(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 105009597 A
(43)申请公布日 2015.10.28

(21)申请号 201480011997.9

(22)申请日 2014.03.12

(30)优先权数据
13/830,598 2013.03.14 US

(85)PCT国际申请进入国家阶段日
2015.09.02

(86)PCT国际申请的申请数据
PCT/US2014/024756 2014.03.12

(87)PCT国际申请的公布数据
WO2014/159689 EN 2014.10.02

(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 R·阿万奇 B·多尔古诺瓦 G·G·罗斯

(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 宋献涛

(51)Int.Cl.
H04N 21/4367(2006.01)
H04N 21/4405(2006.01)
H04L 9/08(2006.01)

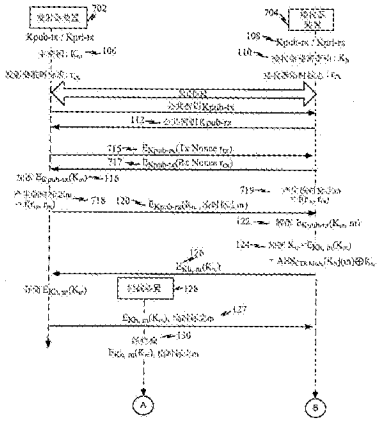
权利要求书5页 说明书10页 附图10页

(54)发明名称

作为阻止密钥恢复攻击的对策的用于发射器-接收器配对的主密钥加密功能

(57)摘要

本发明提供一种在接收器装置上操作的用于交换和/或产生安全密钥的方法。在所述接收器装置处从发射器装置接收第一经加密主密钥Km,所述第一经加密主密钥Km由接收器公共密钥Kpub-rx保护。所述第一经加密主密钥Km可用接收器私用密钥Kpri-rx解密以获得所述主密钥Km。可使用分块加密来加密所述主密钥Km,所述分块加密应用接收器秘密密钥Kh来获得第二经加密主密钥。



CN 105009597 A

1. 一种在接收器装置上操作的用于交换和 / 或产生安全密钥的方法，其包括 ：

从发射器装置接收第一经加密主密钥 Km，所述第一经加密主密钥 Km 由接收器公共密钥 Kpub-rx 保护 ；

用接收器私用密钥 Kpri-rx 解密所述第一经加密主密钥 Km 以获得所述主密钥 Km ；以及

使用分块加密来加密所述主密钥 Km，所述分块加密应用接收器秘密密钥 Kh 来获得第二经加密主密钥。

2. 根据权利要求 1 所述的方法，其中所述接收器公共密钥 Kpub-rx 和接收器私用密钥 Kpri-rx 是所述接收器装置处预先存储的加密密钥对。

3. 根据权利要求 1 所述的方法，其中所述秘密密钥 Kh 预先存储在所述接收器装置中且对于所述发射器装置是未知的。

4. 根据权利要求 1 所述的方法，其中仅在所述接收器装置的功率循环之间或会话期间产生和利用所述接收器公共密钥 Kpub-rx、所述接收器私用密钥 Kpri-rx 和所述秘密密钥 Kh。

5. 根据权利要求 1 所述的方法，其进一步包括 ：

将所述公共密钥 Kpub-rx 从所述接收器装置发送到所述发射器装置 ；以及

将所述第二经加密主密钥发送到所述发射器装置。

6. 根据权利要求 5 所述的方法，其进一步包括 ：

在后续时间从所述发射器装置接收所述第二经加密主密钥，作为其中所述发射器装置将把经保护内容递送到所述接收器装置的过程的一部分。

7. 根据权利要求 1 所述的方法，其中所述接收器装置仅在所述接收器装置的功率循环之间或会话期间将所述主密钥 Km 存储在易失性存储装置中。

8. 根据权利要求 1 所述的方法，其中所述分块加密包含从所述秘密密钥 Kh 产生的多个相异的回合密钥。

9. 根据权利要求 1 所述的方法，其中所述分块加密为在每一回合中实施不可打破函数的 Luby-Rackoff 加密。

10. 根据权利要求 9 所述的方法，其中所述函数为高级加密标准 AES-128 函数和安全散列算法 SHA-256 函数中的一者。

11. 根据权利要求 1 所述的方法，其中在高带宽数字内容保护 HDCP 加密协议内针对复制保护视频内容使用所述主密钥 Km。

12. 一种接收器装置，其包括 ：

通信电路，其用于与发射器装置通信 ；以及

处理电路，其耦合到所述通信电路，所述处理电路适于 ：

从所述发射器装置接收第一经加密主密钥 Km，所述第一经加密主密钥 Km 由接收器公共密钥 Kpub-rx 保护 ；

用接收器私用密钥 Kpri-rx 解密所述第一经加密主密钥 Km 以获得所述主密钥 Km ；以及

使用分块加密来加密所述主密钥 Km，所述分块加密应用接收器秘密密钥 Kh 来获得第二经加密主密钥。

13. 根据权利要求 12 所述的接收器装置，其进一步包括 ：

非易失性存储装置，其用于预先存储所述秘密密钥 Kh，其中所述秘密密钥 Kh 对于所述发射器装置为未知的。

14. 根据权利要求 12 所述的接收器装置，其中所述处理电路进一步适于 ：

将所述公共密钥 Kpub-rx 从所述接收器装置发送到所述发射器装置 ；以及

将所述第二经加密主密钥发送到所述发射器装置。

15. 根据权利要求 14 所述的接收器装置，其中所述处理电路进一步适于 ：

在后续时间从所述发射器装置接收所述第二经加密主密钥，作为其中所述发射器装置将把经保护内容递送到所述接收器装置的过程的一部分。

16. 根据权利要求 12 所述的接收器装置，其中所述分块加密包含从所述秘密密钥 Kh 产生的多个相异的回合密钥。

17. 根据权利要求 12 所述的接收器装置，其中所述分块加密为在每一回合中实施不可打破函数的 Luby-Rackoff 加密。

18. 根据权利要求 12 所述的接收器装置，其中在高带宽数字内容保护 HDCP 加密协议内针对复制保护视频内容使用所述主密钥 Km。

19. 一种接收器装置，其包括

用于从发射器装置接收第一经加密主密钥 Km 的装置，所述第一经加密主密钥 Km 由接收器公共密钥 Kpub-rx 保护 ；

用于用接收器私用密钥 Kpri-rx 解密所述第一经加密主密钥 Km 以获得所述主密钥 Km 的装置 ；以及

用于使用分块加密来加密所述主密钥 Km 的装置，所述分块加密应用接收器秘密密钥 Kh 来获得第二经加密主密钥。

20. 根据权利要求 19 所述的接收器装置，其进一步包括 ：

用于将所述公共密钥 Kpub-rx 从所述接收器装置发送到所述发射器装置的装置 ；以及

用于将所述第二经加密主密钥发送到所述发射器装置的装置。

21. 根据权利要求 20 所述的接收器装置，其进一步包括 ：

用于在后续时间从所述发射器装置接收所述第二经加密主密钥作为其中所述发射器装置将把经保护内容递送到所述接收器装置的过程的一部分的装置。

22. 一种非暂时性机器可读存储媒体，其具有存储于其上的指令，所述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 ：

从所述发射器装置接收第一经加密主密钥 Km，所述第一经加密主密钥 Km 由接收器公共密钥 Kpub-rx 保护 ；

用接收器私用密钥 Kpri-rx 解密所述第一经加密主密钥 Km 以获得所述主密钥 Km ；以及

使用分块加密来加密所述主密钥 Km，所述分块加密应用接收器秘密密钥 Kh 来获得第二经加密主密钥。

23. 根据权利要求 22 所述的机器可读存储媒体，其进一步具有存储于其上的指令，所述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 ：

将所述第二经加密主密钥发送到所述发射器装置 ；以及

在后续时间从所述发射器装置接收所述第二经加密主密钥，作为其中所述发射器装置将把经保护内容递送到所述接收器装置的过程的一部分。

24. 一种在接收器装置上操作的用于交换和 / 或产生安全密钥的方法，其包括 ：

将接收器临时标志 r_{rx} 发射到发射器装置 ；

从所述发射器装置接收发射器临时标志 r_{tx}；

从所述发射器装置接收第一经加密主密钥 Km 和主临时标志 m，其中所述第一经加密主密钥 Km 由接收器公共密钥 Kpub-rx 保护，且所述主临时标志 m 为所述发射器临时标志 t_{rx} 和所述接收器临时标志 r_{rx} 两者的函数 ；

用接收器私用密钥 Kpri-rx 解密所述第一经加密主密钥 Km 以获得所述主密钥 Km ；以及

在高级加密标准 AES 分块加密内使用接收器秘密密钥 Kh 和所述主临时标志 m 加密所述主密钥 Km 以获得第二经加密主密钥。

25. 根据权利要求 24 所述的方法，其中所述接收器公共密钥 Kpub-rx 和接收器私用密钥 Kpri-rx 是所述接收器装置处预先存储的加密密钥对。

26. 根据权利要求 24 所述的方法，其中所述秘密密钥 Kh 预先存储在所述接收器装置中且对于所述发射器装置是未知的。

27. 根据权利要求 24 所述的方法，其中仅在所述接收器装置的功率循环之间或会话期间产生和利用所述接收器公共密钥 Kpub-rx、所述接收器私用密钥 Kpri-rx 对和所述秘密密钥 Kh。

28. 根据权利要求 24 所述的方法，其进一步包括 ：

将所述公共密钥 Kpub-rx 从所述接收器装置发送到所述发射器装置 ；以及

将所述第二经加密主密钥发送到所述发射器装置。

29. 根据权利要求 28 所述的方法，其进一步包括 ：

接收所述发射器临时标志的新实例 r_{tx}' 作为新会话的一部分 ；

接收所述第二经加密主密钥连同所述主临时标志 m ；以及

检验所述主临时标志 m 为所述发射器临时标志的所述新实例 r_{tx}' 和进行所述新会话之前的所述接收器临时标志 r_{rx} 的函数。

30. 根据权利要求 29 所述的方法，其进一步包括 ：

如果所述主临时标志 m 不基于所述接收器临时标志 r_{rx}，那么终止所述新会话。

31. 根据权利要求 24 所述的方法，其中所述接收器装置仅在所述接收器装置的功率循环之间或会话期间将所述主密钥 Km 存储在易失性存储装置中。

32. 根据权利要求 24 所述的方法，其中在高带宽数字内容保护 HDCP 加密协议内针对复制保护视频内容使用所述主密钥 Km。

33. 一种接收器装置，其包括 ：

通信电路，其用于与发射器装置通信 ；以及

处理电路，其耦合到所述通信电路，所述处理电路适于 ：

将接收器临时标志 r_{rx} 发射到发射器装置 ；

从所述发射器装置接收发射器临时标志 r_{tx}；

从所述发射器装置接收第一经加密主密钥 Km 和主临时标志 m，其中所述第一经加密主

密钥 Km 由接收器公共密钥 Kpub-rx 保护，且所述主临时标志 m 为所述发射器临时标志 t_{rx} 和所述接收器临时标志 r_{rx} 两者的函数；

用接收器私用密钥 Kpri-rx 解密所述第一经加密主密钥 Km 以获得所述主密钥 Km；以及

在高级加密标准 AES 分块加密内使用接收器秘密密钥 Kh 和所述主临时标志 m 加密所述主密钥 Km 以获得第二经加密主密钥。

34. 根据权利要求 33 所述的接收器装置，其中所述秘密密钥 Kh 预先存储在所述接收器装置中且对于所述发射器装置是未知的。

35. 根据权利要求 33 所述的接收器装置，其中所述处理电路进一步适于：

将所述公共密钥 Kpub-rx 从所述接收器装置发送到所述发射器装置；以及

将所述第二经加密主密钥发送到所述发射器装置。

36. 根据权利要求 33 所述的接收器装置，其中所述处理电路进一步适于：

接收所述发射器临时标志的新实例 $r_{tx'}$ 作为新会话的一部分；

接收所述第二经加密主密钥连同所述主临时标志 m；以及

检验所述主临时标志 m 为所述发射器临时标志的所述新实例 $r_{tx'}$ 和进行所述新会话之前的所述接收器临时标志 r_{rx} 的函数。

37. 一种接收器装置，其包括：

用于将接收器临时标志 r_{rx} 发射到发射器装置的装置；

用于从所述发射器装置接收发射器临时标志 r_{tx} 的装置；

用于从所述发射器装置接收第一经加密主密钥 Km 和主临时标志 m 的装置，其中所述第一经加密主密钥 Km 由接收器公共密钥 Kpub-rx 保护，且所述主临时标志 m 为所述发射器临时标志 t_{rx} 和所述接收器临时标志 r_{rx} 两者的函数；

用于用接收器私用密钥 Kpri-rx 解密所述第一经加密主密钥 Km 以获得所述主密钥 Km 的装置；以及

用于在高级加密标准 AES 分块加密内使用接收器秘密密钥 Kh 和所述主临时标志 m 加密所述主密钥 Km 以获得第二经加密主密钥的装置。

38. 根据权利要求 37 所述的方法，其进一步包括：

用于将所述第二经加密主密钥发送到所述发射器装置的装置。

用于接收所述发射器临时标志的新实例 $r_{tx'}$ 作为新会话的一部分的装置；

用于接收所述第二经加密主密钥连同所述主临时标志 m 的装置；以及

用于检验所述主临时标志 m 为所述发射器临时标志的所述新实例 $r_{tx'}$ 和进行所述新会话之前的所述接收器临时标志 r_{rx} 的函数的装置。

39. 一种非暂时性机器可读存储媒体，其具有存储于其上的指令，所述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：

将接收器临时标志 r_{rx} 发射到发射器装置；

从所述发射器装置接收发射器临时标志 r_{tx}；

从所述发射器装置接收第一经加密主密钥 Km 和主临时标志 m，其中所述第一经加密主密钥 Km 由接收器公共密钥 Kpub-rx 保护，且所述主临时标志 m 为所述发射器临时标志 t_{rx} 和所述接收器临时标志 r_{rx} 两者的函数；

用接收器私用密钥 Kpri-rx 解密所述第一经加密主密钥 Km 以获得所述主密钥 Km ;以及

在高级加密标准 AES 分块加密内使用接收器秘密密钥 Kh 和所述主临时标志 m 加密所述主密钥 Km 以获得第二经加密主密钥。

作为阻止密钥恢复攻击的对策的用于发射器 - 接收器配对的主密钥加密功能

技术领域

[0001] 各种特征涉及密钥配对交换中的密钥的保护，且更明确地说涉及改进采用自反转运算的安全算法。

背景技术

[0002] 高带宽数字内容保护 (HDCP) 为用于复制保护视频内容的加密协议，且并入到数字视频连接接口中以阻止对此内容的未经授权的发射和再现。随着 HDCP 版本 2.0 和 2.1 的发布，HDCP 变成独立于接口的，且可应用于源与显示器之间的有线或无线、压缩或未经压缩的任何双向数字发射。HDCP 协议包括三个阶段 :验证、内容加密和可再生性。

[0003] 在验证阶段期间，在 HDCP 发射器与 HDCP 接收器之间交换加密的消息和公共密钥以确定接收器的身份和接受经保护内容的资格。如果认为验证成功，那么发射器前进到内容加密阶段。发射器使用通常作为验证阶段中密钥交换协议的一部分而产生的主密钥 K_m（即，配对主密钥）加密受保护的音频和 / 或视频 (A/V) 内容。

[0004] 然而，一些接收器可能计算能力有限且可不包含或具有对非易失性存储装置 / 存储器的写入存取权，借此阻止接收器产生和 / 或存储主密钥 K_m。在不了解主密钥 K_m 的情况下，接收器不能够解密经加密的 A/V 内容。

[0005] 图 1 说明发射器装置 102 与接收器装置 104 之间的验证阶段的实例。发射器装置 102 具备公共密钥 Kpub-tx 和对应的私用密钥 Kpri-tx。类似地，接收器装置 104 具备或产生公共密钥 Kpub-rx 和对应的私用密钥 Kpri-rx 108 连同接收器秘密密钥 K_h110。在验证阶段（其包含密钥交换）期间，发射器装置 102 将其公共密钥 Kpub-tx 发送到接收器装置 104，且接收器装置 104 将其公共密钥 Kpub-rx 发送 112 到发射器装置 102。应注意，在接收器装置 104 并不包含非易失性存储器的情况下，可由接收器装置 104 针对特定功率循环或会话产生公共密钥 Kpub-rx、对应的私用密钥 Kpri-rx 和接收器秘密密钥 K_h。

[0006] 在此安全系统中，发射器装置 102 可具备对应于每一接收器装置的主密钥。然而，在一些情况下，不存在针对接收器装置的对应主密钥（例如，接收器装置并不具有非易失性存储器）。因此，接收器装置 104 可接收来自发射器装置 102 的指示其并不具有对应于接收器装置的主密钥 K_m 的消息。

[0007] 因此，发射器装置 102 可将主密钥 K_m 提供到接收器装置 104。发射器装置 102 用接收器的公共密钥 Kpub-rx 加密 116 主密钥 K_m 且产生临时标志 m 118。经加密的主密钥和临时标志 $E_{Kpub\ rx}(K_m$、临时标志 m) 发送 120 到接收器装置 104。接收器装置 104 随后使用其私用密钥 Kpriv-rx 解密 122 经加密的主密钥和临时标志 m。临时标志 m 可用于产生初始化向量 (IV)。接收器装置 104 随后使用其自身的秘密密钥 K_h、所接收的临时标志 m，以及使用高级加密标准 (AES) 分块加密来加密 124 主密钥 K_m。举例来说，AES 分块加密可为计数器 (CTR) 模式中的 AES-128（高级加密标准 128 位算法）：

[0008] Encrypt $K_m = E_{Kh,m}(K_m) = AES_{CTR\ Mode}[K_h](m) \oplus K_m$。

[0009] 接收器装置 104 随后将此经加密主密钥 $E_{Kh,m}(K_m)$ 发送到发射器装置 102。此经加密主密钥 $E_{Kh,m}(K_m)$ 可由发射器装置 102 存储且用于发射器装置 102 到接收器装置 104 之间的后续同步交换。在后续同步交换时，发射器装置 102 发送 127 经加密主密钥 $E(K_h)(K_m)$ 以及临时标志 m，使得接收器装置 104 可将其解密且检验其为接收器先前发送的相同经加密主密钥，借此验证发射器。

[0010] HDCP 2 协议（版本 2.0 和 2.1）具有脆弱性：中间人 (MITM)（拦截装置 128）可拦截 130 发射器装置 102 与接收器装置 104 之间的涉及主密钥 K_m 的发射 127 且滥用接收器装置 104 解密此主密钥 K_m。然而，所发射的 $E_{Kh,m}(K_m)$ 127 仅为主密钥 K_m 与接收器的秘密 K_h 和临时标志 m 的异或。攻击者将拦截 $E(K_h)(K_m)$ 的此发射 127，起始其自身的与接收器装置 104 的会话 132。拦截装置 128 在此新会话中装作发射器。

[0011] 拦截装置 128 可接收 132 接收器装置的公共密钥 Kpub-rx 且用于加密所拦截的经加密主密钥 $E_{Kh,m}(K_m)$ 和临时标志 m 136 以供发射 138 到接收器装置 104。接收器装置 104 随后使用其私用密钥 Kpriv-rx 解密 $140E_{Kpub\ rx}(E_{Kh,m}(K_m)、m)$。接收器装置 104 随后使用其接收器秘密密钥 K_h 和临时标志 m 加密 $E_{Kh,m}(K_m)$ 如下：

[0012] Encrypt $E_{Kh,m}(E_{Kh,m}(K_m)) = AES[K_h](m) \oplus (E_{Kh,m}(K_m))$

[0013] $= AES[K_h](m) \oplus AES[K_h](m) \oplus K_m = K_m$。

[0014] 接收器装置 104 随后发送回 $144E(K_h)(E(K_h)(K_m))$，其仅为 K_m。因此，拦截装置 128 归因于由接收器装置 104 使用的加密的自反转性质而能够获得主密钥 K_m。利用主密钥 K_m，拦截装置 128 可能够解码发射器装置 102 可发送到接收器装置 104 的经加密内容。

[0015] 因此，需要一种防止拦截装置利用接收器装置使用的加密的弱点的改进的安全措施。

发明内容

[0016] 本发明提供一种在接收器装置上操作的用于交换和 / 或产生安全密钥的方法。接收器装置可包含接收器公共密钥 Kpub-rx 和接收器私用密钥 Kpri-rx，其可为预先存储在接收器装置处的加密密钥对。另外，接收器装置还可包含预先存储在接收器装置中且对于发射器装置是未知的秘密密钥 Kh。接收器公共密钥 Kpub-rx、接收器私用密钥 Kpri-rx 和秘密密钥 Kh 可仅在接收器装置的功率循环之间或会话期间产生和利用。

[0017] 公共密钥 Kpub-rx 可从接收器装置发送 / 发射到发射器装置。从发射器装置接收第一经加密主密钥 Km，其中所述第一经加密主密钥 Km 由接收器公共密钥 Kpub-rx 保护。第一经加密主密钥 Km 可随后用接收器私用密钥 Kpri-rx 解密以获得主密钥 Km。接收器装置可仅在接收器装置的功率循环之间或会话期间将主密钥 Km 存储在易失性存储装置中。主密钥 Km 随后由接收器装置使用分块加密而加密，所述分块加密应用接收器秘密密钥 Kh 获得第二经加密主密钥。第二经加密主密钥随后发送到发射器装置。在后续时间，可在接收器装置处从发射器装置接收第二经加密主密钥，作为其中发射器装置将把经保护内容递送到接收器装置的过程的一部分。

[0018] 在一个实例中，分块加密可包含从秘密密钥 Kh 产生的多个相异的回合密钥。举例来说，分块加密可为在每一回合中实施不可打破函数的 Luby-Rackoff 加密。所述函数可为高级加密标准 (AES)-128 函数和安全散列算法 (SHA)-256 函数中的一者。

[0019] 在一个实施方案中，主密钥 Km 可在高带宽数字内容保护 (HDCP) 加密协议内针对复制保护视频内容使用。

[0020] 还提供一种接收器装置，其包括通信电路、非易失性存储装置和处理电路。所述通信电路可用以与发射器装置通信。非易失性存储装置可用以预先存储秘密密钥 Kh，其中秘密密钥 Kh 对于发射器装置是未知的。

[0021] 所述处理电路适于：(a) 将公共密钥 Kpub-rx 从接收器装置发送到发射器装置；(b) 从发射器装置接收第一经加密主密钥 Km，所述第一经加密主密钥 Km 由接收器公共密钥 Kpub-rx 保护；(c) 利用接收器私用密钥 Kpri-rx 解密第一经加密主密钥 Km 以获得主密钥 Km；(d) 使用分块加密来加密主密钥 Km，所述分块加密应用接收器秘密密钥 Kh 来获得第二经加密主密钥；(e) 将第二经加密主密钥发送到发射器装置；和 / 或 (f) 在后续时间从发射器装置接收第二经加密主密钥，作为其中发射器装置将把经保护内容递送到接收器装置的过程的一部分。

[0022] 提供在接收器装置上操作的用于交换和 / 或产生安全密钥的另一方法。接收器装置可包含接收器公共密钥 Kpub-rx 和接收器私用密钥 Kpri-rx，其可为预先存储在接收器装置处的加密密钥对。另外，接收器装置还可包含预先存储在接收器装置中且对于发射器装置是未知的秘密密钥 Kh。接收器公共密钥 Kpub-rx、接收器私用密钥 Kpri-rx 和秘密密钥 Kh 可仅在接收器装置的功率循环之间或会话期间产生和利用。

[0023] 接收器装置可将公共密钥 Kpub-rx 以及接收器临时标志 r_{rx} 发送到发射器装置。接收器装置可从发射器装置接收发射器临时标志 r_{tx}。还可从发射器装置接收第一经加密主密钥 Km 和主临时标志 m，其中第一经加密主密钥 Km 由接收器公共密钥 Kpub-rx 保护，且主临时标志 m 为发射器临时标志 t_{rx} 和接收器临时标志 r_{rx} 两者的函数。接收器装置可随后利用接收器私用密钥 Kpri-rx 解密第一经加密主密钥 Km 以获得主密钥 Km。主密钥 Km 可在高级加密标准 (AES) 分块加密内使用接收器秘密密钥 Kh 和主临时标志 m 来加密以获得第二经加密主密钥。第二经加密主密钥可由接收器装置发送到发射器装置。

[0024] 随后，可接收发射器临时标志的新实例 $r_{tx'}$ 作为新会话的一部分。另外，还可接收第二经加密主密钥连同主临时标志 m。接收器装置可检验主临时标志 m 为发射器临时标志的新实例 $r_{tx'}$ 和进行新会话之前的接收器临时标志 r_{rx} 的函数。

[0025] 如果主临时标志 m 不基于接收器临时标志 r_{rx}，那么接收器装置可终止新会话。

[0026] 接收器装置可仅在接收器装置的功率循环之间或会话期间将主密钥 Km 存储在易失性存储装置中。主密钥 Km 可在高带宽数字内容保护 (HDCP) 加密协议内针对复制保护视频内容使用。

[0027] 还提供一种接收器装置，其包括通信电路、非易失性存储装置和处理电路。所述通信电路可用以与发射器装置通信。非易失性存储装置可用以预先存储秘密密钥 Kh，其中秘密密钥 Kh 对于发射器装置是未知的。

[0028] 所述处理电路可适于：(a) 将公共密钥 Kpub-rx 从接收器装置发送到发射器装置；(b) 将接收器临时标志 r_{rx} 发射到发射器装置；(c) 从发射器装置接收发射器临时标志 r_{tx}；(d) 从发射器装置接收第一经加密主密钥 Km 和主临时标志 m，其中所述第一经加密主密钥 Km 由接收器公共密钥 Kpub-rx 保护，且所述主临时标志 m 为发射器临时标志 t_{rx} 和接收器临时标志 r_{rx} 两者的函数；(e) 利用接收器私用密钥 Kpri-rx 解密第一经加密主密钥 Km 以

获得主密钥 Km；(f) 在高级加密标准 (AES) 分块加密内使用接收器秘密密钥 Kh 和主临时标志 m 加密主密钥 Km 以获得第二经加密主密钥；(g) 将第二经加密主密钥发送到发射器装置；(h) 接收发射器临时标志的新实例 $r_{tx'}$ 作为新会话的一部分；(i) 接收第二经加密主密钥连同主临时标志 m；和 / 或 (j) 检验主临时标志 m 为发射器临时标志的新实例 $r_{tx'}$ 和进行新会话之前的接收器临时标志 r_{rx} 的函数。

附图说明

[0029] 结合图式考虑，从下文阐述的详细描述可显而易见各种特征、性质和优点，在图式中相同参考标号始终对应地进行识别。

[0030] 图 1 说明发射器装置与接收器装置之间的验证阶段的实例。

[0031] 图 2 说明第一方法，其中使用 AES 加密而非计数器模式中的 AES 加密进行接收器装置处主密钥 K_m 的加密。

[0032] 图 3 说明第二方法，其中使用分块加密而非计数器模式中的 AES 加密（其视为流加密）进行接收器装置处主密钥 K_m 的加密。

[0033] 图 4 为说明作为分块加密的实例的 Feistel 加密的实例的框图。

[0034] 图 5 为说明适于根据图 3 的方法安全地产生主密钥的接收器装置的框图。

[0035] 图 6 说明在接收器装置中操作以根据图 3 的方法安全地产生主密钥的方法。

[0036] 图 7（包括图 7A 和 7B）说明第三方法，其中提供发射器装置和接收器装置中的每一者以分别发射临时标志 r_{tx} 和接收临时标志 r_{rx}。

[0037] 图 8 为说明适于根据图 7 的方法安全地产生主密钥的接收器装置的框图。

[0038] 图 9 说明在接收器装置中操作以根据图 7 的方法安全地产生主密钥的方法。

具体实施方式

[0039] 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，所属领域的一般技术人员将理解，可在不具有这些具体细节的情况下实践所述方面。举例来说，可用框图展示电路以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。

[0040] 词语“示范性”在本文中用以指“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。

[0041] 概述

[0042] 解决上文所论述的安全弱点的一个方法为，改变接收器装置使用的用于将主密钥 K_m 发送回到发射器装置的加密函数。然而，此可受一些接收器装置（例如，并不包含或能够存取非易失性存储装置 / 存储器的接收器装置，借此阻止接收器产生和存储密钥）的有限处理能力约束。

[0043] 揭示各种示范性方法来改进其中在发射器装置与接收器装置之间导出加密密钥的验证协议的安全性。在一个实例中，此些示范性方法可适用于由高带宽数字内容保护 (HDCP) 针对复制保护视频内容分布使用的验证协议。

[0044] 通常，提供解决方案，其中接收器装置实施不是解密算法的反转形式的加密算法。

也就是说，通过避免纯粹自反转加密 / 解密运算，暴露主密钥 K_m 的风险得以缓解。

[0045] 第一方法实施高级加密标准 (AES) 算法用于接收器装置处的加密。普通 AES（而非计数器模式）极其快速、简单且有效，但具有潜在地需要接收器装置处的额外硬件的缺点。

[0046] 第二方法使用 HDCP 2 规范已经要求的基元且在分块加密（例如，Luby-Rackoff 构造加密）中使用所述基元以提供不是其自身的反转形式的加密。此方法少许较慢（归因于分块加密）但不需要实施额外基元。

[0047] 这前两个方法保持与 HDCP 2 规范的互操作性且不需要对发射器装置的改变。

[0048] 第三方法改变计算 AES 计数器模式加密的初始化向量 (IV) 的方式来加密主密钥 K_m。因此，此方法可需要对接收器和发射器装置两者的改变。

[0049] 第一示范性解决方案

[0050] 图 2 说明第一方法，其中使用 AES 加密而非计数器模式中的 AES 加密进行接收器装置处主密钥 K_m 的加密。AES 加密可为基于在多个回合中将明文变换为密文且反之亦然的取代 - 置换网络的加密。计数器模式中的 AES 加密连续加密“计数器”的值，其中此计数器可为产生保证长时间内不重复的序列的任何函数。

[0051] 在图 1 中说明的方法中，接收器装置 104 仅使用 AES 加密而非 AES 解密，因为接收器装置 104 进行的所有解密都使用接收器的加密密钥 (Kpub-rx、Kpri-rx) 进行。在一个实例中，此接收器装置可包含加密装置（例如，以实施计数器模式中的 AES 加密）而非解密装置。因此，接收器装置的加密密钥 (Kpub-rx、Kpri-rx) 用于解密。

[0052] 在图 2 中说明的方法中，接收器装置 204 具备 AES 加密和 AES 解密能力，其可使用所述能力获得主密钥 K_m，作为与发射器装置 202 的加密密钥交换的一部分。在图 2 中，代替于使用与主密钥 K_m 的自反转异或运算，在 AES 内使用主密钥 K_m，而不仅仅进行异或运算。因此，即使拦截装置 128 拦截发射 227 且尝试将经加密主密钥 K_m 重新发送 138 到接收器装置 204，但接收器装置 204 当其尝试加密 242 经加密主密钥 $E_{Kh}(K_m)$ 时也不再产生 K_m。如此处所说明，在步骤 244 中，拦截装置 128 不再得到主密钥 K_m，而是其无法用于解码或访问任何地方的经双倍加密的主密钥 $E_{Kh}(E_{Kh}(K_m))$。

[0053] 如果接收器装置包含可编程固件，那么此解决方案并不需要任何额外硬件来使用 AES 实施加密（在步骤 224 处）和解密（在步骤 231 处）两者。否则，接收器装置必须包含硬件来执行 AES 解密，这使半导体的裸片区域较大。此解决方案的另一缺点为，许多接收器装置具有有限的计算能力，从而使 AES 解密的实施不合需要。

[0054] 第二示范性解决方案

[0055] 图 3 说明第二方法，其中使用分块加密而非计数器模式中的 AES 加密（其视为流加密）进行接收器装置处主密钥 K_m 的加密。流加密一次一个地对信息的位加密（即，一次对 1 个数据位操作）。流加密可包含在每一状态转变处输出一个信息位的状态机。此输出位流通常称为运行密钥。块加密通过将其划分为（固定大小）块（例如，多个位）且对每一块中的数据加密而将信息加密。分块加密加密法通常包含明文和密钥位的多个回合的位移位、异或运算、置换和取代。流加密与块加密相比实施起来较快且较小，然而其具有重要的安全缺陷。如果使用相同密钥流，那么特定类型的攻击可致使信息被揭露。

[0056] 在此第二方法中，AES 加密仅用作分块加密的构建块，借此接收器装置可以非反转方式加密和解密。在一个实例中，分块加密可基于 Luby-Rackoff 加密 (Feistel 网络 / 加

密），具有 3 或 4 个回合。

[0057] 图 4 为说明作为分块加密的实例的 Feistel 加密的实例的框图。如图 4 中所说明，“明文”（例如，主密钥 K_m）的右侧 $R_{0\cdots n+1}$ 用作到函数 F 的输入，其输出随后与“明文”（例如，主密钥 K_m）的左侧 $L_{0\cdots n+1}$ 进行异或运算，经过多个回合。左侧和右侧在每一回合反转或调换。函数 F 可为（例如）高级加密标准 (AES)-128 或安全散列算法 (SHA)-256，具有不同回合密钥 k_0、k_1、…k_n，其可经选择作为接收器的秘密密钥 K_h 的不同 64 位区段。在 Luby-Rackoff 加密中，假定函数 F 不可打破，因此 3 或 4 个回合将足以保护主密钥 K_m。

[0058] 取决于 AES-128 和 SHA-256 的相对性能，将 Feistel 网络的回合函数界定为与对应回合密钥 k_0、k_1、…k_n（用零填补）进行异或运算或串接的输入的 SHA-256 的低 64 位可能是有用的。

[0059] 另一变型使用 AES 与回合密钥以及 SHA-256 与同对应回合密钥预先进行异或运算的输入的各种组合而组合 Feistel 网络中的不同回合函数。

[0060] 以此方式，接收器装置 304 的加密能力用于提供加密和解密能力两者。

[0061] 在图 3 中，代替于使用与主密钥 K_m 的自反转异或运算，在 Luby-Rackoff 加密 (LR_Cipher) 内使用主密钥 K_m，而不仅仅进行异或运算。因此，即使拦截装置 128 拦截发射 327 且尝试将经加密主密钥 K_m 重新发送 138 到接收器装置 304，但接收器装置 304 当其尝试加密 342 经加密主密钥 $E_{Kh}(K_m)$ 时也不再产生 K_m。如此处所说明，在步骤 344 中，拦截装置不再得到 K_m，而是其无法用于解码或访问任何地方的经双倍加密的密钥 $E_{Kh}(E_{Kh}(K_m))$（即，使用 Luby-Rackoff 加密双倍地加密）。应注意，在第一加密操作中，在步骤 324 处，在主密钥 K_m 上应用 Luby-Rackoff 加密，而在第二加密操作上，在步骤 342 处，在经加密主密钥 $E_{Kh}(K_m)$ 上应用 Luby-Rackoff 加密。

[0062] 图 5 为说明适于根据图 3 的方法安全地产生主密钥的接收器装置的框图。接收器装置 500 可包含耦合到通信电路 518 的处理电路 502、易失性存储器装置 504 和 / 或非易失性存储器装置 506。通信电路 518 可用以到和 / 或从发射器装置通信。

[0063] 易失性存储器装置 504 可用以存储会话期间（或功率循环之间）产生的信息，例如主密钥 K_m512，但无法存储功率循环之间的信息。

[0064] 非易失性存储器装置 506 可为（例如）保持功率循环之间的信息的快闪存储器。在一些实施方案中，非易失性存储器装置 506 可为只读存储器，或对于处理电路 502 来说不可存取以用于写入 / 存储操作。在一些实施方案中，非易失性存储器装置 506 可存储接收器公共 / 私用加密密钥对 516 和 / 或接收器秘密密钥 K_h514。

[0065] 处理电路 502 可包含加密电路 510 和 / 或解密电路 508。加密电路 510 和 / 或解密电路 508 可（例如）用以执行与发射器装置的验证交换和 / 或密钥交换。此验证和 / 或密钥交换可准许接收器装置访问由发射器装置（经由通信电路 518）发送的经加密内容。

[0066] 在一个实例中，处理电路可适于将公共密钥 Kpub-rx 从接收器装置发送到发射器装置（经由通信电路 518）。应注意，接收器公共 / 私用密钥对 516 可预先产生 / 预先存储在非易失性存储器装置 506 内。或者，处理电路 502 可适于动态地产生此接收器公共 / 私用密钥对 516。作为响应，接收器装置 508 可从发射器装置接收（经由通信电路 518）第一经加密主密钥 Km。当接收时，第一经加密主密钥 Km 可由接收器公共密钥 Kpub-rx 保护。解密电路 508 可随后利用接收器私用密钥 Kpri-rx 解密第一经加密主密钥 Km 以获得主密钥

Km。加密电路 510 可随后使用分块加密使用秘密密钥 Kh 加密主密钥 Km 以获得第二经加密主密钥。处理电路可随后将第二经加密主密钥发送到发射器装置（经由通信电路 518）。

[0067] 在后续时间，可从发射器装置接收第二经加密主密钥，作为其中发射器装置将把经保护内容递送到接收器装置 500 的过程的一部分。

[0068] 图 6 说明在接收器装置中操作以根据图 3 的方法安全地产生主密钥的方法。此方法可（例如）由图 5 的接收器装置 500 的一或多个组件实施用于交换和 / 或产生安全密钥。

[0069] 接收器装置可获得（例如，从非易失性存储器）或动态地产生接收器公共密钥 Kpub-rx、接收器私用密钥 Kpri-rx 对和秘密密钥 Kh 602。接收器公共密钥 Kpub-rx 和接收器私用密钥 Kpri-rx 可为接收器装置处预先存储的加密密钥对。秘密密钥 Kh 可预先存储在接收器装置中且对于发射器装置是未知的。在一个实例中，接收器公共密钥 Kpub-rx、接收器私用密钥 Kpri-rx 和秘密密钥 Kh 仅在接收器装置的功率循环之间或会话期间产生和利用。

[0070] 接收器装置可将公共密钥 Kpub-rx 从接收器装置发送到发射器装置 604。作为响应，接收器装置可从发射器装置接收第一经加密主密钥 Km，所述第一经加密主密钥 Km 由接收器公共密钥 Kpub-rx 保护 606。接收器装置可随后利用接收器私用密钥 Kpri-rx 解密第一经加密主密钥 Km 以获得主密钥 Km 608。接收器装置可随后使用分块加密来加密主密钥 Km，所述分块加密应用接收器秘密密钥 Kh 来获得第二经加密主密钥 610。第二经加密主密钥可随后发送到发射器装置 612。在后续时间，接收器装置可从发射器装置接收第二经加密主密钥，作为其中发射器装置将把经保护内容递送到接收器装置的过程的一部分 614。

[0071] 接收器装置可仅在接收器装置的功率循环之间或会话期间将主密钥 Km 存储在易失性存储装置中。在一个实例中，可在高带宽数字内容保护 (HDCP) 加密协议内针对复制保护视频内容使用主密钥 Km。

[0072] 在一个实例中，分块加密可包含从秘密密钥 Kh 产生的多个相异的回合密钥。举例来说，分块加密可为在每一回合中实施不可打破的函数的 Luby-Rackoff 加密。所述函数可为高级加密标准 (AES)-128 函数和安全散列算法 (SHA)-256 函数中的一者。

[0073] 第三示范性解决方案

[0074] 图 7（包括图 7A 和 7B）说明第三方法，其中提供发射器装置 702 和接收器装置 704 中的每一者以分别发射临时标志 r_{tx} 和接收临时标志 r_{rx}。发射器装置 702 和接收器装置 704 交换其临时标志 r_{tx}715 和 r_{rx}717。随后分别由发射器装置 702 和接收器装置 704 独立地产生 718/719 主临时标志 m。

[0075] 在此实例中，主临时标志 m 为 r_{tx} 和 r_{rx} 两者的函数。此允许接收器装置 704 检查发射器（例如，发射器装置 702 或拦截装置 128）是否在同步交换期间正发送正确的主临时标志 m。举例来说，在一个实例中，主临时标志 $m = (r_{tx}r_{rx})$ 用零填补。在另一实例中，主临时标志 $m = r_{tx}$ 和 r_{rx} 的串接。

[0076] 当拦截装置 128 拦截经加密主密钥 $E_{Kh,m}(K_m)$ 和主临时标志 m 时，其可试图起始新会话 132，在新会话 132 中其与接收器装置 704 交换公共密钥 734 和 736。发射器装置 702 和接收器装置 704 还可交换临时标志 $r_{tx'}$740 和 r_{rx}742。应注意，针对拦截装置 128 的发射器临时标志 $r_{tx'}$ 不同于针对发射器装置 702 的发射器临时标志 r_{tx}。

[0077] 当拦截装置 128 尝试将所拦截的经加密主密钥和临时标志 m（例如，

$E_{Kpub\ rx}(E_{Kh,m}(K_m),m))$ 呈现给接收器装置 704 时，接收器装置 104 检查所接收的主临时标志 m 是否为临时标志 $r_{tx'}$ 和 r_{rx} 的函数。在此情况下，因为拦截装置的临时标志 $r_{tx'}$ 不同于发射器的装置临时标志 r_{tx}，所以检查 748 将失败。接收器装置 704 可随后终止或中止与拦截装置 128 的同步交换，借此阻止拦截装置 128 获得主密钥 K_m。

[0078] 图 8 为说明适于根据图 7 的方法安全地产生主密钥的接收器装置的框图。接收器装置 800 可包含耦合到通信电路 818 的处理电路 802、易失性存储器装置 804 和 / 或非易失性存储器装置 806。通信电路 818 可用以到和 / 或从发射器装置通信。

[0079] 易失性存储器装置 804 可用以存储会话期间（或功率循环之间）产生的信息，例如主密钥 K_m812，但无法存储功率循环之间的信息。

[0080] 非易失性存储器装置 806 可为（例如）保持功率循环之间的信息的快闪存储器。在一些实施方案中，非易失性存储器装置 806 可为只读存储器，或对于处理电路 802 来说不可存取以用于写入 / 存储操作。在一些实施方案中，非易失性存储器装置 806 可存储接收器公共 / 私用加密密钥对 816、接收器秘密密钥 K_h814 和 / 或接收器临时标志 r_{rx}817。

[0081] 处理电路 802 可包含加密电路 810 和 / 或解密电路 808。加密电路 810 和 / 或解密电路 808 可（例如）用以执行与发射器装置的验证交换和 / 或密钥交换。此验证和 / 或密钥可交换可准许接收器装置访问由发射器装置（经由通信电路 818）发送的经加密内容。

[0082] 在一个实例中，处理电路可适于将接收器临时标志 r_{rx} 发送 / 发射（经由通信电路 818）到发射器装置。作为回馈，处理电路可从发射器装置接收（经由通信电路 818）发射器临时标志 r_{tx}。另外，接收器装置还可从发射器装置接收（经由通信电路 818）第一经加密主密钥 Km 和主临时标志 m，其中所述第一经加密主密钥 Km 由接收器公共密钥 Kpub-rx 保护，且主临时标志 m 为发射器临时标志 t_{rx} 和接收器临时标志 r_{rx} 两者的函数。

[0083] 解密电路 808 可随后利用接收器私用密钥 Kpri-rx 解密第一经加密主密钥 Km 以获得主密钥 Km。加密电路 810 可在高级加密标准 (AES) 分块加密内使用接收器秘密密钥 Kh 和主临时标志 m 加密主密钥 Km 以获得第二经加密主密钥。第二经加密主密钥随后发送 / 发射到发射器装置（经由通信电路 818）。

[0084] 随后，接收器装置可接收发射器临时标志的新实例 $r_{tx'}$ 作为新会话的一部分。另外，接收器装置还可接收第二经加密主密钥连同主临时标志 m。临时标志检验器电路 811 可随后检验主临时标志 m 为发射器临时标志的新实例 $r_{tx'}$ 和进行新会话之前的接收器临时标志 r_{rx} 的函数。

[0085] 图 9 说明在接收器装置中操作以根据图 7 的方法安全地交换和 / 或产生主密钥的方法。接收器装置可获得或产生接收器公共密钥 Kpub-rx、接收器私用密钥 Kpri-rx 和秘密密钥 Kh 902。接收器公共密钥 Kpub-rx 和接收器私用密钥 Kpri-rx 可为接收器装置处预先存储的加密密钥对。秘密密钥 Kh 可预先存储在接收器装置中且对于发射器装置是未知的。仅可在接收器装置的功率循环之间或会话期间产生和利用接收器公共密钥 Kpub-rx、私用密钥 Kpri-rx 和秘密密钥 Kh。

[0086] 接收器装置可将公共密钥 Kpub-rx 从接收器装置发送到发射器装置 904。接收器装置还可将接收器临时标志 r_{rx} 发送 / 发射到发射器装置 906。作为响应，接收器装置可从发射器装置接收发射器临时标志 r_{tx}908。另外，接收器装置可从发射器装置接收第一经加密主密钥 Km 和主临时标志 m，其中所述第一经加密主密钥 Km 由接收器公共密钥 Kpub-rx 保

护，且主临时标志 m 为发射器临时标志 t_{rx} 和接收器临时标志 r_{rx} 两者的函数 910。第一经加密主密钥 Km 可用接收器私用密钥 Kpri-rx 解密以获得主密钥 Km 912。主密钥 Km 可随后由接收器装置在高级加密标准 (AES) 分块加密内使用接收器秘密密钥 Kh 和主临时标志 m 加密以获得第二经加密主密钥 914。接收器装置可随后将第二经加密主密钥发送到发射器装置 916。

[0087] 随后，接收器装置可接收发射器临时标志的新实例 $r_{tx'}$ 作为新会话的一部分。接收器装置还可接收第二经加密主密钥连同主临时标志 m。接收器装置可随后检验主临时标志 m 为发射器临时标志的新实例 $r_{tx'}$ 和进行新会话之前的接收器临时标志 r_{rx} 的函数。如果主临时标志 m 不基于接收器临时标志 r_{rx}，那么新会话终止。

[0088] 仅可在接收器装置的功率循环之间产生和利用接收器公共密钥 Kpub-rx、私用密钥 Kpri-rx 和秘密密钥 Kh。接收器装置可仅在接收器装置的功率循环之间或会话期间将主密钥 Km 存储在易失性存储装置中。在一个实例中，可在高带宽数字内容保护 (HDCP) 加密协议内针对复制保护视频内容使用主密钥 Km。

[0089] 图式中所说明的组件、步骤、特征和 / 或功能中的一或多者可重新布置和 / 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，还可添加额外的元件、组件、步骤和 / 或功能。图式中所说明的设备、装置和 / 或组件可经配置以执行图式中描述的方法、特征或步骤中的一或多者。本文中所描述的算法也可有效地实施于软件中和 / 或嵌入于硬件中。

[0090] 此外，在本发明的一个方面中，图 5 和 8 中说明的处理电路 502 和 / 或 802 可为经特定地设计和 / 或硬连线以执行图 2、3、4、6、7 和 / 或 9 中描述的算法、方法和 / 或步骤的专门处理器 (例如，专用集成电路 (例如，ASIC))。因此，此专门处理器 (例如，ASIC) 可为用于执行图 2、3、4、6、7 和 / 或 9 中描述的算法、方法和 / 或步骤的装置的一个实例。处理器可读存储媒体可存储指令，所述指令在由专门处理器 (例如，ASIC) 执行时致使所述专门处理器执行本文中所描述的算法、方法和 / 或步骤。

[0091] 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循序过程，但许多操作可并行或同时执行。另外，操作的次序可重新布置。过程在其操作完成时终止。过程可对应于方法、函数、进程、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。

[0092] 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。

[0093] 此外，本发明的方面可由硬件、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等机器可读媒体中。处理器可执行必要任务。代码段可表示进程、

函数、子程序、程序、例程、子例程、模块、软件包、类别，或者指令、数据结构或程序语句的任何组合。一代码段可通过传递和 / 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、令牌传递、网络发射等任何合适的手段传递、转发或发射。

[0094] 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、元件和 / 或组件可用通用处理器、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，处理器可为任何常规的处理器、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。

[0095] 结合本文所揭示的实例描述的方法或算法可以处理单元、编程指令或其它指示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，且可包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，存储媒体可与处理器成一体式。

[0096] 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、电路和算法步骤可实施为电子硬件、计算机软件或两者的组合。为清楚说明硬件与软件的此互换性，上文已大致关于其功能性描述各种说明性组件、块、模块、电路和步骤。此功能性是实施为硬件还是软件取决于特定应用和强加于整个系统的设计约束。

[0097] 本文中描述的本发明的各种特征可实施于不同系统中而不脱离本发明。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、修改和变化。

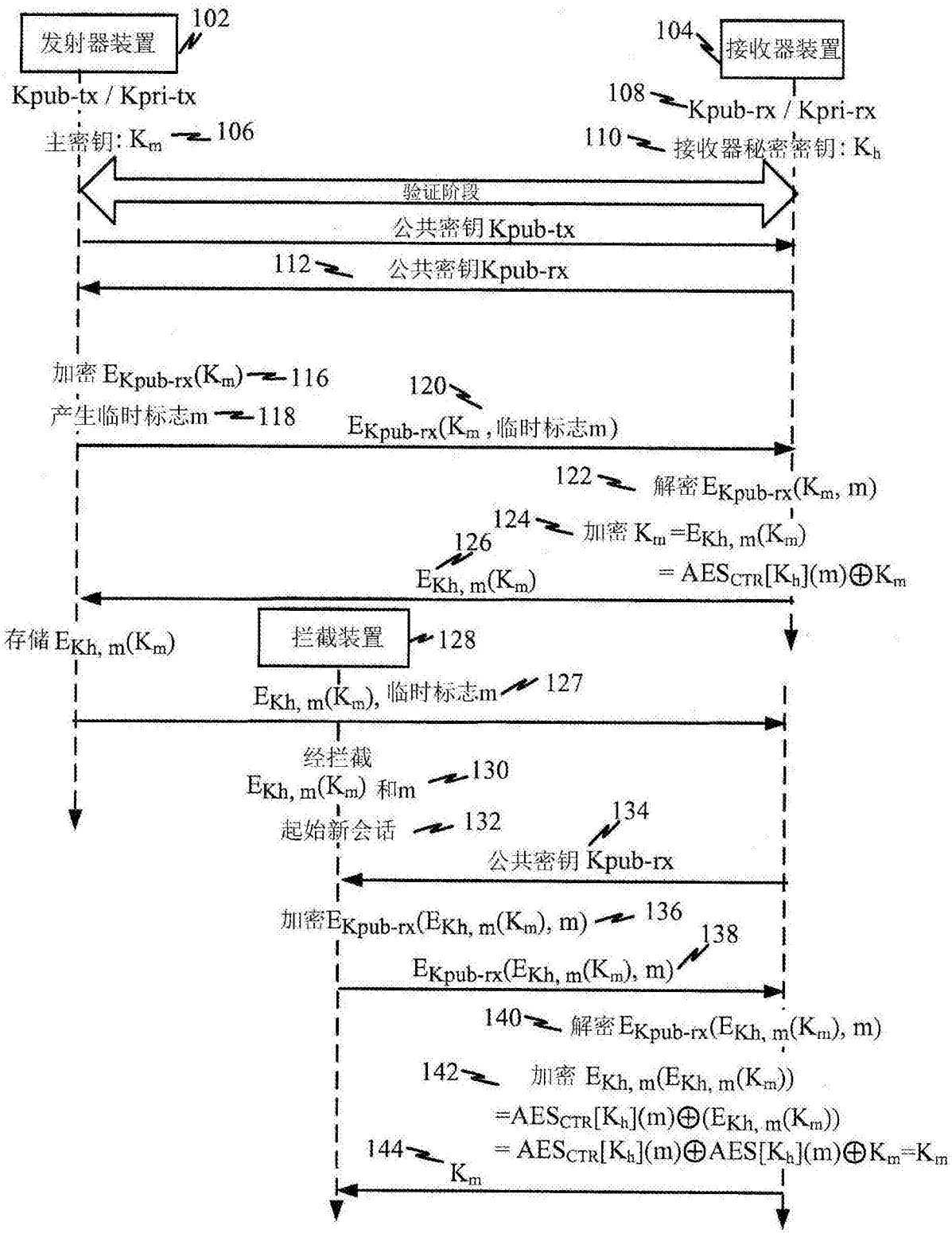

发射器装置
102
Kpub-tx / Kpri-tx
主密钥: K_m
106
104
接收器装置
108
Kpub-rx / Kpri-rx
110
接收器秘密密钥: K_h
验证阶段
公共密钥 Kpub-tx
112
公共密钥Kpub-rx
加密 $E_{Kpub-rx}(K_m)$
116
产生临时标志m
118
120
$E_{Kpub-rx}(K_m$, 临时标志m)
122
解密 $E_{Kpub-rx}(K_m, m)$
124
加密 $K_m = E_{Kh, m}(K_m)$
126
$E_{Kh, m}(K_m)$
$= AES_{CTR}[K_h](m) \oplus K_m$
存储 $E_{Kh, m}(K_m)$
拦截装置
128
$E_{Kh, m}(K_m)$, 临时标志m
127
经拦截
$E_{Kh, m}(K_m)$ 和m
130
起始新会话
132
134
公共密钥 Kpub-rx
加密$E_{Kpub-rx}(E_{Kh, m}(K_m), m)$
136
138
$E_{Kpub-rx}(E_{Kh, m}(K_m), m)$
140
解密 $E_{Kpub-rx}(E_{Kh, m}(K_m), m)$
142
加密 $E_{Kh, m}(E_{Kh, m}(K_m))$
$= AES_{CTR}[K_h](m) \oplus (E_{Kh, m}(K_m))$
$= AES_{CTR}[K_h](m) \oplus AES[K_h](m) \oplus K_m = K_m$
144
K_m

图 1（现有技术）

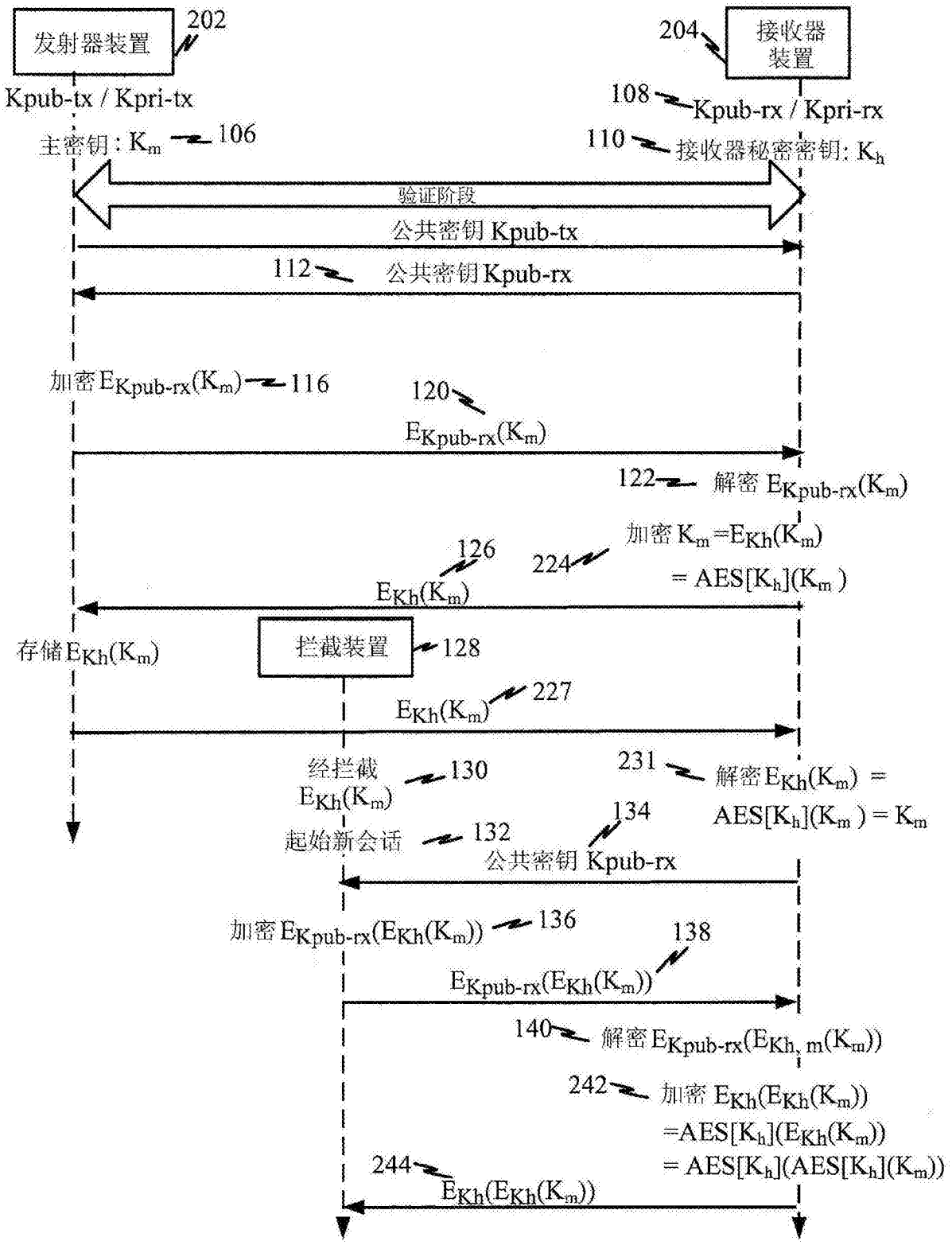

发射器装置
202
接收器装置
204
Kpub-tx / Kpri-tx
108
Kpub-rx / Kpri-rx
主密钥 : Km
106
110
接收器秘密密钥: Kh
验证阶段
公共密钥 Kpub-tx
112
公共密钥Kpub-rx
加密EKpub-rx(Km)
116
120
EKpub-rx(Km)
122
解密 EKpub-rx(Km)
加密 Km =EKh(Km)
= AES[Kh](Km)
126
224
EKh(Km)
存储EKh(Km)
拦截装置
128
EKh(Km)
227
经拦截
EKh(Km)
130
231
解密EKh(Km) =
AES[Kh](Km) = Km
起始新会话
132
134
公共密钥 Kpub-rx
加密EKpub-rx(EKh(Km))
136
138
EKpub-rx(EKh(Km))
140
解密EKpub-rx(EKh, m(Km))
242
加密 EKh(EKh(Km))
=AES[Kh](EKh(Km))
= AES[Kh](AES[Kh](Km))
244
EKh(EKh(Km))

图 2

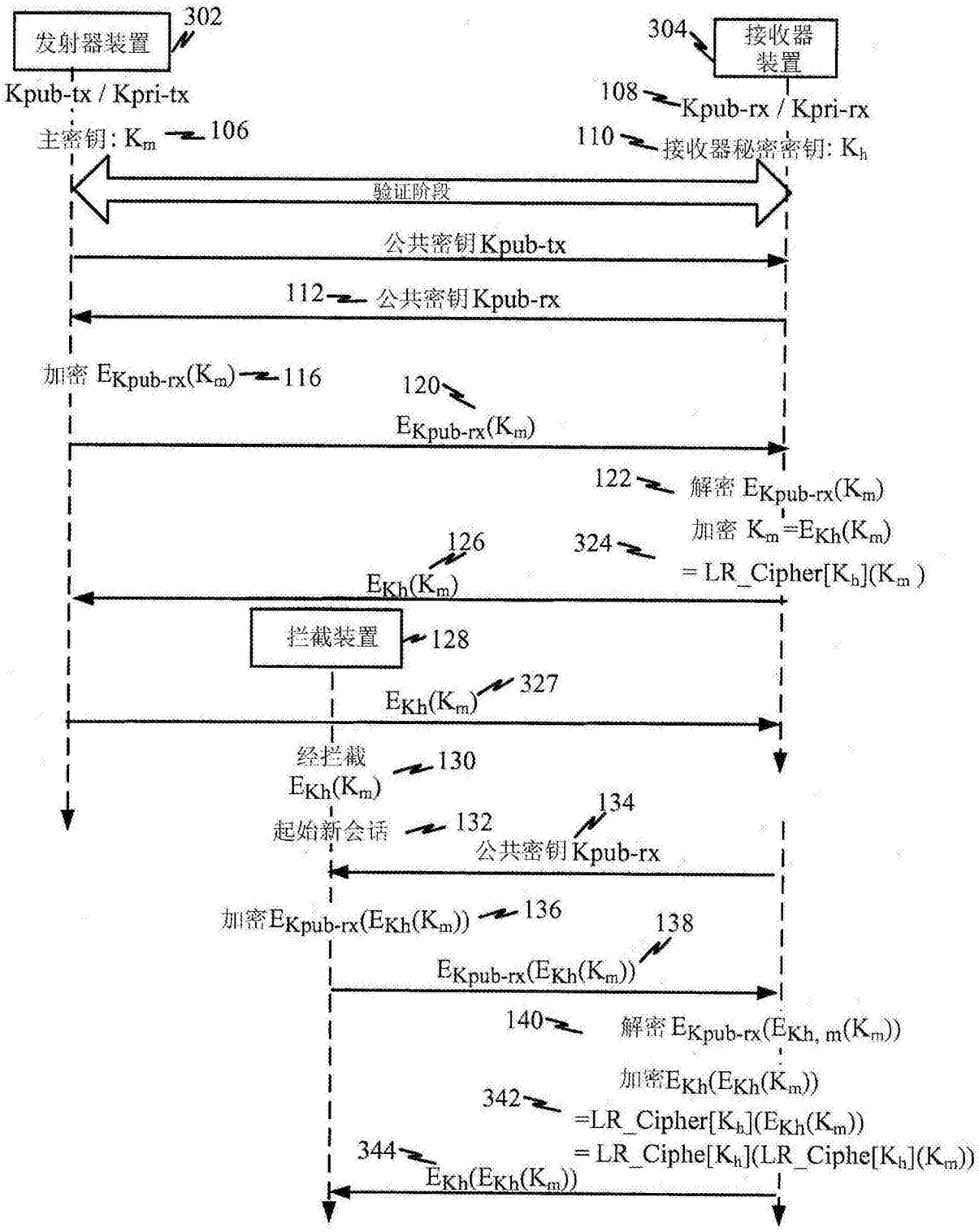

发射器装置
302
Kpub-tx / Kpri-tx
主密钥: K_m
106
接收器装置
304
108
Kpub-rx / Kpri-rx
110
接收器秘密密钥: K_h
验证阶段
公共密钥Kpub-tx
112
公共密钥Kpub-rx
加密 $E_{Kpub-rx}(K_m)$
116
120
$E_{Kpub-rx}(K_m)$
122
解密 $E_{Kpub-rx}(K_m)$
加密 $K_m=E_{Kh}(K_m)$
324
$= LR_Cipher[K_h](K_m)$
126
$E_{Kh}(K_m)$
拦截装置
128
$E_{Kh}(K_m)$
327
经拦截
$E_{Kh}(K_m)$
130
起始新会话
132
134
公共密钥Kpub-rx
加密$E_{Kpub-rx}(E_{Kh}(K_m))$
136
138
$E_{Kpub-rx}(E_{Kh}(K_m))$
140
解密 $E_{Kpub-rx}(E_{Kh,\,m}(K_m))$
加密$E_{Kh}(E_{Kh}(K_m))$
342
$=LR_Cipher[K_h](E_{Kh}(K_m))$
$= LR_Ciphe[K_h](LR_Ciphe[K_h](K_m))$
344
$E_{Kh}(E_{Kh}(K_m))$

图 3

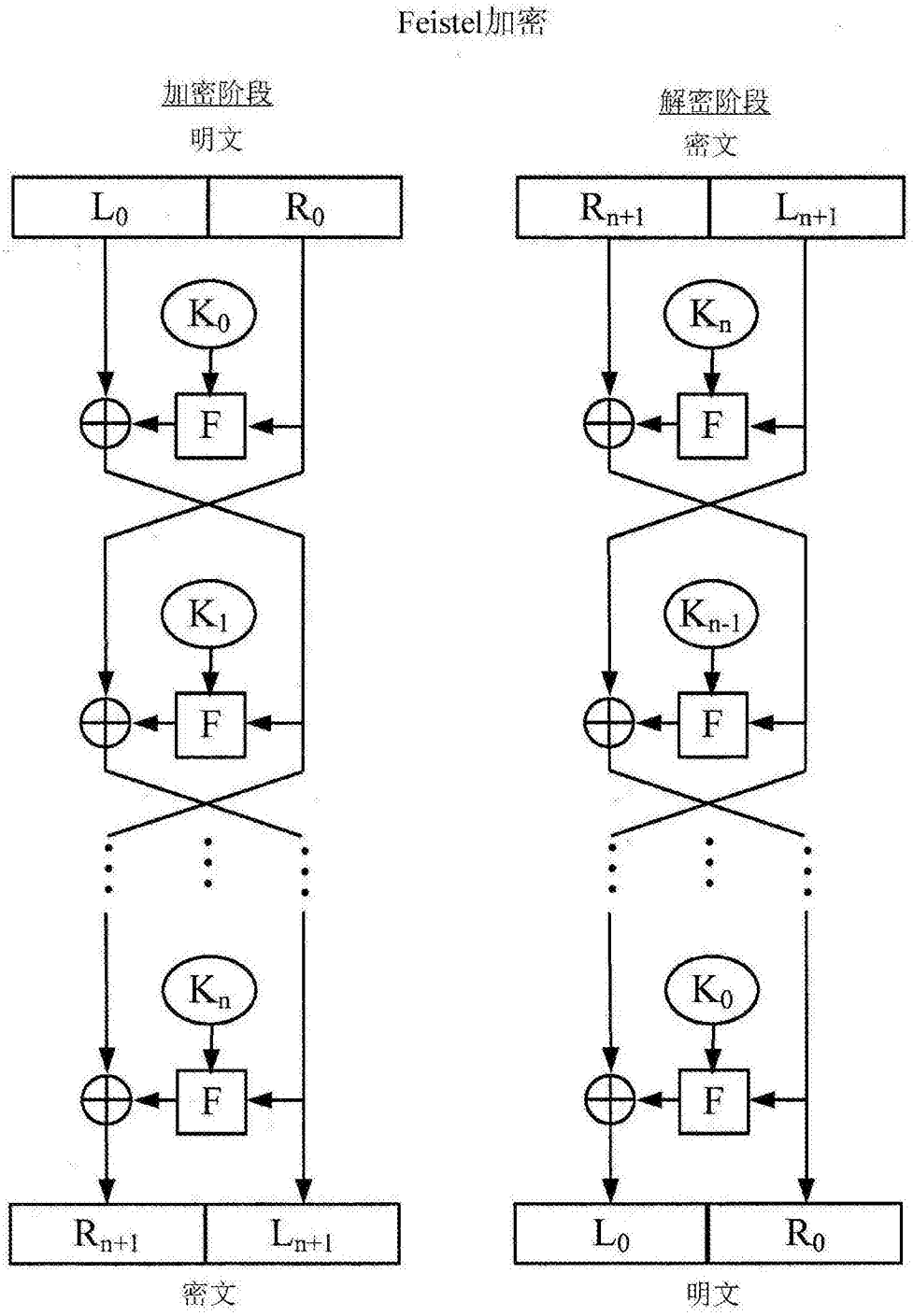

Feistel加密
加密阶段
明文
L_0
R_0
K_0
F
K_1
F
K_n
F
R_{n+1}
L_{n+1}
密文
解密阶段
密文
R_{n+1}
L_{n+1}
K_n
F
K_{n-1}
F
K_0
F
L_0
R_0
明文

图 4

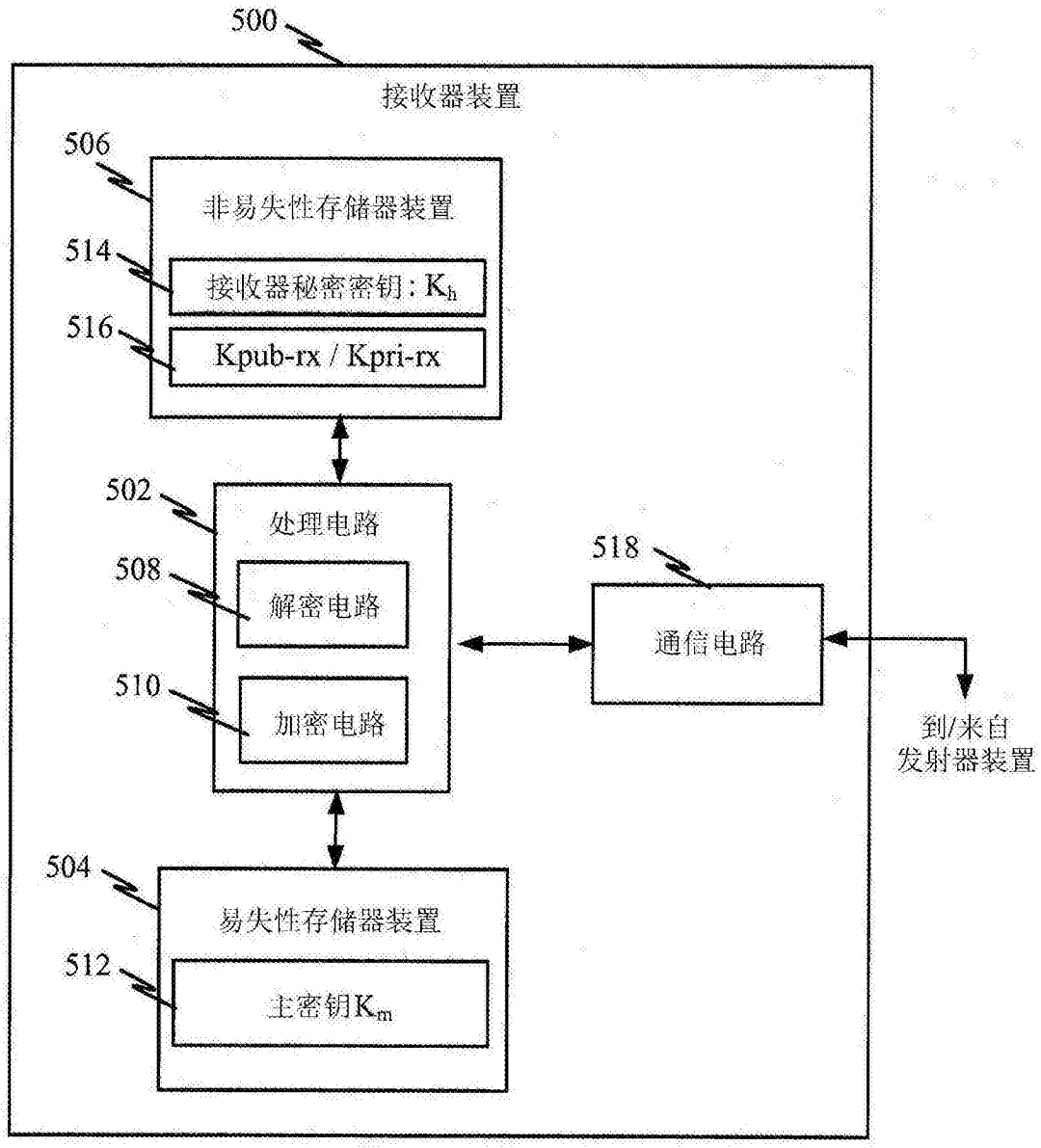

500
接收器装置
506
非易失性存储器装置
514
接收器秘密密钥：K_h
516
Kpub-rx / Kpri-rx
502
处理电路
508
解密电路
510
加密电路
518
通信电路
到/来自
发射器装置
504
易失性存储器装置
512
主密钥K_m

图 5

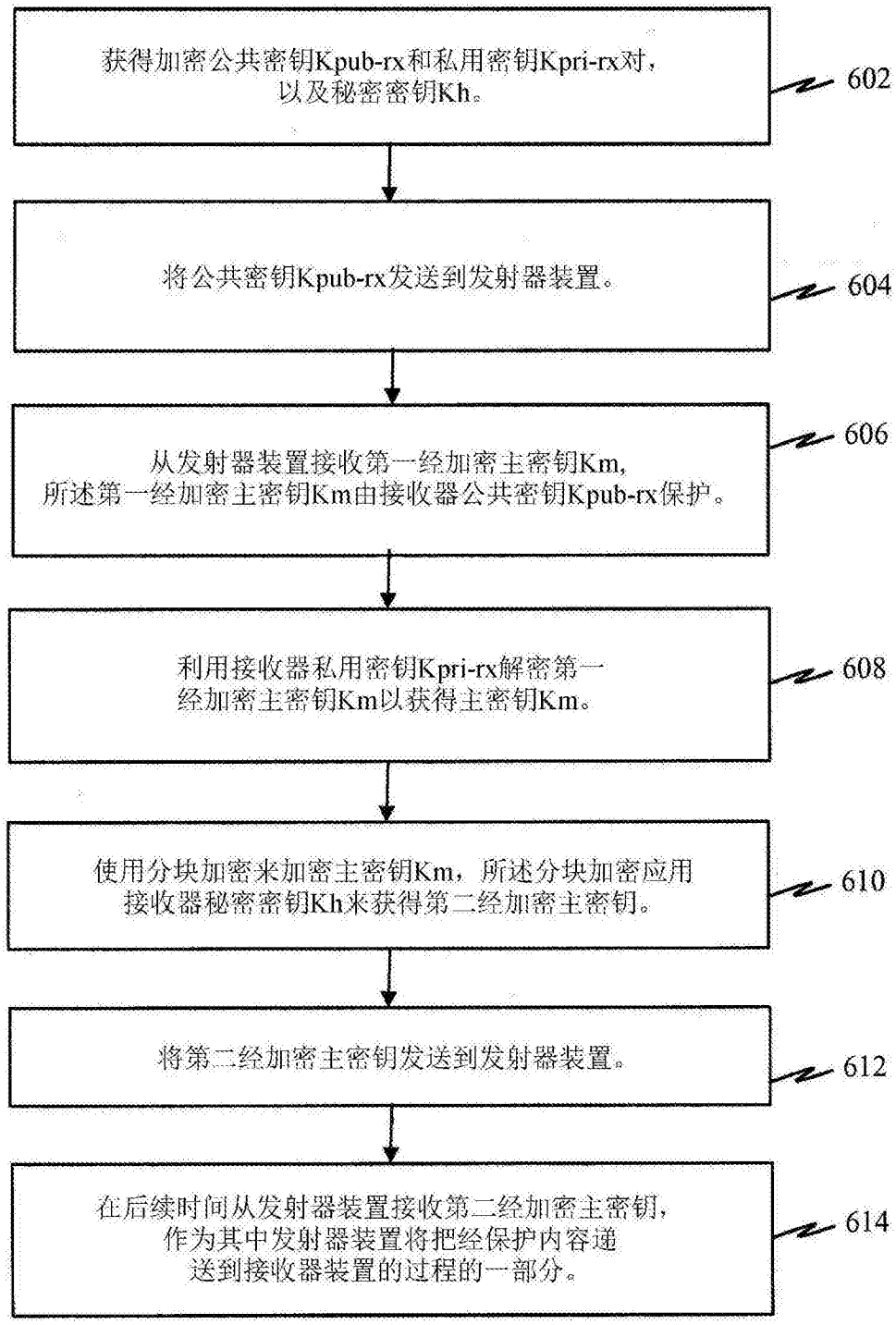

获得加密公共密钥Kpub-rx和私用密钥Kpri-rx对，以及秘密密钥Kh。
602
将公共密钥Kpub-rx发送到发射器装置。
604
从发射器装置接收第一经加密主密钥Km，所述第一经加密主密钥Km由接收器公共密钥Kpub-rx保护。
606
利用接收器私用密钥Kpri-rx解密第一经加密主密钥Km以获得主密钥Km。
608
使用分块加密来加密主密钥Km，所述分块加密应用接收器秘密密钥Kh来获得第二经加密主密钥。
610
将第二经加密主密钥发送到发射器装置。
612
在后续时间从发射器装置接收第二经加密主密钥，作为其中发射器装置将把经保护内容递送到接收器装置的过程的一部分。
614

图 6

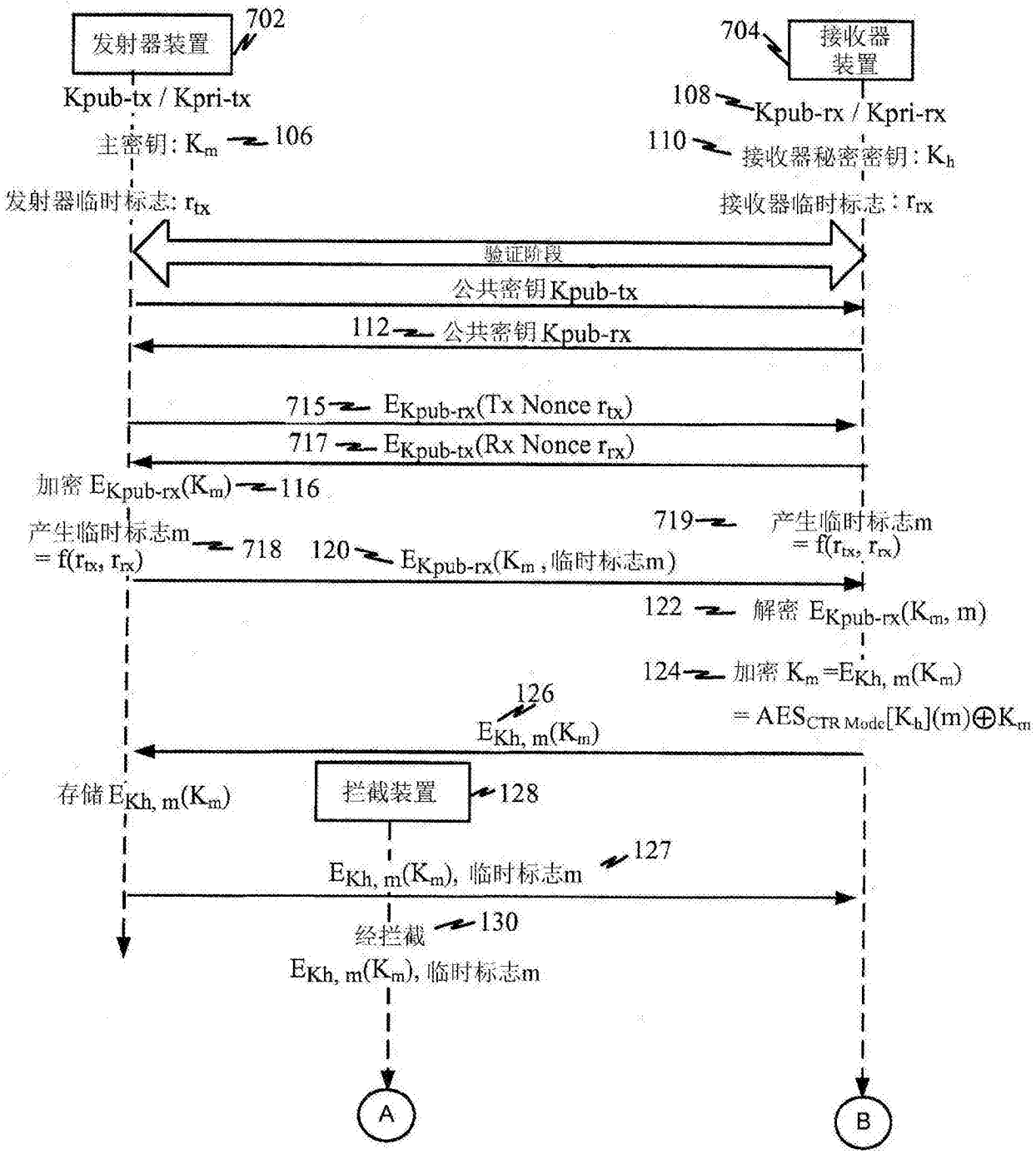

发射器装置
702
Kpub-tx / Kpri-tx
主密钥: K_m
106
发射器临时标志: r_{tx}
704
接收器装置
108
Kpub-rx / Kpri-rx
110
接收器秘密密钥: K_h
接收器临时标志: r_{rx}
验证阶段
公共密钥 Kpub-tx
112
公共密钥 Kpub-rx
715
$E_{Kpub-rx}$(Tx Nonce r_{tx})
717
$E_{Kpub-tx}$(Rx Nonce r_{rx})
加密 $E_{Kpub-rx}(K_m)$
116
产生临时标志m = $f(r_{tx}, r_{rx})$
718
120
$E_{Kpub-rx}(K_m$, 临时标志m)
719
产生临时标志m = $f(r_{tx}, r_{rx})$
122
解密 $E_{Kpub-rx}(K_m, m)$
124
加密 $K_m = E_{Kh, m}(K_m)$
$= AES_{CTR\ Mode}[K_h](m) \oplus K_m$
126
$E_{Kh, m}(K_m)$
存储 $E_{Kh, m}(K_m)$
拦截装置
128
$E_{Kh, m}(K_m)$, 临时标志m
127
经拦截
130
$E_{Kh, m}(K_m)$, 临时标志m
A
B

图 7A

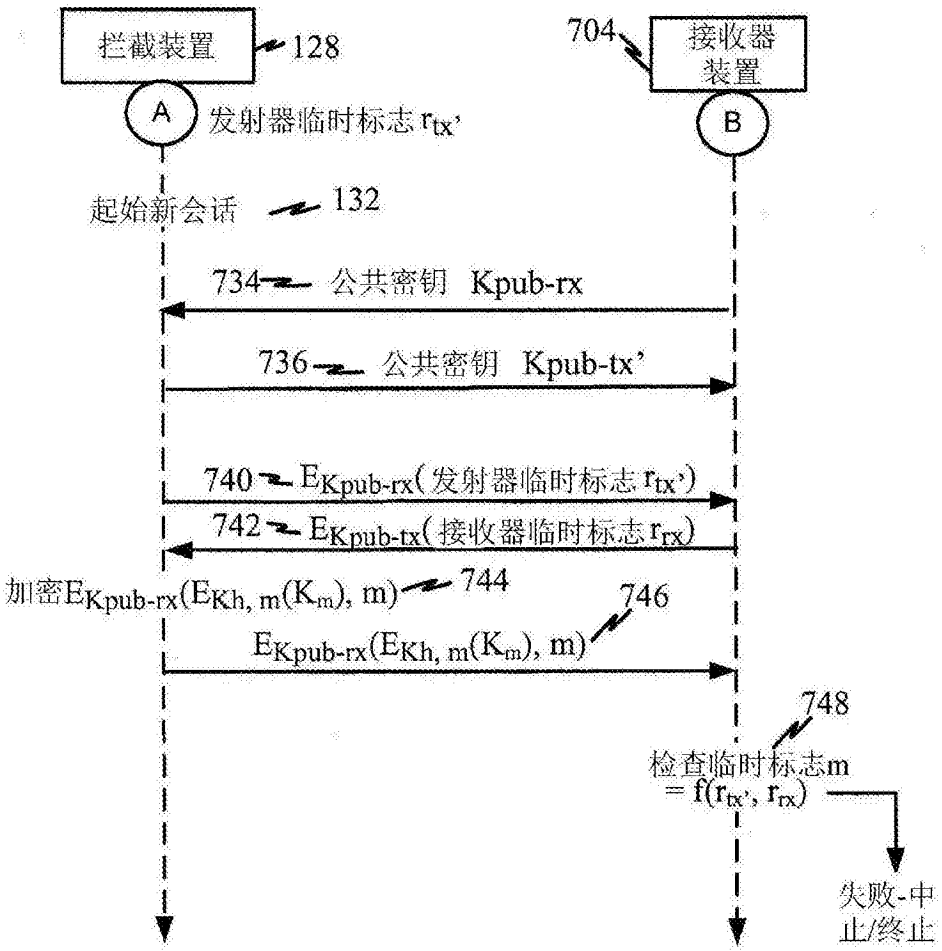

拦截装置
128
704
接收器装置
A
发射器临时标志 r_{tx}'
B
起始新会话
132
734
公共密钥 Kpub-rx
736
公共密钥 Kpub-tx'
740
$E_{Kpub-rx}$(发射器临时标志 r_{tx}')
742
$E_{Kpub-tx}$(接收器临时标志 r_{rx})
加密$E_{Kpub-rx}(E_{Kh,\ m}(K_m),\ m)$
744
746
$E_{Kpub-rx}(E_{Kh,\ m}(K_m),\ m)$
748
检查临时标志m
$= f(r_{tx'},\ r_{rx})$
失败-中止/终止

图 7B

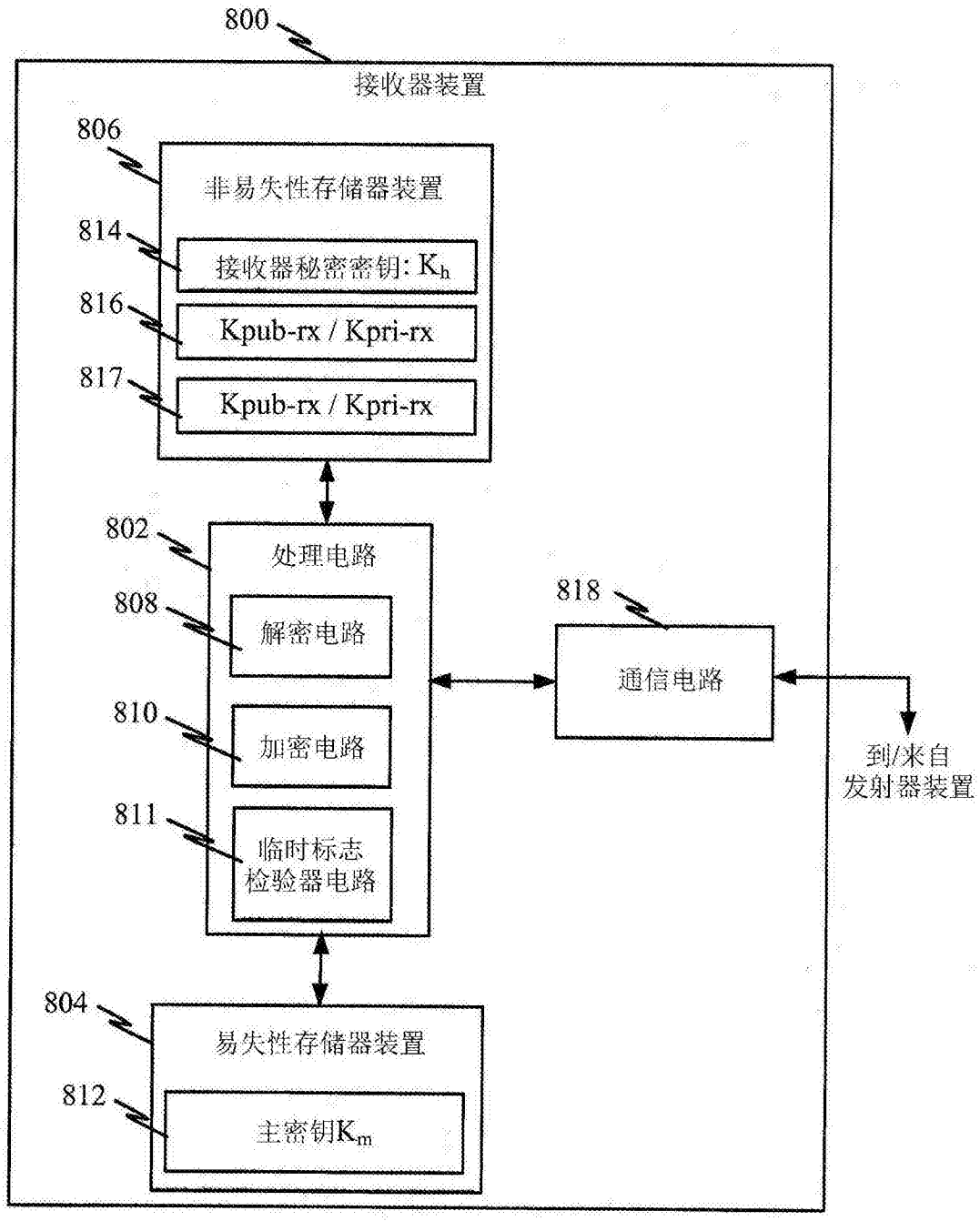

800
接收器装置
806
非易失性存储器装置
814
接收器秘密密钥: K_h
816
Kpub-rx / Kpri-rx
817
Kpub-rx / Kpri-rx
802
处理电路
808
解密电路
810
加密电路
811
临时标志检验器电路
818
通信电路
到/来自发射器装置
804
易失性存储器装置
812
主密钥K_m

图 8

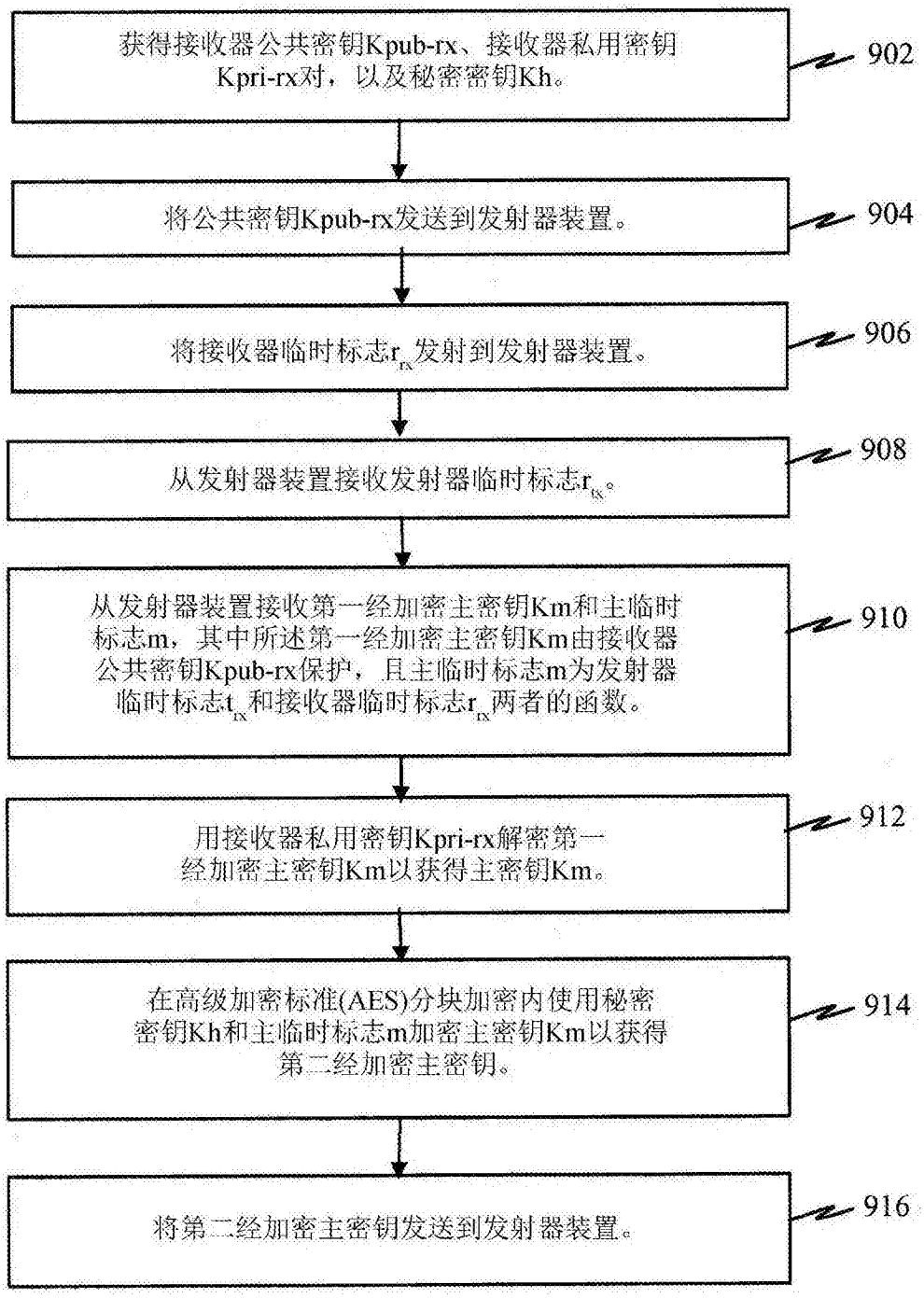

获得接收器公共密钥Kpub-rx、接收器私用密钥Kpri-rx对，以及秘密密钥Kh。
902
将公共密钥Kpub-rx发送到发射器装置。
904
将接收器临时标志r_{rx}发射到发射器装置。
906
从发射器装置接收发射器临时标志r_{tx}。
908
从发射器装置接收第一经加密主密钥Km和主临时标志m，其中所述第一经加密主密钥Km由接收器公共密钥Kpub-rx保护，且主临时标志m为发射器临时标志t_{tx}和接收器临时标志r_{rx}两者的函数。
910
用接收器私用密钥Kpri-rx解密第一经加密主密钥Km以获得主密钥Km。
912
在高级加密标准(AES)分块加密内使用秘密密钥Kh和主临时标志m加密主密钥Km以获得第二经加密主密钥。
914
将第二经加密主密钥发送到发射器装置。
916

图 9