(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 1822165 B
(45)授权公告日 2010.08.18

(21)申请号 200610005156.4

(22)申请日 2006.01.13

(30)优先权数据
05100406.7 2005.01.24 EP

(73)专利权人 汤姆森许可贸易公司
地址 法国布洛里

(72)发明人 埃里克·迪尔 阿兰·迪朗

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 罗松梅

(51)Int.Cl.
G11B 20/00(2006.01)

(56)对比文件
JP 11-250192 A,1999.09.17, 摘要、说明书[006]-[007],图 1.
WO 99/38162 A1,1999.07.29, 说明书第 12 页第 1 行至第 16 页第 11 行,图 1、4、5.
WO 2005/003886 A2,2005.01.13, 说明书第 61 页第 8 行至第 63 页第 16 行,图 1、6、9.
CN 1398401 A,2003.02.19, 全文.
全文.
CN 1234900 A,1999.11.10, 全文.

审查员 胡文娟

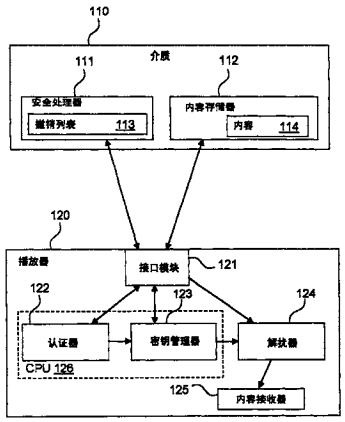
权利要求书 2 页 说明书 5 页 附图 3 页

(54)发明名称

安全预记录数字介质及其加密内容的解扰和提供方法

(57)摘要

提出了一种安全预记录介质(110)和对已加密内容(114)进行解扰的方法。当播放器(120)想要访问该内容时,介质上的安全处理器(111)验证(202)该播放器还没有被撤销,优选地通过将播放器的身份与撤销列表(113)中的身份进行比较,之后执行相互认证(204)。然后,安全处理器验证(205)播放器具有访问该内容的权利,并向播放器提供(206,207)对内容进行解扰所需的密钥,之后,播放器对该内容进行解扰(208)。



CN 1822165 B

1. 一种由播放器 (120) 对包括安全处理器 (111) 的安全介质 (110) 上的已加密内容 (114) 进行解扰的方法，所述方法包括步骤：

由安全处理器向播放器提供 (206，207) 对内容进行解扰所需的密钥；以及

由播放器对所述内容进行解扰 (208)，

所述方法的特征在于还包括步骤：

由安全处理器使用存储在安全介质上的撤销列表 (113)，验证 (202) 播放器是否已经被撤销，

其中所述向播放器提供对内容进行解扰所需的密钥的步骤包括步骤：

由播放器从介质上的内容存储器 (112) 中读取 (302) 解扰密钥的已加密版本；

由播放器将已加密的解扰密钥发送 (304) 到安全处理器；

由安全处理器解密 (306) 所述已加密的解扰密钥；以及

由安全处理器将解扰密钥 (310) 发送到播放器。

2. 根据权利要求 1 所述的方法，其特征在于还包括步骤：由安全处理器验证 (205) 播放器具有访问所述内容的权利。

3. 根据权利要求 1 或 2 所述的方法，其特征在于还包括步骤：由安全处理器和播放器相互认证 (204)。

4. 根据权利要求 1 所述的方法，其特征在于安全处理器能够访问撤销列表 (113)，并且验证播放器还没有被撤销的步骤是通过将播放器的身份与撤销列表中的身份进行比较来执行的。

5. 根据权利要求 2 所述的方法，其特征在于将所述内容划分为章节，并且所述验证所述播放器具有访问所述内容的权利的步骤是针对每一章节来执行的。

6. 一种将安全介质 (110) 上的已加密内容 (114) 提供给播放器 (120) 的方法，所述安全介质包括安全处理器 (111)，所述方法包括步骤：在安全处理器处，

认证 (204) 播放器；以及

向播放器提供 (206，207) 对内容进行解扰所需的密钥，

所述方法的特征在于还包括步骤：使用存储在安全介质上的撤销列表，验证 (202) 播放器还没有被撤销，

其中向播放器提供对内容进行解扰所需的密钥的步骤包括步骤：

从播放器接收已加密的解扰密钥；

解密 (306) 已加密的解扰密钥；以及

将解扰密钥发送 (310) 到播放器。

7. 根据权利要求 6 所述的方法，其特征在于还包括步骤：验证 (205) 播放器具有访问所述内容的权利。

8. 根据权利要求 7 所述的方法，其特征在于安全处理器能够访问撤销列表 (113)，并且验证播放器还没有被撤销的步骤是通过将播放器的身份与撤销列表中的身份进行比较来执行的。

9. 根据权利要求 7 所述的方法，其特征在于将所述内容划分为章节，并且所述验证所述播放器具有访问所述内容的权利的步骤是针对每一章节来执行的。

10. 根据权利要求 6 所述的方法，其特征在于安全处理器在将密钥提供给播放器之前

对密钥进行加密。

11. 一种由播放器 (120) 使用的介质 (110)，所述介质 (110) 包括用于存储已加密内容 (114) 的内容存储器 (112)，所述介质 (110) 还包括安全处理器 (111)，并存储了撤销列表 (113)，其特征在于所述安全处理器适合于通过如下方式向播放器提供对内容进行解扰所需的密钥：

从播放器接收已加密的解扰密钥；

对已加密的解扰密钥进行解密；以及

将解扰密钥发送给播放器。

12. 根据权利要求 11 所述的介质，其特征在于所述安全处理器适合于验证播放器还没有被撤销。

13. 根据权利要求 11 所述的介质，其特征在于所述安全处理器适合于对播放器进行认证。

14. 根据权利要求 11 所述的介质，其特征在于所述安全处理器适合于验证播放器具有访问所述内容的权利。

15. 根据权利要求 12 所述的介质，其特征在于所述安全处理器能够访问撤销列表 (113)，并且适合于通过将播放器的身份与撤销列表中的身份进行比较来验证播放器还没有被撤销。

16. 根据权利要求 14 所述的介质，其特征在于将所述内容划分为章节，并且所述安全处理器适合于验证针对每一章节，所述播放器具有至少一次访问所述内容的权利。

17. 根据权利要求 11 所述的介质，其特征在于所述安全处理器是射频 (RF) 芯片。

安全预记录数字介质及其加密内容的解扰和提供方法

技术领域

[0001] 本发明通常涉及一种数字记录介质，更具体地，涉及针对预记录数字介质的安全性。

[0002] 背景技术

[0003] 数字记录介质的增长使许多人能够享用诸如电影和音乐，至少在理论上，不存在随着时间的质量恶化。不利地，由于纯粹的数字内容可能被非常容易地拷贝无限多次，这还是为盗版提供了可能。为了与此对抗，已经提出了关于如何保护数字内容的许多不同方案。

[0004] 例如，构成所售卖的介质的大部分的数字通用盘 (DVD) 利用了静态存储区。为了防止非法拷贝，利用内容加扰系统 (CSS) 算法对 DVD 上的数字内容进行编码。用于编码的密钥是专用的，并且用于解码的相应密钥对制造者的每一个播放器均是公用的。

[0005] 针对更多最新的预记录介质的播放器，例如针对受到蓝光盘拷贝保护系统 (BD-CPS) 和针对预记录介质的内容保护 (CPPM) 保护的介质的播放器，每一个均具有一个唯一的密钥集。保护基于广播技术，例如 Fiat-Naor 方案。

[0006] 还已经尝试通过将处理器添加到记录介质上而将静态介质变为动态介质。日本专利申请 10-242555 教导了一种具有与播放器进行通信的嵌入安全处理器的 CD-ROM。该处理器将口令转发到播放器，该口令允许对内容进行解密。然而，该方案易于受到重放攻击。

[0007] 另一日本专利申请 10-050713 公开了一种使用具有内置 IC 芯片的记录介质的系统，保存了针对内容的解码密钥。仅在对主机认证成功时，该 IC 芯片将密钥传递给主机，并且添加了计数器来限制可以传输密钥的次数。然而，该解决方案不能防止盗版者进行伪造。另外，如果盗版者成功地构造了伪播放器，则他能够使用使解码密钥公开的技术。

发明内容

[0008] 因此，可以意识到，需要一种灵活的方案来克服现有技术中的问题并提高预记录数字介质的安全性。本发明提出了这样的解决方案。

[0009] 在第一方面中，本发明涉及一种由播放器对包括安全处理器的安全介质上的已加密内容进行解扰的方法。由安全处理器验证播放器是否已经被撤销；并且向播放器提供对内容进行解扰所需的密钥，并且由播放器对内容进行解扰。

[0010] 优选地，由安全处理器验证播放器具有访问该内容的权利。

[0011] 有利地，将所述内容划分为章节，并且所述安全处理器针对每一章节来验证播放器具有访问该内容的权利。

[0012] 有利地，安全处理器能够访问撤销列表，并且其通过将播放器的身份与撤销列表中的身份进行比较来验证播放器没有被撤销。

[0013] 另外，优选地，由安全处理器和播放器相互认证。

[0014] 另外，优选地，为了向播放器提供所需的密钥，播放器从介质上的内容存储器中读取解扰密钥的已加密版本，并将其发送给安全处理器，安全处理器对该密钥进行解密并将其发送给播放器。

[0015] 在第二方案中，本发明涉及一种对包括安全处理器的安全介质上的已加密内容进行解扰的方法。播放器对安全处理器进行认证；接收对内容进行解扰所需的密钥；并且解扰所述内容。

[0016] 优选地，为了向播放器提供解扰该内容所需的密钥，播放器从介质上的内容存储器中读取解扰密钥的已加密版本，并已加密解扰密钥发送给安全处理器，并从安全处理器接收解扰密钥。

[0017] 在第三方案中，本发明涉及一种将安全介质上的已加密内容提供给播放器的方法，所述安全介质包括安全处理器。安全处理器验证播放器还没有被撤销；认证播放器；以及向播放器提供对内容进行解扰所需的密钥。

[0018] 优选地，所述安全介质验证播放器具有访问该内容的权利。

[0019] 有利地，将所述内容划分为章节，并且所述安全处理器针对每一章节来验证播放器具有访问该内容的权利。

[0020] 另外，优选地，安全处理器能够访问撤销列表，并且安全处理器通过将播放器的身份与撤销列表中的身份进行比较来验证播放器还没有被撤销。

[0021] 另外，优选地，为了向播放器提供解扰该内容所需的密钥，安全处理器从播放器中接收已加密的解扰密钥，对已加密解扰密钥进行解密，并将解扰密钥发送给播放器。

[0022] 另外，优选地，安全处理器在将密钥提供给播放器之前对密钥进行加密。

[0023] 在第四方案中，本发明涉及一种由播放器使用的介质。所述介质包括用于存储已加密内容的内容存储器和安全处理器，并且其存储了撤销列表。

[0024] 优选地，所述安全处理器适合于验证播放器还没有被撤销。

[0025] 有利地，安全处理器能够访问撤销列表，并且其通过将播放器的身份与撤销列表中的身份进行比较来验证播放器没有被撤销。

[0026] 此外，优选地，所述安全处理器适合于对播放器进行认证。

[0027] 另外，优选地，所述安全处理器适合于验证播放器具有访问该内容的权利。

[0028] 有利地，将所述内容划分为章节，并且所述安全处理器针对每一章节来验证播放器具有至少一次访问该内容的权利。

[0029] 另外，安全处理器适合于向播放器提供解扰该内容所需的密钥。

[0030] 有利地，为了向播放器提供对内容进行解扰所需的密钥，所述安全处理器从播放器接收已加密的解扰密钥；对已加密的解扰密钥进行解密；以及将解扰密钥发送给播放器。

[0031] 另外，优选地，所述安全处理器是射频（RF）芯片。

附图说明

[0032] 参考附图，作为示例，现在将描述本发明的优选特征，其中，

[0033] 图 1 示出了根据本发明的安全预记录介质和相应的播放器的交互；

[0034] 图 2 示出了根据本发明的介质访问方法；以及

[0035] 图 3 示出了所需解扰密钥的传递。

具体实施方式

[0036] 图 1 示出了根据本发明的安全预记录介质 110 和相应的播放器 120 的交互。

[0037] 该介质 110 将已加密内容 114 存储在内容存储器 112，内容存储器 112 可由播放器 120 任意访问。将解密内容 114 所需的诸如解密密钥等信息存储在安全处理器 111 中。本领域的技术人员将会意识到安全处理器 111 可以具有内在的存储容量（未示出），但是其也可以使用介质存储容量，例如内容存储器 112，并且利用安全处理器内部的密钥来使该存储区安全。

[0038] 播放器 120 包括接口模块 121，处理与介质 110 的安全处理器 111 和内容存储器 112 的通信，即，其能够从内容存储器 112 中读取内容 114，并与安全处理器 111 进行通信。该接口模块可能能够进行光学交互、无线电交互、或同时进行光学和无线电交互，例如，与内容存储器 112 进行光学交互而与安全处理器 111 进行无线电交互。播放器 120 还包括认证器 122、密钥管理器 123 和解扰器 124，所有这些将在下面进一步描述。在特定的优选实施例中，认证器 122 和密钥管理器 123 被包括在中央处理单元 (CPU) 126 中，而解扰器 124 是高级加密标准 (AES) 解扰芯片。接口模块 121 还可以与这三个单元 122、123、124 进行通信。播放器 120 还可以包括内容接收器 125，尽管其并非本发明的一部分，但是下面将简要描述其。

[0039] 图 2 示出了根据本发明的介质访问的方法。当介质 110 要由播放器 120 来读取时，通常当用户将介质插入到播放器且已经按下了“播放”等时，该方法在步骤 201 “开始”处开始。

[0040] 在步骤 202“被撤销？”，安全处理器 111 验证播放器 120 是否已经被撤销。例如，通过将播放器的身份与安全处理器的存储器中的撤销列表 113 进行比较来实现这一点。如果播放器已经被撤销（“是”），则安全处理器 111 中止该方法，步骤 203 “停止，并且拒绝与播放器 120 进行通信。这意味着已认证介质仅能够在还未撤销的播放器上播放。

[0041] 然而，如果播放器还未被撤销，则该方法继续。

[0042] 于是，播放器 120 的认证器 122 和安全处理器 111 在步骤 204 “认证”彼此相互认证。

[0043] 如果认证器 122 未能认证该介质 110，则“不成功”，然后，播放器 120 中止该方法，在步骤 203 停止，并拒绝播放该介质 110。因此，该播放器仅播放来自已认证提供者的介质，这在一定程度上对抗了有组织的盗版。

[0044] 如果一方面安全处理器 111 未能认证播放器 120（“未成功”），则其中止该方法，进行到步骤 203，并拒绝与播放器 120 通信。因此，在一定程度上确保了已认证介质仅在已认证播放器上播放。

[0045] 在相互认证成功时（“成功”），该方法转到步骤 205 “权利？”，安全处理器 111 验证该播放器 120 具有播放内容 114 所需的权利。在许多情况下，这是自动为真的（在该情况下，该步骤是不必要的），但是存在进一步的限制 - 例如，仅针对特定播放器、仅针对内容 114 的特定部分，关于介质能够播放的次数的限制 - 是所需的。例如，安全处理器 111 可以验证其具有存储在其存储器中的播放器 120 的身份。如果安全处理器 111 发现该播放器没有适当的权利，则其中止该方法，进行到步骤 203，并拒绝与播放器 120 进行通信。然而，如果播放器 120 确实具有所需的权利，则该方法在步骤 206 处继续。

[0046] 一旦已经确定介质 110 可以将内容 114 传递到播放器 120。则安全处理器 111 通过接口模块 121 将对内容 114 解密所需的信息发送到密钥管理器 123（步骤 206“秘密送往

密钥管理器”）。例如，该信息可以具有所需解密密钥或解密密钥自身的类型，尽管这绝非完整的列举。该信息可以对应于完整内容 114 或内容 114 的一部分，例如要被播放的部分。优选地，使用加密来确保信息传输的安全。

[0047] 在步骤 207“计算密钥”，密钥管理器 123 使用接收到的信息来计算解密密钥并将其传递给解扰器 124。

[0048] 在步骤 208“解扰内容”，内容模块 121 从内容存储器 112 读取加密内容 114，并将其转发到解扰器 124，继续操作直到其用完针对其具有解密密钥的内容。解扰器 124 利用从密钥管理器 123 接收到的解密密钥对内容进行解密，并将已解密内容发送到内容接收器 125，例如使用该内容的数字总线。

[0049] 在步骤 209“更多内容？”，验证是否存在更多要播放的内容。如果情况并非如此（“否”），则该方法在步骤 203 处停止。然而，如果存在更多的内容（“是”），则该方法在步骤 205“权利？”处继续，以验证该播放器是否具有针对即将到来的内容的所需权利，如前所述。在可选实施例中，该方法直接在步骤 206“密钥到密钥管理器”继续，而无需验证权利。在两个实施例中，在适当的时间处来执行，从而使解扰器 124 总是拥有其对内容进行解密所需的密钥，当然，假定播放器具有所需权利。

[0050] 在特别优选的实施例中，介质 110 的安全处理器 111 是射频 (RF) 芯片，不需要电池，不需要与播放器 120 进行物理接触，并且即使在诸如被合理量的污物覆盖的情况下也能够被读取。接口模块 121 包括射频接口，其发射低频无线电波场以为安全处理器 111 供电，并且还包括传统光学读取器，以读取内容存储器 112 中所存储的内容 114。

[0051] 另外，在特别优选的实施例中，内容存储器 112 存储按章节（例如歌曲和场景）组织的已加扰内容 114，其中每一章节 i 利用密钥 K_i 通过 AES 来加扰。安全处理器 111 存储了由第一认证权威机构 A 签名的唯一公用 / 专用密钥对、第二认证权威机构 B 的公用密钥、撤销列表 113 和标题密钥 TK。认证器 122 存储了由第二认证权威机构 B 签名的唯一公用 / 专用密钥对和第一认证权威机构 A 的公用密钥。

[0052] 另外，在特别优选的实施例中，在步骤 202“被撤销？”中，安全处理器 111 验证在撤销列表 113 中未发现认证器 122 的公用密钥的证书。利用各个公用 / 专用密钥对来执行步骤 204“认证”。安全处理器 111 和认证器 122 利用诸如创建了共享会话密钥 K_{sess} 的认证 Diffie-Hellman 密钥交换来建立安全已认证信道。对于步骤 205“权利？”，介质 110 的拥有者赋予永久的权利。

[0053] 图 3 示出了所需解扰密钥的传递。在步骤 206，当开始新章节 i 时，密钥管理器 123 在步骤 302 加载第一已加密解扰密钥 Eki，并在步骤 304 将其传递给安全处理器 111，安全处理器 111 利用标题密钥 TK 在步骤 306 处对解扰密钥进行解密，并在步骤 308 利用会话密钥 K_{sess} 通过 AES 对其重新加密。然后，在步骤 310，安全处理器 111 将重新加密的解扰密钥传递给密钥管理器 123，在步骤 312，密钥管理器 123 接收该解扰密钥，在步骤 314，利用会话密钥 K_{sess} 通过 AES 对其进行解密，并且在步骤 316，将已解密的解扰密钥提供给解扰器芯片 124。

[0054] 将会理解，纯粹作为示例描述了本发明，在不脱离本发明的范围的情况下，可以进行细节上的修改。

[0055] 可以独立地和以任意适当的组合来提供权利要求和（如果适当）权利要求和附图

中所公开的每一个特征。在硬件中实现的所述特征也可以由软件来实现，反之亦然。如果适当，可以将连接实现为无线连接或有线连接，不必是直接或专用的连接。

[0056] 在权利要求中所出现的附图标记仅是说明性的，对权利要求的范围没有任何限定效果。

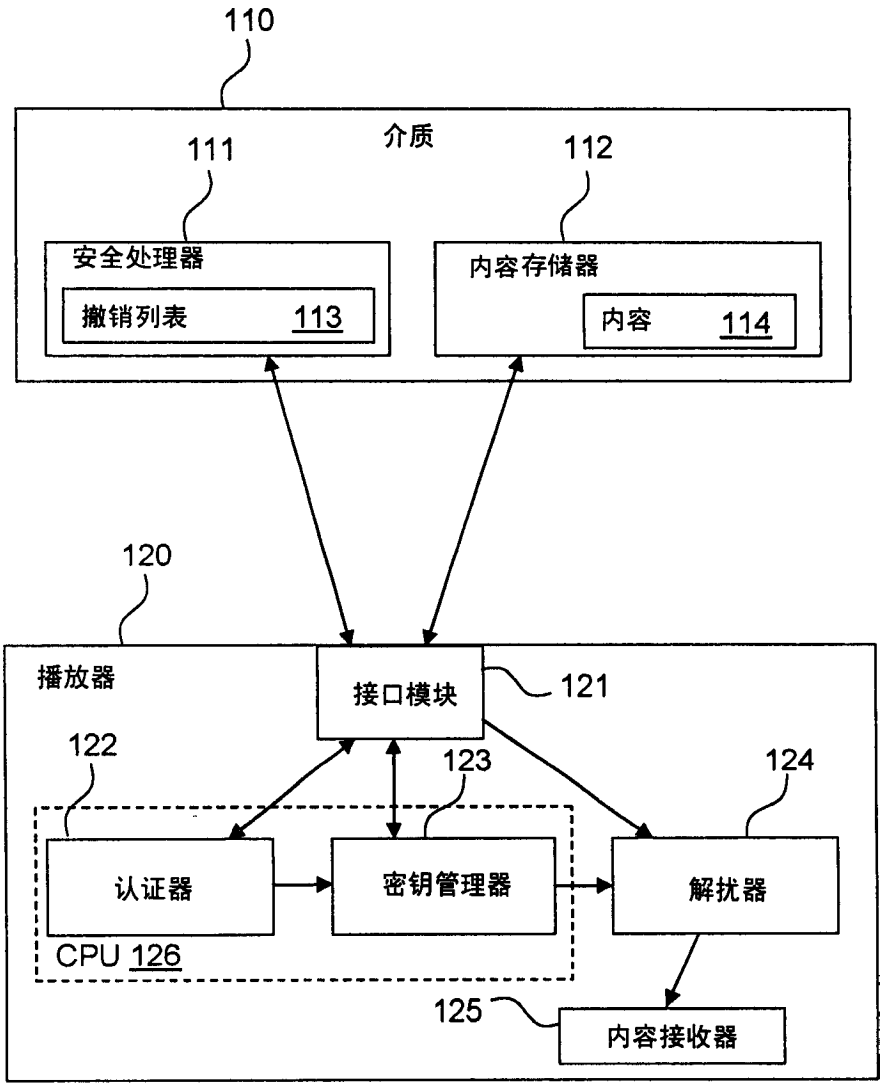

110
介质
111
112
安全处理器
撤销列表 113
内容存储器
内容 114
120
播放器
接口模块
121
122
123
124
认证器
密钥管理器
解扰器
CPU 126
125
内容接收器

图 1

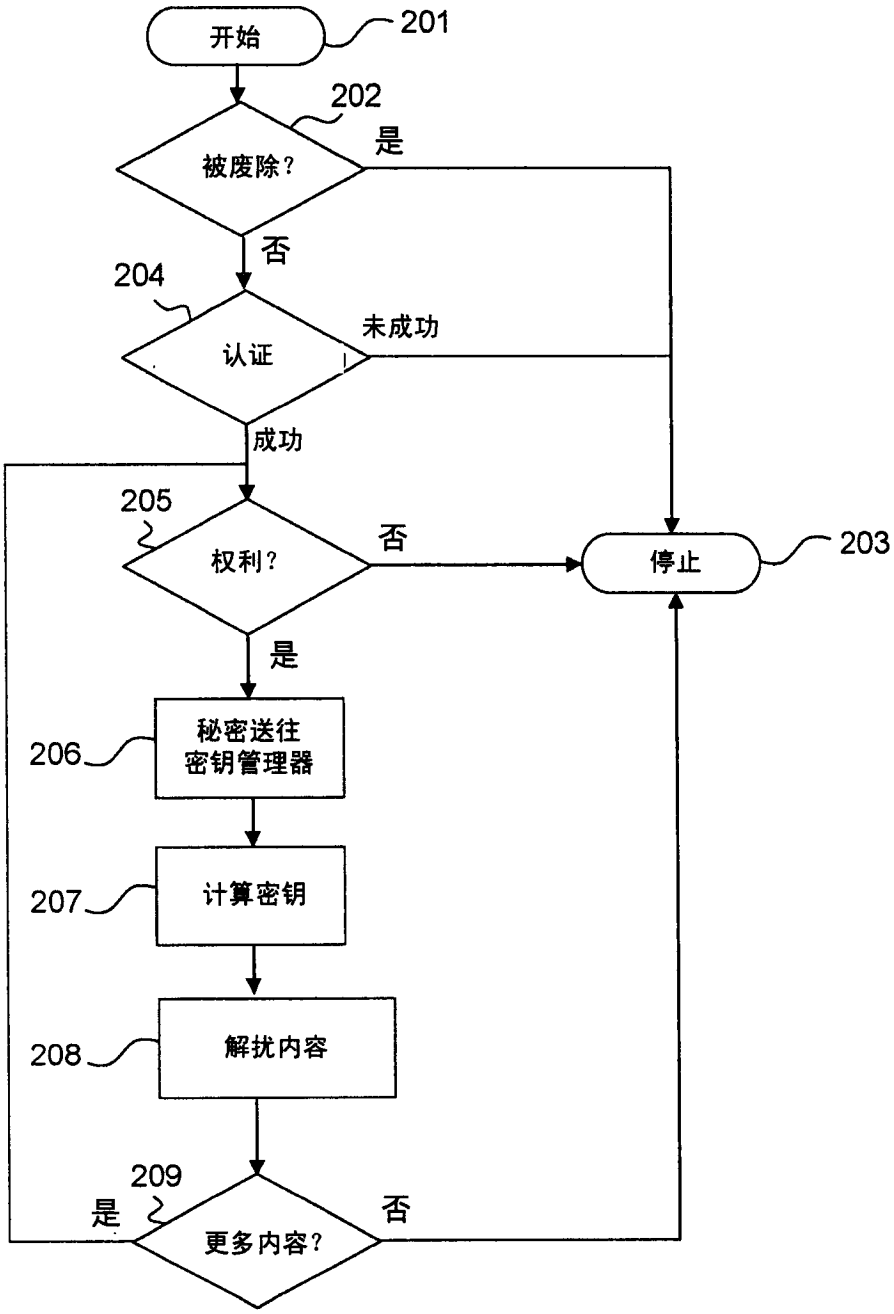

开始
201
202
被废除？
是
否
204
认证
未成功
成功
205
权利？
否
停止
203
是
206
秘密送往
密钥管理器
207
计算密钥
208
解扰内容
209
是
更多内容？
否

图 2

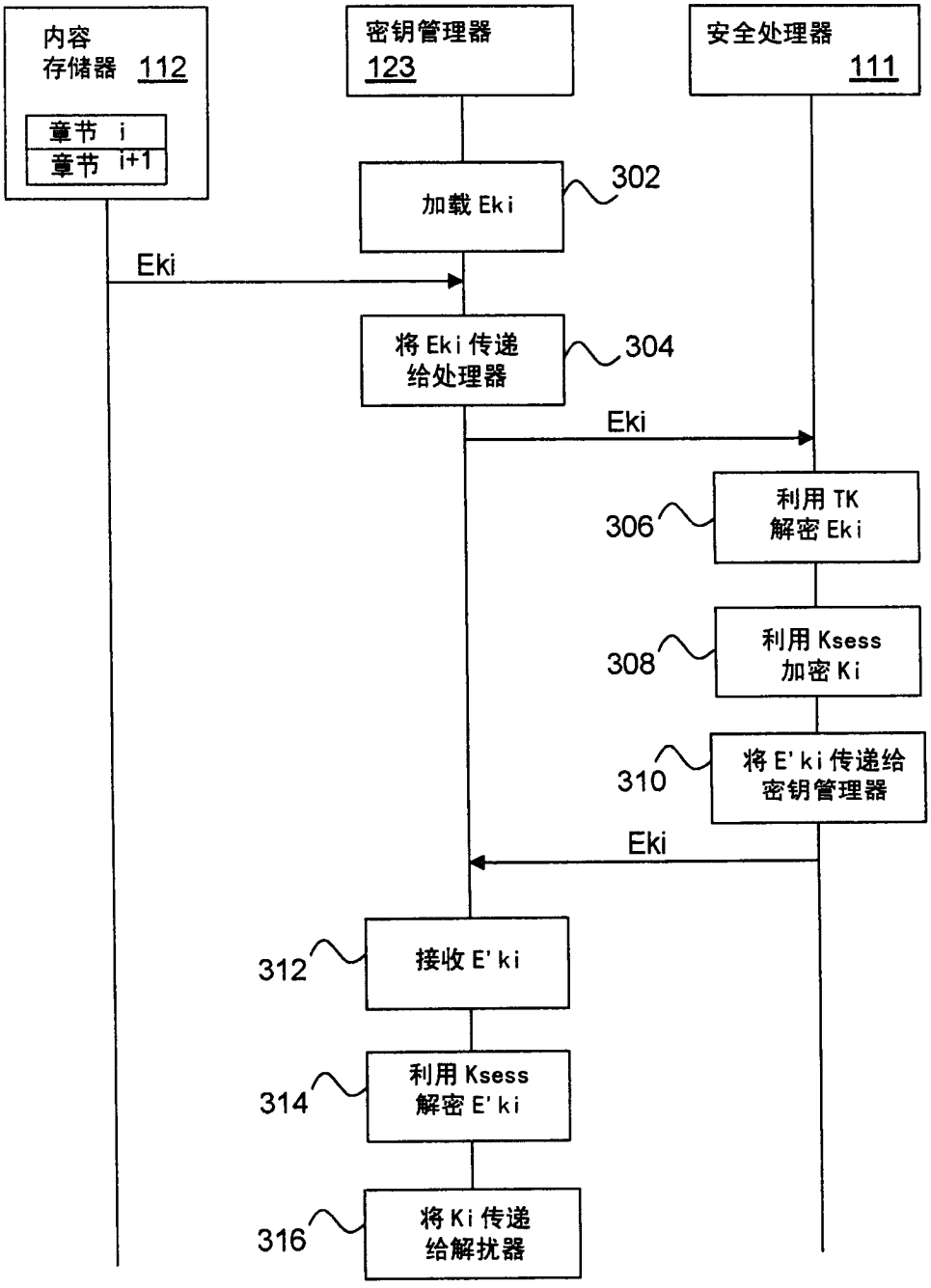

内容
存储器 112
章节 i
章节 i+1
密钥管理器
123
安全处理器
111
加载 Eki
302
Eki
将 Eki 传递
给处理器
304
Eki
306
利用 TK
解密 Eki
308
利用 Ksess
加密 Ki
310
将 E'ki 传递给
密钥管理器
Eki
312
接收 E'ki
314
利用 Ksess
解密 E'ki
316
将 Ki 传递
给解扰器

图 3