[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G11B 20/00 (2006.01)
G06F 1/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 02820542.1

[45] 授权公告日 2007 年 8 月 1 日

[11] 授权公告号 CN 1329909C

[22] 申请日 2002.10.15 [21] 申请号 02820542.1
[30] 优先权
[32] 2001.10.17 [33] EP [31] 01203967.3
[86] 国际申请 PCT/IB2002/004266 2002.10.15
[87] 国际公布 WO2003/034428 英 2003.4.24
[85] 进入国家阶段日期 2004.4.16
[73] 专利权人 皇家飞利浦电子股份有限公司
地址 荷兰艾恩德霍芬
[72] 发明人 F·L·A·J·坎佩曼
[56] 参考文献
EP0809244A2 1997.11.26
WO0062290A1 2000.10.19
WO9918506A1 1999.4.15
EP1035543A2 2000.9.13
审查员 刘楠娟

[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 邹光新 王忠忠

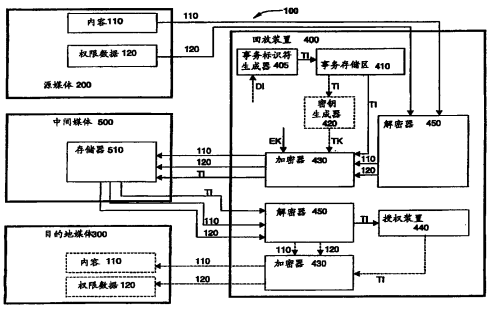
权利要求书 3 页 说明书 8 页 附图 1 页

[54] 发明名称

安全的单驱动器复制方法和设备

[57] 摘要

一种经由中间媒体传送数据信息的方法，包括：从源媒体读取数据信息到回放装置；解密数据信息；从回放装置的存储区检索一个事务标识符；将解密的数据信息与检索到的事务标识符结合起来；加密结合起来的信息；将加密的结合信息传送到中间媒体；从中间媒体读取加密的结合信息；将加密的结合信息解密；将加密的结合信息去结合成数据信息和事务标识符；将事务标识符与存储在存储区中的一组事务标识符相比较；以及如果在存储在回放装置中的事务标识符组中找到了解密的事务标识符，则将该事务标识符从存储在回放装置中的事务标识符组中删除；并且如果从存储在回放装置中的事务标识符组中找到了解密的事务标识符的值，则将数据信息存储在目的媒体上。



1. 一种经由中间媒体传送数据信息的方法，该方法包括下列步骤：

从源媒体中读取数据信息到回放装置；

解密所述数据信息；

从所述回放装置的存储区中检索一个事务标识符；

将所述解密的数据信息与所述检索到的事务标识符结合成结合起来的信息；

加密所述结合起来的信息；

将所述加密的结合起来的信息传送到中间媒体；

从所述中间媒体读取所述加密的结合起来的信息；

将所述加密的结合起来的信息解密；

将所述加密的结合起来的信息去结合成所述数据信息和所述事务标识符；

将所述事务标识符与存储在所述存储区中的一组事务标识符相比较；以及

如果在存储在所述回放装置中的所述事务标识符组中找到了所述解密的事务标识符，则将所述事务标识符从存储在所述回放装置中的所述事务标识符组中删除；

而如果从存储在所述回放装置中的所述事务标识符组中找到了所述解密的事务标识符的值，则将所述数据信息存储在目的媒体上。

2. 权利要求 1 中所述的方法，其中结合所述数据信息和所述事务标识符是通过使用密钥散列法和/或加密来实现的。

3. 权利要求 1 或 2 所述的方法，其中将所述数据信息存储到所述目的地媒体的所述步骤进一步包括在加密器中对所述数据信息进行重新加密的步骤。

4. 权利要求 3 所述的方法，其中对所述数据信息重新加密的步骤进一步包括使用一种加密密钥，该加密密钥是与所述回放装置所独有的私有密钥相对应的公开密钥。

5. 权利要求 4 所述的方法，其中对所述数据信息重新加密进一步包括使用基于所述事务标识符的值的附加的加密密钥。

6. 权利要求 3 所述的方法，其中对所述数据信息重新加密的步

骤进一步包括使用一种加密密钥，该加密密钥是对称式密钥。

7. 权利要求 1 所述的方法，进一步包括如下步骤：如果在存储于所述回放装置中的所述事务标识符组中找到了所述传送的事务标识符，则将所述传送的事务标识符加密并将经过加密的所述传送的事务标识符存储在所述目的地媒体中。

8. 权利要求 1 所述的方法，其中从所述源媒体读取数据信息进一步包括读取内容资料和读取限制对该内容资料的访问的相关权限数据。

9. 权利要求 1 所述的方法，进一步包括生成一个独特的事务标识符，并把所述生成的事务标识符添加到所述事务标识符组里。

10. 权利要求 1 所述的方法，其中所述事务标识符包括对所述回放装置的驱动器标识的引用。

11. 一种用于经由中间媒体传送数据信息的设备，所述中间媒体还包括存储区，该设备包括配置成执行如下操作的回放装置：

从源媒体中读取数据信息到回放装置；

包括解密所述数据信息的解密器；

从所述回放装置的存储区中检索一个事务标识符；

将所述解密的数据信息与所述检索到的事务标识符结合成结合起来的信息；

进一步包括用于加密所述结合起来的信息的加密器；

将所述加密的结合起来的信息传送到中间媒体；

从所述中间媒体读取所述加密的结合起来的信息；

所述解密器将所述加密的结合起来的信息解密；

将所述加密的结合起来的信息去结合成所述数据信息和所述事务标识符；

将所述事务标识符与存储在所述存储区中的一组事务标识符相比较；以及

如果于存储在所述回放装置中的所述事务标识符组中找到了所述解密的事务标识符，则将所述事务标识符从存储在所述回放装置中的所述事务标识符组中删除；

而如果于存储在所述回放装置中的所述事务标识符组中找到了所述解密的事务标识符的值，则将所述数据信息存储在目的媒体上，

进一步包括授权装置，该授权装置被配置为于存储在所述事务存储器中的所述事务标识符组中找到所述中间媒体上存储的所述事务标识符的解密值时，授权所述事务；而于存储在所述事务存储器中的所述事务标识符组中未找到所述中间媒体上存储的所述事务标识符的解密值时，拒绝所述信息传送。

12. 权利要求 11 所述的设备，其中所述回放装置进一步配置为在执行将信息传送到目的地媒体的授权传送之前对该信息进行重新加密。

安全的单驱动器复制方法和设备

技术领域

本发明涉及电子安全领域，更具体地说是涉及从一个设备向另一个设备传送信息的安全系统和方法。

背景技术

数字媒体存储数字形式的数据，包括所有种类的 CD 和 DVD 光盘技术。存储在数字媒体中的数据包括视频、文本、音频、计算机数据或者其他形式的数字信息。数字媒体经常存有授予了版权的信息，这种信息可能会被非法制作出高质量复制品并加以传播。使用 DRM（数字权限管理）系统将会在数字信息的传播过程中保护上述的版权，并且方便应交和/或汇付给数字信息的拥有者的版税计算。例如，一个 DRM 系统提供一个容器（即一个能够安全保存和传送数字内容的数据单元）、为了使用（回放或复制）数字内容而必须被软件和硬件设备遵守的一套使用规则、以及保证使用规则的密钥。该使用规则和加密密钥在下文中被称为“权限数据”。

为了使用一个单驱动器系统从一张盘向另一张盘复制内容和权限数据，DRM 系统首先检索源盘中的内容和权限数据，将该内容和权限数据存储在硬盘驱动器（HDD）中，然后将该内容和权限数据传送到一张目的地盘（使用者要用目的地盘替换源盘），最后从硬盘驱动器中删除权限数据。在这种环境下的一个“重放攻击（replay attack）”的实例是一种破坏复制保护方案的方法，该方法意味着一个未经授权的使用者（例如一个电脑黑客）复制存储在 HDD 上的权限，并且试图欺骗 DRM 系统将该权限重放进第三张盘中。以这种方式，黑客就能够得到原件的伪造复件。由于数字内容是加密的，所以仅仅通过使用一个硬盘驱动器作为中间存储器就能将该数字内容从源媒体复制到目的地媒体。因此为了防止重放攻击，问题就在于如何安全地复制权限数据（包括密钥，通过它可以解密和访问数字内容）。

众所周知，定义一个安全鉴定渠道（SAC），以用于将权限数据从源设备和媒体安全地传送到目的地设备和媒体。根据这种方法，传送

权限和复制内容需要必须具有实时的相互作用的两个设备和媒体。然而，一个典型的消费者仅拥有一个 CD-DRM 驱动器。而且权限的传输必须以一种安全的方式来进行。

另一种用于传送数字内容同时保存相关权限的方案是仅仅将加密的内容从源盘复制到目的地盘。然后为了使用该内容就需要购买权限或者通过一个受保护的渠道（典型是通过 SAC）从网站或服务器那里得到。这种方法必须依赖于服务器连接的完整性。

PCT 专利申请号 NO.WO0062290（代理人案号 PHA 23637）的专利和本申请是同一受让人，它公开了用于防止重放攻击的单驱动器系统，在该系统中，使用存储在记录媒体的一个只读存储器元件中的动态记录指示符来对内容加密密钥进行加密。使用对应于目标回放装置的私有密钥的一个公开密钥对该内容加密密钥进一步加密。这样，内容加密密钥的解密同时需要记录指示符的值和设备私有密钥。

因为每当数据被记录到记录媒体时，记录媒体都会产生一个新的并且可能是随机的记录指示符，随后的非法记录（重放攻击）不可能提供一个相同的加密密钥，所以回放装置将不能对内容加密密钥和内容本身解密，这样就防止了重放攻击。然而，这种方法需要最初的记录指示符能够被可靠、安全地从记录媒体传递给回放装置（可能通过使用数字签名），这是因为执行保护方案的是回放装置。另外，该方法将记录指示符存储在记录媒体的存储区，而该存储区易于被非法窜改。

因此，需要一种改进的系统和方法，使用单独的回放/记录设备从媒体到媒体安全地传送数字内容和权限数据，同时防止对于 DRM 或者类似有限使用方案的重放攻击。

发明内容

本发明通过提供一种将权限数据和数字内容从源盘传送到目的地盘的安全方法满足了上述需要，根据本发明，该方法仅使用一个 CD-DRM 驱动器和一个中间存储媒体。一个加密的事务标识符和权限数据一起被传送到中间存储媒体，从而在将权限数据保存在中间存储媒体时保证了权限数据的安全性。

更特别的，根据本发明的一个实施例的方法，至少产生了一个事

物标识符并将其存储在一个回放装置（该回放装置还具有记录能力）的存储区内。该回放装置分配了一个事物标识符，然后从源媒体中读取数字内容并使用权限数据，解密该权限数据，然后使用一个加密密钥对权限数据和分配的事物标识符一起再次加密，该加密密钥包括诸如对称式密码术或者一个对应于存储在回放装置中的私有密钥的公开密钥。

由回放装置执行的加密可能还包括一个对应于所分配的事物标识符的事务密钥，例如将事务密钥和一个对称式或公开密钥结合起来。进一步讲，除了将权限数据和事务标识符一起加密之外，可以实现一个完整性机构（例如一个数字签名或者散列法方案）从而实现对窜改的检测。回放装置将数字内容和重新加密的权限数据连同相应的加密事务标识符从源媒体传送到硬盘驱动器的本地存储器中。在将该传送信息传送到目的地媒体之前，回放装置检查事务标识符和任意完整性机构来确定是否进行了重放攻击。如果实现了完整性机构，则可以检查传送信息是否有窜改。

通过将权限数据和被传送到硬盘驱动器的加密的事务标识符解密并且将该事务标识符与回放装置中安全的本地存储器中的事务标识符做比较，来继续进行重放检查。通常，当且仅当该传输的事务标识符与回放装置中的事务标识符匹配时，才将重新加密的权限数据写入目的地盘。

本发明方法的一个优势是：每一个独特的事务标识符以未加密的形式存放在更加不易窜改的回放装置中，但当该事务标识符存在于中间媒体中时就被加密并且伴随一个完整性机构。因此，本发明消除了对于一个安全的中间媒体的需要，这是因为通过回放装置实现和加强了安全性。

简而言之，本发明包括使用一个单放装置安全传送数据（特别是DRM 保护的使用权限）的系统和方法。至少一个由一系列或随机数字组成的事务标识符被存储在回放装置的存储区内。在本发明的一个方面，一个事务标识符可能包括对唯一驱动器标识符的引用。与存储在源盘中的内容相联系的使用权限被解密，然后通过使用与特定回放装置有关的而且仅对于该回放装置可知的密钥与分配的事务标识符一起被重新加密，从而保证了权限数据只能在该特定回放装置中重放。使

用权限和事务标识符的加密可以包含基于该事务标识符的事务密钥。当将重加密的使用权限连同数字内容从源盘传送到中间媒体的存储器例如一个硬盘驱动器（HDD）时，回放装置包含了加密的事务标识符。在将内容（可能被加密）和加密的使用权限从 HDD 传送到目的地媒体时，回放装置将存储在 HDD 中的该事务标识符与存储在回放装置中的事务标识符列表相比较。如果存储在 HDD 中的该事务标识符与事务标识符列表中的一个事务标识符相匹配，则由回放装置进行的加密被反向进行，从而该内容和使用权限能够被写入目的地媒体。此外，在将信息从源媒体传送到目的地媒体一次之后通过把该事务标识符从回放装置的存储器中删除，可以执行本发明的方法以便权限数据只能在回放装置中重放一次。换句话说，仅当中间媒体上的系列/随机数字与存储在回放装置中的事务数字一致的时候，中间媒体上的权限数据被回放装置接收。在权限数据被接收并被成功处理之后，回放装置中的事务标识符被删除从而防止权限数据被重放。

存储在回放装置中的事务标识符的最大数量取决于由回放装置制造商分配的存储器资源，该最大数量在回放装置制造之后可以被重新配置。事务标识符可以在被存储在事务存储器之前在回放装置内部或外部被生成。每一个事务标识符都是一个独特的值，该值由例如一个系列数字、随机生成的数字、或者权限数据的散列码构成。尽管每一个事务标识符都必须是唯一的，但当耗尽时、请求时或者在固定的时间间隔都可以补充事务标识符（通过产生或存储至少一个新的事务标识符）。

本发明的另一个实施例是将回放装置用作中间媒体，例如通过将使用权限存储在回放装置的内部存储器中。当写入目的地媒体时，权限数据从回放装置的存储器传送而内容则从中间媒体中传送，然后从驱动器存储器中删除。该实施例使用了与前一个实施例相同的事务验证技术。本发明的这种方法也能利用一个具有存储容量有限的单独存储装置作为用于权限数据和事务标识符的外部存储单元。

本发明的其他目标、优势以及新颖的特征中的一部分将在后文中给出，另一部分可由本领域技术人员在阅读下文时轻易得出，或者可能在实践本发明时学会。

当参考说明时，包含在并且作为本说明书的构成部分的附图说明

了本发明。

附图说明

附图 1 是本发明的一个优选实施例的部件的功能关联的框图。

具体实施方式

正如所需要的，在此公开了本发明的详细实施例；然而应当理解，该公开的实施例只是本发明的一个示例，该示例可以以各种可替换的形式给出。图形不是按照比例给出的；一些特征可能被放大或缩小来详细地表示特定的部件。因此，在这里公开的结构和功能细节不是限制性的，仅仅作为权利要求的基础，并作为指导本领域技术人员以各种形式实现本发明的基础。

现在详细地参看本发明的一个优选实施例，该实施例由附图进行图解，在附图中相同的数字指示相同的部件，附图 1 是加密系统 100 的一个示例性实施例的功能部件的结构图，该系统以一种防止重放攻击的方式将受保护的数字内容传送到目的地媒体 300。加密系统 100 包括一个源媒体 200、一个目的地媒体 300 和一个回放装置 400。源媒体 200 包括加密的数字内容 110 和相关联的使用权限数据 120（使用规则和密钥），该使用权限数据被写入目的地媒体 300，用于由回放装置 400 重放。根据目的地媒体 300 的形式和结构，可以使用任何一种传统的写入技术。为了简化的目的，在附图 1 中没有示出用于写入目的地媒体 300 和从源媒体 200 读出的部件。

根据本发明，回放装置 400 是通过一个唯一驱动器标识符（例如驱动器号 DI）被识别的，并且该回放装置包括一个事务存储区 410，其中包含了至少一个唯一事务标识符 TI 的列表。在制造回放装置 400 时就设定了事务存储区 410。事务标识符 TI 通过使用任意多种技术和机构（例如随机数字生成和一个日期/时间标记）由事务标识符生成器 405 产生，并且在制造回放装置 400 之后该事务标识符 TI 在事务存储区 410 中至少被存储一次。根据本发明的一个实施例，如所要求的，通过事务标识符生成器 405 生成每一个事务标识符 TI，例如当一个使用者希望制作权限数据 120 的一个可允许的复件时。作为可替换的方案，在制造回放装置 400 时，事务标识符 TI 被存储在事务存储

区 410 中。每一个事务标识符 TI 可以包括对驱动器标识符 DI 的引用，其中事务标识符生成于该驱动器标识符 DI。

在本发明的示例性实施例方法的操作中，当接收到一个数据传输命令时，回放装置 400 从源媒体 200 中读取内容 110 和权限数据 120，通常读取内容 110 和权限数据 120 中的任一者或二者是进行了预加密的。解密器 450 将权限数据 120 解密，在可选方案中也将内容 110 解密。一个事务标识符 TI 从存储在事务存储区 410 中的事务标识符列表中取出。该事务标识符 TI 中可能包括对唯一的设备标识符 DI 的引用，在制造时该设备标识符 DI 就被存储在回放装置 400 中。然后一个加密器 430 通过应用对该回放装置是唯一的密钥 EK 将权限数据 120 和事务标识符 TI 一起加密，所述的密钥例如是在制造时被存储在回放装置中的一个对称式密钥或者一个公开/私有密钥对。

可替换的方案是，由加密器 430 对权限数据 120 和事务标识符 TI 进行的加密进一步包括了事务密钥 TK，该事务密钥由密钥生成器 420 生成，并且来源于事务标识符 TI。与权限无关的内容 110 也可以类似地由加密器 430 加密。可替换的方案是，预加密的与权限无关的内容可以不需要进一步加密而直接复制。因此从源媒体 200 到目的地媒体 300 的信息传送可以仅使用一个回放装置 400 来完成，加密内容 110 和权限数据 120 连同加密的事务标识符 TI 被传送到中间媒体 500 的一个本地存储器 510 中。中间媒体 500 是一个存储设备，例如个人电脑的外部的硬盘驱动器、外部的和/或专用的存储模块，或者回放装置自身的存储区。因为典型的回放装置 400 缺乏足够大存储空间来“储存”源媒体 200 的所有内容，所以中间媒体 500 的作用是至少提供用于被传送信息的临时存储器。根据本发明的一个示例性实施例，被传送的信息包括内容 110、加密权限数据 120 以及加密的事务标识符 TI。

在一个可替换的实施例中，非权限内容 110 被传送到中间媒体，同时加密权限数据 120 和加密事务标识符 TI 被传送到回放装置 400 的存储区。当数据被存储在中间媒体 500 中时，权限数据 120 和事务标识符 TI 的加密状态和所实现的完整性机构实现了对于窜改的检测和对于数据的保密。

重放保护主要是在源媒体 200 从回放装置 400 中分离并被目的地媒体 300 取代时实现的。在处理的这个阶段，回放装置 400 不断地处

理将内容 110 和权限数据 120 通过中间媒体 500 传送到目的地媒体 300 的请求，在此之前该信息已经以一种加密的状态传送到该中间媒体 500 中。为了证实该传送请求的合法性，回放装置 400 中的一个授权装置 440 检查完整性机构，从而检测当信息存储在中间媒体 500 中时发生的任何窜改。

解密器 450 将事务标识符 TI（当事务标识符 TI 与权限数据一起加密时，此处加上权限数据 120）解密，该事务标识符被加密器 430 加密，并且传送到中间媒体 500。解密器 450 通过逆转使用加密密钥 EK 和事务密钥 TK（如果使用了）进行的加密来解密信息。然后回放装置 400 中的授权装置 440 将从中间媒体 500 的存取器 510 中读取的解密的事务标识符 TI 与存储在回放装置 400 的事务存储区 410 中的事务标识符列表相比较。如果解密的传送事务标识符 TI 的值没有在事务存储区 410 中找到，则该请求是非法的，并且可能正在进行一个重放攻击。如果传送事务标识符 TI 的值能够在事务存储区 410 中找到，则该传送已经通过验证，并且将执行从中间媒体 500 到目的地媒体 300 的传送。

为了完成一个已经验证的请求，回放装置 400 中的加密器 430 将权限数据 120 和事务标识符 TI 重新加密。将内容 110 和重新加密的权限数据 120 写入目的地媒体 300 中，从而完成了信息传送。在一个可替换的实施例中，不必对权限数据 120 和传送标识符 TI 重新加密。根据本发明的一个方面，事务标识符 TI 在被重新加密后，也可以被传送到目的地媒体中。

一旦授权装置 440 授权或者拒绝一个传送请求，就将事务标识符 TI 从存储在事务存储区 410 中的事务标识符列表中删除，以防止将来的重放攻击。进一步来说，当授权装置 440 已经拒绝了一个传送请求时，将内容 110、加密权限数据 120 和传送的事务标识符 TI 从中间媒体 500 中删除。如果传送请求已经被授权装置 440 授权，则将内容 110、权限数据 120（如果一些权限在传送之后已经被“用尽”，则权限数据 120 可能已经改变）和事务标识符 TI 保留在中间媒体 500 中，以利于附加授权的传输，这一点是使用规则所允许的。

通过上文可以理解，本发明提供了一种系统和方法，其中仅使用一个重放和记录装置来安全地从媒体到媒体传送数字内容和相关权限

数据。而且应当理解的是，上述内容仅仅涉及到本发明的示例性实施例，而且在不偏离下述权利要求书所限定的本发明的精神和范围的情况下，可以进行许多改变。

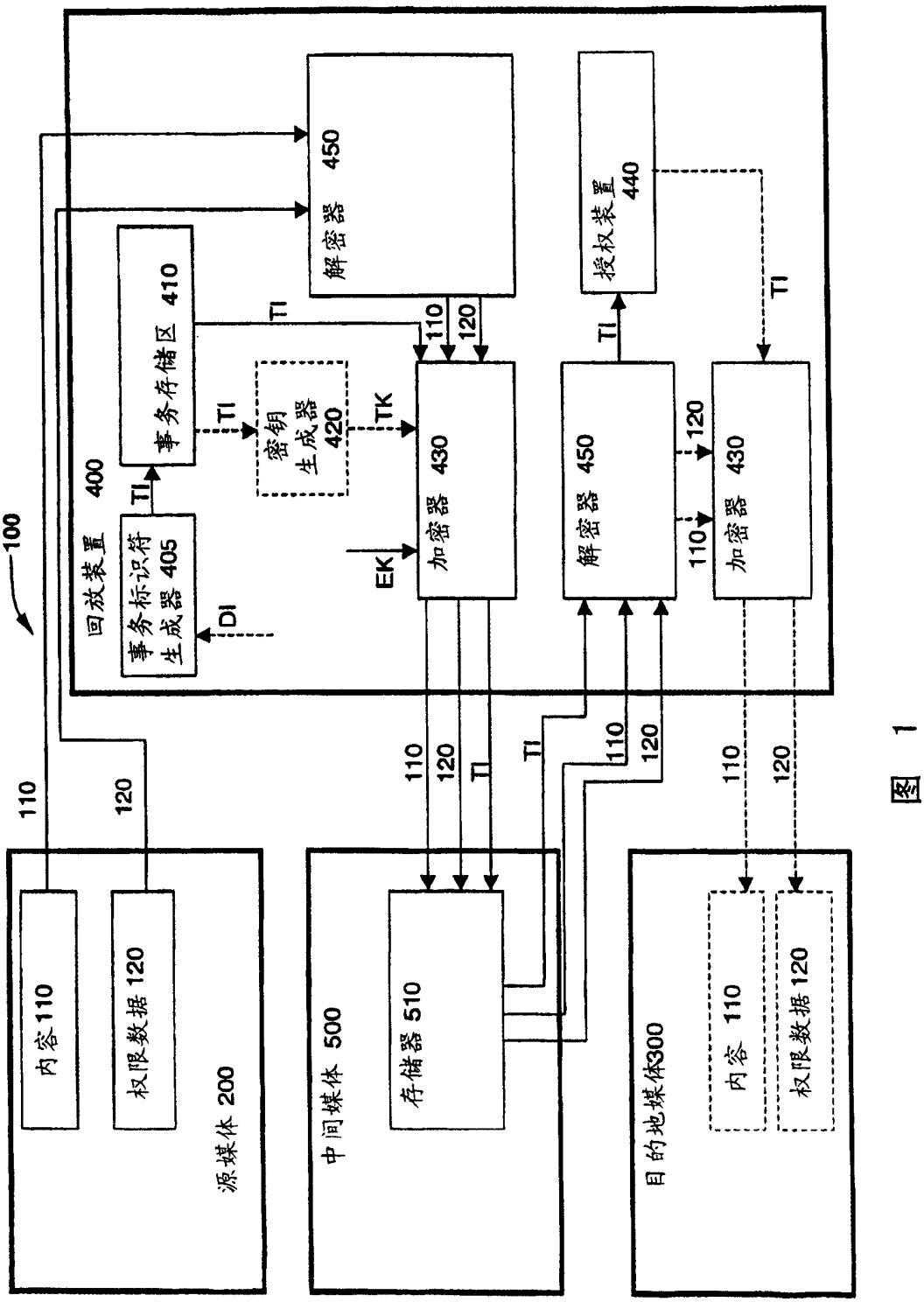

100
回放装置 400
事务存储区 410
事务标识符生成器 405
密钥生成器 420
加密器 430
解密器 450
授权装置 440
TI
TK
EK
DI
110
120
源媒体 200
内容 110
权限数据 120
中间媒体 500
存储器 510
目的地媒体300

图 1