(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 101883102 A
(43)申请公布日 2010.11.10

(21)申请号 201010209025.4

(22)申请日 2005.11.08

(30)优先权数据
10-2004-0097998 2004.11.26 KR
60/627,967 2004.11.16 US

(62)分案原申请数据
200580039132.4 2005.11.08

(71)申请人 三星电子株式会社
地址 韩国京畿道

(72)发明人 韩声休 金明宣 刘容国 尹映善
金奉禅 李栽兴

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 钱大勇

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/08(2006.01)
H04L 12/18(2006.01)

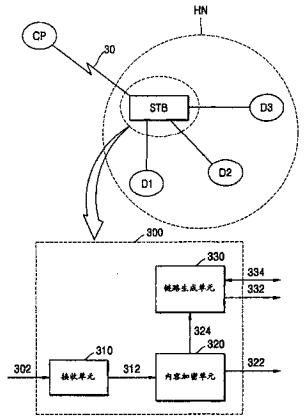
权利要求书 1 页 说明书 7 页 附图 7 页

(54)发明名称

生成链路的方法

(57)摘要

提供了一种生成链路的方法，包括：由用户装置向接收设备发送链路请求消息；发送所述用户装置的公共密钥；由所述接收设备接收使用所述公共密钥加密的秘密密钥；接收使用所述秘密密钥加密的内容密钥。



CN 101883102 A

1. 一种生成链路的方法，包括：

由用户装置向接收设备发送链路请求消息；

发送所述用户装置的公共密钥；

由所述接收设备接收使用所述公共密钥加密的秘密密钥；

接收使用所述秘密密钥加密的内容密钥。

2. 如权利要求 1 所述的方法，其还包括：

使用所述用户装置的秘密密钥解密所述使用所述公共密钥加密的秘密密钥，使用所述解密的秘密密钥解密内容密钥的过程。

3. 一种生成链路的方法，包括：

(a) 由用户装置接收链路请求消息；

(b) 接收所述用户装置的公共密钥；

(c) 发送使用所述公共密钥加密的秘密密钥；

(d) 发送使用所述秘密密钥加密的内容密钥。

4. 如权利要求 3 所述的方法，其中步骤 (c) 的过程包括：

比较当前链路数目和链路的最大数目 (c1)；

如果当前链路数目大于链路的最大数目，则发送使用公共密钥加密的秘密密钥 (c2)。

生成链路的方法

[0001] 本案是申请日为 2005 年 11 月 8 日、申请号为 200580039132.4、发明名称为“用于接收广播内容的方法和设备”的发明专利申请的分案申请。

技术领域

[0002] 本发明的设备和方法涉及接收广播内容，更具体地，涉及即使在离线状态下也安全地将广播内容发送到用户装置，其中在离线状态下用户装置未连接到内容提供商。

背景技术

[0003] 数字内容从内容提供商发送到用户。必须保护数字内容使得只有为该数字内容付费并获得其权利的经授权用户才能使用该数字内容。

[0004] 为了防止未授权使用数字内容，使用内容密钥加密数字内容，并且只将内容密钥给予经授权的用户。

[0005] 家庭网络技术中的新近进步使得用户能够拥有两个或更多用户装置，并且在两个或更多用户装置之间交换内容。因此，用户有可能希望通过对内容仅付费一次而在他们的全部装置中使用内容。但是，当允许在装置之间交换内容时，很可能未经授权的用户能够获得并使用内容。为此原因，需要发展允许在经授权的用户的装置之间交换内容并且不允许未经授权的用户获得或使用内容的家庭网络技术。

[0006] 图 1 是图解了经由因特网 10 而接收内容的传统方法的图。参考图 1，内容提供商 CP 经由英特网 10 将内容发送到用户装置 D1、D2 和 D3。因为经由英特网 10 将用户装置 D1 到 D3 连接到内容提供商 CP，可在内容提供商 CP 和每个用户装置 D1 到 D3 之间进行双向通信。

[0007] 从而，内容提供商 CP 可通过确定用户装置 D1 到 D3 是否是经授权装置的用户验证，并通过加密和发送内容和内容密钥，而保护内容防止未经授权的用户。

[0008] 如果用户装置 D1 到 D3 在用户的家庭网络 HN 上，则用户可以使用在用户装置 D1 到 D3 中的内容，而不受未经授权的用户的攻击。

[0009] 图 2 是图解了经由广播信道 20 而接收内容的传统方法的图。参考图 2，内容提供商 CP 经由广播信道 20 将内容发送到用户装置 D1、D2 和 D3。经由被称为机顶盒 (STB) 的数字广播接收器 12 接收内容，并将内容发送到用户装置 D1 到 D3。

[0010] 因为内容提供商 CP 经由广播信号单方地将内容发送到用户装置 D1 到 D3，所以不能在内容提供商 CP 和每个用户装置 D1 到 D3 之间进行双向通信。

[0011] 在这种情况下，内容提供商 CP 不能通过用户验证、并通过加密和发送内容和内容密钥来保护内容防止未经授权的用户，其中用户验证确定用户装置 D1 到 D3 是否是经授权的装置。

[0012] 因此，例如用户验证的内容保护不适用于经由广播信道（即，机顶盒）而接收数字广播内容的情况。具体地，通常机顶盒只具有根据预定的广播协议来接收数字广播内容，并在用户的家庭网络 HN 上将所接收的数字广播内容发送到用户装置 D1 到 D3 的功能。因此，

当使用机顶盒接收数字广播内容时，不可能防止未经授权的用户获得内容。

[0013] 在 2005 年 7 月，联邦通信委员会 (FCC) 已经规定了用于数字广播技术的标准，即在要通过美国数字广播系统广播的高清晰度 (HD) 内容中必须包括 1 比特广播标记；并且必须启动内容保护，当广播标识为 1 时，防止未经授权的用户使用内容。因此，开发用于即使在离线状态下也安全地获得并使用数字广播内容的设备和方法很紧迫，其中在离线状态下用户装置未经由因特网连接到内容提供商，并且因此，不能在内容提供商和用户装置之间进行双向通信。

发明内容

[0014] 本发明提供了当不能在内容提供商和经授权的用户装置之间进行双向通信时，能够允许只在经授权的用户装置中再现内容的广播内容接收设备和方法。

[0015] 如上所述，根据本发明，可能生成在广播内容接收设备和用户装置之间的安全链路，并且即使当用户装置未连接到内容提供商时，也安全地将广播内容发送到用户装置。

[0016] 另外，可能限制能够链接到该设备以接收广播内容的用户装置的数目，从而控制广播内容的使用。

[0017] 用于接收广播内容的设备能够满足 HD 内容标准，如 FCC 在 2005 年 7 月规定的，该标准中 HD 内容必须包括广播标识。

[0018] 根据本发明，提供一种生成链路的方法，包括：由用户装置向接收设备发送链路请求消息；发送所述用户装置的公共密钥；由所述接收设备接收使用所述公共密钥加密的秘密密钥；接收使用所述秘密密钥加密的内容密钥。

[0019] 根据本发明，提供一种生成链路的方法，包括：(a) 由用户装置接收链路请求消息；(b) 接收所述用户装置的公共密钥；(c) 发送使用所述公共密钥加密的秘密密钥；(d) 发送使用所述秘密密钥加密的内容密钥。

附图说明

[0020] 图 1 是图解了经由因特网而接收内容的传统方法的图。

[0021] 图 2 是图解了经由广播信道而接收内容的传统方法的图。

[0022] 图 3 是根据本发明的示例性实施例、用于接收广播内容的设备的框图；

[0023] 图 4 是根据本发明的示例性实施例的用户装置的框图；

[0024] 图 5 是根据本发明的示例性实施例，使用链路生成单元来生成链路的方法的流程图；

[0025] 图 6 是根据本发明的另一个示例性实施例，使用链路生成单元来生成链路的方法的流程图；

[0026] 图 7 是根据本发明的另一个示例性实施例，使用链路生成单元来生成链路的方法的流程图；以及

[0027] 图 8 是根据本发明的示例性实施例接收广播内容的方法的流程图。

具体实施方式

[0028] 根据本发明的一个方面，提供了用于接收广播内容的设备，该设备包含：接收单

元，其根据经由广播信道从内容提供商接收的广播流而生成广播内容；内容加密单元，其使用内容密钥来加密广播内容；以及链路生成单元，其通过与用户装置交换链路消息而生成到用户装置的安全链路，即使当未将设备连接到内容提供商时，经由链路消息之一，该链路生成单元将内容密钥发送到用户装置。链路消息中的第一链路消息包含用户装置的公共密钥和该设备的公共密钥中的一个，而链路消息中的第二链路消息包含该设备的私有密钥、该设备的秘密密钥和用户装置的秘密密钥中的一个。

[0029] 链路生成单元计数从用户装置发送的链路请求消息的数目、比较当前链路的数目与最大可用链路数目，并控制当前链路的数目。

[0030] 链路生成单元可通过使用用户装置的公共密钥加密设备的私有密钥、经由第二链路消息将加密的私有密钥发送到用户装置、使用设备的公共密钥加密内容密钥、并将加密的内容密钥发送到用户装置，而将内容密钥发送到用户装置。

[0031] 链路生成单元可通过使用用户装置的公共密钥加密设备的秘密密钥、经由第二链路消息将加密的秘密密钥发送到用户装置、使用设备的秘密密钥加密内容密钥、并将加密的内容密钥发送到用户装置，而将内容密钥发送到用户装置。

[0032] 链路生成单元可通过经由第二链路消息接收使用设备的公共密钥加密的用户装置的秘密密钥、使用用户装置的秘密密钥加密内容密钥、并将加密的内容密钥发送到用户装置，而将内容密钥发送到用户装置。

[0033] 根据本发明的另一方面，提供了用于接收广播内容的方法，该方法包含：根据经由广播信道从内容提供商接收的广播流而生成内容；使用内容密钥来加密内容；以及通过在用户装置和广播内容接收设备之间交换链路消息而生成用户装置和广播内容接收设备之间的安全链路，并当未将广播内容接收设备连接到内容提供商时，通过安全链路、经由链路消息之一，将内容密钥发送到用户装置。链路消息中的第一链路消息包含用户装置的公共密钥和广播内容接收设备的公共密钥中的一个，而链路消息中的第二链路消息包含广播内容接收设备的私有密钥、广播内容接收设备的秘密密钥、和用户装置的秘密密钥中的一个。

[0034] 根据本发明的另一方面，提供了用于存储执行接收广播内容的方法的程序的计算机可读记录介质。

[0035] 图 3 是根据本发明的示例性实施例、用于接收广播内容的设备 300 的框图。相应于数字广播接收器 STB 的设备 300 包括接收单元 310、内容加密单元 320 和链路生成单元 330。

[0036] 接收单元 310 经由广播信道 30 而接收广播流 302，并且通过从广播流 302 提取相应于用户的希望内容的分组、并组合所提取的分组而生成内容 312。

[0037] 内容加密单元 320 通过使用预定的内容密钥 324 加密内容 312 而获得加密的内容 322。可由内容加密单元 320 生成内容密钥 324，或者外部生成内容密钥 324 并提供到内容加密单元 320。在任何情况下，内容密钥 324 必须仅由经授权的用户获得。当使用内容加密单元 320 时，内容密钥 324 可通过生成随机数而获得。通过链路生成单元 330，安全地将内容密钥 324 发送到用户装置 D1、D2 或 D3。

[0038] 链路生成单元 330 通过与用户装置 D1、D2 或 D3 交换链路消息 334 而生成到用户装置 D1、D2 或 D3 的安全链路，并且使用该安全链路将加密的内容密钥 332 发送到用户装置 D1、D2 或 D3。

[0039] 安全链路是沿着其在数字广播接收器 STB 和每个用户装置 D1 到 D3 之间交换内容密钥 324 的路径。除了数字广播接收器 STB 和每个用户装置 D1 到 D3 以外的装置不允许通过安全链路获得内容密钥 324。后面将参考图 5 到图 7 具体描述在链路生成单元 330 和每个用户装置 D1 到 D3 之间的链路消息 334 的交换。

[0040] 可替换地，链路生成单元 330 可计数当前链路的数目，并根据当前链路的数目来限制要连接到数字播接收器 STB 的用户装置的数目。

[0041] 图 4 是根据本发明的示例性实施例的用户装置 400 的框图。相应于用户装置 D1、D2 或 D3 的用户装置 400 接收来自数字广播接收器 STB 的广播内容，并再现该广播内容。用户装置 400 包括内容解密单元 410、密钥生成单元 420 和再现单元 430。

[0042] 内容解密单元 410 从数字广播接收器 STB，例如图 3 的设备 300 的内容加密单元 320 接收加密内容，并通过使用内容密钥 426 解密所述加密内容 402 而获得解密内容 412。通过密钥生成单元 420 生成内容密钥 426。

[0043] 密钥生成单元 420 通过与数字广播接收器 STB 交换链路消息 404 而从数字广播接收器 STB，例如设备 300 的链路生成单元 330 接收加密的内容密钥 332。后面将参考图 5 到图 7 详细描述在用户装置 400 和链路生成单元 330 之间的链路消息 404 的交换。

[0044] 根据本发明，现在将参考图 5 到图 7 描述通过在链路生成单元和数字广播接收器之间交换链路消息而生成链路、并经由该链路将内容密钥发送到用户装置的方法。

[0045] 图 5 是根据本发明的示例性实施例使用图 3 的链路生成单元 330 来生成链路的方法的流程图。参考图 5，链路生成单元 330 接收请求图 4 的用户装置 400 到图 3 的设备 300 的链路的链路消息 Request（请求），以及来自密钥生成单元 420 的图 4 的用户装置 400 的公共密钥 Kpub_dev（操作 510）。

[0046] 然后，链路生成单元 330 确定可用链路的最大数目 n_C 是否大于当前链路数目 n（操作 515）。如果可用链路的最大数目 n_C 大于当前链路数目 n，则方法前进到操作 520。如果不是，则将拒绝用户装置 400 到设备 300 的链路的链路消息发送到用户装置 400，以拒绝用户装置 400 的链路（操作 580）。

[0047] 在操作 520 中，链路生成单元 330 通过使用在操作 510 中接收的公共密钥 Kpub_dev 来加密设备 300 的私有密钥 Kpri_STB，从而生成加密的私有密钥 E1 = E(Kpub_dev, Kpri_STB)，并将加密的私有密钥 E1 发送到密钥生成单元 420。

[0048] 然后，密钥生成单元 420 通过使用用户装置 400 的私有密钥 Kpri_dev 解密在操作 520 中接收的加密的私有密钥 E1，再现设备 300 的私有密钥 Kpri_STB（操作 530）。

[0049] 然后，链路生成单元 330 通过使用设备 300 的公共密钥 Kpub_STB 来加密内容密钥 K_cont，从而生成加密的内容密钥 E2 = E(Kpub_STB, K_cont)，并将加密的内容密钥 E2 发送到密钥生成单元 420（操作 540）。

[0050] 然后，密钥生成单元 420 通过使用在操作 530 中再现的设备 300 的私有密钥 Kpri_STB 解密经加密的内容密钥 E2，而再现内容密钥 K_cont（操作 550）。

[0051] 然后，密钥生成单元 420 将成功地再现了内容密钥 K_cont 的链路消息 Success（成功）发送到链路生成单元 330（操作 560）。

[0052] 之后，链路生成单元 330 将当前链路的数目 n 增加 1（操作 570），并且方法前进到操作 510。

[0053] 在图 5 的方法中，根据公共密钥基本结构 (PKI)，将内容密钥安全地从数字广播接收设备 300 发送到用户装置 400。也就是说，使用用户装置 400 和广播内容接收设备 300 的私有密钥和公共密钥，将内容密钥安全地发送到用户装置 400。即使操作 510、520 或 540 中所发送的链路消息被外部装置窃取，全部链路消息是加密的，并且因此，外部装置不能再现内容密钥。因此，广播内容接收设备 300 可以经由安全链路将内容密钥发送到用户装置 400。

[0054] 另外，在图 5 的方法中，广播内容接收设备 300 可以安全地将内容发送到在离线状态下的用户装置 400，其中在离线状态下用户装置 400 未连接到内容提供商 CP，并且因此，如 FCC 所规定的，满足于数字广播技术即 HD 内容必须包括广播标记的标准，并且当广播标识为 1 时必须启动内容保护，以防止未经授权的用户使用内容。

[0055] 在图 5 的方法中，操作 515、560、570 和 580 是可选的，包括操作 515、560、570 和 580 使得限定其中再现内容的用户装置的数目成为可能，从而防止内容被非法传播。

[0056] 图 6 是根据本发明的另一个示例性实施例、使用图 3 的设备 300 的链路生成单元 330 来生成链路的方法的流程图。参考图 6，链路生成单元 330 接收请求用户装置 400 到设备 300 的链路的链路消息 Request（请求），以及来自图 4 的用户装置 400 的密钥生成单元 420 的用户装置 400 的公共密钥 Kpub_dev（操作 610）。

[0057] 然后，链路生成单元 330 确定可用链路的最大数目 n_C 是否大于当前链路数目 n（操作 615）。如果可用链路的最大数目 n_C 大于当前链路数目 n，则方法前进到操作 620。如果不是，则将拒绝用户装置 400 到设备 300 的链路的链路消息发送到用户装置 400，以拒绝用户装置 400 的链路（操作 680）。

[0058] 在操作 620 中，链路生成单元 330 通过使用在操作 610 中接收的用户装置 400 的公共密钥 Kpub_dev 来加密设备 300 的秘密密钥 Ksec_STB，从而生成加密的秘密密钥 E1 = E(Kpub_dev, Ksec_STB)，并将加密的秘密密钥 E1 发送到密钥生成单元 420。

[0059] 然后，密钥生成单元 420 通过使用用户装置 400 的私有密钥 Kpri_dev 解密在操作 620 中接收的加密的秘密密钥 E1，来再现设备 300 的秘密密钥 Ksec_STB（操作 630）。

[0060] 然后，链路生成单元 330 通过使用秘密密钥 Ksec_STB 来加密内容密钥 K_cont，从而生成加密的内容密钥 E2 = E(Ksec_STB, K_cont)，并将加密的内容密钥 E2 发送到密钥生成单元 420（操作 640）。

[0061] 然后，密钥生成单元 420 通过使用在操作 630 中生成的秘密密钥 Ksec_STB 来解密经加密的内容密钥 E2，而再现内容密钥 K_cont（操作 650）。

[0062] 然后，密钥生成单元 420 将成功地再现了内容密钥 K_cont 的链路消息 Success（成功）发送到链路生成单元 330（操作 660）。

[0063] 之后，链路生成单元 330 将当前链路的数目 n 增加 1（操作 670），并且方法前进到操作 610。

[0064] 在图 6 的方法中，使用用户装置 400 的私有密钥和公共密钥、以及广播内容接收设备 300 的秘密密钥，安全地发送内容密钥。图 6 的方法不同于图 5 的方法：根据对称密钥结构而将内容密钥从广播内容接收设备 300 发送到用户装置 400。但是如在图 5 的方法中，在图 6 的方法的操作 610、620 和 640 中所交换的全部链路消息被加密并发送。由此，未经授权的用户不能再现内容密钥，并且因此，经由安全链路，可能安全地将内容密钥从广播内容

接收设备 300 发送到用户装置 400。

[0065] 类似地，操作 615、660、670 和 680 是可选的。

[0066] 图 7 是根据本发明的另一个示例性实施例生成链路的方法的流程图。参考图 7，图 3 的设备 300 的链路生成单元 330 从密钥生成单元 420 接收请求图 4 的用户装置 400 到设备 300 的链路的链路消息 Request（请求）（操作 710）。

[0067] 然后，链路生成单元 330 确定可用链路的最大数目 n_C 是否大于当前链路数目 n（操作 715）。如果可用链路的最大数目 n_C 大于当前链路数目 n，则方法前进到操作 720。如果不是，则将请求用户装置 400 到设备 300 的链路的消息发送到用户装置 400，以拒绝用户装置 400 的链路（操作 780）。

[0068] 在操作 720 中，链路生成单元 330 将设备 300 的公共密钥 Kpub_STB 发送到用户装置 400 的密钥生成单元 420。

[0069] 然后，密钥生成单元 420 通过使用在操作 720 中接收的设备 300 的公共密钥 Kpub_STB 来加密用户装置 400 的秘密密钥 Ksec_dev，来生成加密的秘密密钥 E1 ＝ E(Kpub_STB, Ksec_dev)，并将加密的秘密密钥 E1 发送到链路生成单元 330（操作 725）。

[0070] 然后，链路生成单元 330 通过使用设备 300 的私有密钥 Kpri_STB 来解密在操作 725 中接收的用户装置 400 的经加密的秘密密钥 E1，而再现用户装置 400 的秘密密钥 Ksec_dev。（操作 730）。

[0071] 然后，链路生成单元 330 通过使用在操作 730 中生成的用户装置 400 的秘密密钥 Ksec_dev 来加密内容密钥 K_cont，从而生成加密的内容密钥 E2 ＝ E(Ksec_dev, K_cont)，并将加密的内容密钥 E2 发送到密钥生成单元 420（操作 740）。

[0072] 然后，密钥生成单元 420 通过使用用户装置 400 的秘密密钥 Ksec_dev 解密在操作 740 中接收的加密的内容密钥 E2，而再现内容密钥 K_cont（操作 750）。

[0073] 然后，密钥生成单元 420 将成功地再现了内容密钥 K_cont 的消息 Success（成功）发送到链路生成单元 330（操作 760）。

[0074] 然后，链路生成单元 330 将当前链路的数目 n 增加（操作 570），并且方法前进到操作 710。

[0075] 在图 7 的方法中，使用用户装置 400 的秘密密钥加密内容密钥。秘密密钥是分配到用户装置 400 的唯一密钥，并未向外部装置公开。如在图 5 和图 6 的方法中，即使当在操作 710、720、725 和 740 中所发送的链路消息被外部装置窃取时，全部链路消息是加密的，并且因此，不允许外部装置再现内容密钥。因此，经由安全链路，广播内容接收设备 300 能够将内容密钥安全地发送到用户装置 400。

[0076] 与图 5 和图 6 的方法类似，操作 715、760、770 和 780 是可选的。

[0077] 图 8 是根据本发明的示例性实施例接收广播内容的方法的流程图。参考图 8，用于接收广播内容的设备经由广播信道接收广播流，并且根据广播流而再现广播内容（操作 810）。

[0078] 然后，该设备使用预定的内容密钥加密在操作 810 中再现的广播内容，并将其发送到用户装置 400（操作 820）。

[0079] 然后，该设备通过与用户装置交换链路消息而生成安全链路（操作 830）。已经参考图 5 到图 7 描述了生成安全链路的方法。

[0080] 然后，该设备将预定的内容密钥经由在操作 830 中生成的安全链路发送到用户装置（操作 840）。

[0081] 根据本发明接收广播内容的方法可作为计算机程序来实现。本发明所属领域的计算机编程员可容易地导出计算机程序的代码和代码段。可将计算机程序存储在计算机可读介质上，并使用计算机来执行。计算机可读介质的例子包括磁记录介质、光记录介质，或甚至载波（例如在因特网上的传输）。

[0082] 虽然本发明已经参考其示例性实施例被具体示出并描述，但是本领域的技术人员将理解，其中可做出各种形式和细节的改变，而不背离如由所附权利要求所定义的本发明的精神和范围。

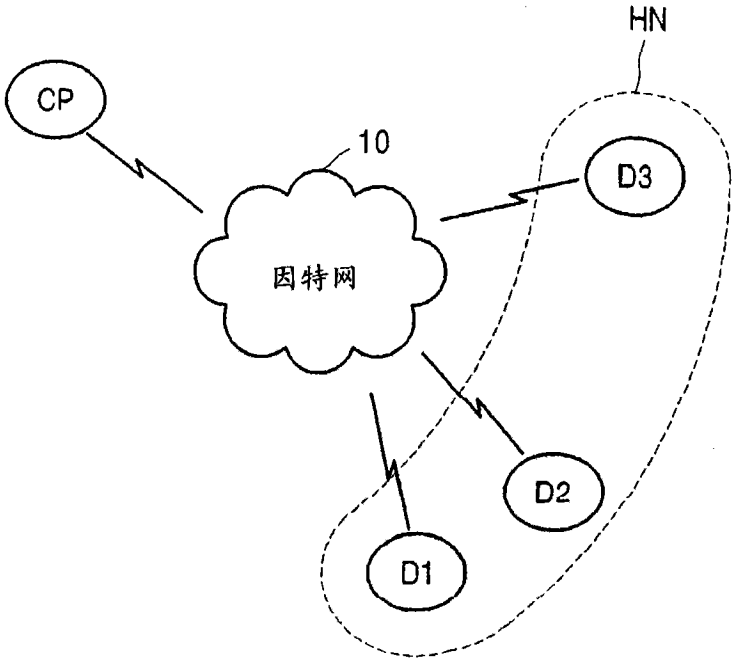


图 1

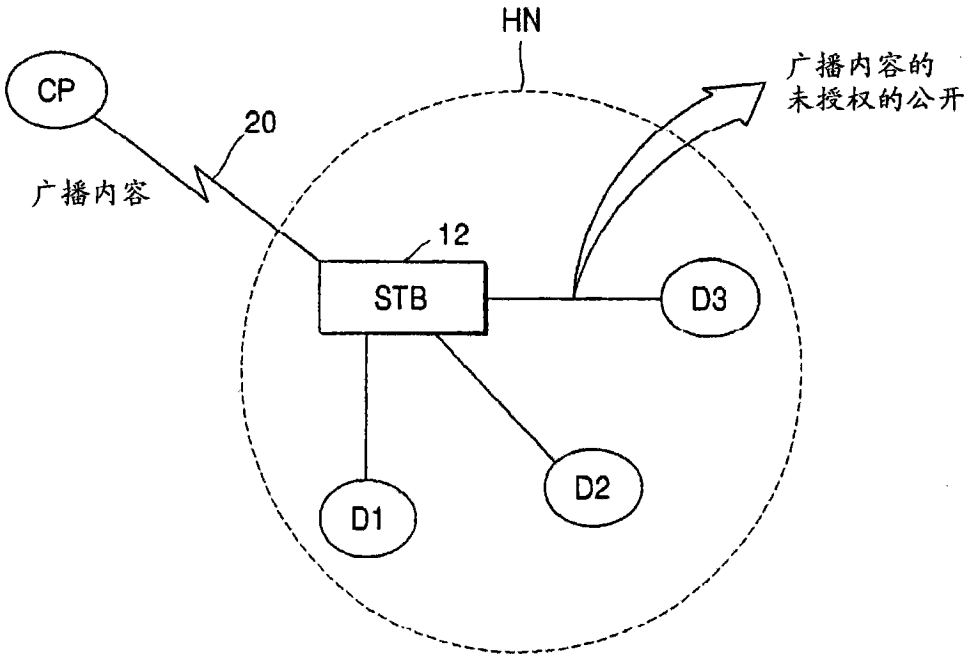


图 2

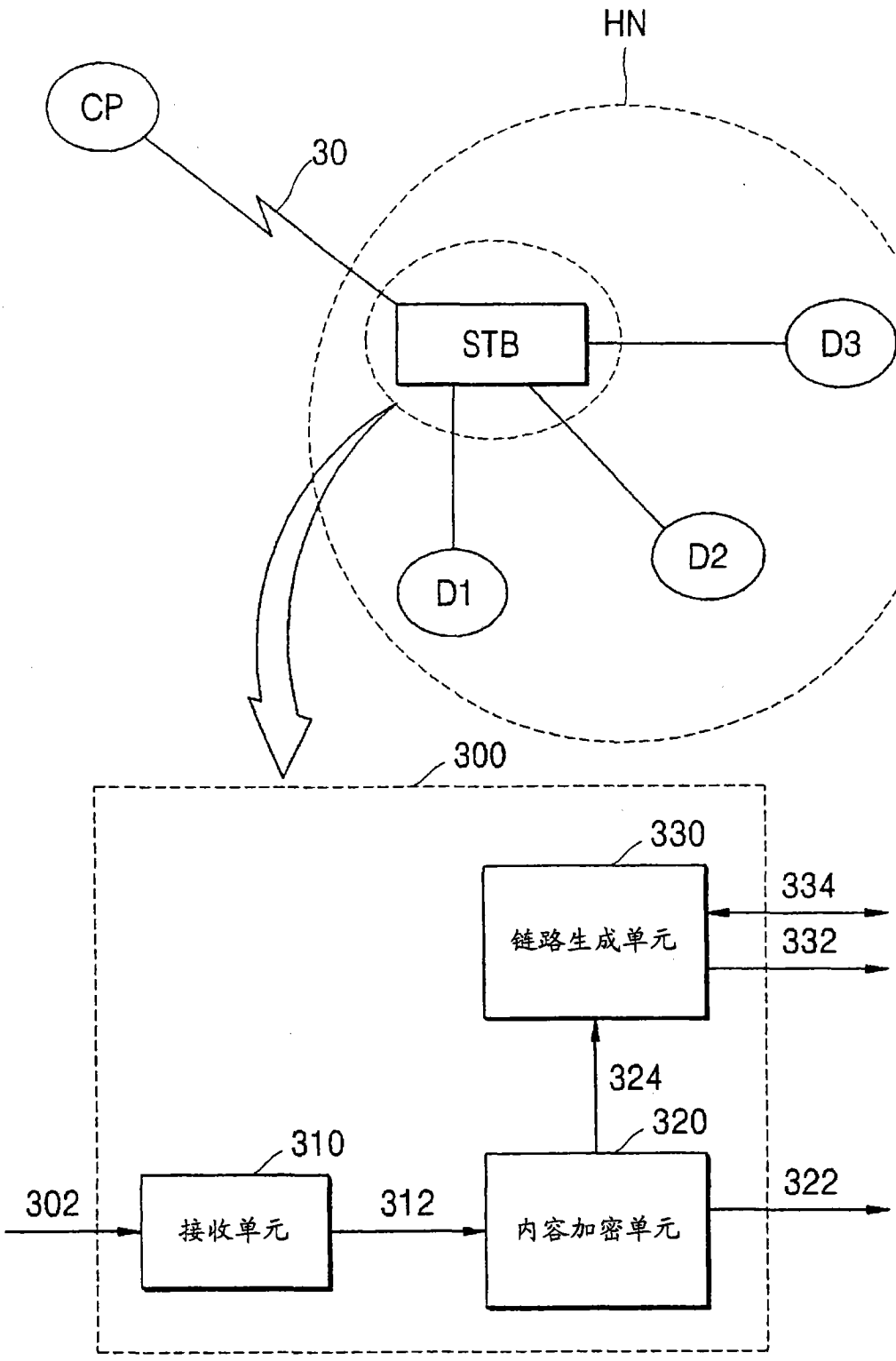

HN
CP
30
STB
D3
D1
D2
300
330
链路生成单元
334
332
324
320
310
302
接收单元
312
内容加密单元
322

图 3

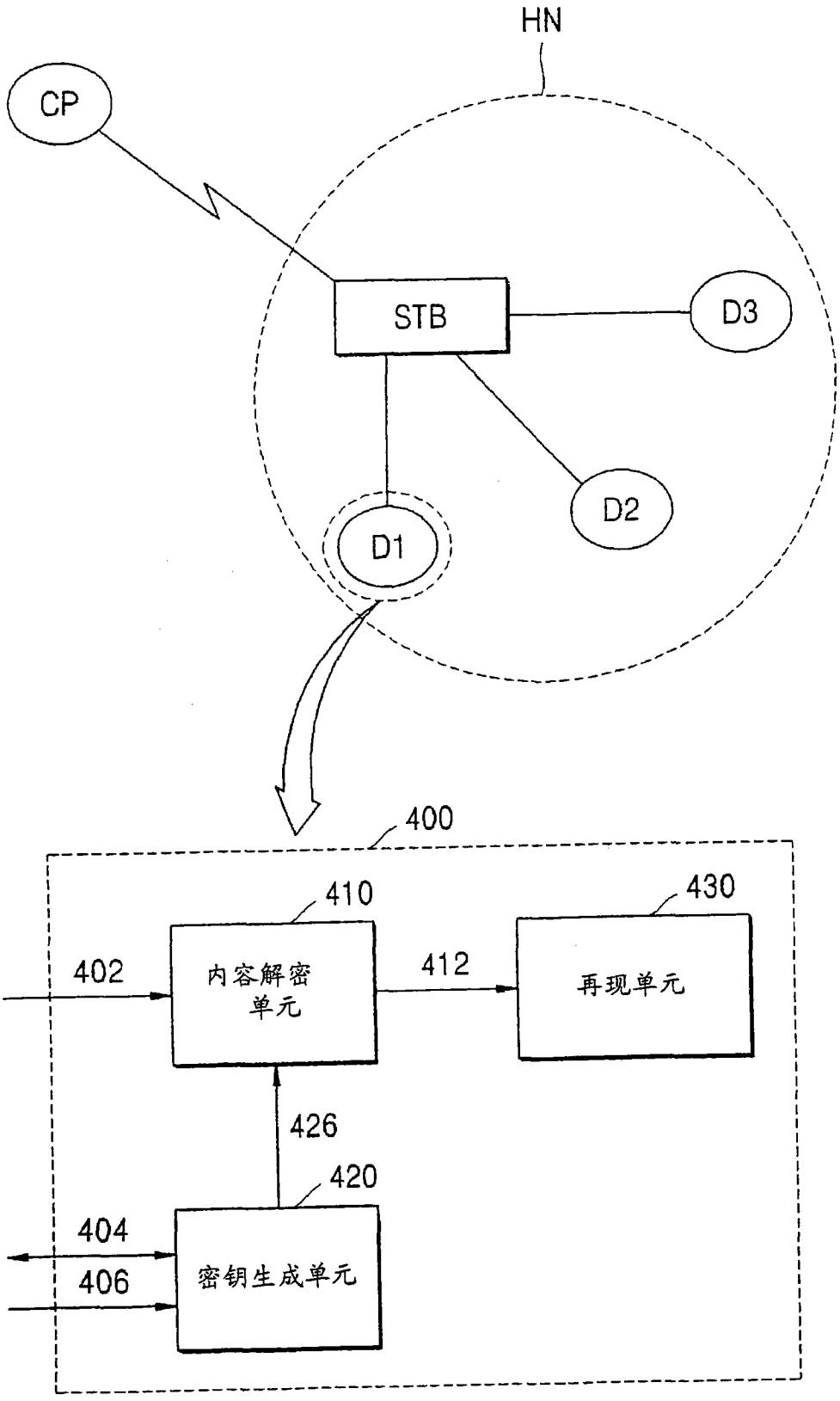

HN
CP
STB
D3
D2
D1
400
410
430
402
内容解密
单元
412
再现单元
426
420
404
406
密钥生成单元

图 4

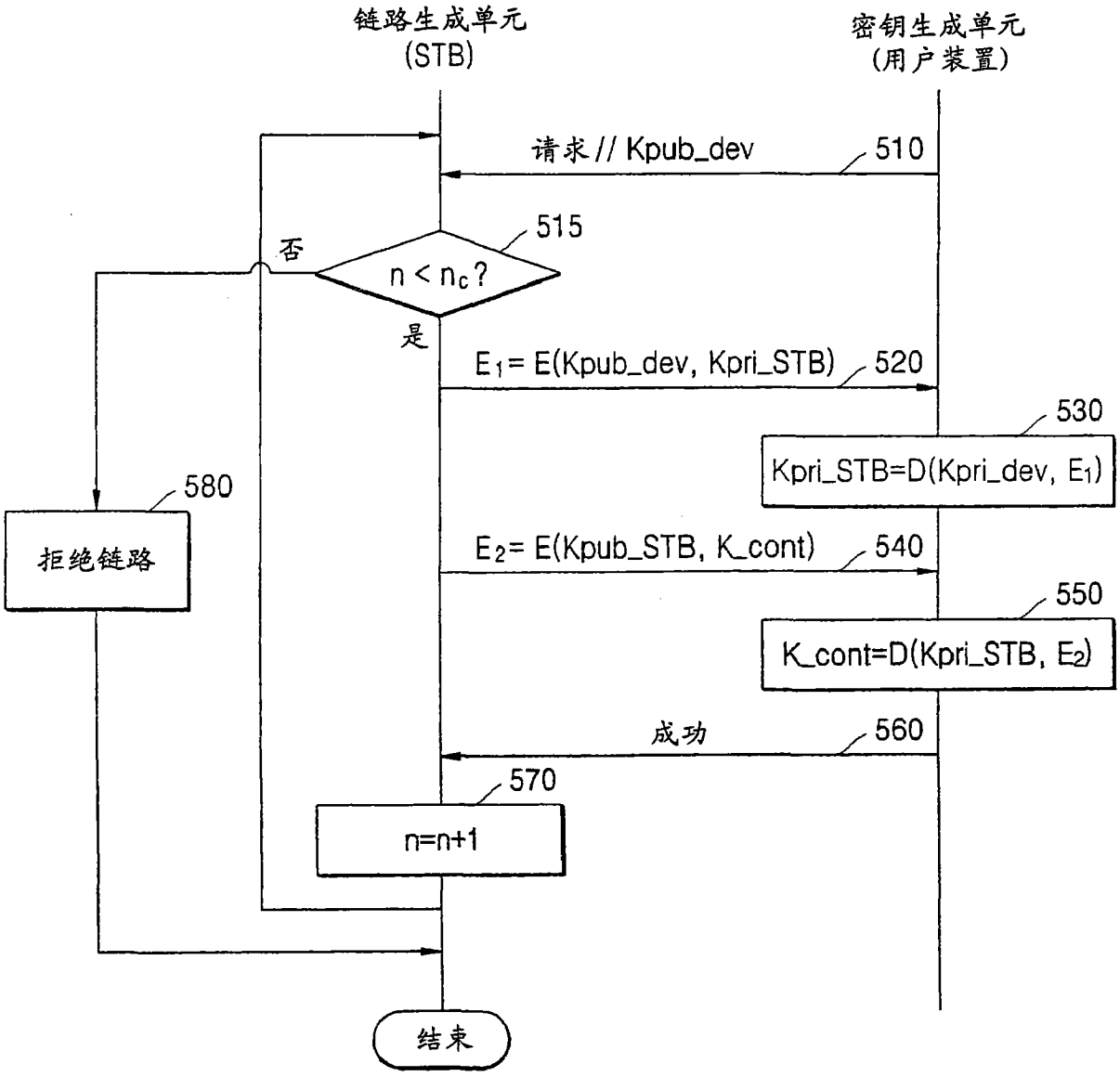

链路生成单元
(STB)
密钥生成单元
(用户装置)
请求 // Kpub_dev
510
515
否
n < nc ?
是
E1 = E(Kpub_dev, Kpri_STB)
520
530
Kpri_STB=D(Kpri_dev, E1)
580
拒绝链路
E2 = E(Kpub_STB, K_cont)
540
550
K_cont=D(Kpri_STB, E2)
成功
560
570
n=n+1
结束

图 5

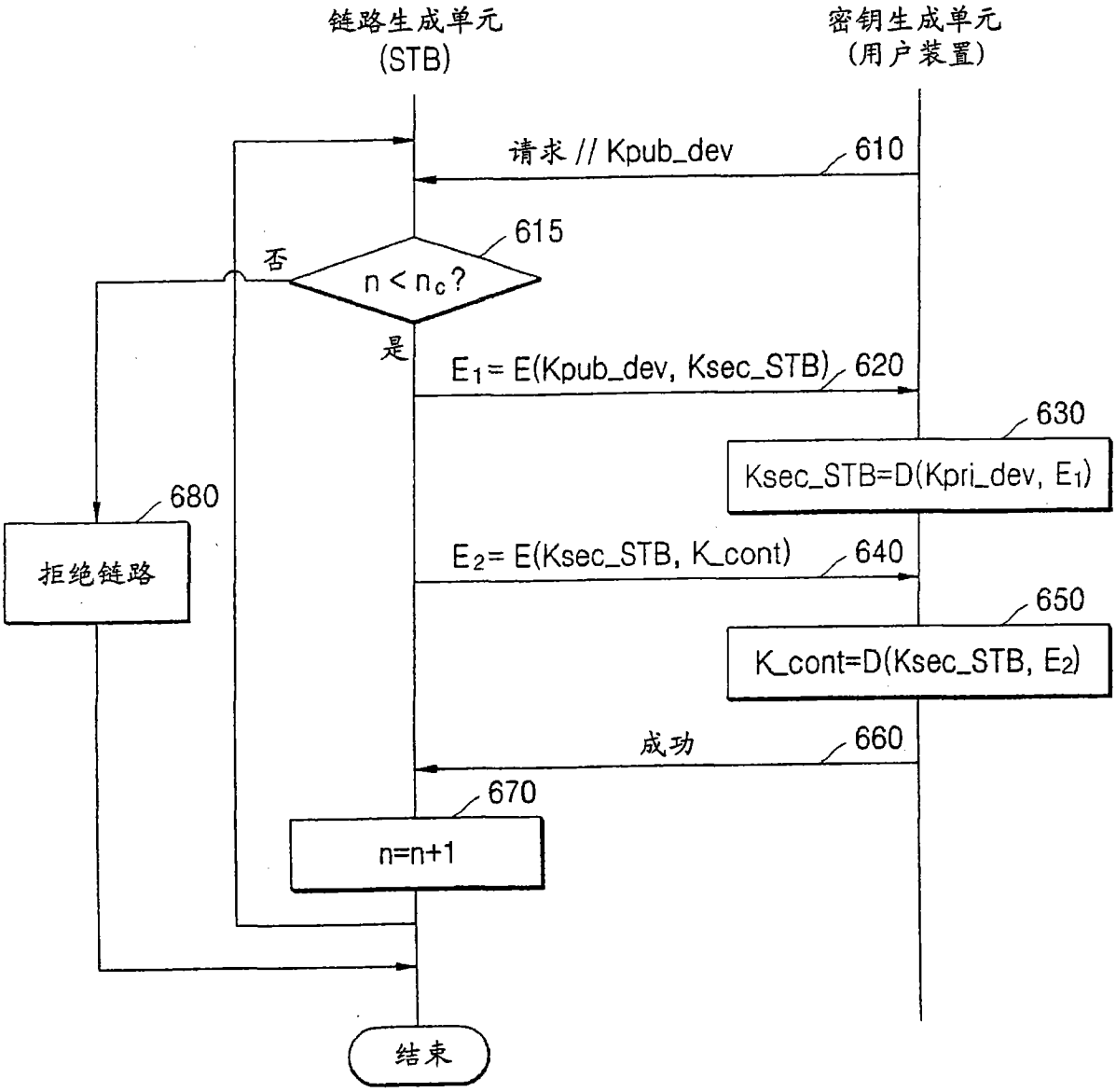

链路生成单元
(STB)
密钥生成单元
(用户装置)
请求 // Kpub_dev
610
615
否
n < nc?
是
E1= E(Kpub_dev, Ksec_STB)
620
630
Ksec_STB=D(Kpri_dev, E1)
680
拒绝链路
E2= E(Ksec_STB, K_cont)
640
650
K_cont=D(Ksec_STB, E2)
成功
660
670
n=n+1
结束

图 6

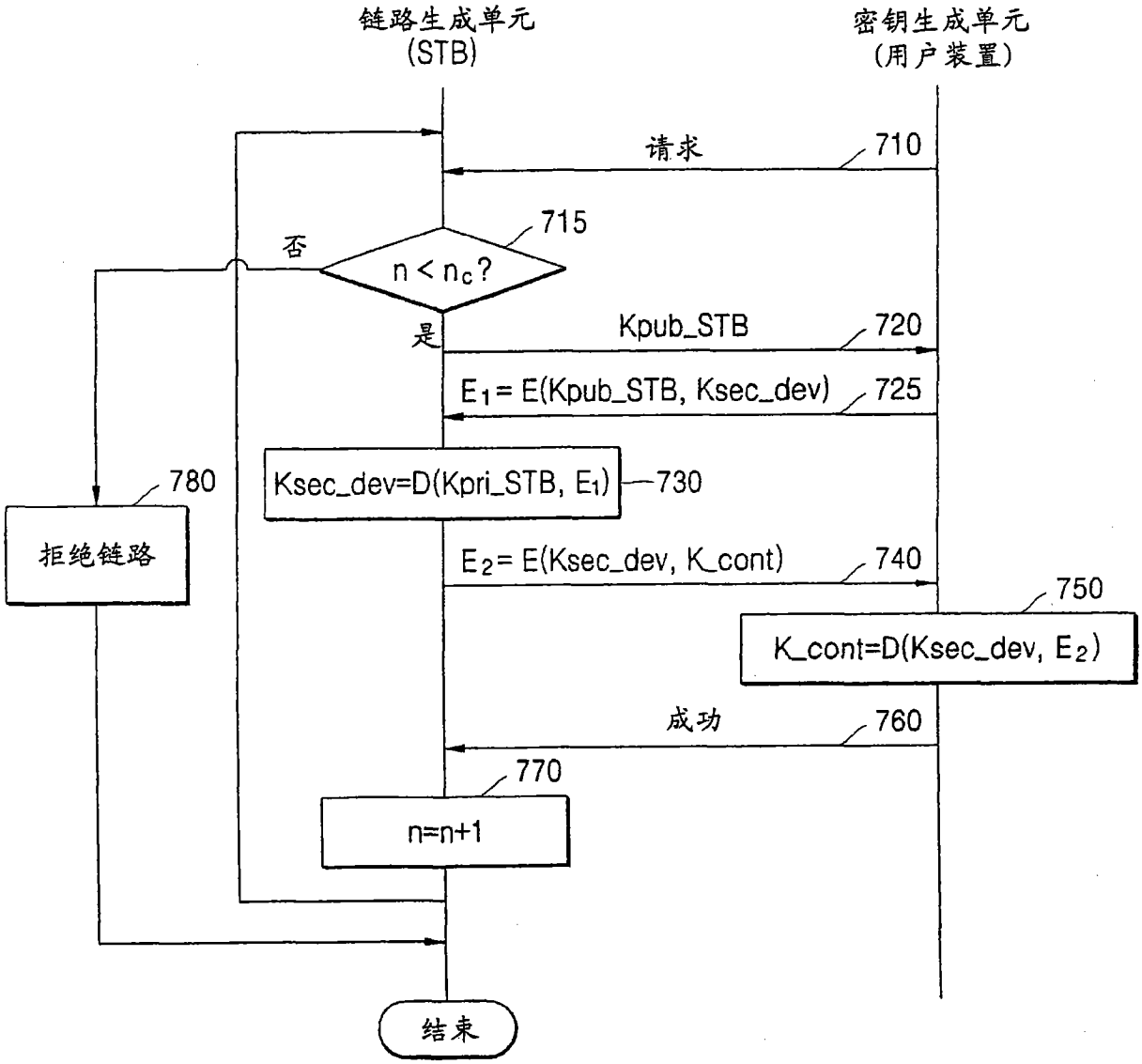

链路生成单元
(STB)
密钥生成单元
(用户装置)
请求
710
715
否
n < nc?
是
Kpub_STB
720
E1= E(Kpub_STB, Ksec_dev)
725
780
Ksec_dev=D(Kpri_STB, E1)
730
拒绝链路
E2= E(Ksec_dev, K_cont)
740
750
K_cont=D(Ksec_dev, E2)
成功
760
770
n=n+1
结束

图 7

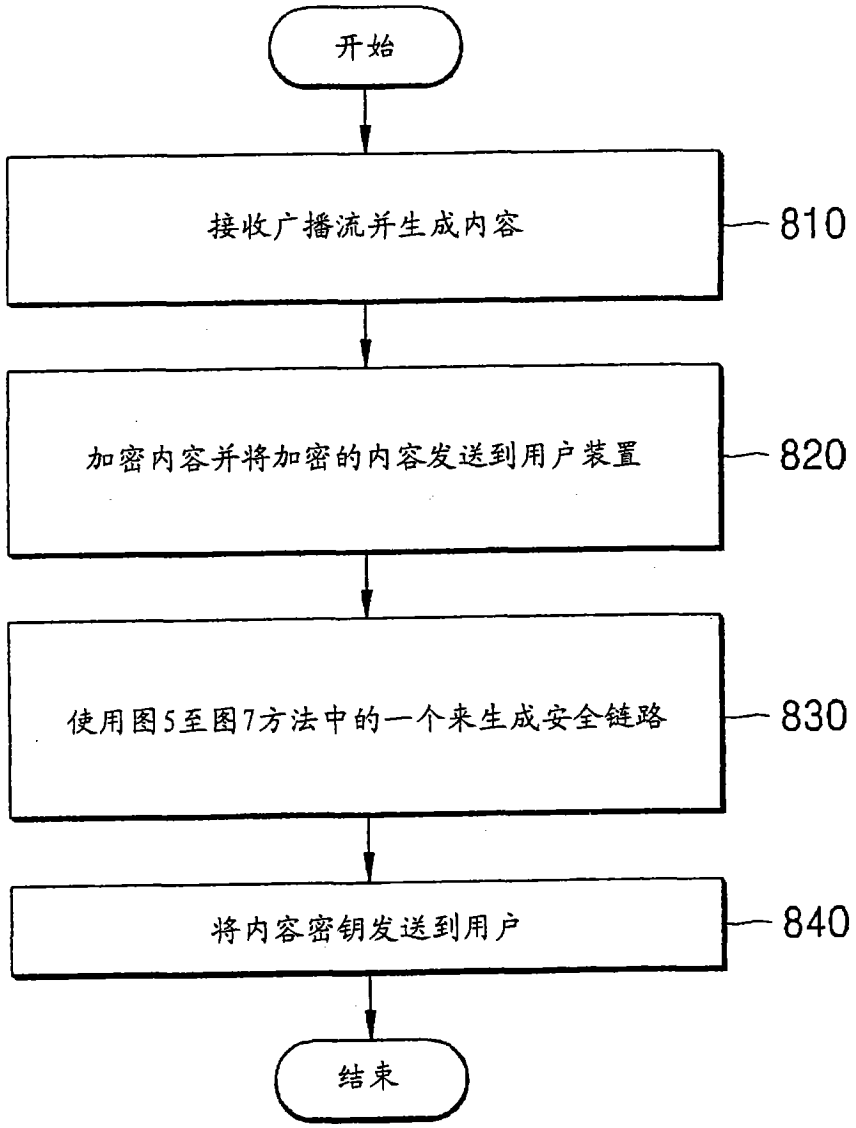

开始
接收广播流并生成内容
810
加密内容并将加密的内容发送到用户装置
820
使用图5至图7方法中的一个来生成安全链路
830
将内容密钥发送到用户
840
结束

图 8