[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G11B 20/10 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200580000202.5

[43] 公开日 2006 年 5 月 10 日

[11] 公开号 CN 1771552A

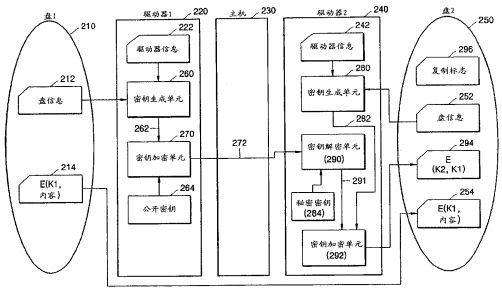
[22] 申请日 2005.1.10
[21] 申请号 200580000202.5
[30] 优先权
[32] 2004.1.10 [33] KR [31] 10-2004-0001813
[86] 国际申请 PCT/KR2005/000070 2005.1.10
[87] 国际公布 WO2005/066952 英 2005.7.21
[85] 进入国家阶段日期 2005.10.31
[71] 申请人 三星电子株式会社
地址 韩国京畿道
[72] 发明人 韩声休 金润相 崔良林 刘容国 韩熙喆
[74] 专利代理机构 北京市柳沈律师事务所
代理人 吕晓章 李晓舒
权利要求书 4 页 说明书 8 页 附图 6 页

[54] 发明名称

从存储媒体中复制和再现数据的方法

[57] 摘要

本发明提供了将存储在第一存储媒体中的数据复制到第二存储媒体的方法。该方法包括将存储在第一存储媒体中的加密数据记录在第二存储媒体上；利用第一存储媒体装入其中的第一驱动器再现用于加密被加密数据的第一内容密钥；加密第一内容密钥；将加密的第一内容密钥发送到第二存储媒体装入其中的第二驱动器；和将加密的第一内容密钥记录在第二存储媒体上。在该方法中，通过主机将存储在第一存储媒体中的加密数据发送到第二存储媒体，而不用解密加密的数据，从而防止数据被未授权用户篡改或访问，并提高复制加密数据的速度。



1. 一种将存储在第一存储媒体中的加密数据复制到第二存储媒体的方法，该方法包括:

将存储在第一存储媒体中的加密数据记录在第二存储媒体上;

利用第一存储媒体装入其中的第一驱动器再现用于加密被加密的数据的第一内容密钥;

将第一内容密钥加密成加密的第一内容密钥;

将加密的第一内容密钥发送到第二存储媒体装入其中的第二驱动器; 和

将加密的第一内容密钥记录在第二存储媒体上。

2. 根据权利要求 1 所述的方法，其中，加密的第一内容密钥是利用公开密钥基础设施进行的。

3. 根据权利要求 2 所述的方法，其中，加密第一内容密钥的步骤包括:

利用第二驱动器的公开密钥加密第一内容密钥，和将加密的第一内容密钥发送到第二驱动器的步骤包括:

将加密的第一内容密钥发送到第二驱动器; 和

利用第二驱动器的秘密密钥解密加密的第一内容密钥，该秘密密钥对应于第二驱动器的公开密钥。

4. 根据权利要求 1 所述的方法，其中，加密第一内容密钥的步骤包括:

根据存储在第二存储媒体中的盘信息再现第二内容密钥; 和

利用第二内容密钥加密第一内容密钥。

5. 根据权利要求 1 所述的方法，进一步包括将复制标志记录在第二存储媒体的预定区域中，该复制标志指示加密数据不是利用从存储在第二存储媒体中的盘信息中提取的第二内容密钥加密的，并是从第一存储媒体复制到第二存储媒体上的。

6. 根据权利要求 5 所述的方法，其中，预定区域是导入区。

7. 根据权利要求 1 所述的方法，其中，根据存储在第一存储媒体中的盘信息再现第一内容密钥。

8. 根据权利要求 7 所述的方法，其中，根据存储在第一存储媒体中的盘信息和存储在第一驱动器中的驱动器信息再现第一内容密钥。

9. 根据权利要求 7 所述的方法，其中，盘信息包括盘标识符、更新密钥

块、媒体密钥、和随机数中的至少一个。

10. 根据权利要求 7 所述的方法，其中，驱动器信息包括设备标识符、设备密钥组、设备密钥、和随机数中的至少一个。

11. 根据权利要求 4 所述的方法，其中，利用存储在第二存储媒体中的盘信息再现第二内容密钥。

12. 根据权利要求 4 所述的方法，其中，利用存储在第二存储媒体中的盘信息和存储在第二驱动器中的驱动器信息再现第二内容密钥。

13. 根据权利要求 11 所述的方法，其中，盘信息包括盘标识符、更新密钥块、媒体密钥、和随机数中的至少一个。

14. 根据权利要求 11 所述的方法，其中，驱动器信息包括设备标识符、设备密钥组、设备密钥、和随机数中的至少一个。

15. 一种从第一存储媒体中再现利用加密的第一内容密钥加密的数据的方法，该方法包括:

利用存储在第一存储媒体中的盘信息再现第二内容密钥;

利用第二内容密钥解密加密的第一内容密钥以便生成解密的第一内容密钥; 和

利用解密的第一内容密钥解密加密的数据，

其中，第一内容密钥是利用第二内容密钥加密的，第二内容密钥可以利用存储在第一存储媒体中的盘信息再现，和第一内容密钥存储在第一存储媒体中。

16. 根据权利要求 15 所述的方法，其中，第一存储媒体存储指示从第二存储媒体复制加密数据的复制标志，和该方法进一步包括检测复制标志。

17. 根据权利要求 16 所述的方法，其中，当复制标志指示不是从第二存储媒体复制加密数据时，进一步包括利用第二内容密钥解密加密的数据。

18. 根据权利要求 15 所述的方法，其中，利用存储在第一存储媒体中的盘信息再现第二内容密钥。

19. 根据权利要求 18 所述的方法，其中，利用存储在第一存储媒体中的盘信息和存储在第一驱动器中的驱动器信息再现第二内容密钥。

20. 根据权利要求 18 所述的方法，其中，盘信息包括盘标识符、更新密钥块、媒体密钥、和随机数中的至少一个。

21. 根据权利要求 18 所述的方法，其中，驱动器信息包括设备标识符、

设备密钥组、设备密钥、和随机数中的至少一个。

22. 一种将利用第一加密密钥加密的音频/视频（AV）数据记录在存储媒体上的方法，该方法包括:

利用有关存储媒体的信息再现第二加密密钥;

利用第二加密密钥加密第一加密密钥，以便生成加密的第一加密密钥;和

将加密的第一加密密钥加密和利用第一加密密钥加密的 AV 数据记录在存储媒体上。

23. 根据权利要求 22 所述的方法，其中，第一加密密钥是加密 AV 数据的密钥信息，和第二加密密钥是加密第一加密密钥的密钥信息。

24. 根据权利要求 22 所述的方法，其中，存储媒体包括可以至少记录 AV 数据一次的激光唱盘、数字多功能盘、和蓝光盘之一。

25. 根据权利要求 22 所述的方法，其中，有关存储媒体的信息包括更新密钥块、记录媒体密钥、记录随机数、和记录媒体标识符中的至少一个，和

利用更新密钥块、记录媒体密钥、记录随机数、和记录媒体标识符中的至少一个再现第二加密密钥。

26. 一种再现利用第一加密密钥加密并存储在存储媒体中的音频/视频（AV）数据的方法，该方法包括:

利用有关存储媒体的信息生成第二加密密钥;

利用第二加密密钥解密第一加密密钥，以便生成解密的第一加密密钥;和

利用解密的第一加密密钥解密 AV 数据。

27. 根据权利要求 26 所述的方法，其中，第一加密密钥是解密 AV 数据的密钥信息，和第二加密密钥是解密第一加密密钥的密钥信息。

28. 根据权利要求 26 所述的方法，其中，存储媒体包括可以至少记录 AV 数据一次的激光唱盘、数字多功能盘、和蓝光盘之一。

29. 根据权利要求 26 所述的方法，其中，有关存储媒体的信息包括更新密钥块、记录媒体密钥、记录随机数、和记录媒体标识符中的至少一个，和

利用更新密钥块、记录媒体密钥、记录随机数、和记录媒体标识符中的至少一个再现第二加密密钥。

30. 一种在存储音频/视频（AV）数据的存储媒体和将 AV 数据记录在存

储媒体上或从存储媒体上再现 AV 数据的装置中生成加密密钥的方法，该方法包括:

从存储媒体中读取更新密钥块、利用媒体密钥加密的盘密钥、和盘标识符;

利用更新密钥块再现媒体密钥;

利用媒体密钥解密盘密钥，以便生成解密的盘密钥;

生成记录随机数; 和

从解密的盘密钥、记录随机数、和从存储媒体中读取的盘标识符的至少一个中生成加密密钥。

从存储媒体中复制和再现数据的方法

技术领域

本发明涉及将数据从一个存储媒体复制到另一个存储媒体的方法，尤其涉及加密存储在一个存储媒体中的数据和通过主机将加密结果记录在另一个存储媒体上，从而防止数据被未授权用户篡改和提高复制数据的速度的数据复制方法。

背景技术

一般说来，作为大容量存储媒体开发的光盘分类成存储音乐数据的激光唱盘（CD）、存储计算机数据的只读光盘存储器（CD-ROM）、和存储视频数据的数字多功能盘（DVD）。

此外，这样的光盘可以分类成在盘制造期间记录数据的只读型和允许用户将数据记录在上面的可记录型。并且，可记录型可以分类成只写一次型和可重写型。可以将数据从一个盘传送到另一个盘或从安装在用户计算机中的硬盘传送到一个盘。这样的数据传送被称为盘复制。

一般说来，对版权保护内容进行加密和将加密结果存储在存储媒体中。详细地说，利用内容密钥加密这样的内容和将加密结果存储在存储媒体中。内容密钥是利用从存储媒体中再现内容的盘驱动器或根据存储在存储媒体中的信息再现的。

图 1 例示了将存储在第一个盘 110 中的内容复制到第二个盘 120 的传统方法。参照图 1，第一个盘 110 存储利用内容密钥 K1 加密的内容 E(K1, Contents)。当将第一个盘 110 装入第一驱动器 112 中时，第一驱动器 112 利用存储在第一个盘 110 或第一驱动器 112 中的信息再现内容密钥 K1。

存储在第一个盘 110 中的信息包括盘标识符（ID）、随机数、和更新密钥块。盘 ID 表示盘标识号和更新密钥块表示使未授权装置得以识别的一组驱动器密钥。存储在第一驱动器 112 中的信息包括作为驱动器识别号的驱动器 ID、和设备密钥组。设备密钥组表示只提供给授权装置以便识别未授权装置的一组密钥。

在再现内容密钥 K1 之后，第一驱动器 112 利用内容密钥 K1 解密已经加密和存储在第一个盘 110 中的内容 E(K1, Contents)，从而获得解密的内容 134。通过主机 130 将解密的内容 134 发送到第二驱动器 122。

第二驱动器 122 根据存储在第二个盘 120 中的信息和存储在第二驱动器 122 中的信息再现内容密钥 K2。存储在第二个盘 120 中的信息和存储在第二驱动器 122 中的信息分别等同于存储在第一个盘 110 中的信息和存储在第一驱动器 112 中的信息。于是，这里省略对它们的详细描述。

接着，第二驱动器 122 利用内容密钥 K2 加密解密的内容 134，从而获取加密的内容 E(K2, Contents)124。将加密的内容 E(K2, Contents)124 记录在第二个盘 120 上。

如上所述，存储在第一个盘 110 中的加密内容 E(K1, Contents)被解密，重新加密，然后复制到第二个盘 120。利用内容密钥 K2 重新加密解密的内容 134 的原因是使除了第一和第二驱动器 112 和 122 之外的新驱动器能够再现内容密钥 K2 和利用内容密钥 K2 解密存储在第二个盘 120 中的加密内容 E(K2, Contents)。换句话说，由于内容密钥是利用盘信息再现的，新驱动器不能利用以前的密钥 K1 解密存储在第二个盘 120 中的加密内容 E(K2, Contents)。

但是，在传统数据复制方法中，将未加密的内容从第一驱动器 112 发送到主机 130，然后，发送到第二驱动器 122，因此，无法保证内容的安全性。例如，这样的内容可能被访问主机 130 的未授权用户截取或篡改。

并且，传统数据复制方法的不利之处在于，由于必须加密、解密、和重新加密内容，将内容从一个存储媒体复制到另一个存储媒体需要大量时间。

发明内容

本发明提供了在通过主机发送数据时为数据提供安全性和缩短数据复制所需的时间的同时，将数据从一个存储媒体复制到另一个存储媒体的方法。

根据本发明，将存储在存储媒体中的加密数据发送到主机而不用解密加密的数据，从而防止数据被未授权用户篡改。

此外，将加密数据从第一存储媒体复制到第二存储媒体而不用解密加密的数据，从而提高复制加密数据的速度。

附图说明

图 1 例示了将存储在一个存储媒体中的数据复制到另一个存储媒体的传统方法;

图 2 例示了根据本发明一个实施例的将存储在一个存储媒体中的数据复制到另一个存储媒体的方法;

图 3 是例示图 2 的方法的流程图;

图 4 例示了根据本发明一个实施例的利用第一驱动器和第二驱动器生成各自内容密钥的方法;

图 5 例示了根据本发明一个实施例的将存储在另一个盘中的数据复制在上面的一个可记录盘的数据结构;

图 6 例示了根据本发明一个实施例的利用驱动器再现复制到存储媒体的数据的方法; 和

图 7 是例示根据本发明一个实施例的再现复制到存储媒体的数据的方法的流程图。

具体实施方式

根据本发明的一个方面，提供了将存储在第一存储媒体中的加密数据复制到第二存储媒体的方法，该方法包括将存储在第一存储媒体中的加密数据记录在第二存储媒体上; 利用第一存储媒体装入其中的第一驱动器再现用于加密被加的密数据的第一内容密钥; 加密第一内容密钥; 将加密第一内容密钥发送到第二存储媒体装入其中的第二驱动器; 和将加密第一内容密钥记录在第二存储媒体上。

加密第一内容密钥是利用公开密钥基础设施进行的。

加密第一内容密钥和将加密第一内容密钥发送到第二驱动器包括利用第二驱动器的公开密钥加密第一内容密钥; 将加密第一内容密钥发送到第二驱动器; 和利用第二驱动器的秘密密钥解密加密第一内容密钥，该秘密密钥对应于第二驱动器的公开密钥。

加密第一内容密钥包括根据存储在第二存储媒体中的盘信息再现第二内容密钥; 和利用第二内容密钥加密第一内容密钥。

该方法进一步包括将复制标志记录在第二存储媒体的预定区域中。

根据本发明的另一个方面，提供了从第一存储媒体中再现利用加密第一内容密钥加密的数据的方法，该方法包括利用存储在第一存储媒体中的盘信

息再现第二内容密钥；利用第二内容密钥解密加密第一内容密钥；和利用解密第一内容密钥解密加密数据，其中，第一内容密钥是利用可以利用存储在第一存储媒体中的盘信息再现的第二内容密钥加密的，并且，存储在第一存储媒体中。

从现在开始，参照附图详细描述本发明的示范性实施例。

图 2 例示了根据本发明一个实施例的将数据从第一个盘 210 复制到第二个盘 250 的方法。第一个盘 210 存储盘信息 212 和加密内容 E(K1, Contents) 214。用于再现内容密钥 K1 262 的盘信息 212 包括盘标识符（ID）和更新密钥块。内容 E(K1, Contents) 214 是利用内容密钥 K1 262 加密的。存储在第一驱动器 220 中的驱动器信息 222 包括驱动器 ID、设备密钥组、和加密媒体密钥。

当将第一个盘 210 装入第一驱动器 220 中时，第一驱动器 220 的密钥生成单元 260 再现内容密钥 K1 262。接着，第一驱动器 220 的密钥加密单元 270 利用第二驱动器 240 的公开密钥 K_pub_dev2 264 加密内容密钥 K1 262，因此获得加密内容密钥 E(K_pub_dev2, K1) 272。利用公开密钥基础设施（未示出）将第二驱动器 240 的公开密钥 K_pub_dev2 264 从第二驱动器 240 发送到第一驱动器 220。

通过主机 230 将加密内容密钥 E(K_pub_dev2, K1) 272 发送到第二驱动器 240。

此外，将存储在第一个盘 210 中的加密内容 E(K1, Contents) 214 依次发送到第一驱动器 220、主机 230、和第二驱动器 240，然后，记录在第二个盘 250 上。在发送期间，对加密内容 E(K1, Contents) 214 既不解密也不加密。尤其，将加密内容 E(K1, Contents) 214 发送到主机 230，从而防止它被未授权用户篡改。

当将第二个盘 250 装入第二驱动器 240 中时，第二驱动器 240 利用盘信息 252 和驱动器信息 242 再现内容密钥 K2 282。与第一驱动器 220 不同，第二驱动器 240 再现的内容密钥 K2 282 不用在加密内容中。也就是说，由于没有解密过程地将存储在第一个盘 210 中的加密内容 E(K1, Contents)作为加密内容 E(K1, Contents) 254 记录在第二个盘 250 上，不需要另外的加密过程，因此，不使用内容密钥 K2 282。

将第一驱动器 220 利用第二驱动器 240 的公开密钥 264 加密的加密内容

密钥 E(K_pub_dev2, K1) 272 发送到第二驱动器 240 的密钥解密单元 290。密钥解密单元 290 利用第二驱动器 240 的秘密密钥 284 解密该加密内容密钥 E(K_pub_dev2, K1) 272，因此获得第一驱动器 220 的内容密钥 K1 291。

将内容密钥 K1 291 发送到第二驱动器 240 的密钥加密单元 292。接着，密钥加密单元 292 通过利用密钥生成单元 280 再现的第二驱动器 240 的内容密钥 K2 282 加密内容密钥 K1 291，获取第一驱动器 220 的加密内容密钥 E(K2, K1) 294。将加密内容密钥 E(K2, K1) 294 记录在第二个盘 250 上。

在记录在第二个盘 250 上之前，已经利用第一驱动器 220 的内容密钥 K1 262，而不是第二驱动器 240 的内容密钥 K2 282 加密了加密内容 E(K1, Contents) 254。因此，必须通知将从第二个盘 250 中再现加密内容 E(K1, Contents) 254 的第三驱动器（未示出）加密内容 E(K1, Contents) 254 是利用内容密钥 K1 262 加密的，而不是利用内容密钥 K2 282 加密的。因此，第二个盘 250 进一步存储代表这种信息的盘复制标志 296。将盘复制标志 296 记录在第二个盘 250 的导入区中。例如，当盘复制标志 296 被设置成预定值，例如，1 时，必须明白，内容 E(K1, Contents) 254 是利用从第一个盘 210 中，而不是从存储内容 E(K1, Contents) 254 的第二个盘 250 中再现的内容密钥 K1 262 加密的。

图 3 是例示图 2 的方法的流程图。参照图 3，第一驱动器 220 再现内容密钥 K1 262（步骤 310）。接着，第一驱动器 220 利用第二驱动器 240 的公开密钥 K_pub_dev2 264 加密内容密钥 K1 262。在加密内容密钥 K1 262 之前，利用公开密钥基础设施将第二驱动器 240 的公开密钥 K_pub_dev2 264 从第二驱动器 240 发送到第一驱动器 220。

在步骤 320 之后，通过主机 230 将经过加密和记录在第一个盘 210 上的内容 E(K1, Contents)、和第一驱动器 210 的加密内容密钥 E(K_pub_dev2, K1) 272 发送到第二驱动器 240（步骤 330）。

接着，第二驱动器 240 再现内容密钥 K2 282（步骤 340）。

接着，第二驱动器 240 通过利用第二驱动器 240 的秘密密钥 K_pri_dev2 284 解密第一驱动器 220 的加密内容密钥 E(K_pub_dev2, K1) 272，恢复第一驱动器 220 的内容密钥 K1 291（步骤 350）。

利用内容密钥 K2 282 加密第一驱动器 220 的恢复内容密钥 K1 291（步骤 360）。

接着，第二驱动器 240 将记录在第二个盘 250 的导入区中的盘复制标志 296 设置成 1（步骤 370）。

接着，第二驱动器 240 将从主机 230 发送的加密内容 E(K1, Contents) 和加密内容密钥 E(K2, K1)记录在第二个盘 250 上（步骤 380）。

返回到图 2，第一驱动器 220 利用驱动器信息 222 和存储在第一个盘 210 中的盘信息 212 再现内容密钥 K1 262，和第二驱动器 240 利用驱动器信息 242 和存储在第二个盘 250 中的盘信息 252 再现内容密钥 K2 282。

现在参照图 4 描述根据本发明一个实施例的利用驱动器生成内容密钥的方法。图 4 例示了根据存储在装入驱动器 410 中的盘 420 中的信息，利用驱动器 410 生成内容密钥 K_{cont} 的方法。内容密钥 K_{cont} 对应于图 2 的第一驱动器 220 的内容密钥 K1 262 或图 2 的第二驱动器 240 的内容密钥 K2 282。如果内容密钥 K_{cont} 是内容密钥 K1 262，它可以用于加密内容，和如果内容密钥 K_{cont} 是内容密钥 K2 282，它可以用于加密被用于加密内容的内容密钥。

在图 4 中，设备标识符 ID_{device} 402、设备密钥组 K_{dev} 404、记录随机数 $Seed_{rec}$ 409、和媒体密钥 K_m 406 对应于图 2 的盘信息 222 或 242。更新密钥块 422、加密盘密钥 K_{ed} 424、和记录随机数 $Seed_{rec}$ 428 对应于图 2 的盘信息 212 或 252。这里，设备表示包括盘驱动器的记录/再现装置。

设备标识符 ID_{device} 402 是盘驱动器（未示出）的标识号，和设备密钥组 K_{dev} 404 是在盘制造期间依次存储在盘驱动器中以防盘驱动器被非法复制的一组密钥。更新密钥块 422 是内容提供者提供给授权盘驱动器以便只允许授权盘驱动器生成媒体密钥 K_m 406 的信息。也就是说，更新密钥块 422 和设备密钥组 K_{dev} 404 防止媒体密钥 K_m 406 被未授权盘驱动器再现。当检测到非法复制的盘驱动器时，更新密钥块 422 被更新，并且提供给授权盘驱动器，从而防止非法复制的盘驱动器再现存储在盘 420 中的信息。

媒体密钥 K_m 406 是利用设备标识符 ID_{device} 402、设备密钥组 K_{dev} 404、和从盘 420 中读取的更新密钥块 422，在驱动器 410 中生成的。此外，媒体密钥生成算法不允许非法复制的盘驱动器再现媒体密钥 K_m 406。这样的媒体密钥生成算法是本领域的普通技术人员所熟知的，因此，这里省略对它们的详细描述。

经过加密和存储在盘 420 中的加密盘密钥 K_{ed} 424 用于保护内容的版权或提供有关盘制造者的信息。盘密钥 K_d 408 是利用媒体密钥 K_m 406 加密的，由

盘制造者存储在盘 420 中。盘密钥 K_d 408 是利用媒体密钥 K_m 406，在驱动器 410 中加密的。

记录随机数 $Seed_{rec}$ 409 是为每次事务处理生成的随机数。记录随机数 $Seed_{rec}$ 409 在驱动器 410 中生成以便用在再现内容密钥 K_{cont} 中，并且记录在盘 420 中，以便除了驱动器 410 之外的其它驱动器可以再现内容密钥 K_{cont}。

作为盘标识号的盘标识符 ID_{disc} 426 记录在盘 420 的导入区中。

上面所有或部分盘信息和驱动器信息可以用于生成内容密钥 K_{cont}。用盘信息还是驱动器信息生成内容密钥 K_{cont} 由加密政策决定。例如，当在确定内容密钥 K_{cont} 是否可用的过程中不需要有关盘制造者的信息时，加密盘标识符 ID_{disc} 426 既不存储在盘 420 中，也不用在生成内容密钥 K_{cont} 中。

授权设备被赋予相同的驱动器信息的设备密钥组 K_{dev} 404 和媒体密钥 K_m 406。只有盘信息的盘标识符 ID_{disc} 426 和记录随机数 $Seed_{rec}$ 428 可以用于标识盘 420。因此，即使将盘 420 装入除了驱动器 410 之外的其它驱动器中，当除了驱动器 410 之外的其它驱动器被确定为是真的时，也可以再现内容密钥 K_{cont}。

图 5 例示了根据本发明一个实施例的从原始盘（未示出）中复制加密内容 E(K, Contents)的可记录盘 500 的数据结构。参照图 5，复制标志 510 表示记录在盘 500 上的加密内容 E(K, Contents)是利用原始盘的内容密钥 K，而不是盘500的内容密钥Kp加密的。从盘500中再现加密内容E(K, Contents)的驱动器（未示出）引用复制标志 510。这里，盘 500 的内容密钥 Kp 是盘驱动器（不是用于数据复制的盘驱动器）根据存储在盘 500 中的盘信息再现的，和原始盘的内容密钥 K 是根据存储在原始盘中的盘信息再现的。

复制标志 510 和加密密钥 E(Kp, K) 520 存储在盘 500 的预定区域中。在本实施例中，预定区域可以是盘 500 的导入区或保留区。

图 6 是例示利用除了用于数据复制的驱动器之外的其它驱动器，从存储在原始盘中的信息复制到其中的盘 610 中再现加密内容 E(K1, Contents) 616 的方法。盘 610 是与图 2 的盘 250 相对应的复制盘。

与传统盘复制方法不同，除了加密内容 E(K1, Contents) 616 之外，盘 610 还存储复制标志 612 和加密内容密钥 E(K2, K1) 614。

驱动器 620 包括密钥生成单元 622、密钥解密单元 624、和内容解密单元 626。当将盘 610 装入驱动器 620 中时，密钥生成单元 622 根据存储在盘 610

中的盘信息和有关驱动器 620 的驱动器信息再现内容密钥 K2。

密钥解密单元 624 从装入盘 610 中读取加密内容密钥 E(K2, K1) 614，和通过用内容密钥 K2 解密加密内容密钥 E(K2, K1) 614 再现解密内容密钥 K1。

内容解密单元 626 从盘 610 中读取加密内容 E(K1, Contents) 616，通过用解密内容密钥 K1 解密加密内容 E(K1, Contents)生成解密内容 632，和将解密内容 632 发送到主机 630。

如上所述，图 6 例示了解密和再现利用原始盘的内容密钥，而不是盘 610，即，复制盘的内容密钥 K1 加密的内容 E(K1, Contents)的方法。让我们假设当利用原始盘的内容密钥，而不是盘 610 的内容密钥 K1 加密内容 E(K1, Contents)时，将复制标志 612 设置成 1，否则，将复制标志 612 设置成 0。如果复制标志 612 被设置成 0，即，当盘 610 不是复制盘时，驱动器 620 像参照图 1 所述的那样，再现内容密钥 K2 和利用内容密钥 K2 解密加密内容 E(K1, Contents)。

图 7 是例示图 6 的方法的流程图。参照图 7，将作为复制盘的盘 610 装入驱动器 620 中，驱动器 620 像参照图 1 所述那样，从盘 610 中读取盘信息和根据盘信息和它的驱动器信息再现盘 610 内容密钥 K2（步骤 710）。

接着，驱动器 620 检验存储在盘 610 的预定区域中的复制标志 612（步骤 720）。如果复制标志 612 被设置成 0，驱动器 620 利用内容密钥 K2 解密存储在盘 610 中的加密内容 E(K1, Contents)（步骤 735）和将解密结果发送到主机 630（步骤 760）。

如果复制标志被设置成 1，驱动器 620 从盘 610 的预定区域中读取加密内容密钥 E(K2, K1)和加密内容 E(K1, Contents)（步骤 730）。

接着，驱动器 620 通过利用在步骤 710 中再现的内容密钥 K2 解密在步骤 730 中读取的加密内容密钥 E(K2, K1)，再现内容密钥 K1（步骤 740）。

接着，驱动器 620 通过利用内容密钥 K1 解密加密内容 E(K1, Contents)，获取解密内容 632(步骤 750)，和将解密内容 632 发送到主机 630(步骤 760)。

在本发明中，存储媒体包括诸如激光唱盘（CD）、数字多功能盘（DVD）、和蓝光盘之类的一次性写入存储媒体或可重写存储媒体。

虽然通过参照本发明的示范性实施例，已经对本发明进行了具体图示和描述，但本领域的普通技术人员应该明白，可以在形式和细节上对其作各种各样的改变，而不偏离所附权利要求书限定的本发明的精神和范围。

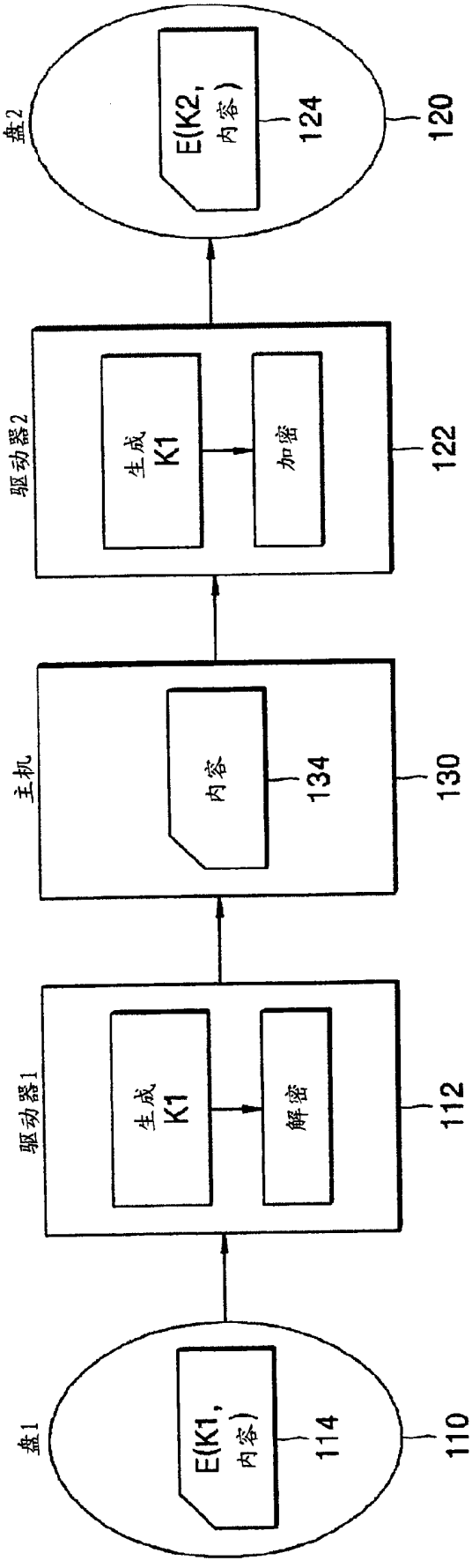

盘1
E(K1, 内容)
114
110
驱动器1
生成 K1
解密
112
主机
内容
134
130
驱动器2
生成 K1
加密
122
盘2
E(K2, 内容)
124
120

图 1

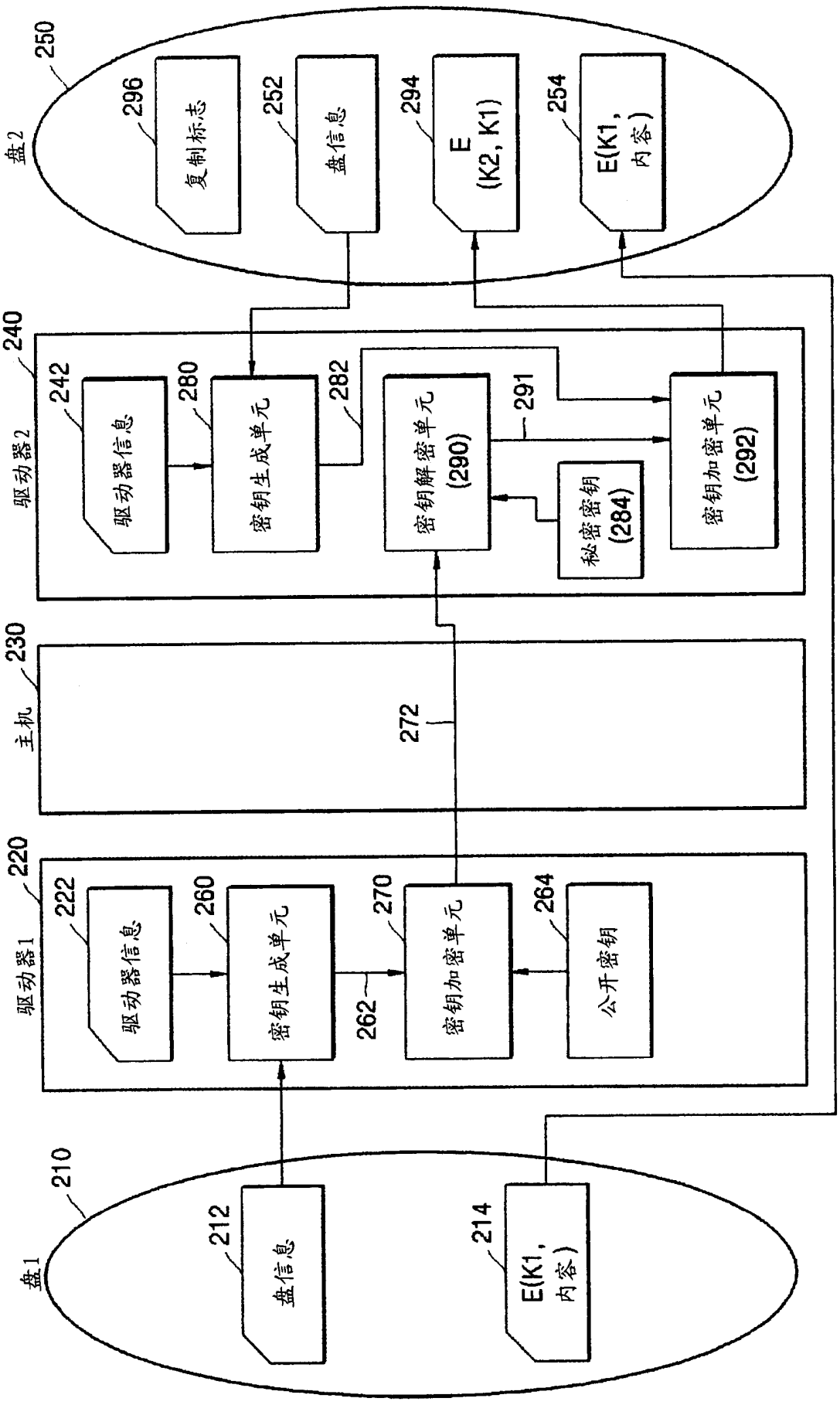

盘1
210
盘信息
212
E(K1, 内容)
214
驱动器1
220
驱动器信息
222
密钥生成单元
260
密钥加密单元
270
公开密钥
264
262
主机
230
272
驱动器2
240
驱动器信息
242
密钥生成单元
280
282
密钥解密单元 (290)
291
秘密密钥 (284)
密钥加密单元 (292)
盘2
250
复制标志
296
盘信息
252
E (K2, K1)
294
E(K1, 内容)
254

图 2

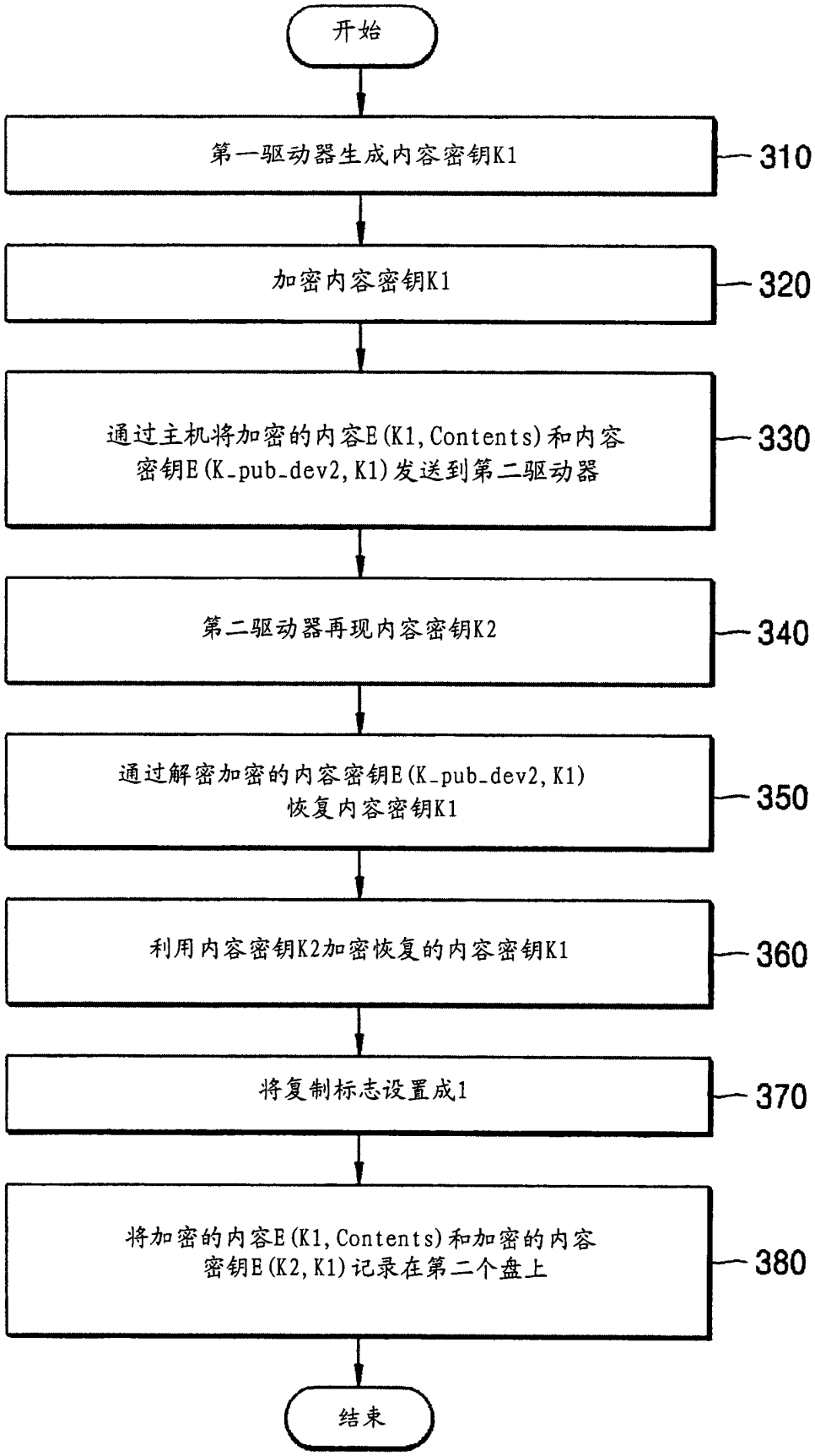

开始
第一驱动器生成内容密钥K1
310
加密内容密钥K1
320
通过主机将加密的内容E(K1,Contents)和内容密钥E(K_pub_dev2,K1)发送到第二驱动器
330
第二驱动器再现内容密钥K2
340
通过解密加密的内容密钥E(K_pub_dev2,K1)恢复内容密钥K1
350
利用内容密钥K2加密恢复的内容密钥K1
360
将复制标志设置成1
370
将加密的内容E(K1,Contents)和加密的内容密钥E(K2,K1)记录在第二个盘上
380
结束

图 3

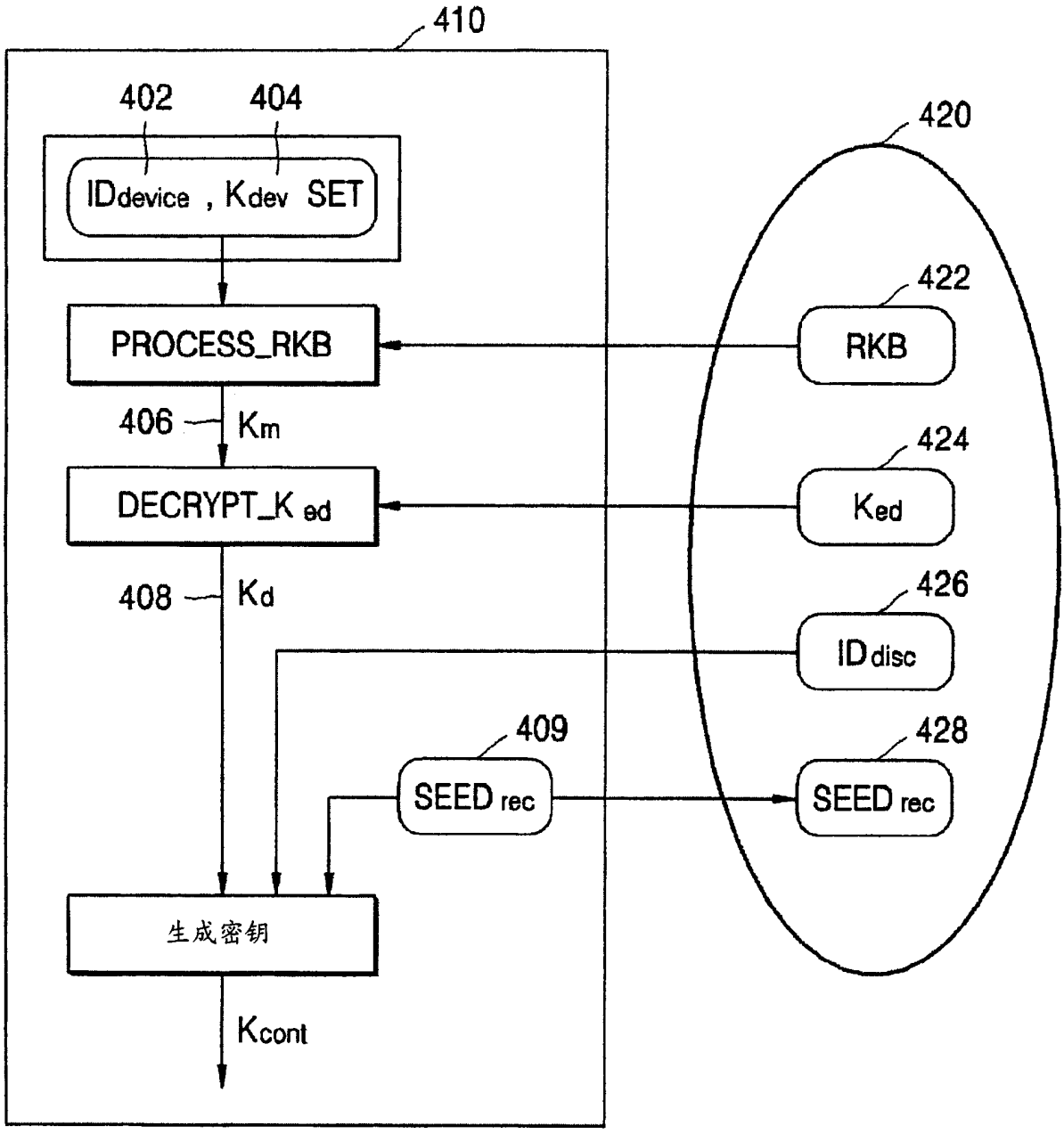

410
402
404
IDdevice , Kdev SET
PROCESS_RKB
406
Km
DECRYPT_K ed
408
Kd
生成密钥
Kcont
420
422
RKB
424
Ked
426
ID disc
409
SEED rec
428
SEED rec

图 4

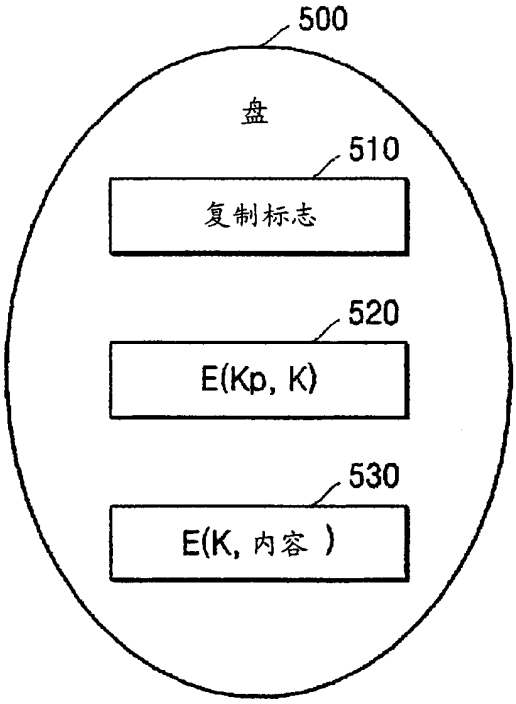

500
盘
510
复制标志
520
E(Kp, K)
530
E(K, 内容)

图 5

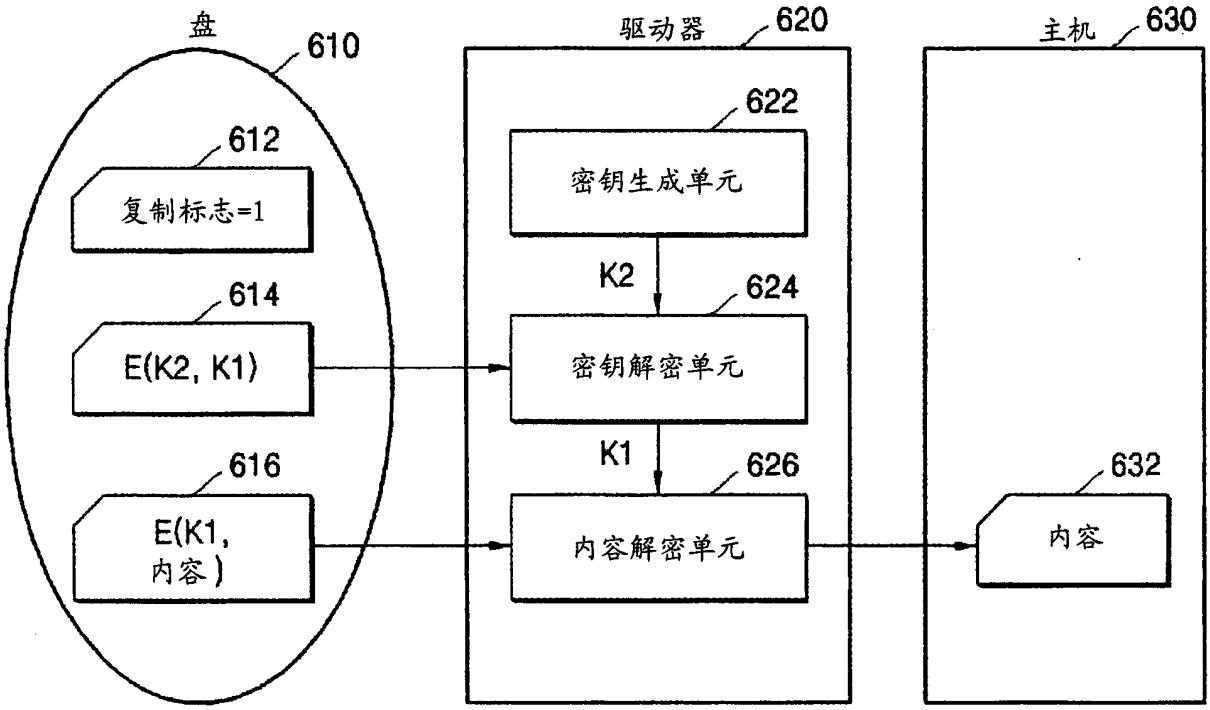

盘
610
612
复制标志=1
614
E(K2, K1)
616
E(K1,
内容)
驱动器
620
622
密钥生成单元
K2
624
密钥解密单元
K1
626
内容解密单元
主机
630
632
内容

图 6

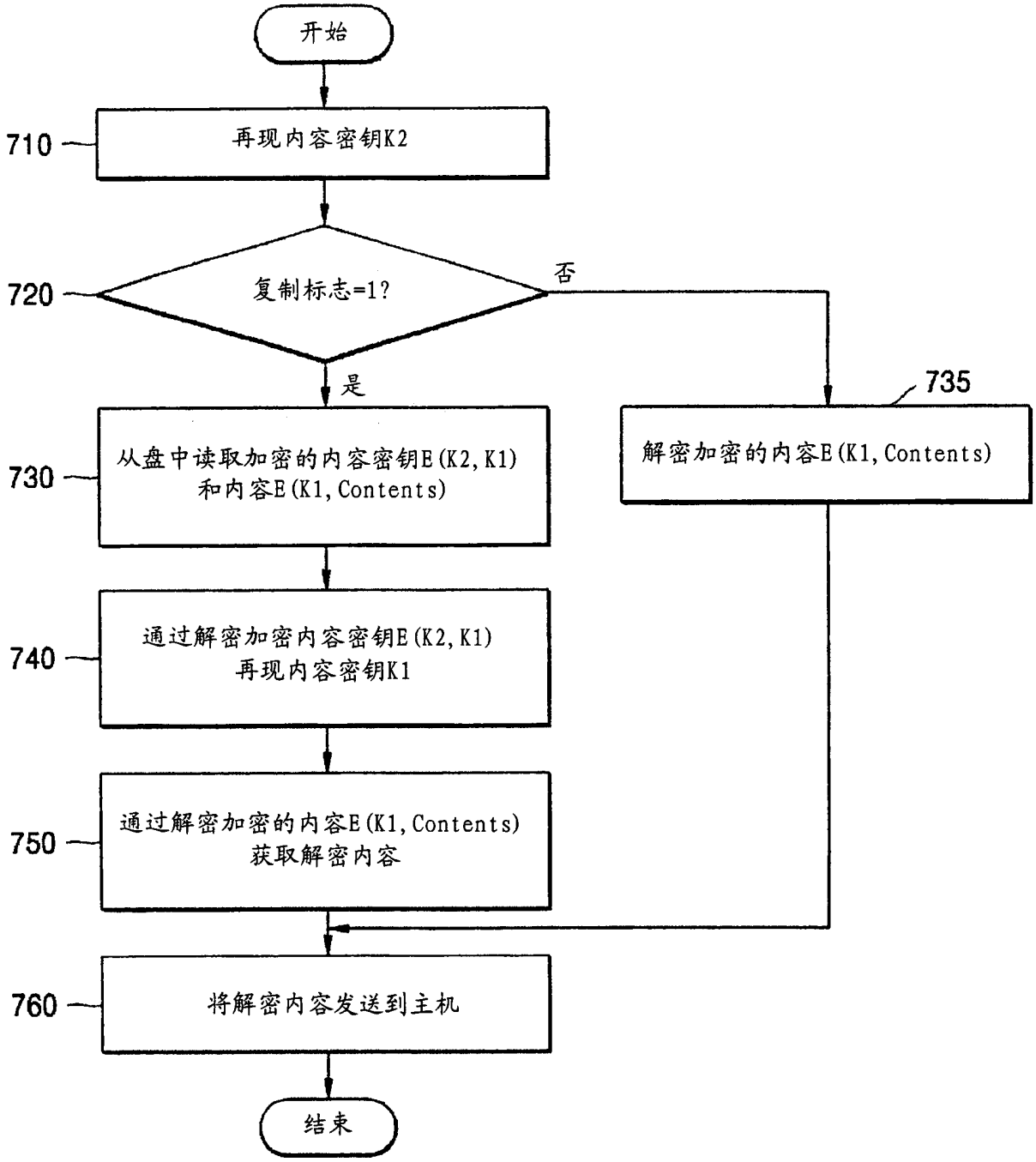

开始
710
再现内容密钥K2
720
复制标志=1?
否
是
735
解密加密的内容E(K1, Contents)
730
从盘中读取加密的内容密钥E(K2, K1)
和内容E(K1, Contents)
740
通过解密加密内容密钥E(K2, K1)
再现内容密钥K1
750
通过解密加密的内容E(K1, Contents)
获取解密内容
760
将解密内容发送到主机
结束

图 7