[19]中华人民共和国国家知识产权局

[51]Int.Cl[7]
G11B 20/10
G11B 19/02 G09C 1/00

[12]发明专利申请公开说明书

[21]申请号 00106020.1

[43]公开日 2000年11月29日

[11]公开号 CN 1274922A

[22]申请日 2000.4.12 [21]申请号 00106020.1
[30]优先权
[32]1999.5.21 [33]JP [31]141269/1999
[71]申请人 日本胜利株式会社
地址 日本神奈川县
[72]发明人 菅原隆幸

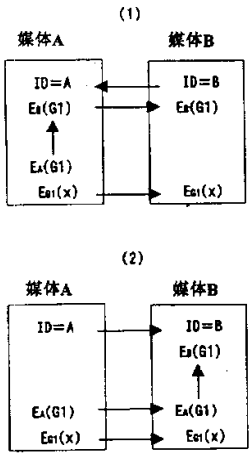
[74]专利代理机构 中原信达知识产权代理有限责任公司
代理人 谢丽娜 余 朦

权利要求书7页 说明书17页 附图页数5页

[54]发明名称 内容信息记录方法及内容信息记录装置

[57]摘要

本发明公开一种内容信息记录方法及内容信息记录装置,既可以防止非法的复 制,又可以在用户间记录内容数据。当对加密内容信息EG1(X)从媒体A向媒体B进行记录时,在媒体A侧读取复制端媒体的ID=B,先在媒体A侧 对用 ID=A 加密的第一加密密钥信息 EA(G1)进行解码,而用复制端的 ID=B 进行再加密,变为第二加密密钥信息EB(G1),传输给媒体B。



ISSN1008-4274

00·04·12

权 利 要 求 书

1. 一种内容信息记录方法，其特征在于：

在第一媒体中记录有用与所述第一媒体 ID 相关的信息作为 ID 密钥对内容信息加密得到的第一加密内容信息，在从所述第一媒体将所述内容信息记录在第二媒体上时，

从所述第一媒体侧将所述第一加密内容信息输出到所述第二媒体侧；

在所述第二媒体侧，根据从所述第一媒体侧得到的与所述第一媒体的 ID 相关的信息，暂时解除所述第一加密内容信息的密码，把用与所述第二媒体的 ID 相关的信息作为 ID 密钥对所述内容信息再加密所得到的第二加密内容信息记录在所述第二媒体上。

2. 一种内容信息记录方法，其特征在于：

在第一媒体中记录有用与所述第一媒体 ID 相关的信息作为 ID 密钥对内容信息加密得到的第一加密内容信息，在从所述第一媒体将所述内容信息记录在第二媒体上时，

在所述第一媒体侧，暂时解除所述第一加密内容信息的密码，将从所述第二媒体侧得到的与所述第二媒体的 ID 相关的信息作为 ID 密钥，对所述内容信息再加密，得到第二加密内容信息，使该第二加密内容信息输出到所述第二媒体侧；

在所述第二媒体侧，使所述第二加密内容信息记录在所述第二媒体上。

3. 一种内容信息记录方法，其特征在于：

在第一媒体中记录有用与所述第一媒体 ID 相关的信息作为 ID 密钥对内容信息加密得到的第一加密内容信息，在从所述第一媒体将所述内容信息记录在第二媒体上时，选择下述的方法[a]或方法[b]，

方法[a]

从所述第一媒体侧，将所述第一加密内容信息输出给所述第二媒

体侧；

在所述第二媒体侧，根据从所述第一媒体侧得到的与所述第一媒体的 ID 相关的信息，暂时解除所述第一加密内容信息的密码，而把使用与所述第二媒体的 ID 相关的信息作为 ID 密钥对所述内容信息再加密所得到的第二加密内容信息记录在所述第二媒体上，

方法[b]

从所述第一媒体侧，暂时解除所述第一加密内容信息的密码，将从所述第二媒体侧得到的与所述第二媒体的 ID 相关的信息作为 ID 密钥，对所述内容信息进行再加密，得到第二加密内容信息，将该第二加密内容信息输出到所述第二媒体侧；

在所述第二媒体侧，将所述第二加密内容信息记录在所述第二媒体上。

4. 根据权利要求 1-3 中的任一项所记载的内容信息记录方法，其特征在于：

所述第一加密内容信息的 ID 密钥，是直接使用所述第一媒体的 ID 的共用密钥，或者是使用对所述第一媒体 ID 按照给定函数进行变换的信息的共用密钥；

所述第二加密内容信息的 ID 密钥，是直接使用所述第二媒体的 ID 的共用密钥，或者是使用对所述第二媒体的 ID 按照给定函数进行变换的信息的共用密钥。

5. 一种内容信息记录方法，其特征在于：

从记录有由规定的内容密钥加密的加密内容信息、及用与第一媒体的 ID 相关的信息作为 ID 密钥对所述内容密钥加密的第一加密密钥信息的所述第一媒体，把所述加密内容信息记录在第二媒体上时，

从所述第一媒体侧将所述加密内容信息和所述加密密钥信息输出给所述第二媒体侧；

在所述第二媒体侧，将所述加密内容信息记录在所述第二媒体上；同时根据从所述第一媒体侧得到的与所述第一媒体的 ID 相关的信

息，暂时解除所述第一加密密钥信息的密码，把用与所述第二媒体的ID相关的信息作为ID密钥对所述内容密钥再加密所得到的第二加密密钥信息记录在所述第二媒体上。

6. 一种内容信息记录方法，其特征在于：

从记录有由规定的内容密钥加密的加密内容信息、及用与第一媒体的ID相关的信息作为ID密钥对所述内容密钥加密的第一加密密钥信息的所述第一媒体，将所述加密内容信息记录在所述第二媒体上时，

在所述第一媒体侧，暂时解除所述第一加密密钥信息的密码，以从所述第二媒体侧得到的与所述第二媒体的ID相关的信息作为ID密钥，对所述内容密钥进行再加密，得到第二加密密钥信息，将该第二加密密钥信息输出到所述第二媒体侧；

在所述第二媒体侧，将从所述第一媒体侧输出的所述加密内容信息和所述第二加密密钥信息记录在所述第二媒体上。

7. 一种内容信息记录方法，其特征在于：

从记录有由规定的内容密钥加密的加密内容信息、及用与第一媒体ID相关的信息作为ID密钥对所述内容密钥加密的第一加密密钥信息的所述第一媒体，将所述加密内容信息记录在第二媒体上时，选择下述的方法[a]或方法[b]，

方法[a]

从所述第一媒体侧，将所述加密内容信息和所述第一加密密钥信息输出给所述第二媒体侧；

在所述第二媒体侧，将所述加密内容信息记录在所述第二媒体上，同时根据从所述第一媒体侧得到的与所述第一媒体的ID相关的信息，暂时解除所述第一加密密钥信息的密码，把使用与所述第二媒体的ID相关的信息作为ID密钥对所述内容密钥再加密所得到的第二加密密钥信息记录在所述第二媒体上；

方法[b]

在所述第一媒体侧，暂时解除所述第一加密密钥信息的密码，以从所述第二媒体侧得到的与所述第二媒体的 ID 相关的信息作为 ID 密钥，对所述内容密钥再加密，得到第二加密密钥信息，将该第二加密密钥信息输出到所述第二媒体侧；

在所述第二媒体侧，将从所述第一媒体侧输出的所述加密内容信息和所述第二加密密钥信息记录在所述第二媒体上。

8. 根据权利要求 5-7 中的任一项所记载的内容信息记录方法，其特征在于：

所述规定的内容密钥是共用密钥或公开密钥；

所述第一加密密钥信息的 ID 密钥，是直接使用所述第一媒体的 ID 的共用密钥或者是使用对所述第一媒体的 ID 按照给定函数进行变换的信息的共用密钥；

所述第二加密密钥信息的 ID 密钥，是直接使用所述第二媒体的 ID 的共用密钥或者是使用对所述第二媒体的 ID 按照给定函数进行变换的信息的共用密钥。

9. 一种内容信息记录装置，其从记录有用与第一媒体的 ID 相关的信息作为 ID 密钥对内容信息加密的第一加密内容信息的所述第一媒体，将所述内容信息记录在第二媒体上，其特征在于：

在所述第二媒体侧，设有记录装置，该记录装置通过从所述第一媒体侧输出的与所述第一媒体的 ID 相关的信息，暂时解除从所述第一媒体侧输出的所述第一加密内容信息的密码，把用与所述第二媒体的 ID 相关的信息作为 ID 密钥对所述内容信息再加密所得到的第二加密内容信息记录在所述第二媒体上。

10. 一种内容信息记录装置，其用与第一媒体的 ID 相关信息作为 ID 密钥，从记录有对内容信息加密的第一加密内容信息的所述第一媒体，将所述内容信息记录在第二媒体上，其特征在于：

在所述第一媒体侧设有记录装置，该记录装置暂时解除所述第一

加密内容信息的密码，将从所述第二媒体侧输出的与所述第二媒体的ID相关的信息作为ID密钥，对所述内容信息进行再加密，得到第二加密内容信息，将该第二加密内容信息输出到所述第二媒体侧，将所述第二加密内容信息记录在所述第二媒体上。

11. 一种内容信息记录装置，其特征在于：

在第一媒体中记录有用与所述第一媒体ID相关的信息作为ID密钥对内容信息加密得到的第一加密内容信息，当从所述第一媒体将所述内容信息记录在第二媒体上时，设有选择下述的记录操作[a]和记录操作[b]的选择装置，

记录操作[a]

在所述第二媒体侧，根据所述第一媒体侧输出的与所述第一媒体的ID相关的信息，暂时解除从所述第一媒体侧输出的所述第一加密内容信息的密码，把用与所述第二媒体的ID相关的信息作为ID密钥对所述内容信息进行再加密所得到的第二加密内容信息记录在所述第二媒体上；

记录操作[b]

在所述第一媒体侧，暂时解除所述第一加密内容信息的密码，以从所述第二媒体侧输出的与所述第二媒体的ID相关的信息作为ID密钥，对所述内容信息进行再加密，得到第二加密内容信息，使该第二加密内容信息输出给所述第二媒体侧，将所述第二加密内容信息记录在所述第二媒体上。

12. 根据权利要求9-11中的任一项所记载的内容信息记录装置，其特征在于：

所述第一加密内容信息的ID密钥，是直接使用所述第一媒体的ID的共用密钥，或者是使用对所述第一媒体的ID按照给定函数进行变换的信息的共用密钥；

所述第二加密内容信息的ID密钥，是直接使用所述第二媒体的ID的共用密钥，或者是使用按照给定函数对所述第二媒体的ID进行

变换的信息的共用密钥。

13. 一种内容信息记录装置，从记录有规定的内容密钥加密的加密内容信息、及用与第一媒体的 ID 相关的信息作为 ID 密钥对所述内容密钥加密的第一加密密钥信息的所述第一媒体，将所述加密内容信息记录在第二媒体上，其特征在于，该装置设有：

加密密钥信息记录装置，在所述第二媒体侧，根据从所述第一媒体侧输出的与所述第一媒体的 ID 相关的信息，暂时解除所述第一加密密钥信息的密码，把用与所述第二媒体的 ID 相关的信息作为 ID 密钥对所述内容密钥进行再加密所得到的第二加密密钥信息记录在所述第二媒体上。

14. 一种内容信息记录装置，从记录有以规定的内容密钥加密的加密内容信息、及用与第一媒体的 ID 相关的信息作为 ID 密钥对所述内容密钥加密的第一加密信息的所述第一媒体，将所述加密内容信息记录在第二媒体上；其特征在于该装置具有：

加密密钥信息记录装置，在所述第一媒体侧，暂时解除所述第一加密密钥信息的密码，将从所述第二媒体侧输出的与所述第二媒体的 ID 相关的信息作为 ID 密钥，对所述内容密钥进行再加密，得到第二加密密钥信息，使该第二加密密钥信息输出到所述第二媒体侧，将所述第二加密密钥信息记录在所述第二媒体上。

15. 一种内容信息记录装置，其特征在于：在从记录有以规定的内容密钥加密的加密内容信息、及用与第一媒体的 ID 相关的信息作为 ID 密钥对所述内容密钥加密的第一加密密钥信息的所述第一媒体，将所述加密的内容信息记录在第二媒体上时，设有选择下述的记录操作[a]和记录操作[b]的选择装置，

记录操作[a]

在所述第二媒体侧，根据从所述第一媒体侧输出的所述第一媒体的 ID 相关信息，暂时解除所述第一加密密钥信息的密码，把用与所述

第二媒体的 ID 相关的信息作为 ID 密钥对所述内容密钥再加密所得到的第二加密密钥信息记录在所述第二媒体上；

记录操作[b]

在所述第一媒体侧，暂时解除所述第一加密密钥信息的密码，以从所述第二媒体侧输出的与所述第二媒体的 ID 相关的信息作为 ID 密钥，对所述内容密钥再加密，得到第二加密密钥信息，使该第二加密密钥信息输出给所述第二媒体侧，将所述第二加密密钥信息记录在所述第二媒体上。

16. 权利要求 13-15 中的任一项所记载的内容信息记录装置，其特征在于：

所述规定的内容密钥是共用密钥或公开密钥；

所述第一加密密钥信息的 ID 密钥，是直接使用所述第一媒体的 ID 的共用密钥，或者是使用对所述第一媒体的 ID 按照给定函数进行变换的信息的共用密钥；

所述第二加密密钥信息的 ID 密钥，是直接使用所述第二媒体的 ID 的共用密钥，或者是使用对所述第二媒体的 ID 按照给定函数进行变换的信息的共用密钥。

00·04·12

说　明　书

内容信息记录方法及内容信息记录装置

本发明涉及对内容信息进行记录重放的内容信息分配系统。

本发明的目的在于提供一种在内容信息分配系统中的内容信息记录方法及内容信息记录装置，对内容信息（特别是音频及视频数据）进行分配，在防止对分配的数据的不正当转让和复制的同时，又可以在用户的媒体间安全地进行数据的转让和复制。

随着加密技术的发展，利用网络对音频及视率的数字数据进行分配的有效方法有在特开平 10-269289 公报中记载的数字内容分配管理方法、数字内容重放方法及装置。在该发明中数字内容的分配方，对数字内容加密及压缩加工，将加工的数字内容和加密的内容密钥以及加密的收费信息发送给通信对方，根据通信对方所发送的内容使用信息，将征收的使用金分配给权利持有者。另一方面，在数字内容的重放侧通过内容密钥对该加工的数字内容进行解码，同时进行解压重放，并根据内容的使用情况将收费信息的减额和内容的使用信息发送给分配方，可以传送所记录的内容。

另外，在特愿平 9-25303（特开平 10-283268）号公报中记载有信息记录媒体、记录装置、信息传输系统、密码解读装置。该发明的信息记录媒体记录有加密的加密信息、及用于将该加密信息解码为原来信息的密钥信号进行加密的加密密钥信息，在加密密钥信息中记录有在非加密状态下对加密信息进行解码时的条件信息。即，在加密密钥信息的控制信息内，由于包括机器信息及区域信息，所以可以防止在用户方将加密的信息直接复制在 HDD 及光盘上，及防止非法使用。

但是所述现有的方法，由于在用户之间不能将记录在媒体上的内

容数据进行转让和复制（即使媒体本身可以转让，但是该媒体上记录的内容数据不能正常重放），所以用户为了得到内容数据，必须要与收费管理机关、数据管理中心等连接。并且，当个人的用户有多个媒体时，也不能在媒体间传送数据。

在解密后传输内容数据时，虽然可以进行内容数据的转让、复制，但是这样就变为非法的转让、复制了，不能确保数据传输的安全性。

本发明的目的在于提供一种在内容信息分配系统中的内容信息记录方法及内容信息记录装置，分配内容信息，在防止所分配数据的非法转让、复制的同时，又可以在用户的媒体之间安全地进行数据的转让、复制。

为了解决上述课题，本发明提供了以下的方法、装置。

（1）内容信息记录方法，其特征在于：

在第一媒体中记录有用与所述第一媒体 ID 相关的信息作为 ID 密钥对内容信息加密得到的第一加密内容信息，在从所述第一媒体将所述内容信息记录在第二媒体上时，

从所述第一媒体侧将所述第一加密内容信息输出到所述第二媒体侧；

在所述第二媒体侧，根据从所述第一媒体侧得到的与所述第一媒体的 ID 相关的信息，暂时解除所述第一加密内容信息的密码，而使用与所述第二媒体的 ID 相关的信息作为 ID 密钥对所述内容信息再加密所得到的第二加密内容信息记录在所述第二媒体上。

（2）内容信息记录方法，其特征在于：

在第一媒体中记录有用与所述第一媒体 ID 相关的信息作为 ID 密钥对内容信息加密得到的第一加密内容信息，在从所述第一媒体将所述内容信息记录在第二媒体上时，

在所述第一媒体侧，暂时解除所述第一加密内容信息的密码，将从所述第二媒体侧得到的与所述第二媒体的 ID 相关的信息作为 ID 密钥，对所述内容信息再加密，得到第二加密内容信息，使该第二加密内容信息输出到所述第二媒体侧；

在所述第二媒体侧，使所述第二加密内容信息记录在所述第二媒体上。

（3）内容信息记录方法，其特征在于：

在第一媒体中记录有用与所述第一媒体 ID 相关的信息作为 ID 密钥对内容信息加密得到的第一加密内容信息，在从所述第一媒体将所述内容信息记录在第二媒体上时，选择下述的方法[a]和方法[b]，

方法[a]

从所述第一媒体侧，将所述第一加密内容信息输出给所述第二媒体侧；

在所述第二媒体侧，根据从所述第一媒体侧得到的与所述第一媒体的 ID 相关的信息，暂时解除所述第一加密内容信息的密码，而把使用与所述第二媒体的 ID 相关的信息作为 ID 密钥对所述内容信息再加密所得到的第二加密内容信息记录在所述第二媒体上。

方法[b]

从所述第一媒体侧，暂时解除所述第一加密内容信息的密码，将从所述第二媒体侧得到的与所述第二媒体的 ID 相关的信息作为 ID 密钥，对所述内容信息进行再加密，得到第二加密内容信息，将该第二加密内容信息输出给所述第二媒体侧；

在所述第二媒体侧，将所述第二加密内容信息记录在所述第二媒体上。

（4）在所述（1）-（3）中的任一项所记载的内容信息记录方法中，其特征在于：

所述第一加密内容信息的 ID 密钥，是直接使用所述第一媒体的 ID 的共用密钥，或者是使用对所述第一媒体的 ID 按照给定函数进行

变换的信息的共用密钥；

所述第二加密内容信息的 ID 密钥，是直接使用所述第二媒体的 ID 的共用密钥，或者是使用对所述第二媒体的 ID 按照给定函数进行变换的信息的共用密钥。

（5）内容信息记录方法，其特征在于：

从记录有由规定的内容密钥加密的加密内容信息、及用与第一媒体的 ID 相关的信息作为 ID 密钥对所述内容密钥加密的第一加密密钥信息的所述第一媒体，把所述加密内容信息记录在第二媒体上时，

从所述第一媒体侧将所述加密内容信息和所述加密密钥信息输出给所述第二媒体侧；

在所述第二媒体侧，将所述加密内容信息记录在所述第二媒体上；同时根据从所述第一媒体侧得到的与所述第一媒体的 ID 相关的信息，暂时解除所述第一加密密钥信息的密码，把用与所述第二媒体的 ID 相关的信息作为 ID 密钥对所述内容密钥再加密所得到的第二加密密钥信息记录在所述第二媒体上。

（6）内容信息记录方法，其特征在于：

从记录有由规定的内容密钥加密的加密内容信息、及用与第一媒体的 ID 相关的信息作为 ID 密钥对所述内容密钥加密的第一加密密钥信息的所述第一媒体，将所述加密内容信息记录在所述第二媒体上时，

在所述第一媒体侧，暂时解除所述第一加密密钥信息的密码，以从所述第二媒体侧得到的与所述第二媒体的 ID 相关的信息作为 ID 密钥，对所述内容密钥进行再加密，得到第二加密密钥信息，使该第二加密密钥信息输出给所述第二媒体侧；

在所述第二媒体侧，将从所述第一媒体侧输出的所述加密内容信息和所述第二加密密钥信息记录在所述第二媒体上。

（7）内容信息记录方法，其特征在于：

从记录有由规定的内容密钥加密的加密内容信息、及用与第一媒体的 ID 相关的信息作为 ID 密钥对所述内容密钥加密的第一加密密钥信息的所述第一媒体，将所述加密内容信息记录在第二媒体上时，选择下述的方法[a]或方法[b]，

方法[a]

从所述第一媒体侧，将所述加密内容信息和所述第一加密密钥信息输出给所述第二媒体侧；

在所述第二媒体侧，将所述加密内容信息记录在所述第二媒体上，同时根据从所述第一媒体侧得到的与所述第一媒体的 ID 相关的信息，暂时解除所述第一加密密钥信息的密码，把用与所述第二媒体的 ID 相关的信息作为 ID 密钥对所述内容密钥再加密所得到的第二加密密钥信息记录在所述第二媒体上。

方法[b]

在所述第一媒体侧，暂时解除所述第一加密密钥信息的密码，以从所述第二媒体侧得到的与所述第二媒体的 ID 相关的信息作为 ID 密钥，对所述内容密钥再加密，得到第二加密密钥信息，将该第二加密密钥信息输出到所述第二媒体侧；

在所述第二媒体侧，将从所述第一媒体侧输出的所述加密内容信息和所述第二加密密钥信息记录在所述第二媒体上。

（8）在所述（5）-（7）中的任一项所记载的内容信息记录方法，其特征在于：

所述规定的内容密钥是共用密钥或公开密钥；

所述第一加密密钥信息的 ID 密钥，是直接使用所述第一媒体的 ID 的共用密钥或者是使用对所述第一媒体的 ID 按照给定函数进行变换的信息的共用密钥；

所述第二加密密钥信息的 ID 密钥，是直接使用所述第二媒体的 ID 的共用密钥或者是使用对所述第二媒体的 ID 按照给定函数进行变换的信息的共用密钥。

（9）内容信息记录装置，其从记录有用与第一媒体的 ID 相关的信息作为 ID 密钥对内容信息加密所得到的第一加密内容信息的所述第一媒体，将所述内容信息记录在第二媒体上，其特征在于：

在所述第二媒体侧，设有记录装置，该记录装置通过从所述第一媒体侧输出的与所述第一媒体的 ID 相关的信息，暂时解除从所述第一媒体侧输出的所述第一加密内容信息的密码，把用与所述第二媒体的 ID 相关的信息作为 ID 密钥对所述内容信息再加密所得到的第二加密内容信息记录在所述第二媒体上。

（10）内容信息记录装置，其从记录有用与第一媒体的 ID 相关信息作为 ID 密钥对内容信息加密的第一加密内容信息的所述第一媒体，将所述内容信息记录在第二媒体上，其特征在于：

在所述第一媒体侧，设有记录装置，该记录装置暂时解除所述第一加密内容信息的密码，将从所述第二媒体侧输出的与所述第二媒体的 ID 相关的信息作为 ID 密钥，对所述内容信息进行再加密，得到第二加密内容信息，使该第二加密内容信息输出给所述第二媒体侧，将所述第二加密内容信息记录在所述第二媒体上。

（11）内容信息记录装置，其特征在于：

在第一媒体中记录有用与所述第一媒体 ID 相关的信息作为 ID 密钥对内容信息加密得到的第一加密内容信息，当从所述第一媒体将所述内容信息记录在第二媒体上时，设有选择下述的记录操作[a]和记录操作[b] 的选择装置，

记录操作[a]

在所述第二媒体侧，根据所述第一媒体侧输出的与所述第一媒体的 ID 相关的信息，暂时解除从所述第一媒体侧输出的所述第一加密内容信息的密码，把用与所述第二媒体的 ID 相关的信息作为 ID 密钥对所述内容信息再加密所得到的第二加密内容信息记录在所述第二媒体上，

记录操作[b]

00·04·12

在所述第一媒体侧，暂时解除所述第一加密内容信息的密码，以从所述第二媒体侧输出的与所述第二媒体的 ID 相关的信息作为 ID 密钥，对所述内容信息进行再加密，得到第二加密内容信息，使该第二加密内容信息输出给所述第二媒体侧，将所述第二加密内容信息记录在所述第二媒体上。

（12）在所述（9）-（11）中的任一项所记载的内容信息记录装置中，其特征在于：

所述第一加密内容信息的 ID 密钥，是直接使用所述第一媒体的 ID 的共用密钥，或者是使用进行对所述第一媒体的 ID 按照给定函数进行变换的信息的共用密钥；

所述第二加密内容信息的 ID 密钥，是直接使用所述第二媒体的 ID 的共用密钥，或者是使用对所述第二媒体的 ID 按照给定函数进行变换的信息的共用密钥。

（13）内容信息记录装置，从记录有以规定的内容密钥加密的加密内容信息、及用与第一媒体的 ID 相关的信息作为 ID 密钥对所述内容密钥加密的第一加密密钥信息的所述第一媒体，将所述加密内容信息记录在第二媒体上，其特征在于该装置设有：

加密密钥信息记录装置，在所述第二媒体侧，根据从所述第一媒体侧输出的与所述第一媒体的 ID 相关的信息，暂时解除所述第一加密密钥信息的密码，把用与所述第二媒体的 ID 相关的信息作为 ID 密钥对所述内容密钥再加密所得到的第二加密密钥信息记录在所述第二媒体上。

（14）内容信息记录装置，从记录有以规定的内容密钥加密的加密内容信息、及用与第一媒体的 ID 相关的信息作为 ID 密钥对所述内容密钥加密的第一加密密钥信息的所述第一媒体，将所述加密内容信息记录在第二媒体上，其特征在于该装置具有：

加密密钥信息记录装置，在所述第一媒体侧，暂时解除所述第一

加密密钥信息的密码，将从所述第二媒体侧输出的与所述第二媒体的ID相关的信息作为ID密钥，对所述内容密钥进行再加密，得到第二加密密钥信息，使该第二加密密钥信息输出到所述第二媒体侧，将所述第二加密密钥信息记录在所述第二媒体上。

（15）内容信息记录装置，其特征在于：在从记录有以规定的内容密钥加密的加密内容信息、及用与第一媒体的ID相关的信息作为ID密钥对所述内容密钥加密的第一加密密钥信息的所述第一媒体，将所述加密的内容信息记录在第二媒体上时，设有选择下述的记录操作[a]记录操作[b]的选择装置，

记录操作[a]

在所述第二媒体侧，根据从所述第一媒体侧输出的与所述第一媒体的ID相关的信息，暂时解除所述第一加密密钥信息的密码，把用与所述第二媒体的ID相关的信息作为ID密钥对所述内容密钥再加密所得到的第二加密密钥信息记录在所述第二媒体上。

记录操作[b]

在所述第一媒体侧，暂时解除所述第一加密密钥信息的密码，以从所述第二媒体侧输出的与所述第二媒体的ID相关的信息作为ID密钥，对所述内容密钥再加密，得到第二加密密钥信息，将该第二加密密钥信息输出给所述第二媒体侧，把所述第二加密密钥信息记录在所述第二媒体上。

（16）在（13）-（15）中的任一项所记载的内容信息记录装置中，其特征在于：

所述规定的内容密钥是共用密钥或公开密钥；

所述第一加密密钥信息的ID密钥，是直接使用所述第一媒体的ID的共用密钥，或者是使用对所述第一媒体的ID按照给定函数进行变换的信息的共用密钥；

所述第二加密密钥信息的ID密钥，是直接使用所述第二媒体的ID的共用密钥，或者是使用对上述第二媒体的ID按照给定函数进行

变换的信息的共用密钥。

由上述可知，根据本发明，可以防止非法的转让、复制，并可以在用户之间对媒体上记录的内容数据进行转让、复制，用户不一定与收费管理机关、数据管理中心等连接，就可以得到内容数据。

另外，根据本发明，当个人的用户有多个媒体时，可以提供在其媒体间进行转让、复制的系统。

并且，可以经常在加密的安全性很高的状态下对内容数据进行转让、复制。

本发明的这些和其他目的、优点及特征将通过结合附图对本发明的实施例的描述而得到进一步说明，在这些附图中：

图 1 为说明一实施例中采用的数据分配时加密的图。

图 2 是表示一实施例的构成图。

图 3 是一实施例的功能说明图。

图 4 是一实施例的其他功能说明图。

图 5 是一实施例的媒体内的数据结构图。

图 6 是表示一实施例详细构成的方框图。

下面参照附图对实施例进行说明。

首先，利用图 2 说明本发明的一实施例的构成。媒体中设定有媒体固有的 ID，可以在媒体控制器中进行设置。如果媒体是可以记录重放、并可设定固有的 ID，则其也可以是固体存储器及磁盘、磁带等。但条件是 ID 信息具有规定的抗窜改性。即对于 ID 及加密所需要密钥的保管最好处于很难对其非法读出、改写信息的状态。

最简单的是存储器类型，该存储卡具有只通过规定的存储器控制

器才能读出 ID 及加密密钥信息的结构，但要能安全、简单地制成。在工厂生产存储卡时就在每张卡上记录固有的 ID。或者通过发行装置进行发行时，将该存储器固有的 ID 记录在 EEPROM 等中之后，用树脂封装等方法埋入。这样，以后就无法变更用户对应密钥信息了，即不能进行非法窜改。在媒体上具有只可对一部分数据进行媒体间复制的媒体总线。

媒体控制器设置媒体，连接到 PC 机或专用设备等终端上。媒体控制器具有媒体内的数据、与终端的接口功能，和用规定的 ID 进行数据加密、及解码功能。媒体控制器具有从终端不能对存储器的内部进行非法存取的抗窜改性。终端连接到将外部的内容信息进行信息分配的中心（分配信息中心），经过收费、认证等规定的手续后，接收内容信息。与中心的连接除了因特网等网络外，也可以与 ISDN 及广播、有线电视、PHS 等进行无线连接。

内容信息基本上是对每个内容以不同的密钥（内容密钥）进行加密。内容在通过 MPEG 等的规定压缩方式压缩之后，进行 DES 等加密。例如 DES 的情况下，加密密钥为 64 位左右。数据库、中心与终端间的关系如图 1 所示。在中心内设置的数据库对内容信息进行管理，用加密密钥 G1 对内容 X1 加密，用加密密钥 G2 对不同的内容 X2 加密。

在该中心中，多个终端由网络进行连接。向终端的信息传输考虑到安全性，以公开密钥方式进行加密发送。此处以终端 1（T1）的公开密钥为 T1P、解码密钥为 T1D，则由数据库 1 管理的内容 X1 由加密密钥 G1 加密，变为所称的 EG1（X1）加密内容信息。加密密钥 G1 为了向终端 T1 发送信息，使用终端 T1 的公开密钥 T1P 进行加密，变为加密密钥的信息 ET1P（G1）。并将加密内容信息 EG1（X1）和加密密钥的信息 ET1P（G1）两个信息发送给终端 1（T1）。

在终端 1 上为了重放该内容信息，利用终端 1 的解码密钥 T1D，

对加密密钥的信息 ET1P（G1）进行解码，得到加密密钥 G1，由该加密密钥 G1 对加密内容信息 EG1（X1）进行解码，得到内容 X1，通过进行 MPEG 等解码就可以重放。但其前提是不在终端上重放所发送的数据，而是直接记录在与终端连接的媒体上。上面说明了使用公开密钥向终端发送的数据情况，但本发明既可以支持共用密钥方式也可以支持其他方式。

下面参照图 3、4、5，对本发明的内容信息和密钥信息的交接功能进行说明。

首先说明在终端 T1 侧的媒体 A（第 1 媒体）上从信息分配中心接受内容数据的情况。先在媒体控制器设置媒体 A。终端 T1 设置媒体控制器，形成“数据记录方式”。进行收费、认证等规定手续。当手续结束后，由规定的加密密钥 G1 对内容数据加密，从中心向终端进行信息分配。

即，发送由加密密钥 G 1 对内容 X 进行加密的加密内容信息 EG1（X）。另外，为了将加密密钥 G1 发送给终端，使用终端 T1 的公开密钥 T1P 对加密密钥 G1 进行加密的加密密钥信息 ET1P（G1）发送到终端 T1。由于在终端用于解码的密钥是 T1D，所以该加密密钥信息 ET1P（G1）可由解码密钥 T1D 解码。使该状态表现为 ET1P（G1）。在终端上再用解码密钥 T1D 对该加密密钥信息 ET1P（G1）进行解码，得到加密密钥 G1。由解码的加密密钥 G1 对内容数据 X 进行解码，将该内容数据 X 传送给媒体 A。

下面参照图 3 对在媒体上通过媒体的 ID 对内容重新加密 R 方式进行说明。

当媒体控制器接收该内容数据 X 时，在媒体控制器内部将媒体 A 的 ID 作为 ID 密钥重新加密。在媒体 A 上记录第一加密内容信息 EA

（X）。若直接将该加密内容复制在媒体 B 上，由于媒体 B 中 ID=B，所以不能重放该 EA（X）。但是在媒体 A 上解码，将可重放状态的新信号数据向媒体 B 传输的话，就存在安全上的问题。

为此，如图 3（1）所示，在媒体 A 侧读取复制端媒体的 ID=B，先在媒体 A 侧，将 ID=A 作为 ID 密钥，对加密的内容数据进行解码，再将复制端的 ID=B 作为 ID 密钥进行再加密，作为第二加密内容信息 EB（X）传输给媒体 B。

或者如图 3（2）所示，将由 ID=A 进行加密的内容数据 EA（X）直接传输给媒体 B，在媒体 B 上读取复制源的媒体 A 的 ID，对由 ID=A 加密的内容数据进行解码，由 ID=B 再加密，作为 EB（X）进行记录。这样，由于内容数据以其中某一个 ID 加密的状态进行传输，所以可保证安全性。

另外，在一个记录装置中，也可以任意选择图 3（1）中所示的方法和图 3（2）中所示的方法中的一种。

下面参照图 4 说明由内容密钥（加密密钥）加密的加密内容信息、及将在此使用的内容密钥（加密密钥）再作为用与该媒体或者终端的 ID 相关的信息作为 ID 密钥进行加密的情况。首先说明在终端 T1 侧的媒体 A（第一媒体）上从信息分配中心接收内容数据的情况。先在媒体控制器设置媒体 A。终端 T1 设置媒体控制器，形成“数据记录方式”。进行收费、认证等规定的手续。手续结束后，由规定的加密密钥 G1 对内容数据加密，从中心向终端分配信息。

即，发送用加密密钥 G1 对内容 X 进行加密的加密内容信息 EG1（X）。另外，为了将加密密钥 G1 发送给终端 T1，使用终端 T1 的公开密钥 T1P 对加密密钥 G1 进行加密的加密密钥信息 ET1P（G1）发送给终端 T1。由于在终端上用于解码的密钥是 T1D，所以该加密密钥信

息 ET1P(G1)可以用解码密钥 T1D 解码。使该状态表现为 ET1P(G1)。在终端上用解码密钥 T1D 对该加密密钥信息 ET1P（G1）进行解码，得到加密密钥 G1。

媒体控制器接收该数据，在媒体 A 上记录加密内容信息 EG1（X），同时媒体控制器识别所放置的媒体的 ID，以媒体 A 的固有 ID 的 A 值对该密钥 G1 进行再加密，得到第一加密密钥信息 EA（G1），将其记录在媒体 A 上。这时的数据结构例如图 5 所示。在加密内容信息的头部记录有 64 位的加密密钥信息。该结构也不一定是一体化的，如果能够进行成对管理，分离开也可以。

即使将该第一加密密钥信息 EA（G1）直接复制在媒体 B 上，由于媒体 B 上是 ID=B，所以不能对该 EA（G1）进行解码。为此，如图 4（1）所示，在媒体 A 侧读取复制目标端媒体的 ID，先在媒体 A 侧对以 ID=A 加密的第一加密密钥信息 EA（G1）进行解码，再由复制端的 ID=B 进行再加密，变为第二加密密钥信息 EB（G1），传输给媒体 B。

或者如图 4（2）所示，将以 ID=A 加密的第一加密密钥信息 EA（G1）直接传输给媒体 B，在媒体 B 侧，读取复制源的媒体 A 的 ID，对由 ID=A 加密的第一加密密钥信息 EA（G1）进行解码，以 ID=B 进行再加密，变为第二加密密钥信息 EB（G1），进行记录。

这样，不仅以内容数据被加密的状态 EG1（X）进行传输，加密密钥 G1 也可以以其中某个媒体的 ID 进行加密的状态（EA（G1）或 EB（G1））进行传输，所以可确保安全性。

当内容数据 X 的容量很大时，如图 4 所示，采用再以与该媒体或终端的 ID 相关的信息作为 ID 密钥对加密内容信息 EG（X）的加密密钥（内容密钥）G1 进行加密的方式（用 EA（G1）或 EB（G1）的方式），由于只对密钥信息进行解码、加密的方法进行复制，因此可以

高速地操作。

另外，在一个记录装置中，也可以任意选择图 4（1）中所示的方法和图 4（2）中所示的方法中的一种。

下面参照图 6 对本发明的内容信息记录装置的一实施例的方框图进行说明。该方框图采用了对加密密钥（内容密钥）G1 再用与该媒体或终端的 ID 相关的信息作为 ID 密钥进行加密的方式（采用 EA（G1）或 EB（G1）的方式），下面以从图 4（1）的媒体 A 向媒体 B 的记录为例进行说明。

首先说明在媒体 A 上从信息分配中心接收内容数据的情况。先在媒体控制器 21 设置媒体 A。再由终端 T1 来设置媒体控制器 21，通过外部接口由媒体控制器 21 的方式设定部 51 设定为“数据记录方式”。当收费、认证等规定手续结束后，从中心以规定的加密密钥 G1 对内容数据 X 进行加密，作为加密内容信息 EG1（X）对终端 T1 进行信息分配。在“数据记录方式”时，方式设定部 51 使开关 1 和开关 2 切换到与密钥加密部 52 相连接的状态。

为了从中心将加密密钥 G1 与加密内容信息 EG1（X）一起发送给终端 T1，则使用 T1 的公开密钥 T1P，发送对加密密钥 G1 进行加密的 ET1P（G1）。由于在终端 T1 上用于解码的密钥是 T1D，所以该加密密钥信息 ET1P（G1）可以由 T1D 进行解码。使该状态表现为 ET1P（G1）。在终端 T1 上以 T1D 对该加密密钥信息 ET1P（G1）解码。

媒体控制器 21 接收该数据，在媒体 A 上记录该 EG1（X），媒体控制器 21 由媒体 ID 读取部 53 识别被设置的媒体 A 的 ID，在密钥加密部 52 上以 ID=A 对加密密钥 G1 进行加密，将加密密钥信息 EA(G1) 发送给加密密钥信息写入部 54。在加密密钥信息写入部 54，将加密密钥信息记录在由媒体 A 记录的加密内容信息 EG1(X)的头部 64 位中。

下面说明对媒体 A 中记录的加密内容信息 EG1（X）进行重放的情况。在媒体控制器 21 设置媒体 A，通过外部接口由媒体控制器 21 的方式设定部 51 设定为“数据重放方式”。由媒体 A 侧的媒体 ID 发生部 31 产生的信号，通过媒体控制器 21 的媒体 ID 读取部 53 检测媒体的 ID=A，发送给加密密钥解码部 56。

媒体控制器 21 从媒体 A 的存储部 32 读出加密内容信息 EG1（X），发送给加密密钥信息读取部 55。加密密钥信息读取部 55 读取位于头部的 64 位加密密钥信息，通过开关 1 将加密密钥信息 EA（G1）发送给加密密钥解码部 56。当由方式设定部 51 设定为“数据重放方式”时，开关 1 转换到加密密钥解码部 56 侧。

在加密密钥解码部 56，使用输入的媒体 ID=A，对加密密钥信息 EA（G1）进行解码。将解码的加密密钥 G1 发送给加密内容数据解码部 57。另外，由加密密钥信息读取部 55 除去头部的加密内容数据，发送给加密内容数据解码部 57。在加密内容数据解码部 57，通过所输入的加密内容数据 EG1（X）和加密密钥 G1 对加密内容数据进行解码，作为重放数据输出。

下面说明从媒体 A 向媒体 B 复制内容数据的情况。在从记录有内容的复制源媒体 A 向复制目标端媒体 B 复制加密内容信息 EG1（X）时，首先在媒体控制器 21 设置媒体 A。通过外部接口，由媒体控制器 21 的方式设定部 51 设定为“数据复制输出方式”。

由媒体 A 的媒体 ID 发生部 31 产生的信号，通过媒体控制器 21 的媒体 ID 读取部 23 检测媒体的 ID=A，发送给加密密钥解码部 56。由方式设定部 51 设定为“数据复制输出方式”时，开关 1、2 切换为与加密密钥解码部 56 相连接的状态。

在媒体 A 上所记录的加密内容信息 EG1（X）发送给加密密钥信息读取部 55，在此读取头部 64 位的加密密钥信息 EA（G1）。所读取的加密密钥信息 EA（G1）发送给加密密钥解码部 56。在加密密钥解码部 56 中，从输入的 ID=A 和加密密钥信息 EA（G1）对加密密钥 G1 进行解码，暂时记录在密钥存储器 58 中。

另一方面，加密内容数据 EG1（X）被存储在媒体 A 侧的存储部 32 的数据移动用区域中，通过媒体总线 33，高速传送给连接在媒体总线 33 上的媒体 B。该媒体总线将媒体 A 和媒体 B 进行物理连接，进行数据传输。由于传输的数据本身只有加密内容数据才能通过该媒体总线，所以安全性很高。

接着在媒体控制器 21 设置媒体 B。通过媒体控制器 21 的媒体 ID 读取部 53 检测出媒体的 ID=B。当由方式设定部 51 设定为“数据复制输入方式”时，开关 1、2 切换到与密钥加密部 52 连接的状态。在密钥加密部 52 上，从密钥存储器 58 读出加密密钥 G1，使用从媒体 ID 读取部 53 输入的 ID=B，用 ID=B 对加密密钥 G1 进行加密，变为 EB（G1）。加密密钥信息 EB（G1）被送到加密密钥信息写入部 54。加密密钥信息 EB（G1）被记录在媒体 B 的存储部 32B 中。

下面说明对在媒体 B 中所记录的加密内容信息 EG1（X）进行重放的情况。这与对在媒体 A 中所记录的加密内容信息 EG1（X）进行重放的情况相同。即，在媒体控制器 21 设置媒体 B，通过外部接口，由媒体控制器 21 的方式设定部 51 设定为“数据重放方式”。由媒体 B 侧的媒体 ID 发生部 31B 产生的信号，通过媒体控制器 21 的媒体 ID 读取部 53 检测出媒体的 ID=B，发送给加密密钥解码部 56。

媒体控制部 21 从媒体 B 的存储部 32B 读出加密内容信息 EG1（X），发送给加密密钥信息读取部 55。加密密钥信息读取部 55 读出位于头部的 64 位加密密钥信息，通过开关 1 将加密密钥信息 EB（G1）

发送给加密密钥解码部 56。当由方式设定部 51 设定为“数据重放方式”时，开关 1 切换到加密密钥解码部 56 侧。

加密密钥解码部 56 使用所输入的媒体 ID=B，对加密密钥信息 EB（G1）进行解码。解码的加密密钥 G1 被发送给加密内容数据解码部 57。另外，由加密密钥信息读取部 55 除去头部后的加密内容数据被发送给加密内容数据解码部 57。在加密内容数据解码部 57，通过输入的加密内容数据 EG1（X）和加密密钥 G1，对加密内容数据进行解码，输出作为重放数据的内容数据 X。

这样，在本实施例的记录装置中，不仅内容数据以加密的状态 EG1（X）进行传输，而且加密密钥 G1 也以媒体 B 的 ID 加密的状态（EB（G1））进行传输，所以可确保安全性。

在上述实施例中，是在发送侧（媒体 A 侧）对加密密钥 G1 进行解码，用媒体 B 的 ID 进行再加密处理。从而，在接收专用的媒体控制器中就不需要密钥加密部 52、开关 1、2 了，可以构造只能发送给系统所限定的用户的系统。

另外，当从媒体 A 向媒体 B 对内容数据不是复制而是转让时，从媒体 A 侧至少消去加密密钥信息 EA（G1）及加密内容数据 EG1（X）中的一个。

作为实现图 3（1）所示方法的记录装置，在媒体 A 侧设置记录装置，暂时解除第一加密内容信息 EA（X）的密码，以从媒体 B 侧输出的媒体 B 的 ID=B 作为 ID 密钥，对内容信息进行再加密，得到第二加密内容信息 EB（X），将该第二加密内容信息 EB（X）输出给媒体 B 侧，使第二加密内容信息 EB（X）记录在媒体 B 中。

说 明 书 附 图

图1

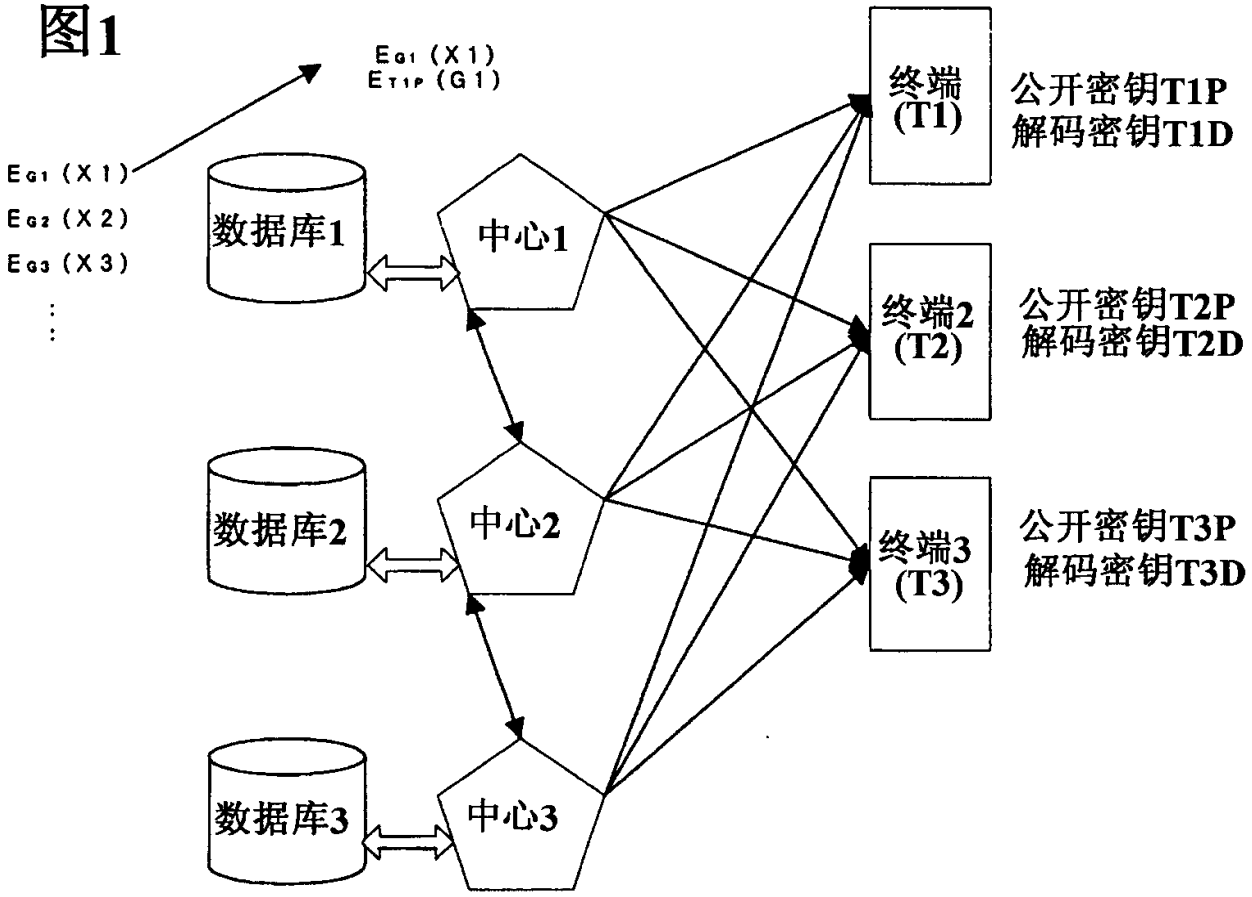

EG1 (X1)
ET1P (G1)
EG1 (X1)
EG2 (X2)
EG3 (X3)
数据库1
数据库2
数据库3
中心1
中心2
中心3
终端 (T1)
终端2 (T2)
终端3 (T3)
公开密钥T1P
解码密钥T1D
公开密钥T2P
解码密钥T2D
公开密钥T3P
解码密钥T3D

图2

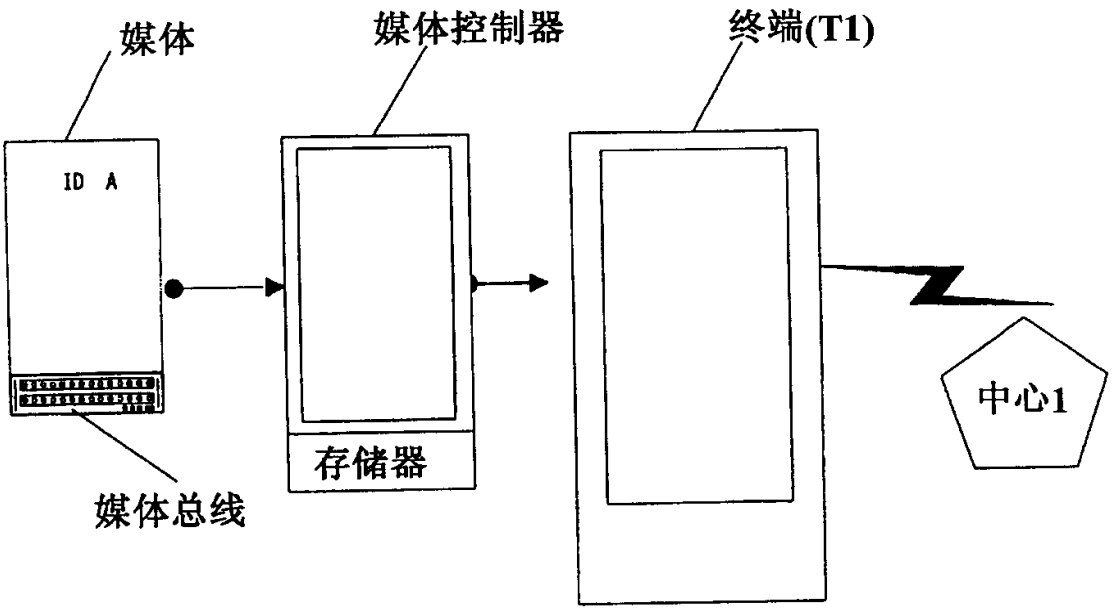


图3

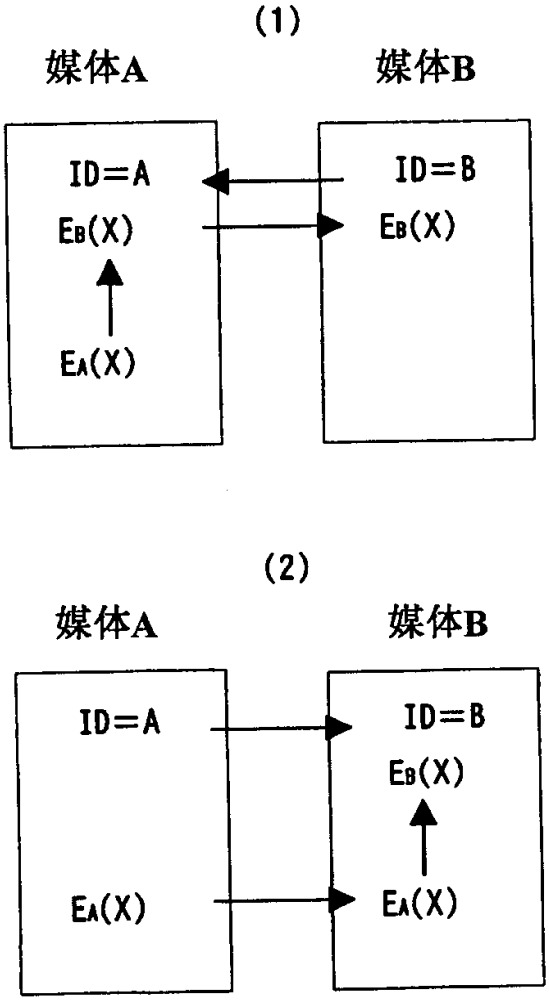


图4

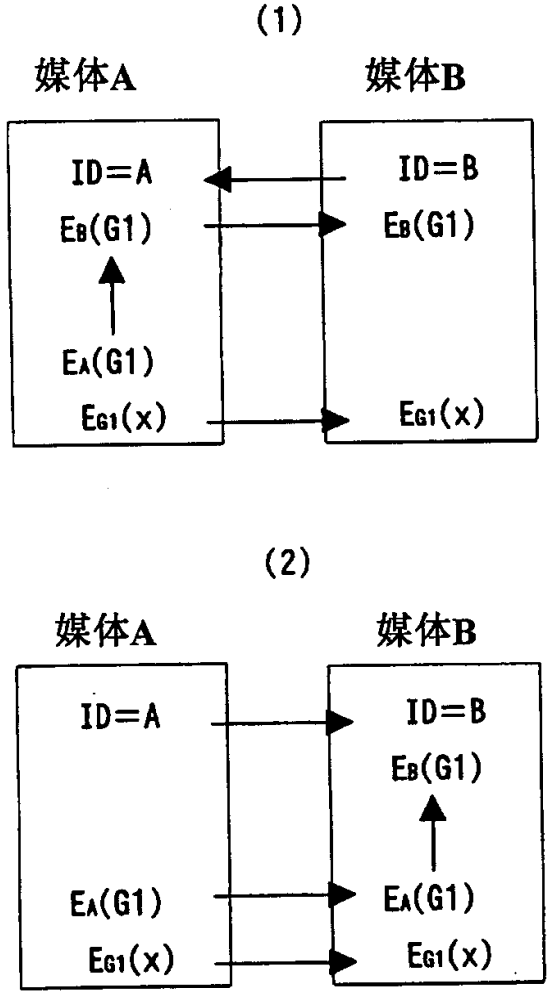

(1)
媒体A
媒体B
ID=A
EB(G1)
EA(G1)
EG1(x)
ID=B
EB(G1)
EG1(x)
(2)
媒体A
媒体B
ID=A
EA(G1)
EG1(x)
ID=B
EB(G1)
EA(G1)
EG1(x)

图5

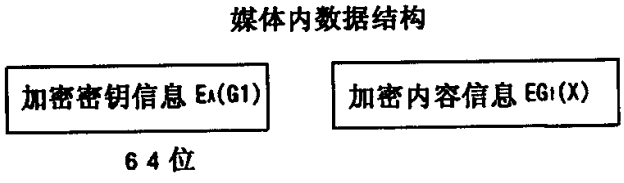
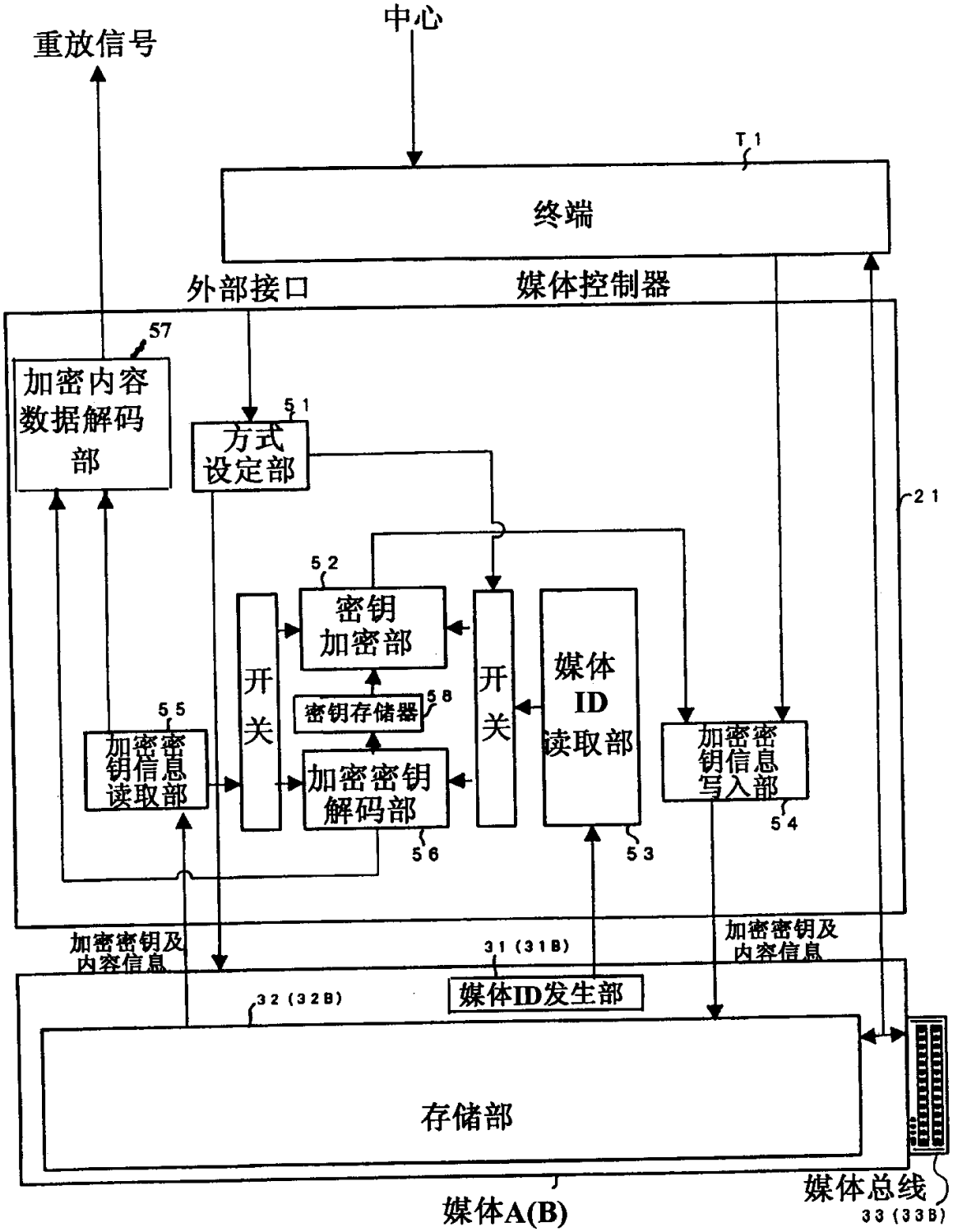

媒体内数据结构
加密密钥信息 EA(G1)
加密内容信息 EG1(X)
64位

图6


重放信号
中心
T1
终端
外部接口
媒体控制器
57
加密内容数据解码部
51
方式设定部
21
52
密钥加密部
开关
开关
媒体ID读取部
密钥存储器
58
55
加密密钥信息读取部
加密密钥解码部
56
53
加密密钥信息写入部
54
加密密钥及内容信息
31(31B)
加密密钥及内容信息
32(32B)
媒体ID发生部
存储部
媒体A(B)
媒体总线
33(33B)