处理器(例如，图2的解密处理器208)使用该会话密钥，对由发射机发送的加密的内容进行解密。因此，该会话密钥是解密密钥。

[0092] 如通过图11可以看到的，发射机通过生成会话密钥K_s和64比特伪随机数r_{iv}，来发起过程。随后，发射机执行密钥推导以生成dkey2。随后，发射机将128会话密钥加密成$E_{dkey}(K_s)=K_s XOR(dkey_2 XOR r_{rx})$。随后，发射机将加密的会话密钥$K_s$与64比特伪随机数$r_{iv}$发送给接收机。

[0093] 随后，认证处理器(例如，图2的认证处理器206)接收加密的会话密钥K_s与r_{iv}，对该会话密钥进行解密。这通过首先执行密钥推导以生成$dkey_2$来完成。随后，认证处理器将128比特会话密钥K_s解密成$E_{dkey}(K_s)XOR(dkey_2 XOR r_{rx})$。认证处理器还计算$K_s$ XOR 1c 128，并且经由后门密钥装载，将解密的会话密钥发送给解密处理器(例如，图2的解密处理器208)。在将解密的会话密钥装载到解密处理器之前，将解密的会话密钥存储在认证处理器的处理器寄存器中，并且在主处理器(例如，图2的处理器202)上运行的软件代码不可访问该解密的会话密钥。这为诸如图1的系统100之类的无线显示系统提供了安全的和健壮的内容保护。

[0094] 可以将本公开的实施例提供成计算机程序产品或者软件，其可以包括具有指令的机器可访问介质或机器可读介质上的制品。机器可访问介质或机器可读介质上的指令可以用于对计算机系统或其它电子设备进行编程。该机器可读介质可以包括，但不限于：软盘、光盘、CD-ROM、以及磁光碟或者其它类型的适合于存储或发送电指令的媒体/机器可读介质。本文中描述的技术并不限于任何特定的软件配置。可以在任何计算或处理环境中发现它们的适用性。本文中使用的术语“机器可访问介质”或“机器可读介质”应当包括：能够对用于由机器执行的指令序列进行存储或者编码，并使得该机器执行本文中描述的方法中的任何一个的任何介质。此外，本领域中通常提到采取动作或产生结果的一种或另一种形式的软件(例如，代码、程序、过程、进程、应用、模块、单元、逻辑、块等等)。这些表述只是陈述由处理系统执行软件造成该处理器执行动作从而产生结果的简易方式。

[0095] 下面的例子关于进一步的实施例。在一个实施例中，一种内容处理集成电路包括片上系统(SoC)，其还包括：处理器，用于从外部设备接收认证请求以认证是否准许所述SoC从所述外部设备接收加密的内容，以及一旦对所述SoC进行了认证，则接收所述加密的内容。提供了耦合到所述处理器的认证处理器，用于当所述处理器接收到所述认证请求时，针对所述外部设备对所述SoC进行认证，以及生成用于对所述加密的内容进行解密的解密密钥。提供了耦合到所述处理器和所述认证处理器的解密处理器，用于从所述认证处理器接

收所述解密密钥，以及使用所述解密密钥对所述加密的内容进行解密。

[0096] 在另一个实施例中，所述认证处理器是与所述处理器分离的安全引擎处理器，并经由通信链路来耦合到所述处理器。

[0097] 在另一个实施例中，所述安全引擎处理器还包括在所述安全引擎处理器内的存储软件指令的存储器，当所述软件指令被所述安全处理器执行时，实现也由所述外部设备实现的预定的内容保护协议。

[0098] 在另外的实施例中，其中，所述预定的内容保护协议是高带宽数字内容保护(HDCP)协议。

[0099] 在另外的实施例中，所述认证处理器包括处理器寄存器，在将所生成的解密密钥直接发送给所述解密处理器之前，所述处理器寄存器存储所述解密密钥。不将所述解密密钥发送给所述处理器，并且不将所述解密密钥暴露给在所述处理器上运行的任何软件。

[0100] 在另外的实施例中，所述解密处理器与所述处理器是分离的，并经由通信链路来耦合到所述处理器。所述解密处理器还执行传输流解复用功能，以在对所述加密的内容进行解密之前，使所述加密的内容中的视频内容与音频内容相分离。

[0101] 在另外的实施例中，所述解密密钥是基于会话的密钥，其中在会话完成之后，所述基于会话的密钥失效。

[0102] 在另外的实施例中，上面所引用的内容处理集成电路还包括：耦合到所述处理器的无线通信模块，用于从所述外部设备无线地接收所述认证请求和所述加密的内容，以及将所述认证请求和所述加密的内容传送给所述处理器。所述无线通信模块还耦合到所述认证处理器以在所述外部设备和所述认证处理器之间传达认证信息。

[0103] 在另外的实施例中，一种无线显示系统包括：内容源设备，用于生成和无线地发送加密的内容；片上系统(SoC)无线接收机，用于从所述内容源设备接收认证请求以认证是否准许所述接收机接收所述加密的内容，以及一旦对所述接收机进行了认证，则接收所述加密的内容；耦合到所述接收机的内容渲染设备，用于接收和显示所述解密的内容。所述SoC无线接收机还包括：处理器，耦合为接收所述认证请求和所述加密的内容；认证处理器，耦合到所述处理器以(1)在所述处理器接收到认证请求时，针对内容源设备对所述接收机进行认证，以及(2)生成用于对所述加密的内容进行解密的解密密钥；解密处理器，耦合为从所述认证处理器接收所述解密密钥，以及使用所述解密密钥对所述加密的内容进行解密。

[0104] 在另外的实施例中，该认证处理器是与所述处理器分离的安全引擎处理器，并经由通信链路来耦合到所述处理器。所述安全引擎处理器还包括在所述安全引擎处理器内的存储软件指令的存储器，当所述软件指令被所述安全处理器执行时，实现也由所述内容源设备实现的预定的内容保护协议，以对所述加密的内容进行加密。

[0105] 在另外的实施例中，所述预定的内容保护协议是高带宽数字内容保护(HDCP)协议。

[0106] 在另外的实施例中，认证处理器包括处理器寄存器，在将所生成的解密密钥直接发送给所述解密处理器之前，所述处理器寄存器存储所述解密密钥，其中不将所述解密密钥发送给所述处理器，并且不将所述解密密钥暴露给在所述处理器上运行的任何软件。

[0107] 在另外的实施例中，所述解密处理器与所述处理器是分离的，并且经由通信链路来耦合到所述处理器。所述解密处理器还执行传输流解复用功能，以在对所述加密的内容

进行解密之前，使所述加密的内容中的视频内容与音频内容相分离。

[0108] 在另外的实施例中，所述解密密钥是基于会话的密钥，其中在会话完成之后，所述基于会话的密钥失效。

[0109] 在另外的实施例中，该无线显示系统还包括：耦合到所述处理器的无线通信模块，用于从内容源设备无线地接收所述认证请求和所述加密的内容，以及将所述认证请求和所述加密的内容传送给所述处理器。所述无线通信模块还耦合到所述认证处理器以在内容源设备和认证处理器之间传达认证信息。

[0110] 在另外的实施例中，一种在片上系统(SoC)媒体处理装置中提供安全和健壮的内容保护的方法，包括：在所述SoC媒体处理装置的处理器中，从外部设备接收认证请求以认证是否准许所述SoC媒体处理装置从所述外部设备接收加密的内容，以及一旦对所述SoC媒体处理装置进行了认证，则接收所述加密的内容；使所述认证处理器(1)根据预定的内容保护协议，针对所述外部设备对所述SoC媒体处理装置进行认证，以及(2)针对根据所述预定的内容保护协议而加密的所述加密的内容，生成解密密钥；以及一旦对所述SoC媒体处理装置进行了认证并且生成了所述解密密钥，则由所述处理器从所述外部设备接收所述加密的内容，以及向所述SoC媒体处理装置的解密处理器发送所述加密的内容，以使所述解密处理器利用直接从所述认证处理器接收的所述解密密钥对所述加密的内容进行解密。

[0111] 在另外的实施例中，上面所引用的方法还包括：在接收到所述认证请求时，由所述处理器向所述外部设备发送所述SoC媒体处理装置的证书。

[0112] 在另外的实施例中，上面所引用的方法还包括：在发送所述证书之后，在所述处理器中从所述外部设备接收加密的主密钥；向所述认证处理器发送所述加密的主密钥用于解密；从所述认证处理器接收以随机生成的数字的形式的所述主密钥的解密的确认；以及向所述外部设备发送所述随机生成的数字，以对所述主密钥的解密和验证进行确认。

[0113] 在另外的实施例中，上面所引用的方法还包括：使所述认证处理器对来自所述外部设备的本地检验请求进行响应。

[0114] 在另外的实施例中，其中，使所述认证处理器生成针对所述加密的内容的解密密钥，还包括：从所述外部设备接收加密的会话密钥；以及向所述认证处理器发送所述加密的会话密钥用于解密，以变成所述解密密钥。

[0115] 在另外的实施例中，上面所引用的方法还包括：一旦对所述SoC媒体处理装置进行了认证并且在认证处理器中生成和存储了所述解密密钥，则使所述解密处理器经由后门密钥装载，直接从所述认证处理器接收所述解密密钥。

[0116] 在另外的实施例中，一种具有指令序列的计算机可读介质，所述指令序列包括当被执行时，使得处理器执行设备认证和内容解密的指令，其包括：从外部设备接收认证请求以认证是否准许所述处理器从所述外部设备接收加密的内容，以及一旦对所述处理器进行了认证，则接收所述加密的内容；使与所述处理器分离的外部认证处理器(1)根据预定的数字内容保护协议，针对所述外部设备对所述处理器进行认证，以及(2)针对根据所述预定的数字内容保护协议而加密的所述加密的内容，生成解密密钥；一旦对所述处理器进行了认证并且生成了所述解密密钥，则从所述外部设备接收所述加密的内容，并且使与所述处理器分离的解密处理器直接从所述认证处理器接收所述解密密钥；以及向所述解密处理器发送所述加密的内容，以利用所述解密密钥进行解密。

[0117] 在另外的实施例中，所述解密密钥是在所述外部设备处被加密的并被发送给所述处理器的解密的会话密钥。

[0118] 在另外的实施例中，上面所引用的计算机可读介质还包括：使所述解密处理器经由后门密钥装载，直接从所述认证处理器接收所述解密的会话密钥。

[0119] 在另外的实施例中，上面所引用的计算机可读介质还包括：在接收到所述认证请求时，由所述处理器向所述外部设备发送所述处理器的证书；在发送所述证书之后，在所述处理器中从所述外部设备接收加密的主密钥；由所述处理器向所述认证处理器发送所述加密的主密钥用于解密；从所述认证处理器接收以随机生成的数字的形式的所述主密钥的解密的确认；以及向所述外部设备发送所述随机生成的数字，以对所述主密钥的解密和验证进行确认。

[0120] 在另外的实施例中，上面所引用的计算机可读介质还包括：使所述认证处理器对来自所述外部设备的本地检验请求进行响应。

[0121] 在另外的实施例中，其中，使所述认证处理器生成针对所述加密的内容的解密密钥，还包括：从所述外部设备接收加密的会话密钥；以及向所述认证处理器发送所述加密的会话密钥用于解密，以变成所述解密密钥。

[0122] 虽然在附图和前面的描述中详细地说明和描绘了本公开，但这种说明和描绘应被视作为示例性和非限制性的。应当理解的是，仅仅示出和描述了本公开的示例性实施例，并且意图是保护与本公开和所陈述的权利要求相一致的所有变化和修改。

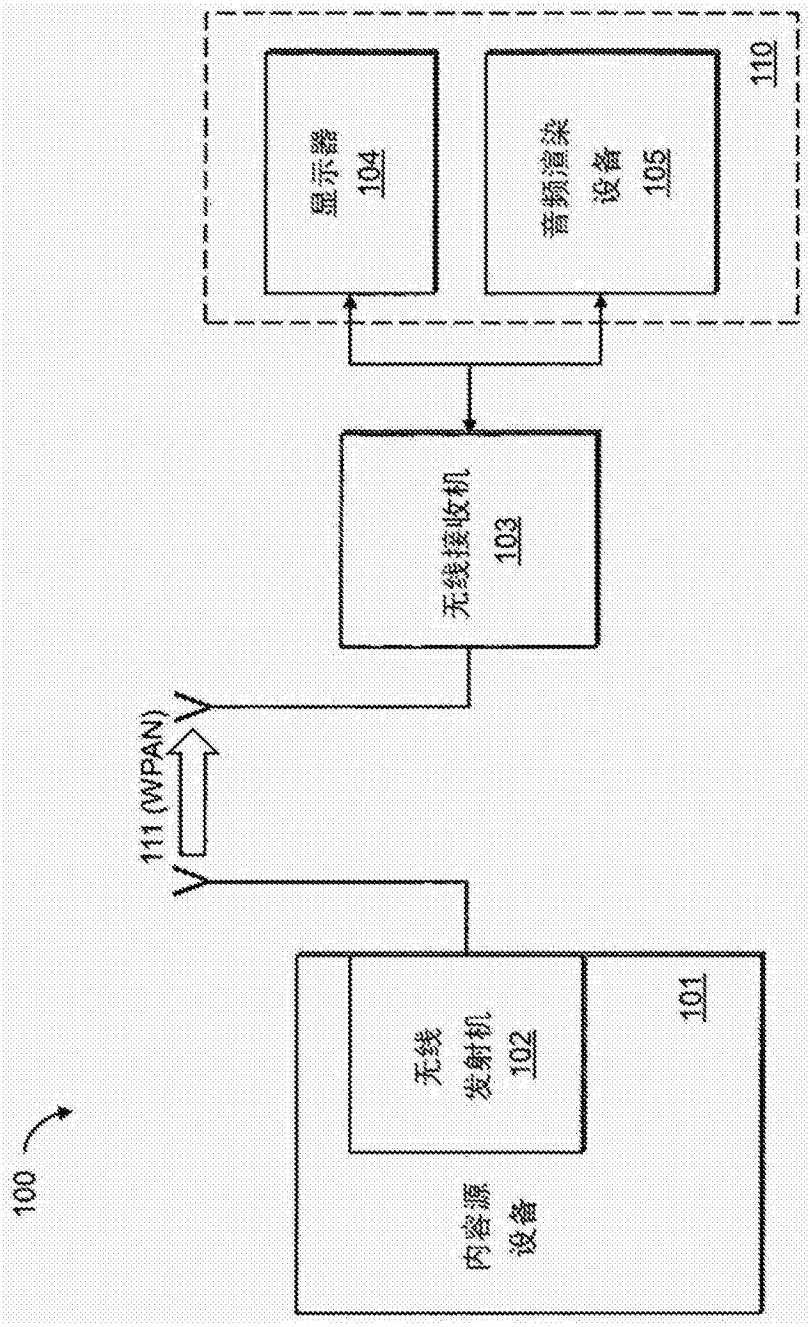

110
显示器
104
音频渲染
设备
105
无线接收机
103
111 (WPAN)
无线
发射机
102
101
内容源
设备
100

图1

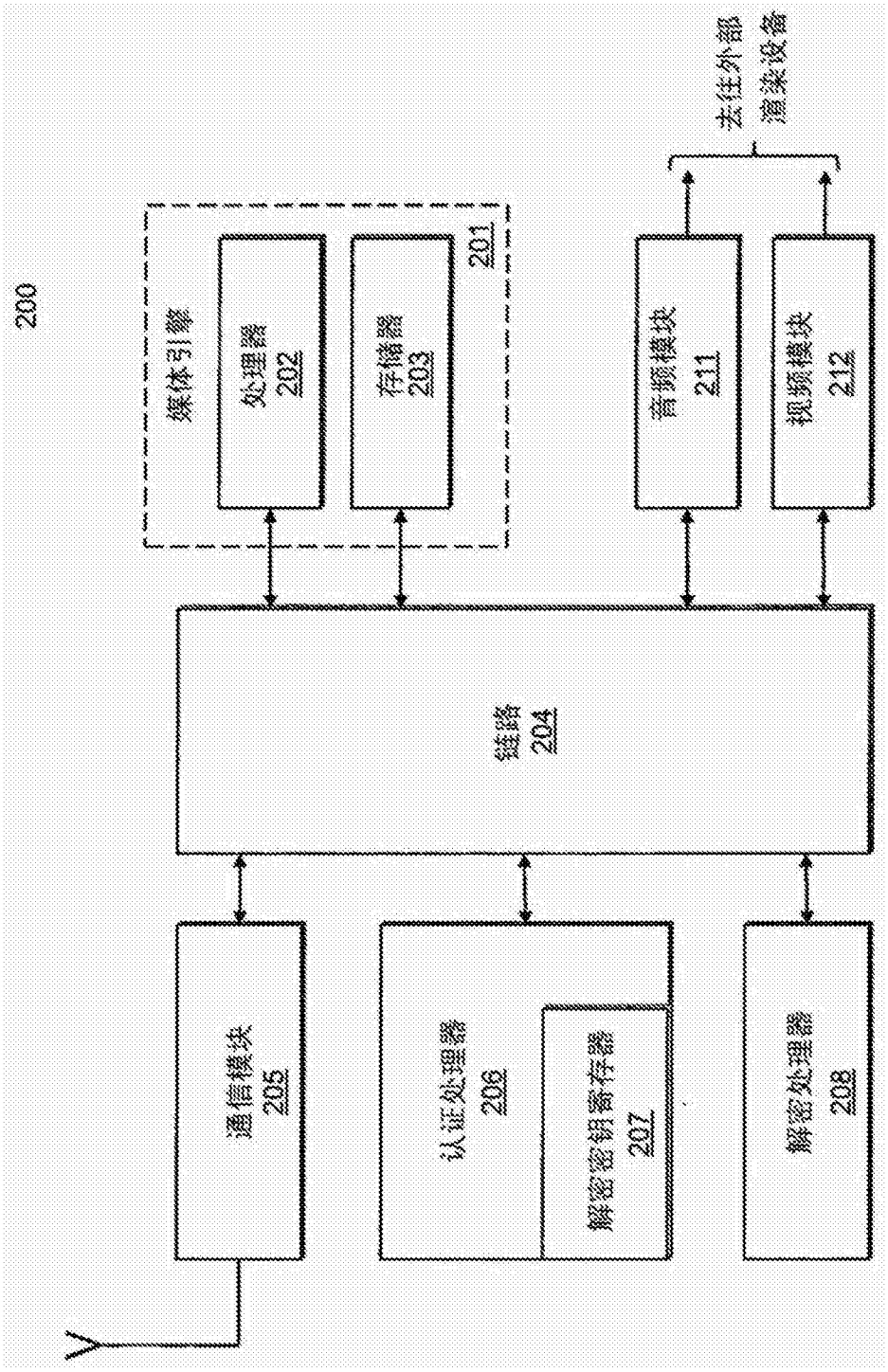

200
媒体引擎
201
处理器
202
存储器
203
音频模块
211
视频模块
212
去往外部
渲染设备
链路
204
通信模块
205
认证处理器
206
解密密钥寄存器
207
解密处理器
208

图2

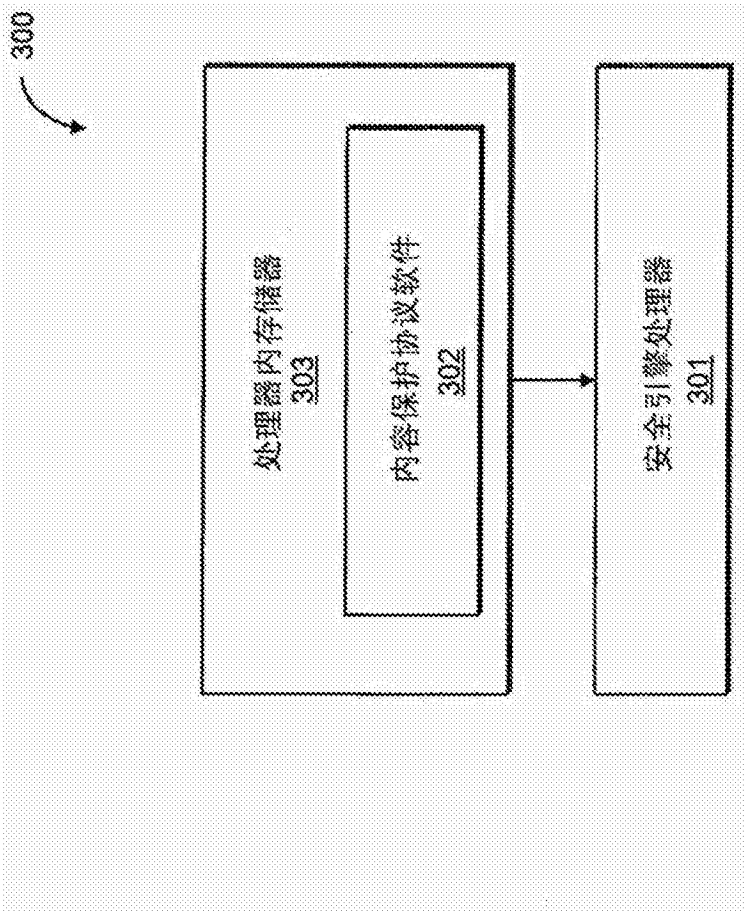


图3

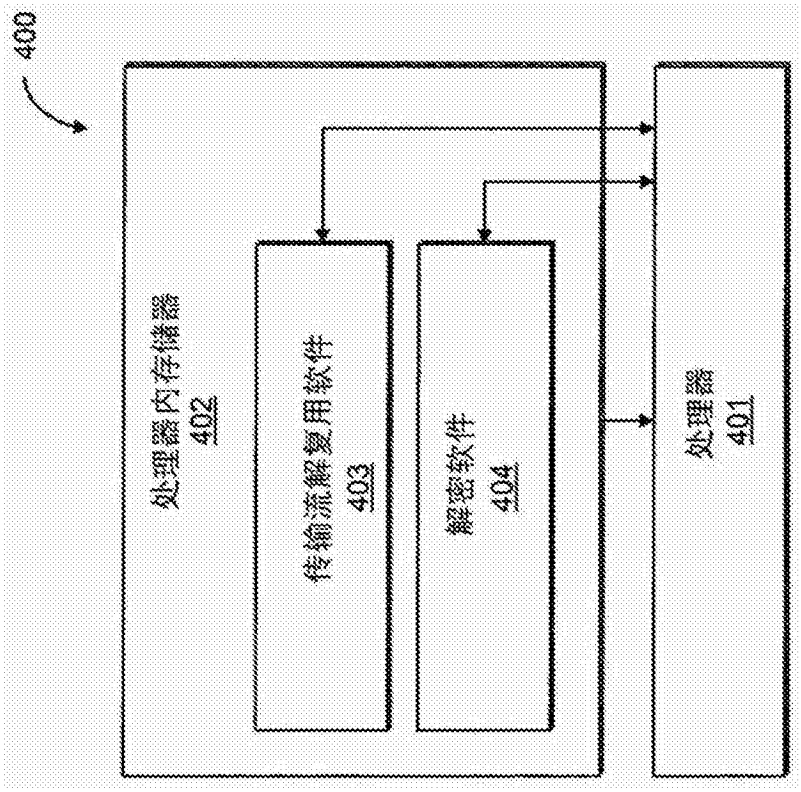


图4

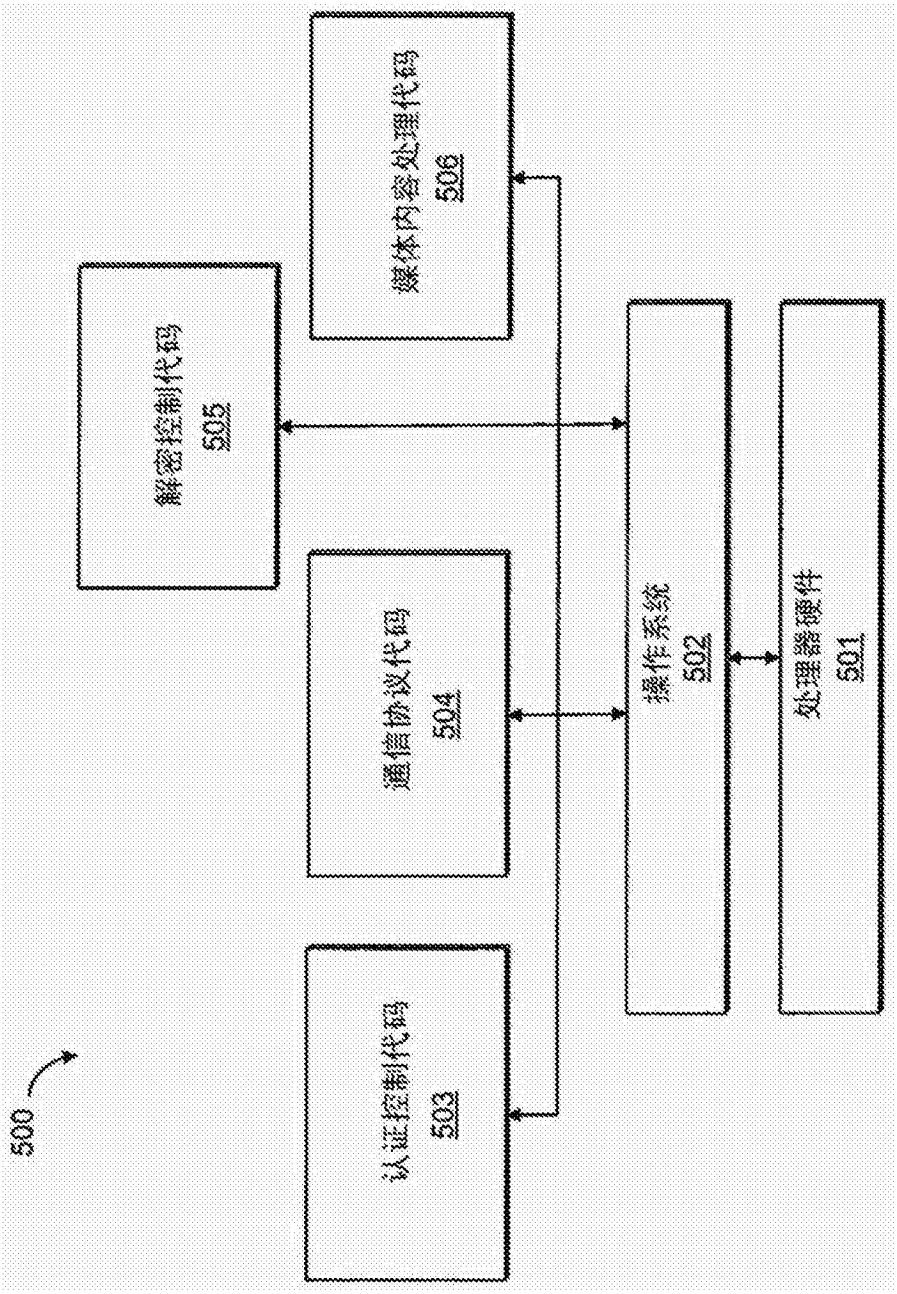

媒体内容处理代码
506
解密控制代码
505
通信协议代码
504
操作系统
502
处理器硬件
501
认证控制代码
503
500

图5

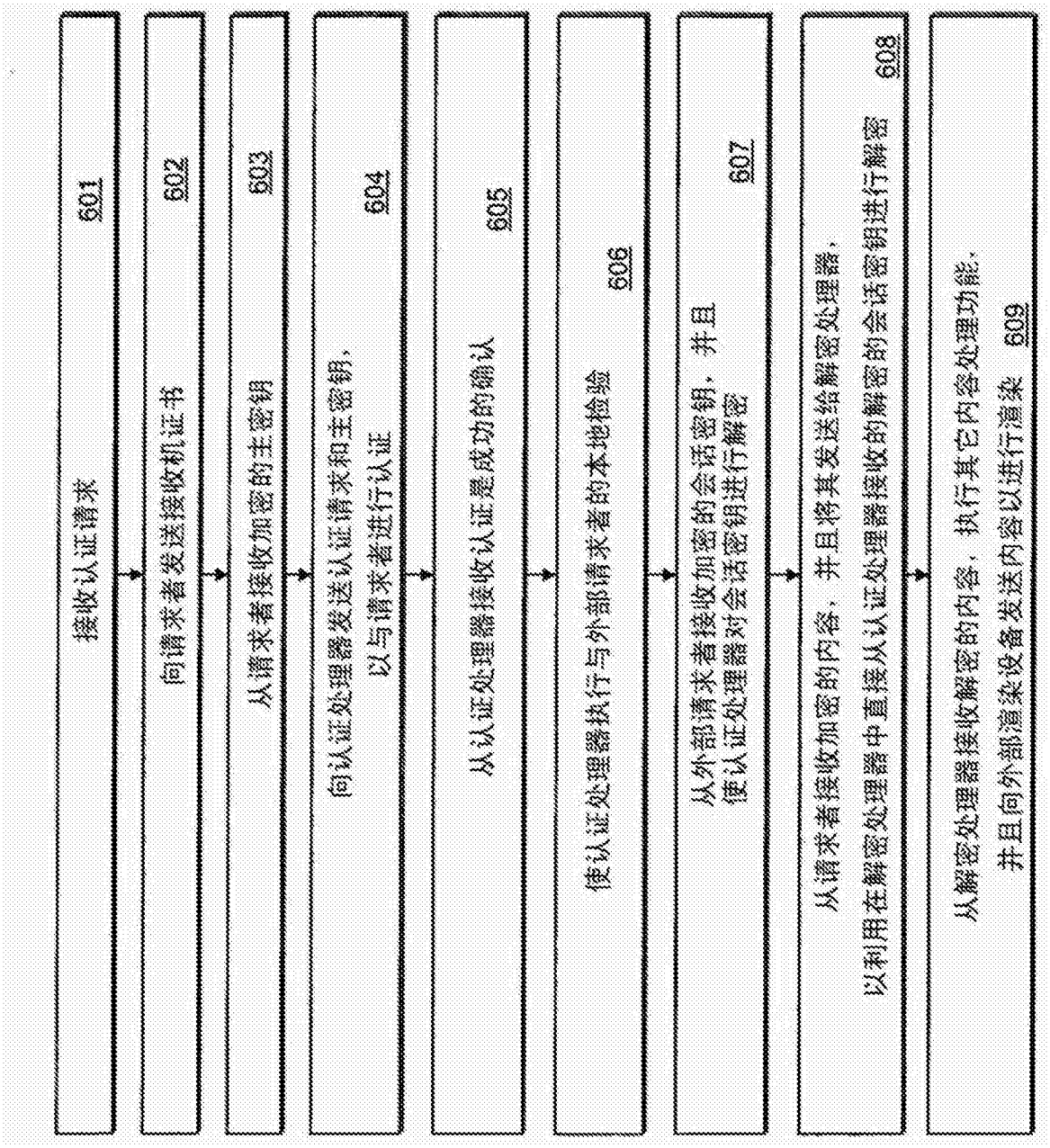

接收认证请求 601
向请求者发送接收机证书 602
从请求者接收加密的主密钥 603
向认证处理器发送认证请求和主密钥，
以与请求者进行认证 604
从认证处理器接收认证是成功的确认 605
使认证处理器执行与外部请求者的本地检验 606
从外部请求者接收加密的会话密钥，并且
使认证处理器对会话密钥进行解密 607
从请求者接收加密的内容，并且将其发送给解密处理器，
以利用在解密处理器中直接从认证处理器接收的解密的会话密钥进行解密 608
从解密处理器接收解密的内容，执行其它内容处理功能，
并且向外部渲染设备发送内容以进行渲染 609

图6

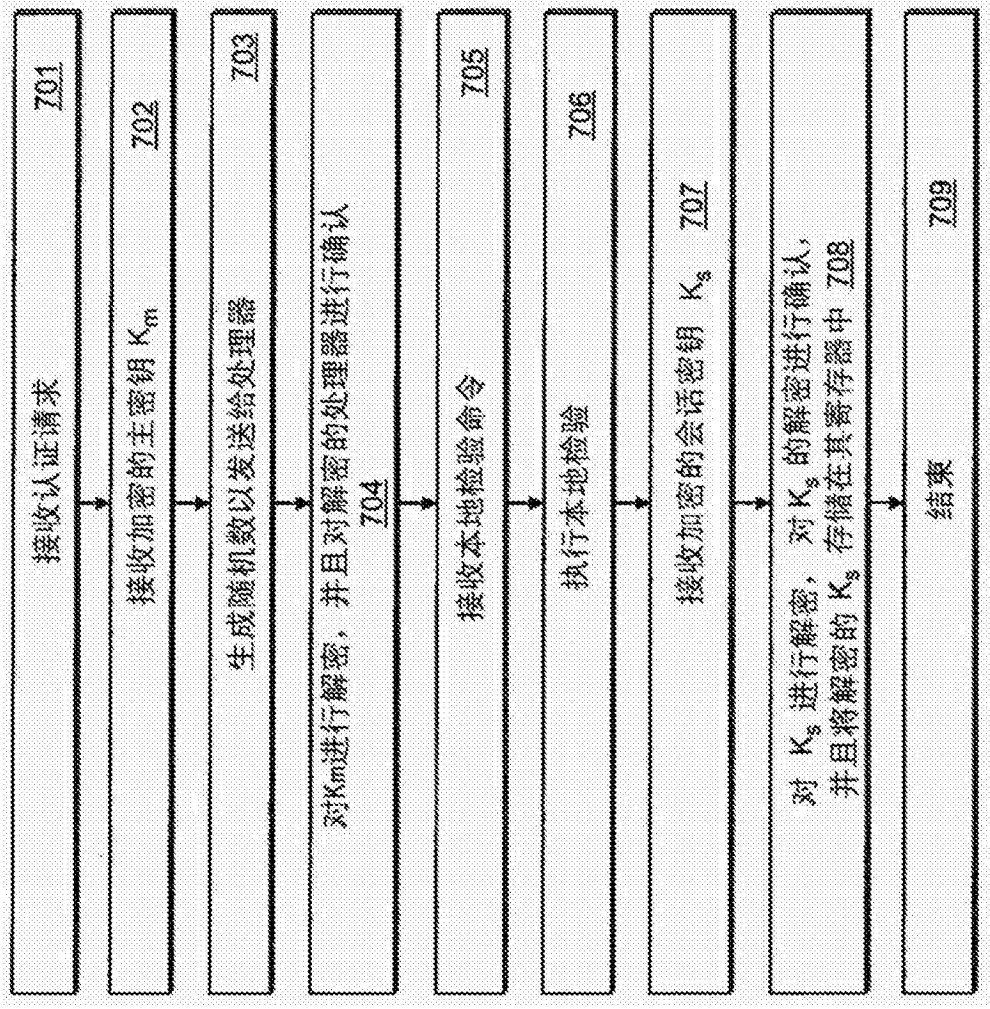

Z01
接收认证请求
Z02
接收加密的主密钥 K_m
Z03
生成随机数以发送给处理器
Z04
对Km进行解密，并且对解密的处理器进行确认
Z05
接收本地检验命令
Z06
执行本地检验
Z07
接收加密的会话密钥 K_s
Z08
对 K_s 进行解密，对 K_s 的解密进行确认，
并且将解密的 K_s 存储在其寄存器中
Z09
结束

图7

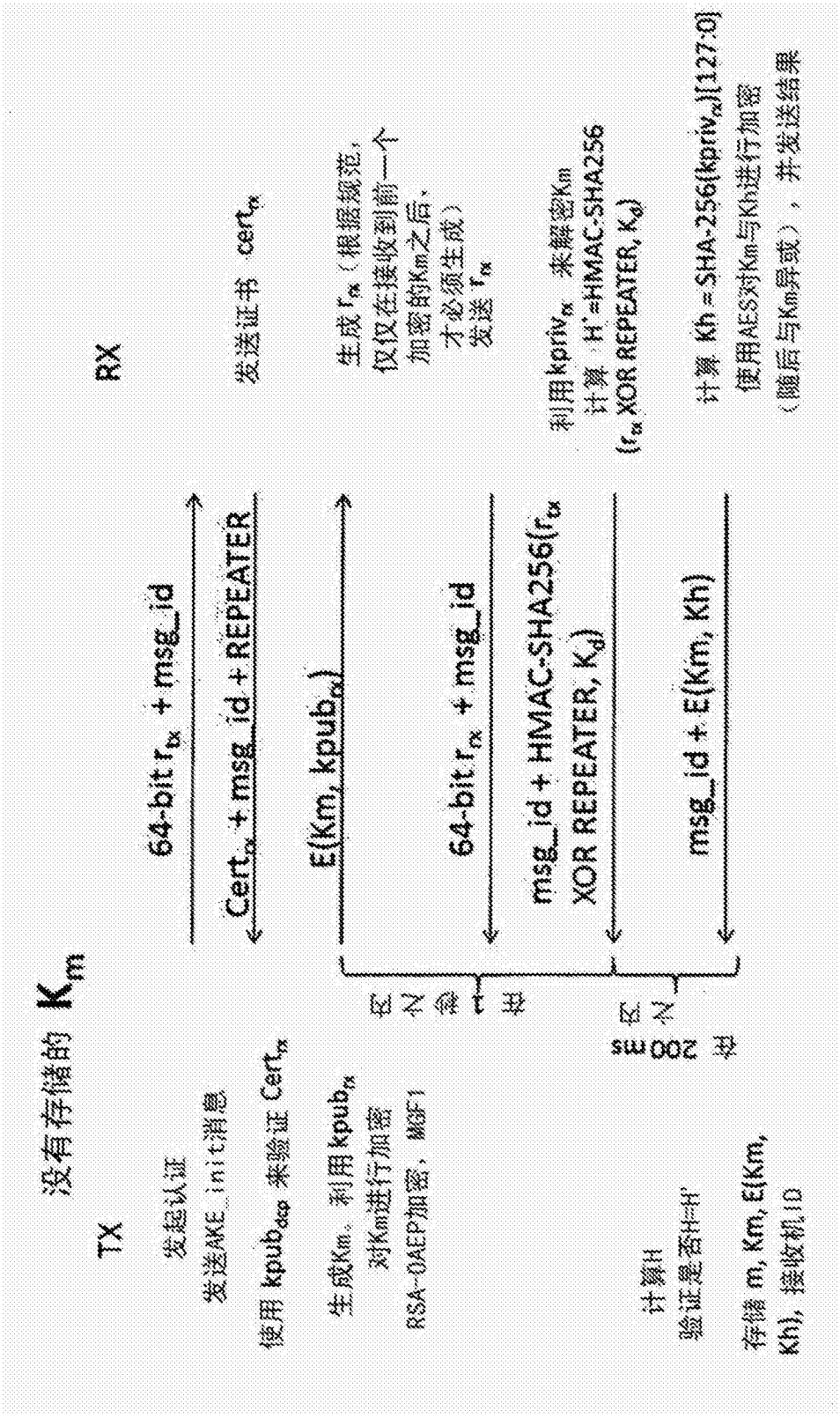

没有存储的 K_m
TX
RX
发起认证
发送AKE_init消息
使用 $kpub_{tx}$ 来验证 $Cert_{rx}$
生成Km，利用 $kpub_{rx}$ 对Km进行加密
RSA-OAEP加密，MGF1
计算H
验证是否H='
存储 m, Km, E(Km, Kh), 接收机ID
64-bit r_{tx} + msg_id
$Cert_{rx}$ + msg_id + REPEATER
发送证书 $cert_{rx}$
生成 r_{rx}（根据规范，仅仅在接收到前一个加密的K_m之后，才必须生成）
发送 r_{rx}
E(Km, $kpub_{rx}$)
利用 $kpriv_{rx}$ 来解密Km
计算 H'=HMAC-SHA256 (r_{rx} XOR REPEATER, K_d)
64-bit r_{rx} + msg_id
msg_id + HMAC-SHA256(r_{tx} XOR REPEATER, K_d)
计算 Kh = SHA-256($kpriv_{rx}$)[127:0]
使用AES对Km与Kh进行加密（随后与K_m异或），并发送结果
msg_id + E(Km, Kh)
208 ms
发送方等待时间
接收方等待时间

图8

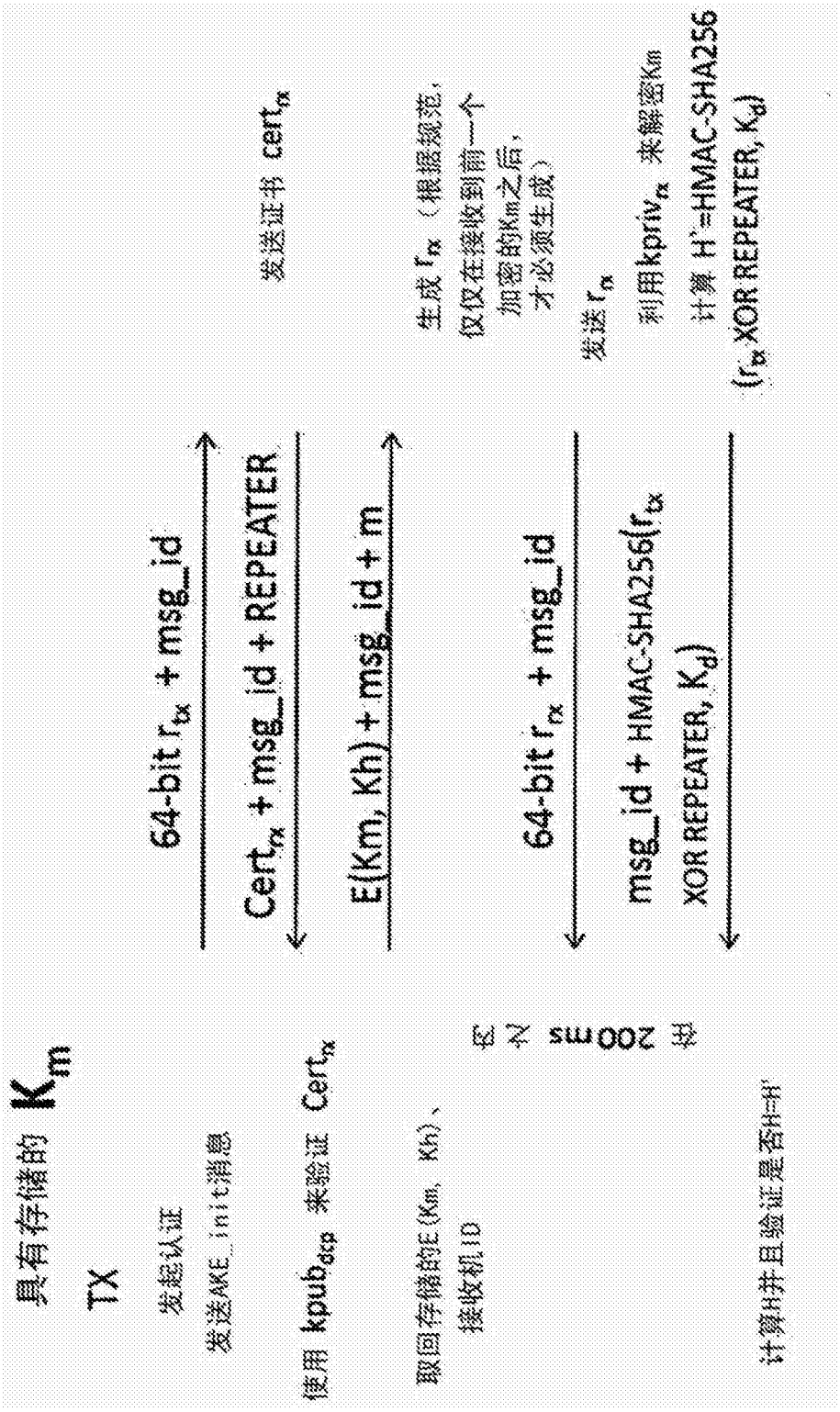

具有存储的 K_m
TX
发起认证
发送AKE_Init消息
使用 $kpub_{dcp}$ 来验证 $Cert_{rx}$
取回存储的E(Km, Kh)、
接收机ID
计算H并且验证是否H=H'
64-bit r_{tx} + msg_id
$Cert_{rx}$ + msg_id + REPEATER
E(Km, Kh) + msg_id + m
64-bit r_{rx} + msg_id
msg_id + HMAC-SHA256(r_{tx} XOR REPEATER, K_d)
发送证书 $cert_{rx}$
生成 r_{rx}（根据规范，仅仅在接收到前一个加密的Km之后，才必须生成）
发送 r_{rx}
利用 $kpriv_{rx}$ 来解密Km
计算 H'=HMAC-SHA256 (r_{tx} XOR REPEATER, K_d)
在 200ms 之内

图9

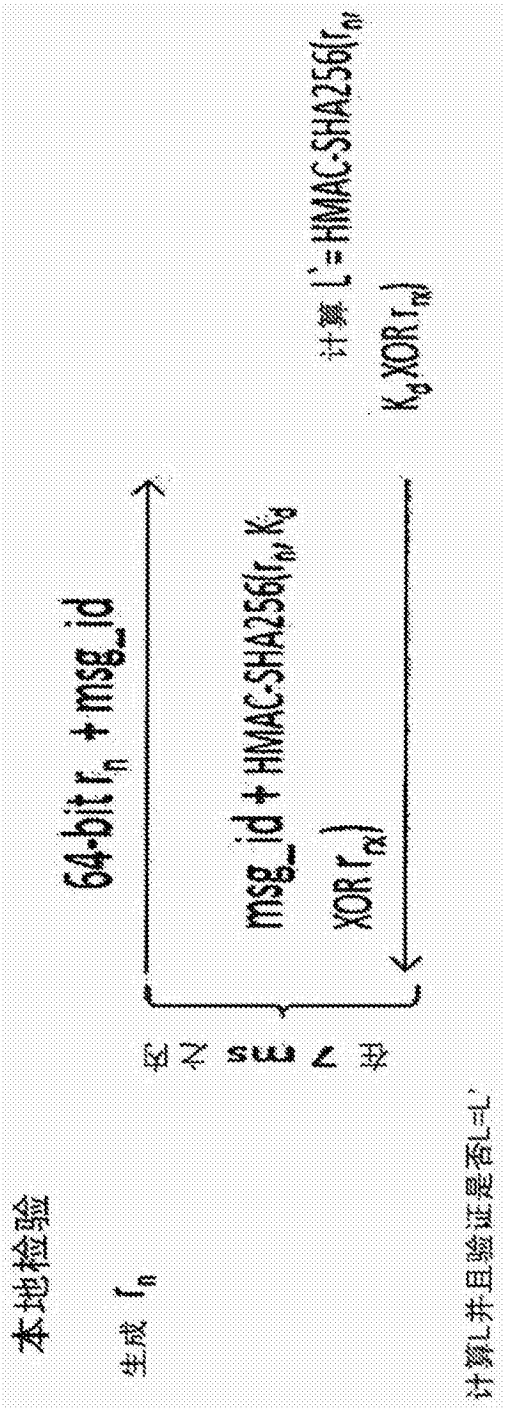

本地检验
生成 r_n
64-bit r_n + msg_id
msg_id + HMAC-SHA256(r_n, K_g
XOR r_n)
K_g XOR r_n)
计算 L'= HMAC-SHA256(r_n
计算L并且验证是否L=L'

图10

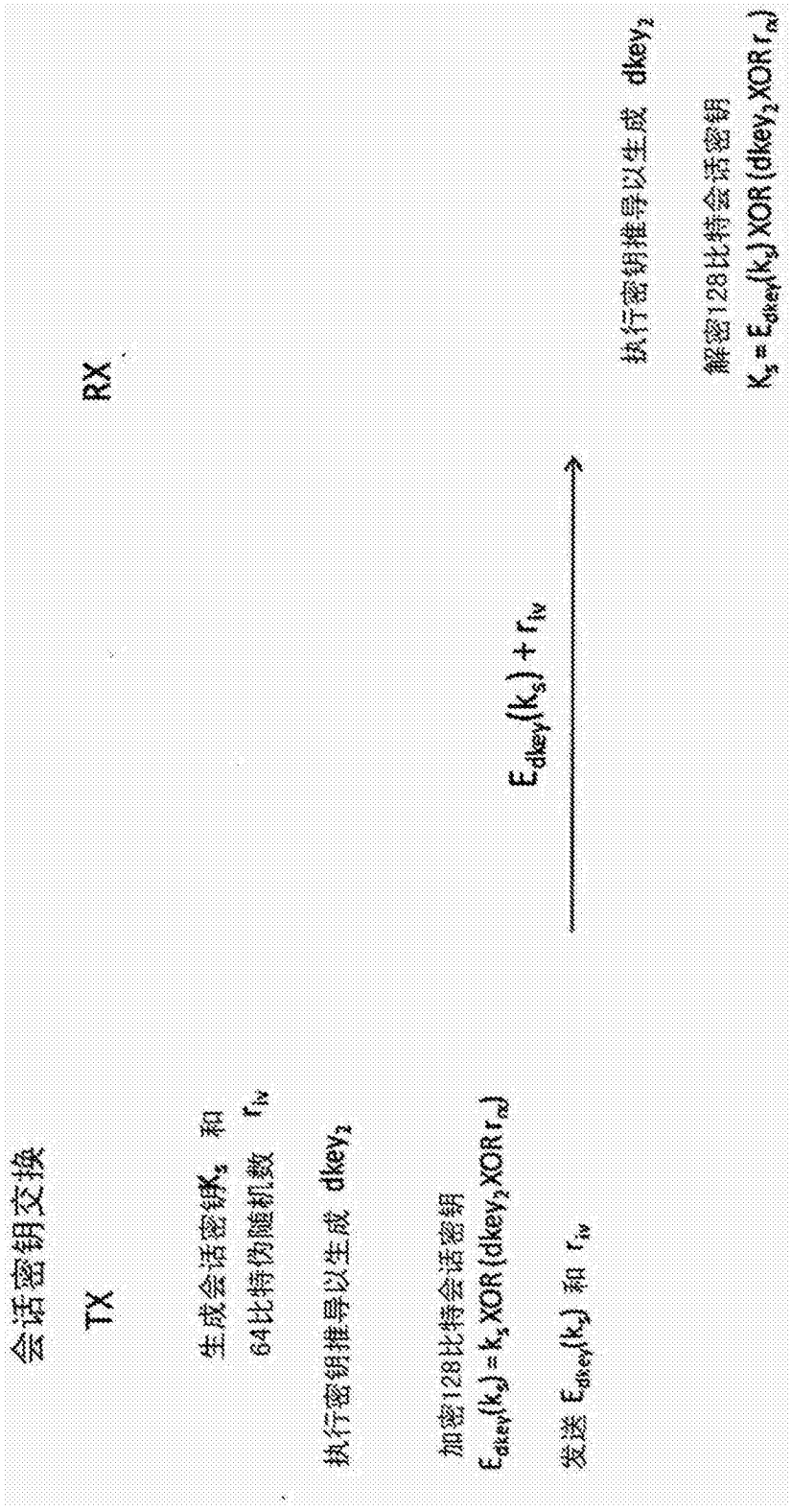

会话密钥交换
TX
RX
生成会话密钥K_s 和
64比特伪随机数 r_{rv}
执行密钥推导以生成 $dkey_2$
加密128比特会话密钥
$E_{dkey_2}(k_s) = k_s XOR (dkey_2 XOR r_{rv})$
发送 $E_{dkey_2}(k_s)$ 和 r_{rv}
$E_{dkey_2}(k_s) + r_{rv}$
执行密钥推导以生成 $dkey_2$
解密128比特会话密钥
$K_s = E_{dkey_2}(k_s) XOR (dkey_2 XOR r_{rv})$

图11