(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 101103585 B
(45)授权公告日 2012.07.18

(21)申请号 200680002047.5

(22)申请日 2006.01.09

(30)优先权数据
10/905,570 2005.01.11 US

(85)PCT申请进入国家阶段日
2007.07.10

(86)PCT申请的申请数据
PCT/EP2006/050099 2006.01.09

(87)PCT申请的公布数据
WO2006/074987 EN 2006.07.20

(73)专利权人 国际商业机器公司
地址 美国纽约
专利权人 华特迪士尼公司

(72)发明人 杰弗里·B.·鲁特斯皮奇
斯科特·F.·沃森

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 康建忠

(51)Int.Cl.
H04L 9/00(2006.01)
H04L 9/08(2006.01)

(56)对比文件
CN 1525452 A,2004.09.01, 说明书第96页第32行-第97页第4行、摘要.
CN 1389041 A, 说明书第11页第26行-第12页第30行, 第19页第16行-第30页第28行、图1,7,11,14A-23.
WO 03/049106 A2,2003.06.12, 第6页第22行-第7页第12行, 第9页第6行-第10页第32行、图1,6,7A,7B.

审查员 陈娟

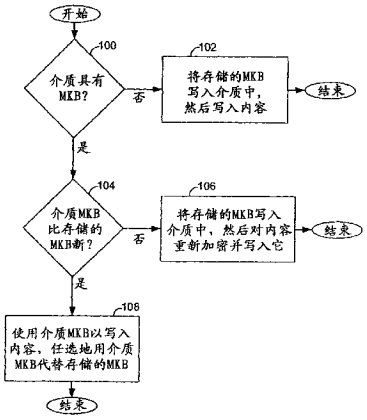
权利要求书 2 页 说明书 5 页 附图 1 页

(54)发明名称

通过介质密钥块的验证控制对被保护数字内容的访问的系统和方法

(57)摘要

一种记录器系统包含介质密钥块(MKB)并根据以下内容保护逻辑选择性地将被保护的内容写入记录介质中以防止对被保护内容的盗用:如果介质没有MKB,那么记录器将其存储的MKB写入介质中并将保护的内容写入介质中;如果介质具有比记录器中的存储的MKB旧的MKB,那么记录器将存储的MKB写入介质中,然后对保护的内容进行重新加密并将其写入介质中。如果介质具有比存储的MKB新的MKB,那么介质中的MKB被用于内容保护。记录器可将新的MKB存储在非易失性存储器中,从而有效地更新其以前存储的MKB,因此记录器将具有最新的MKB用于内容保护。



CN 101103585 B

1. 一种计算机实现的方法，用于通过记录介质中的介质密钥块 (MKB) 的验证控制对被保护的数字内容的访问，该方法包括 ：

a) 在记录装置中存储只读 MKB，其中介质包含唯一的介质 ID，其中所述介质 ID 包括唯一 ID 和用只在具有许可时可得到的秘密密钥对该唯一的 ID 的加密，记录装置利用所述介质 ID 存储被保护的数字内容 ；

b) 如果介质没有 MKB，那么在将内容写入介质之前将存储的只读 MKB 写到介质上 ；

c) 如果介质具有比存储的只读 MKB 旧的 MKB，那么将存储的只读 MKB 写入介质中、对内容进行重新加密并将其写入介质中 ；和

d) 如果介质具有比存储的只读 MKB 新的 MKB，那么使用介质中的 MKB 用于内容保护。

2. 根据权利要求 1 的方法，其中，重新加密包含用基于新介质密钥的密钥对介质中的所有标题进行重新加密。

3. 根据权利要求 1 或 2 的方法，其中，步骤 d 还包含在记录装置中的非易失性存储器中用新的 MKB 代替存储的只读 MKB。

4. 根据权利要求 3 的方法，其中，记录装置使用不同的格式专用 MKB 用于不同地格式化的内容。

5. 根据权利要求 3 的方法，其中，记录装置将验证 MKB 写入介质中。

6. 根据权利要求 3 的方法，其中，MKB 在介质中的预定位置上。

7. 根据权利要求 3 的方法，其中，记录装置仅对已知的格式更新 MKB。

8. 根据权利要求 3 的方法，其中，如果记录装置在写入过程中失败，那么备份 MKB 协议保护内容。

9. 根据权利要求 3 的方法，其中，验证 MKB 在制造过程中被写入介质中。

10. 根据权利要求 1 的方法，其中，如果使用秘密密钥对加密的唯一的 ID 的解密与唯一 ID 匹配，则介质被确认。

11. 一种用于通过记录介质中的介质密钥块 (MKB) 的验证控制对被保护的数字内容的访问的系统，包括 ：

a) 用于在记录装置中存储只读 MKB 的装置，其中介质包含唯一的介质 ID，其中所述介质 ID 包括唯一 ID 和用只在具有许可时可得到的秘密密钥对该唯一的 ID 的加密，记录装置利用所述介质 ID 存储被保护的数字内容 ；

b) 用于在介质没有 MKB 的情况下，在将内容写入介质之前将存储的只读 MKB 写入介质中的装置 ；

c) 用于在介质具有比存储的只读 MKB 旧的 MKB 的情况下，将存储的只读 MKB 写入介质中、对内容进行重新加密并将其写入介质中的装置 ；和

d) 用于在介质具有比存储的只读 MKB 新的 MKB 的情况下，使用介质中的 MKB 用于内容保护的装置。

12. 根据权利要求 11 的系统，其中，重新加密包含用基于新介质密钥的密钥对介质中的所有标题进行重新加密。

13. 根据权利要求 11 或 12 的系统，其中，记录装置在记录装置中的非易失性存储器中用新的 MKB 代替存储的只读 MKB。

14. 根据权利要求 13 的系统，其中，记录装置使用不同的格式专用 MKB 用于不同地格式

化的内容。

15. 根据权利要求 13 的系统，其中，记录装置将验证 MKB 写入介质中。

16. 根据权利要求 13 的系统，其中，MKB 在介质中的预定位置上。

17. 根据权利要求 13 的系统，其中，记录装置仅对已知的格式更新 MKB。

18. 根据权利要求 13 的系统，其中，如果记录装置在写入过程中失败，那么备份 MKB 协议保护内容。

19. 根据权利要求 13 的系统，其中，验证 MKB 在制造过程中被写入介质中。

20. 根据权利要求 11 的系统，其中，如果使用秘密密钥对加密的唯一的 ID 的解密与唯一 ID 匹配，则介质被确认。

通过介质密钥块的验证控制对被保护数字内容的访问的系统和方法

技术领域

[0001] 本发明一般涉及用于控制对被保护内容的访问、特别是用于可记录介质的加密密钥的管理。

背景技术

[0002] 数字化视频和音乐有很多优点，但一个明显的缺陷是，由于被数字化，因此内容比较容易在没有版权所有人的授权的情况下被完全复制。对内容的盗用当前每年给内容供给者造成几十亿美元的损失。因此，已开发了很多方案以解决该问题，但对于给定的大量的内容实例和处理内容的装置不是所有的方案都是实用的。

[0003] 美国专利 No.6118873 提供用于安全广播程序、包含对授权的家用数字视频装置的更新的加密系统。该专利公开了用于对广播音乐、视频和其它内容加密的系统，使得只有被授权的播放器 - 记录器并且只有根据由内容的销售商建立的规则才能播放和 / 或复制内容。被授权的播放器或记录器从称为介质密钥块 (media key block)(MKB) 的装置密钥 (device key) 的矩阵被发放软件实现的装置密钥。这些密钥可相互同时或随着时间的过去被发放，但在任意情况下，没有播放器 - 记录器被认为每个矩阵列具有多于一个的装置密钥。虽然两个装置可能共享来自同一列的同一密钥，但当密钥被随机分配时，任意两个装置刚好共享来自所有矩阵列的同一组密钥的机会非常小。密钥被用于对内容解密。可通过以各种方式对将来的被保护内容进行加密使得特定选择的装置不能适当地对其解密，将装置“废除 (revoke)”。

[0004] 在可记录介质的情况下，内容保护常规上基于在各介质实例上具有介质密钥块（在本申请中，术语“介质”可指特定的数据存储产品或多个这种数据存储产品）。该 MKB 允许相容的装置计算适当的介质密钥，同时防止欺骗装置这样做。迄今为此，重要的是，MKB 是只读型的，尽管其余的介质，当然，是读 / 写型即可记录型的。MKB 需要是只读型的是因为以下的所谓的“低级介质”攻击 ：如果 MKB 是读 / 写型的，那么攻击者可在介质上写入旧的破坏的 MKB，然后要求相容的 (compliant) 装置对攻击者所关心的内容加密和记录。由于 MKB 被破坏，因此攻击者知道介质密钥并可对该内容进行解密。攻击者因此不受阻碍地得到被保护内容，从而有效地挫败内容保护方案的目标。

[0005] 但是，在读 / 写介质上具有只读区域常常是有问题的。例如，在 DVD-RAM、DVD-R 和 DVD-R/W 介质中，MKB 被预先刻录 (pre-emboss) 到作为不被记录器写入的盘的一部分的导入区上。导入区具有有限的容量。因此，该方法固有地限制 MKB 的大小，由此限制可被废除的欺骗装置的数量。在 DVD+R 和 DVD+R/W 介质的情况下，导入区是读 / 写型的。在该技术中使用的方法是只将 MKB 的摘要写入“烧刻区 (BCA)”中，该烧刻区是接近盘的盘毂 (hub) 的非常有限的只读区。不幸的是，写入 BCA 中对各盘的成本增加额外的 0.05 美元。

[0006] 可能更严重的问题是，这些方法要求盘复制人涉及该过程。不是所有的盘复制人都希望变为给定内容保护方案的被许可人，因此至今各种类型的介质都有两种版本 ：一个

具有 MKB，一个没有。由于只有包含 MKB 的介质可被用于记录被保护内容，因此存在消费者弄混的很大的可能性。并且，盘复制人必须受许可约束，以不用同一 MKB 生产许多盘。如果这样做了，那么该 MKB 的介质密钥会变为严重的公开秘密 (global secret)，其妥协结果是可对内容保护方案造成严重损害。但是，由于复制的成本强烈依赖于可制成的相同复制品的数量，因此涉及成本 / 安全性折衷。至今，所做的该折衷完全偏重于低成本 ：复制人被允许使用单一 MKB 一百万次。

发明内容

[0007] 因此，提供一种通过记录介质中的介质密钥块 (MKB) 的验证防止被保护数字内容的盗用的计算机实现的方法，该方法包括 ：a) 在记录装置中存储 MKB ；b) 如果介质没有 MKB，那么在将内容写入介质之前将存储的 MKB 写到介质上 ；c) 如果介质具有比存储的 MKB 旧的 MKB，那么将存储的 MKB 写入介质中、对内容进行重新加密并将其写入介质中 ；和 d) 如果介质具有比存储的 MKB 新的 MKB，那么使用介质中的 MKB 用于内容保护。

[0008] 本发明提供存储在各记录器装置上的只读 MKB 而不是在来自盘复制人的空白介质上具有只读 MKB。记录器装置根据存储的 MKB 和可存在于记录介质中的任何 MKB 的时间选择性地将被保护数字内容写到记录介质上。如果在介质中没有 MKB，那么记录器将其存储的 MKB 写入介质中并然后前进到写入被保护内容。如果介质中的 MKB 比存储的 MKB 旧，那么记录器将存储的 MKB 写入介质中然后对保护的内容重新加密并然后写入它，从而消除被破坏的旧的 MKB 可被用于盗版的可能性。如果介质中的 MKB 比存储的 MKB 新，那么记录器使用该新的 MKB 用于写入被保护内容，但可任选地用该新的 MKB 更新其存储的 MKB，从而消除被破坏的旧的 MKB 可被用于盗版的可能性。

[0009] 优选地，提供一种用于防止盗用被保护数字内容的系统，该系统包括存储介质密钥块 (MKB) 并根据包含以下逻辑的逻辑规则选择性地将内容写入介质中的记录装置 ：如果介质没有 MKB，那么在将内容写入介质之前将存储的 MKB 写入介质中 ；如果介质具有比存储的 MKB 旧的 MKB，那么将存储的 MKB 写入介质中、对内容进行重新加密并将其写入介质中 ；如果介质具有比存储的 MKB 新的 MKB，那么使用介质中的 MKB 用于内容保护。

[0010] 具有唯一介质 ID 或序列号的任何可记录介质可被系统使用以存储被保护内容。制造过程中的介质的成本上的变化可被避免，并且对 MKB 的大小的限制被有效消除。

附图说明

[0011] 现在仅作为例子参照在以下附图中示出的本发明的优选实施例说明本发明 ：

[0012] 图 1 是根据本发明的实施例的、通过介质密钥块确认防止盗用被保护数字内容的步骤的流程图。

具体实施方式

[0013] 在示例性实施例中，本发明通过具有存储在各记录器装置中的只读 MKB 而不是在来自盘复制人的空白介质上具有只读 MKB 消除上述困难。记录器可选择性地将存储的 MKB 写到介质上。在本领域中存在几种已知的用于有效地使得装置能够在密码上 (cryptographically) 确定两个密钥中的哪一个是更新的，因此本发明利用这些方案以帮

助解决上述的常规方法的问题。参见例如美国专利No.5081677和美国专利No.5412723,这些专利说明被周期性“刷新”用于提高安全性的加密密钥用版本号的使用。但注意,本发明不限于任何特定的用于确定密钥或MKB的相对新旧的方案。

[0014] 因此,现在参照图1并根据本发明,当记录器被要求记录一段被保护的内容时,在记录器中遵循的内容保护逻辑如下:

[0015] 1.如果在步骤100中确定介质没有MKB,那么在步骤102中,记录器首先将其自身的MKB写入介质中,然后写入由MKB保护的内容。

[0016] 2.否则,在步骤104中记录器将在介质上存在的MKB与其自身的MKB相比较。如果介质上的MKB旧,那么在步骤106中记录器用其自身的MKB代替介质上的MKB。作为该代替的一部分,记录器必须用基于新的(即,记录器的)介质密钥的密钥对当前在介质上存在的所有标题进行重新加密。

[0017] 3.如果介质上的MKB新,那么在步骤108中记录器使用介质上的而不是其自身的MKB。如果记录器具有其自身的内部非易失性存储器,那么它可在该存储器中存储该新的MKB,然后从该点开始使用该新的MKB作为其自身的MKB用于内容保护。

[0018] 因此,使用本发明,MKB不再有任何实际的大小限制。并且,任意的空白介质,只要具有唯一的序列号或介质ID,都可被用作内容保护的介质,因此可避免消费者弄混。(如果克隆的序列号被使用,那么这些相同的介质可被用于仅仅通过进行位对位(bit-for-bit)复制进行未授权的复制。)最后,由于记录器-播放器装置已使用可编程的只读存储器用于唯一的装置密钥,因此每个装置具有唯一的MKB只会需要稍多的可编程存储器,而不需要新的、成本高的盘制造步骤。因此,使用本发明,介质密钥可变为公开秘密的机会会大大降低。

[0019] 但存在一些微妙之处。如果MKB改变,那么每个被加密的标题密钥必须被更新,并且记录器一般不知道内容的所有可能的格式。它们不知道对于所不知的格式被加密的标题密钥被存储在哪里,并因此不能够在它们改变MKB时对它们进行重新加密。该问题简单地通过具有用于不同格式的不同MKB被解决。记录器只更新其理解的格式的MKB。但是,“备份MKB”协议可被限定,使得如果记录器在更新过程中失败,内容不丢失。示例性的备份MKB协议如下:

[0020] 如果被加密的标题密钥在单一文件中,那么记录器通过以下的这些逻辑步骤在开始写入新的加密标题密钥文件之前,将旧的加密标题密钥重命名为定义的备份名称:

[0021] 1.检查是否备份MKB和备份加密标题密钥文件是否都存在。如果它们都存在,那么前进到步骤2,否则擦除剩余的备份文件并退出。

[0022] 2.如果当前的MKB不存在或是毁坏,那么将备份MKB和备份加密标题密钥文件重命名为当前的文件并退出。

[0023] 3.通过使用备份MKB对备份标题解密文件中的标题密钥进行解密,并通过使用当前的MKB对标题密钥重新加密,写入当前的标题密钥文件。

[0024] 4.删除备份MKB和备份标题密钥文件,修改与备份加密标题密钥文件相关的任何现时文件(nonce)。

[0025] 在一些应用中,可在多于一个的文件中发现加密标题密钥。在这种情况下,记录器单独地为各文件运行备份协议,在所有标题密钥文件都得到处理之前不删除备份MKB。

[0026] 并且，如果 MKB 只是文件系统中的文件，那么对于记录器来说可能很难发现它（即，对于光学介质，盘驱动验证要求盘读取 MKB，但从哪里？）。盘驱动器不习惯于理解盘上的文件系统的格式，并且会偏好简单地访问盘上的固定位置上的数据。可以通过除了将 MKB 以逻辑的方式放在文件系统中以外还可通过盘格式操作将其放在盘上的预定位置上，适应这种偏好。随后的 MKB 可简单地在同一位置上覆写以前的 MKB。记录器必须不能接收没有被正确格式化的盘，并且必须能够将它们自身格式化并然后写入“验证 MKB”。出于其它原因，记录器必须确定无疑地执行格式化。验证 MKB 应是所有的格式特定的 MKB 之外的，并且记录器必须准备好更新它知道的任何 MKB。它总是知道验证 MKB。

[0027] 从历史上看，想要使用欺骗程序的攻击者保存旧的介质用于低级 (down-level) 介质攻击，因为他们希望那些 MKB 将被破坏。本发明改变针对内容保护方案的可能的攻击的本性。例如，在本领域的当前状态中，攻击者采用这种攻击，其中他们保存当方案被首次引入时问世的介质（在被废除之前）。一旦出现欺骗装置（例如，流氓记录器 (rogue recorder)），他们将被新介质废除，但仍将能够使用旧介质。然后，攻击者让相容的记录器在旧介质上记录内容。攻击者然后使用欺骗装置进行未授权的复制。该攻击在某种程度上通过攻击者必须避开的 MKB 扩展 (extension) 被避免，但 MKB 扩展总是任选的。

[0028] 在本发明中，类似的攻击进行如下：攻击者购买当方案被首次引入时问世的装置（而不是介质）。这些旧的记录器用旧的介质密钥块将介质格式化。攻击者让旧的装置记录内容，并然后使用欺骗装置进行未授权的复制。攻击者必须避免在新的记录器中使用特定的介质 - 如果记录器具有用于它们已发现的用于随后的写入用途的最新更新的 MKB 的非易失性存储器，那么攻击变得更加困难。

[0029] 如果流氓复制人克隆被认为是唯一的介质 ID 怎么办？在这种情况下，在现有技术和在本发明中，仅有的依靠是法律。考虑本领域的当前状态中的法律形势。如果复制人已许可了内容保护方案并构建克隆的介质，那么他违反了该许可。如果他不是被许可人，那么他违反了以下内容保护方案的知识产权：获得版权的 MKB、商业秘密和相关的专利。在任一种情况下，复制人可能被指控规避“技术保护手段”并在 U.S.Digital Millennium Copyright Act(DMCA) 下被起诉。

[0030] 本发明允许复制人不需要是内容保护方案的被许可人的可能性。如果复制人不需要为被许可人，那么所有的介质将均可用于内容保护，并且将很少出现用户弄混的机会。在这种情况下，如果复制人正在克隆，那么内容保护方案的所有人可能在法庭上没有法律地位，并且保护依靠 DMCA 的力量。但是，复制人必须一直是特定介质格式的被许可人。如果格式许可做出唯一 ID 必须实际上唯一的合理要求，那么法律形势回到本发明之前的方式。只是格式所有人而不是内容保护方案所有人现在是法律上遭受损失一方。

[0031] 如果由于一些原因该形势是不令人满意的，那么内容保护方案可添加一些可许可的要素到介质中。介质 ID 可被分成两个部分，例如，唯一的 ID 和用只在具有许可时可得到的秘密密钥对该 ID 的加密。播放器装置会被给予密钥，使得它们可检查两半匹配。播放器只会播放许可的介质。但是，由于该许可不再限制复制品的数量并且不需要现行的许可费，因此许可被认为不会使复制人承担过重的法律责任。所有复制人能够选择在这些条款下为被许可人，并且会避免消费者弄混。

[0032] 使复制人初始地在介质制造时记录验证 MKB 也在本发明的范围内。在这种情况

下，又出现消费者弄混问题，但是，由于上面提及的攻击现在同时要求旧介质和旧播放器成功，因此内容保护方案的安全性提高。

[0033] 通用计算机根据这里的创造性特征被编程。本发明还可体现为被数字处理装置使用以执行本发明的逻辑的制造的物品－机器部件。本发明在导致数字处理装置执行这里的创造性的方法步骤的关键机器部件中被实现。本发明可通过作为一系列计算机可执行指令被计算机内的处理器执行的计算机程序被体现。这些指令可驻留在例如计算机的 RAM 中或计算机的硬盘驱动器或光盘驱动器上，或者指令可被存储在 DASD 阵列、磁带、电子只读存储器或其它的适当的数据存储装置中。

[0034] 这里示出和说明的特定的读 / 写介质密钥块是本发明的目前优选的实施例，并因此代表本发明广泛设想的主题：本发明的范围完全包含对本领域技术人员变得十分明显的其它实施例，并且本发明的范围因此只是由所附的权利要求限制，在这些权利要求中，除非明确指出，提到的单数的元件目的不是意味着“有且仅有一个”，而是“一个或更多个”。本领域技术人员公知或以后变为公知的上述优选实施例的元件的所有结构性或功能性等同在这里明确地被包含作为参考，并且意图在于被本发明的权利要求包含。并且，对于装置或方法不必解决本发明寻求解决的各个或每个问题，这些问题的解决要由本发明的权利要求包含。并且，不管本公开的元件、部件或方法步骤是否在权利要求中被明确记载，该元件、部件或方法步骤目的都不在于专门针对公众。这里的权利要求要素，除非明确记载使用短语“用于 ... 的装置”，不应根据 35 U.S.C.112 第六段的条款被解释。

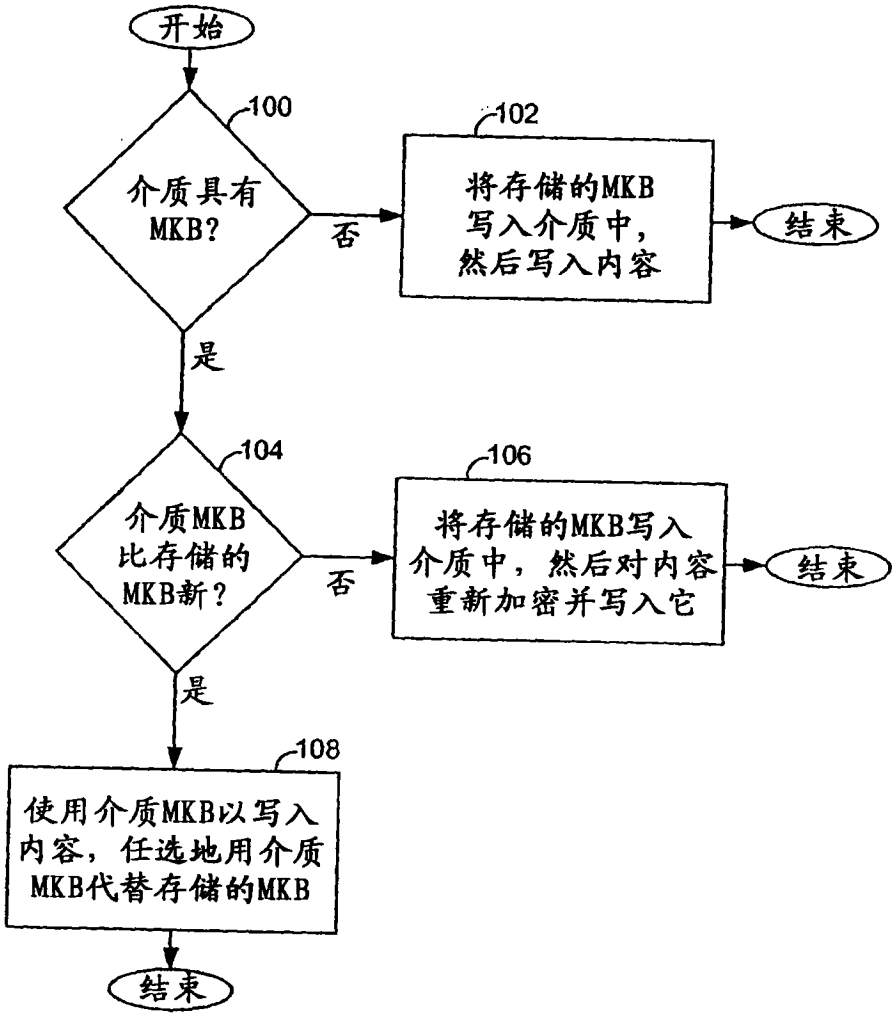

开始
100
介质具有MKB?
否
102
将存储的MKB写入介质中，然后写入内容
结束
是
104
介质MKB比存储的MKB新?
否
106
将存储的MKB写入介质中，然后对内容重新加密并写入它
结束
是
108
使用介质MKB以写入内容，任选地用介质MKB代替存储的MKB
结束

图 1