(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102694648 A
(43)申请公布日 2012.09.26

(21)申请号 201210029102.7
(22)申请日 2012.02.10
(30)优先权数据
2011-027300 2011.02.10 JP
(71)申请人 索尼公司
地址 日本东京都
(72)发明人 林隆道 久野浩 加藤元树
上田健二朗 小林义行 山本和夫
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 郭定辉
(51)Int.Cl.
H04L 9/30(2006.01)
H04L 9/06(2006.01)
G06F 21/00(2006.01)

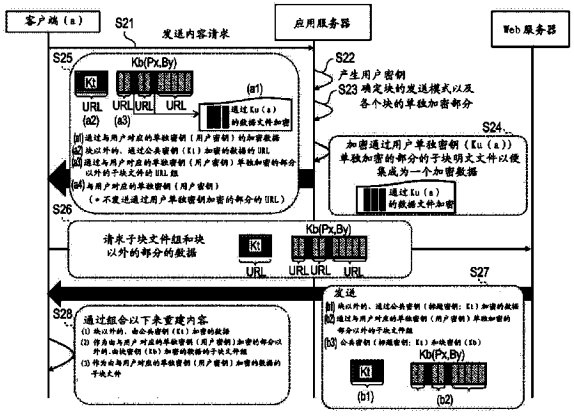
权利要求书 3 页 说明书 21 页 附图 21 页

(54)发明名称

信息处理设备、信息处理方法和程序

(57)摘要

信息处理设备包括：数据处理单元，配置为产生要供给客户端的内容，数据处理单元从原始内容提取多个块（块1到i）作为内容配置数据，将模式1到k设为包括提取的块1到i的块行的多个模式，产生应用根据各个模式和各个块不同的块密钥Kb(Px，By)的加密块，Px指示k个模式标识符(P1到Pk)，By指示i个块标识符(B1到Bi)，在每个内容发送中随机从模式1到k选择加密块1到i，通过应用与作为内容发送目的地的客户端对应的单独密钥（用户密钥Ku）加密所选块的部分配置数据以产生单独加密部分，产生包括执行通过块密钥Kb(Px，By)的加密处理的加密块和执行通过单独密钥（用户密钥Ku）的加密处理的单独加密部分的加密内容作为要供给客户端的内容。



CN 102694648 A

1. 一种信息处理设备，包括：

数据处理单元，其配置为产生要提供给客户端的内容，

其中，所述数据处理单元

从原始内容中提取多个块（块 1 到 i）作为内容配置数据，

将模式 1 到 k 设置为包括所提取的块 1 到 i 的块行的多个模式，

产生应用根据各个模式和各个块不同的块密钥 Kb(Px,By) 的加密块，其中 Px 指示 k 个模式标识符 (P1 到 Pk)，By 指示 i 个块标识符 (B1 到 Bi)，

在每一个内容发送中随机地从模式 1 到 k 中选择加密块 1 到 i，

通过应用与作为内容发送目的地的客户端对应的单独密钥（用户密钥 Ku）来加密所选择块的配置数据的一部分，从而产生单独加密的部分，以及

产生包括执行了通过块密钥 Kb(Px，By) 的加密处理的加密块以及执行了通过单独密钥（用户密钥 Ku）的加密处理的单独加密部分的加密内容，作为要提供给客户端的内容。

2. 如权利要求 1 所述的信息处理设备，

其中，所述数据处理单元执行将以下各部分发送到客户端的处理

执行了通过块密钥 Kb(Px，By) 的加密处理的加密块，

执行了通过单独密钥（用户密钥 Ku）的加密处理的单独加密部分，以及

应用于加密块的解密处理的块密钥 Kb(Px，By) 和单独密钥（用户密钥 Ku）。

3. 如权利要求 1 所述的信息处理设备，

其中，所述数据处理单元产生用于识别作为提供目的地的客户端的客户端标识信息与待提供的内容的块排列信息相关联的管理信息，并且将管理信息存储在存储单元中。

4. 如权利要求 3 所述的信息处理设备，

其中，所述数据处理单元进一步产生所述客户端标识信息与提供给客户端的加密密钥信息相关联的管理信息，并且将管理信息存储在存储单元中。

5. 如权利要求 3 所述的信息处理设备，

其中，所述数据处理单元执行分发内容中包括的块排列的分析处理，以通过执行分析的块排列信息与所述管理信息的登记信息之间的检查处理来识别作为内容发送目的地的客户端。

6. 如权利要求 4 所述的信息处理设备，

其中，所述数据处理单元通过执行分发的块密钥或单独密钥中的至少一个的密钥信息与所述管理信息的登记信息之间的检查处理，识别作为块密钥或单独密钥的发送目的地的客户端。

7. 如权利要求 1 所述的信息处理设备，

其中，所述数据处理单元以通过进一步分割块所获得的子块为单位，执行单独加密部分的设置。

8. 如权利要求 1 所述的信息处理设备，

其中，所述数据处理单元通过应用对于向其发送内容的多个客户端共同的公共密钥来加密从原始内容中提取的多个块以外的块区域外部的数据，并且产生执行了通过公共密钥的加密的块区域外部的数据，作为提供给客户端的内容。

9. 如权利要求 8 所述的信息处理设备，

其中，所述公共密钥是与内容的标题对应的标题密钥 Kt。

10. 如权利要求 1 所述的信息处理设备，

其中，所述数据处理单元产生包括内容的加密配置信息的内容配置信息，作为要提供给客户端的数据。

11. 一种内容发送系统，包括：

内容提供单元，其关于客户端执行内容提供处理；以及

所述客户端，其从所述内容提供单元接收内容，

其中，要提供给客户端的内容包括多个块和块区域外部的数据，

所述内容提供单元的配置单元 A 在存储单元中存储

(1) 通过公共密钥 (Kt) 加密块区域外部的数据所获得的公共密钥加密的数据，以及

(2) 分别通过彼此不同的块密钥 (Kb) 加密块数据所获得的加密的块数据；

所述内容提供单元的配置单元 B 在存储单元中存储

(3) 块数据的明文数据，

所述内容提供单元的配置单元 B 根据来自客户端的内容的请求，

产生与客户端对应的单独密钥（用户密钥），

选择要提供给客户端的块数据，

通过要提供给客户端的、与客户端对应的单独密钥（用户密钥）加密所选择的块的配置数据的一部分，以及

向客户端提供数据标识信息，用于识别通过单独密钥（用户密钥）加密的数据以外的内容配置数据，并且

所述内容提供单元的配置单元 A 从客户端接收数据标识信息，并向客户端提供由接收到的数据标识信息指定的数据。

12. 如权利要求 11 所述的内容发送系统，

其中，用于识别内容配置数据的数据标识信息是 URL（统一资源定位符）。

13. 一种信息处理设备，包括：

数据处理单元，其配置为执行内容再现处理，

其中，所述数据处理单元通过参照作为内容的加密配置信息的内容配置信息来确定通过公共密钥加密的区域、通过块密钥加密的区域以及通过与用户对应的单独密钥加密的区域，并且通过切换公共密钥、块密钥和单独密钥来执行解密处理以执行内容的再现。

14. 如权利要求 13 所述的信息处理设备，

其中，通过块密钥加密的区域包括分别由不同的块密钥加密的多个块区域，以及

所述数据处理单元确定加密区域的各个块通过哪些块密钥加密，并通过参照内容配置信息切换块密钥来执行解密处理。

15. 一种由信息处理设备执行的信息处理方法，所述信息处理设备产生要向客户端提供的内容，所述信息处理方法包括：

通过所述信息处理设备

从原始内容中提取多个块（块 1 到 i）作为内容配置数据；

将模式 1 到 k 设置为包括所提取的块 1 到 i 的块行的多个模式，

产生应用根据各个模式和各个块不同的块密钥 Kb(Px,By) 的加密块，其中 Px 指示 k 个

模式标识符 (P1 到 Pk)，By 指示 i 个块标识符 (B1 到 Bi)，

在每一个内容发送中随机地从模式 1 到 k 中选择加密块 1 到 i，

通过应用与作为内容发送目的地的客户端对应的单独密钥 (用户密钥 Ku) 来加密所选择块的配置数据的一部分，从而产生单独加密的部分，以及

产生包括执行了通过块密钥 Kb(Px，By) 的加密处理的加密块以及执行了通过单独密钥 (用户密钥 Ku) 的加密处理的单独加密部分的加密内容，作为要提供给客户端的内容。

16. 一种由执行内容再现处理的信息处理设备执行的信息处理方法，包括 ：

通过参照作为内容的加密配置信息的内容配置信息来确定通过公共密钥加密的区域、通过块密钥加密的区域以及通过与用户对应的单独密钥加密的区域 ；以及

通过切换公共密钥、块密钥和单独密钥来执行解密处理以执行内容的再现。

17. 一种允许信息处理设备执行如下信息处理的程序，所述信息处理设备产生要提供给客户端的内容 ：

通过所述信息处理设备

从原始内容中提取多个块 (块 1 到 i) 作为内容配置数据 ；

将模式 1 到 k 设置为包括所提取的块 1 到 i 的块行的多个模式，

产生应用根据各个模式和各个块不同的块密钥 Kb(Px,By) 的加密块，其中 Px 指示 k 个模式标识符 (P1 到 Pk)，By 指示 i 个块标识符 (B1 到 Bi)，

在每一个内容发送中随机地从模式 1 到 k 中选择加密块 1 到 i，

通过应用与作为内容发送目的地的客户端对应的单独密钥 (用户密钥 Ku) 来加密所选择块的配置数据的一部分，从而产生单独加密的部分，以及

产生包括执行了通过块密钥 Kb(Px，By) 的加密处理的加密块以及执行了通过单独密钥 (用户密钥 Ku) 的加密处理的单独加密部分的加密内容，作为要提供给客户端的内容。

18. 一种允许执行内容再现处理的信息处理设备执行如下信息处理的程序 ：

通过参照作为内容的加密配置信息的内容配置信息来确定通过公共密钥加密的区域、通过块密钥加密的区域以及通过与用户对应的单独密钥加密的区域 ；以及

通过切换公共密钥、块密钥和单独密钥来执行解密处理以执行内容的再现。

信息处理设备、信息处理方法和程序

技术领域

[0001] 本公开涉及信息处理设备、信息处理方法和程序。特别地，本公开涉及在能够防止内容的非法使用或者跟踪非法分发内容源的系统中使用的信息处理设备、信息处理方法和程序。

背景技术

[0002] 近年来，经由网络（如，因特网）的数据通信已经被广泛使用，并且大量图像数据、音乐数据等经由网络广阔地分发。

[0003] 由制造商、销售商持有许多内容（如，音乐数据和图像数据）的版权、分发权。因此，例如，当服务提供商经由网络从服务器向用户提供内容时，常见的是，进行控制以便仅允许具有授权的使用权的用户来使用内容。

[0004] 具体来说，例如，执行将内容作为加密内容发送的控制，所述加密内容仅可以通过向已经进行了正常内容购买处理的用户提供的加密密钥来解密。然而，即使当执行以上控制时，如果由已经获取了加密内容或加密密钥的用户解密的内容被非法分发或公开，则仍会出现不特定数量的内容的非法使用。特别在近年中，广泛地进行经由网络的数据的非法公开和发送，并且如何防止非法行为是个大问题。

[0005] 将参照附图说明加密密钥和内容的非法分发的特定示例。

[0006] 图 1 是示出加密密钥的非法公开的示例的图。内容发送服务器 10 提供通过将加密密钥 12 应用于已经完成了正常内容购买过程的客户端 A21 和 B22 以加密密钥 12 加密的加密内容 11。

[0007] 客户端 A21 和客户端 B22 可以通过应用加密密钥 12 来解密加密内容 11，从而再现内容。

[0008] 假设这样的情况 :客户端 B22 通过使用加密密钥 12，例如在可以由任何人访问的网络一侧进行了公开加密密钥 12 的动作。

[0009] 当进行公开密钥的处理时，可以由不特定数量的用户获取公开的加密密钥 31。

[0010] 结果，例如，可以由尚未完成正常内容购买的未授权用户 23 经由网络获取公开的加密密钥 31，进一步，通过使用公开的加密密钥 31，可以解密和再现从另一客户端等获取的加密内容的拷贝 32。

[0011] 如果这种情形发生，则内容的非法使用将会广泛蔓延。

[0012] 由于在图 1 的示例中向所有客户端提供相同的加密密钥，因此如果一个非法人泄露了密钥，那么可以通过非法密钥来解密向其它客户端提供的所有内容。识别已经非法公开密钥的客户端是困难的。

[0013] 作为解决以上问题的方法，通过不同的加密密钥来加密要向各个客户端提供的加密内容的配置是有效的。

[0014] 即，如图 2 所示，内容发送服务器 10 提供通过将加密密钥 A14 应用于客户端 A24 以加密密钥 A14 加密的加密内容，提供通过将加密密钥 B15 应用于客户端 B25 以加密密钥

B15 加密的加密内容，并且提供通过将加密密钥 C16 应用于客户端 C26 以加密密钥 C16 加密的加密内容。

[0015] 根据以上设置，如果万一泄露了任何加密密钥，则可通过泄露密钥解密的内容限于通过泄露密钥加密的一个加密内容，并且可以识别泄露源（即，已经公开了加密密钥的未授权客户端）。

[0016] 然而，内容发送服务器 10 必须产生根据各个客户端而不同的加密内容，用于针对各个客户端改变加密密钥，这引起服务器侧的处理负荷增大的问题。

[0017] 参照图 1 和图 2 说明的示例是进行应用于内容的加密 / 解密处理的加密密钥的非法公开 / 泄露的示例。不仅加密密钥，而且解密内容也可以是非法公开 / 泄露的目标。

[0018] 图 3 示出了解密内容的非法公开的示例。

[0019] 内容发送服务器 10 向客户端 28 提供通过应用加密密钥 12 加密的加密内容 11。执行提供处理，作为正常的内容购买处理。

[0020] 然而，当客户端 28 通过应用加密密钥 12 来解密加密内容 11 并且非法公开解密内容 11 时，结果，非法公开内容 33 变为处于由包括图 3 中所示的未授权用户 29 的不特定数量的用户可用的状态。

[0021] 如果公开解密内容，则解密内容的非法使用将广泛蔓延，并且即使当对于每个客户端改变加密密钥时，也难以识别已经非法公开了解密内容的客户端。

发明内容

[0022] 鉴于以上情形，期望提供能够识别非法公开的内容的公开源的信息处理设备、信息处理方法和程序。

[0023] 还期望提供实现能够识别已经非法公开了内容的公开源而不过度地增大服务器的处理负荷的配置的信息处理设备、信息处理方法和程序。

[0024] 根据本公开的实施例针对一种信息处理设备，包括 :数据处理单元，其配置为产生要提供给客户端的内容，其中所述数据处理单元从原始内容中提取多个块（块 1 到 i），作为内容配置数据，将模式 (pattern)1 到 k 设置为包括所提取的块 1 到 i 的块行的多个模式，产生应用根据各个模式和各个块不同的块密钥 Kb(Px,By) 的加密块，其中 Px 指示 k 个模式标识符 (P1 到 Pk)，并且 By 指示 i 个块标识符 (B1 到 Bi)，在每一个内容发送中随机地从模式 1 到 k 中选择加密块 1 到 i，通过应用与作为内容发送目的地的客户端对应的单独密钥（用户密钥 Ku）来加密所选择块的配置数据的一部分，从而产生单独加密的部分，以及产生包括执行了通过块密钥 Kb(Px,By) 的加密处理的加密块以及执行了通过单独密钥（用户密钥 Ku）的加密处理的单独加密部分的加密内容，作为要提供给客户端的内容。

[0025] 在根据本公开实施例的信息处理设备中，所述数据处理单元可以执行发送执行了通过块密钥 Kb(Px，By) 的加密处理的加密块、执行了通过单独密钥（用户密钥 Ku）的加密处理的单独加密部分、以及应用于加密块的解密处理的块密钥 Kb(Px，By) 和单独密钥（用户密钥 Ku）到客户端的处理。

[0026] 此外，在根据本公开实施例的信息处理设备中，所述数据处理单元可以产生用于识别作为提供目的地的客户端的客户端标识信息与待提供的内容的块排列信息 (block arrangement information) 相关联的管理信息，并且可以将所述管理信息存储在存储单元

中。

[0027] 此外，在根据本公开实施例的信息处理设备中，所述数据处理单元可以进一步产生所述客户端标识信息与提供给客户端的加密密钥信息相关联的管理信息，并且可以将所述管理信息存储在存储单元中。

[0028] 此外，在根据本公开实施例的信息处理设备中，所述数据处理单元可以执行分发内容中包括的块排列的分析处理，以通过执行分析的块排列信息与所述管理信息的登记信息之间的检查处理来识别作为内容发送目的地的客户端。

[0029] 此外，在根据本公开实施例的信息处理设备中，所述数据处理单元可以通过执行分发的块密钥或单独密钥中的至少一个的密钥信息与所述管理信息的登记信息之间的检查处理来识别作为块密钥或单独密钥的发送目的地的客户端。

[0030] 此外，在根据本公开实施例的信息处理设备中，所述数据处理单元可以以通过进一步分割块所获得的子块为单位，执行单独加密部分的设置。

[0031] 此外，在根据本公开实施例的信息处理设备中，所述数据处理单元可以通过应用对于向其发送内容的多个客户端共同的公共密钥来加密从原始内容中提取的多个块以外的块区域外部的数据，并且可以产生执行了通过公共密钥的加密的块区域外部的数据，作为提供给客户端的内容。

[0032] 此外，在根据本公开实施例的信息处理设备中，所述公共密钥可以是与内容的标题对应的标题密钥 Kt。

[0033] 此外，在根据本公开实施例的信息处理设备中，所述数据处理单元可以产生包括内容的加密配置信息的内容配置信息，作为要提供给客户端的数据。

[0034] 本公开的另一个实施例针对一种内容发送系统，包括：内容提供单元，其关于客户端执行内容提供处理；以及所述客户端，其从所述内容提供单元接收内容，其中要提供给客户端的内容包括多个块和块区域外部的数据，所述内容提供单元的配置单元 A 在存储单元中存储

[0035] (1) 通过公共密钥 (Kt) 加密块区域外部的数据所获得的公共密钥加密的数据，以及

[0036] (2) 分别通过彼此不同的块密钥 (Kb) 加密块数据所获得的加密的块数据，

[0037] 所述内容提供单元的配置单元 B 将在存储单元中存储

[0038] (3) 块数据的明文数据，并且

[0039] 所述内容提供单元的配置单元 B 根据来自客户端的内容的请求产生与客户端对应的单独密钥（用户密钥），选择要提供给客户端的块数据，通过要提供给客户端的、与客户端对应的单独密钥（用户密钥）加密所选择的块的配置数据的一部分，以及向客户端提供数据标识信息，用于识别通过单独密钥（用户密钥）加密的数据以外的内容配置数据，并且所述内容提供单元的配置单元 A 从客户端接收数据标识信息，并向客户端提供由接收到的数据标识信息指定的数据。

[0040] 在根据本公开实施例的内容发送系统中，用于识别所述内容配置数据的所述数据标识信息可以是 URL（统一资源定位符）。

[0041] 本公开的再一个实施例针对一种信息处理设备，包括：数据处理单元，其配置为执行内容再现处理，其中所述数据处理单元通过参照作为内容的加密配置信息的内容配置信

息确定通过公共密钥加密的区域、通过块密钥加密的区域以及通过与用户对应的单独密钥加密的区域，并且通过切换公共密钥、块密钥和单独密钥来执行解密处理以执行内容的再现。

[0042] 在根据本公开实施例的内容发送系统中，通过块密钥加密的区域可以包括分别由不同的块密钥加密的多个块区域，并且所述数据处理单元可以确定加密区域的各个块通过哪些块密钥加密，并通过参照内容配置信息切换块密钥来执行解密处理。

[0043] 本公开的又一个实施例针对一种由信息处理设备执行的信息处理方法，所述信息处理设备产生要向客户端提供的内容，所述信息处理方法包括：通过所述信息处理设备从原始内容中提取多个块（块 1 到 i）作为内容配置数据；将模式 1 到 k 设置为包括所提取的块 1 到 i 的块行的多个模式，产生应用根据各个模式和各个块不同的块密钥 Kb(Px，By) 的加密块，其中 Px 指示 k 个模式标识符 (P1 到 Pk)，并且 By 指示 i 个块标识符 (B1 到 Bi)，在每一个内容发送中随机地从模式 1 到 k 中选择加密块 1 到 i，通过应用与作为内容发送目的地的客户端对应的单独密钥（用户密钥 Ku）来加密所选择块的配置数据的一部分，从而产生单独加密的部分，以及产生包括执行了通过块密钥 Kb(Px，By) 的加密处理的加密块以及执行了通过单独密钥（用户密钥 Ku）的加密处理的单独加密部分的加密内容，作为要提供给客户端的内容。

[0044] 本公开的又一个实施例针对一种由信息处理设备执行的信息处理方法，所述信息处理设备执行内容再现处理，所述信息处理方法包括：通过参照作为内容的加密配置信息的内容配置信息来确定通过公共密钥加密的区域，通过块密钥加密的区域，以及通过与用户对应的单独密钥加密的区域；以及通过切换公共密钥、块密钥和单独密钥来执行解密处理以执行内容的再现。

[0045] 本公开的又一个实施例针对一种允许信息处理设备执行如下信息处理的程序，所述信息处理设备产生要提供给客户端的内容：通过所述信息处理设备从原始内容中提取多个块（块 1 到 i）作为内容配置数据；将模式 1 到 k 设置为包括所提取的块 1 到 i 的块行的多个模式，产生应用根据各个模式和各个块不同的块密钥 Kb(Px，By) 的加密块，其中 Px 指示 k 个模式标识符 (P1 到 Pk)，并且 By 指示 i 个块标识符 (B1 到 Bi)，在每一个内容发送中随机地从模式 1 到 k 中选择加密块 1 到 i，通过应用与作为内容发送目的地的客户端对应的单独密钥（用户密钥 Ku）来加密所选择块的配置数据的一部分，从而产生单独加密的部分，以及产生包括执行了通过块密钥 Kb(Px，By) 的加密处理的加密块以及执行了通过单独密钥（用户密钥 Ku）的加密处理的单独加密部分的加密内容，作为要提供给客户端的内容。

[0046] 本公开的又一个实施例针对一种允许信息处理设备执行如下信息处理的程序，所述信息处理设备执行内容再现处理：通过参照作为内容的加密配置信息的内容配置信息来确定通过公共密钥加密的区域、通过块密钥加密的区域、以及通过与用户对应的单独密钥加密的区域；以及通过切换公共密钥、块密钥和单独密钥来执行解密处理以执行内容的再现。

[0047] 根据本公开实施例的程序例如可以提供给能够以计算机可读格式通过存储介质和通信介质执行各种程序代码信息处理设备和计算机系统。当以计算机可读格式提供这种程序时，在信息处理设备或计算机系统上实现根据该程序的处理。

[0048] 基于后面描述的本公开的实施例和附图，本公开的其它特征和优点将通过详细描

述而清楚化。在本说明书中，系统是指多个设备的逻辑集合，其不限于各个设备处于同一外壳中的配置。

[0049] 根据本公开的实施例，提供了可以在泄露加密内容的加密密钥的情况下防止内容的完全再现的配置。

[0050] 具体来说，在每一个内容发送中，设置其中通过不同块密钥加密作为内容配置数据的块 1 到 i 的模式 1 到 k 并随机地选择块，从而向客户端提供具有不同块 1 到 i 的块排列（模式顺序，pattern sequence）的内容。要提供给客户端的内容的块排列被登记为管理信息。如果泄露了用作一部分内容的加密密钥的公共密钥（标题密钥），则难以再现内容的完全再现。也可以通过从非法分发的内容获取块排列并以管理信息的登记信息检查排列来识别作为非法分发内容的源的客户端。

附图说明

[0051] 图 1 是用于说明由于加密密钥的非法公开而导致的内容的非法使用的示例的视图；

[0052] 图 2 是用于说明由于加密密钥的非法公开而导致的内容的非法使用的示例的视图；

[0053] 图 3 是用于说明由于解密内容的非法公开而导致的内容的非法使用的示例的视图；

[0054] 图 4 是用于说明本公开的概要的视图；

[0055] 图 5 是用于说明由服务器提供的内容的特定示例的图；

[0056] 图 6 是用于说明要由服务器提供的内容的特定示例的图表；

[0057] 图 7 示出规定要由服务器向客户端提供的内容的配置的参数的图；

[0058] 图 8 是用于说明规定要由服务器向客户端提供的内容的配置的特定示例的图表；

[0059] 图 9 是用于说明从服务器向客户端的内容提供处理的顺序的图；

[0060] 图 10 是用于说明服务器的存储单元中保存的管理信息的数据配置示例的图表；

[0061] 图 11 是用于说明由多个服务器关于客户端的内容提供处理的配置示例的图；

[0062] 图 12 是用于说明在多个服务器关于客户端执行内容提供处理的配置中由 Web 服务器保存的数据的配置示例的图；

[0063] 图 13 是用于说明在多个服务器关于客户端执行内容提供处理的配置中由应用服务器保存的数据的配置示例的图；

[0064] 图 14 是用于说明当由多个服务器关于客户端执行内容提供处理时的内容提供处理的顺序的图；

[0065] 图 15 是用于说明客户端中的内容再现处理的示例的图；

[0066] 图 16 是用于说明由服务器（如，服务提供商）执行的内容产生处理的顺序的流程图；

[0067] 图 17 是用于说明由服务器（如，服务提供商）执行的内容提供处理的顺序的流程图；

[0068] 图 18 是用于说明客户端中的内容再现处理的流程图；

[0069] 图 19 是用于说明当发现非法分发内容时执行的源确定处理顺序的流程图；

[0070] 图 20 是用于说明服务器的硬件配置示例的图；以及

[0071] 图 21 是用于说明客户端的硬件配置示例的图。

具体实施方式

[0072] 在下文中，将参照附图说明根据本公开实施例的信息处理设备、信息处理方法和程序。将以如下顺序进行说明。

[0073] 1. 本公开的概要

[0074] 2. 由服务器进行的内容提供处理的特定示例

[0075] 3. 规定内容配置的参数

[0076] 4. 内容发送顺序

[0077] 5. 提供内容的服务器的系统示例

[0078] 6. 客户端中的内容再现处理

[0079] 7. 服务器中的内容产生和提供处理顺序

[0080] 7-1. 服务器中的内容产生处理顺序

[0081] 7-2. 服务器中的内容提供处理顺序

[0082] 8. 客户端中的内容再现顺序

[0083] 9. 基于服务器中的非法分发内容的源确定处理顺序

[0084] 10. 各个设备的硬件配置示例

[0085] [1. 本公开的概要]

[0086] 在下文中，将参照附图详细说明根据本公开实施例的信息处理设备、信息处理方法和程序。

[0087] 将参照图 4 说明本公开的概要。根据本公开的实施例，例如，可以识别网络上分发的非法内容的公开源。

[0088] 由提供内容（如，电影和音乐）的服务提供商管理的服务器示出在图 4 中。

[0089] 例如，客户端 120（如，PC）访问服务器 100，并进行正常的内容购买过程，从而获取内容。客户端 120 经由图 4 中所示的网络上的路径 (a) 获取授权内容。

[0090] 允许客户端 120 的用户在固定用途限制之下执行再现正常购买内容的处理。例如，在发送的内容是加密内容的情况下，授权购买者可以通过使用从服务器提供的用于解密的密钥来解密加密内容以再现内容。

[0091] 然而，存在这样的可能性：客户端 120 的用户经由网络向其它用户（图中所示的客户端 131 到 133 的用户）提供解密内容。例如，可能出现经由图 4 中所示的网络上的路径 (b) 向不特定数量的用户提供解密内容的情形。例如，存在这样的可能性：执行将解密内容放在不特定数量用户可访问的网络上的站点中的处理。

[0092] 还存在这样的情况：客户端 120 的用户通过非法地将解密内容记录在介质（如，盘）中来创建大量非法拷贝的记录介质，并向其它用户提供介质。例如，介质是图 4 中所示的盘 141。

[0093] 根据本公开的实施例，当暴露内容的这种非法分发时，可以识别非法内容的源。在图 4 中所示的情况下，源是客户端 120。也可以实现以上配置而不过度地增大服务器 100 的处理负荷。

[0094] [2. 由服务器进行的内容提供处理的特定示例]

[0095] 如上所述，根据本公开的实施例，可以跟踪非法内容的源。提供授权内容的服务器 100 产生要提供给客户端的具有特有配置的内容。

[0096] 将参照图 5 以及后续的图来说明要由例如服务提供商等管理的服务器（内容发送服务器等）提供给客户端（用户装置）的内容的配置。服务器创建特有内容，用于使得可以识别已经非法公开或分发内容的客户端或用户，向各个客户端提供特有内容。

[0097] 图 5 是用于说明由服务器预先准备的数据的图。

[0098] 在图 5 中，示出了

[0099] (a) 内容，

[0100] (b) 块区域外部的数据，以及

[0101] (c) 块区域中的数据。

[0102] 服务器提取内容中包括的多个部分数据作为块。在这种情况下，当块数为 i 时，提取 i 个块。

[0103] 从内容中提取的块以外的数据区域是图 5 的 (b) 中所示的块区域外部的数据。

[0104] 块区域外部的数据 (b) 通过应用一个加密密钥（标题密钥 (Kt)）而被加密。标题密钥是例如设置到内容的标题的一个加密密钥。

[0105] 关于从内容中提取的 i 个块，产生如图 5 的 (c) 中所示的加密数据。

[0106] 首先，准备 k 块行（其每一个具有从内容中提取的 i 个块）。

[0107] 这些块行是模式 1(P1) 到 k(Pk)。

[0108] 接着，通过应用不同的块密钥来单独加密各个模式中包括的各个块。

[0109] 例如，将应用于模式 1(P1) 的块 (B1) 的加密的块密钥表示为 Kb(P1，B1)。

[0110] 如图 5 所示，将模式 1(P1) 中包括的 i 个块设置为由不同的块密钥（其为块密钥 Kb(P1，B1) 到 Kb(P1，Bi)）加密的加密块的集合。

[0111] 此外，将模式 2(P2) 中包括的 i 个块设置为由不同的块密钥（其为块密钥 Kb(P2，B1) 到 Kb(P2，Bi)）加密的加密块的集合。

[0112] 产生以上模式的 K 个模式。

[0113] 模式 1 到 k 的每一个中包括的块数是 i，因此，应用于产生 k 个模式的块密钥将如下。

[0114] 模式 1 :Kb(Pk，B1) 到 Kb(P1，Bi)

[0115] 模式 2 :Kb(P2，B1) 到 Kb(P2，Bi)

[0116] 模式 k :Kb(Pk，B1) 到 Kb(Pk，Bi)

[0117] 即，用于产生 k 个模式的块密钥的总数为 i×k 个块密钥，其为 Kb(P1，B1) 到 Kb(Pk，Bi)。

[0118] 如上所述，首先，服务器产生

[0119] 由标题密钥 (Kt) 加密的 (b) 块区域外部的数据，以及

[0120] 基于 (a) 内容，由各个块的单独块密钥加密的 (c)k 个模式。

[0121] 接下来，将参照图 6 说明对于客户端（用户装置）的数据发送。

[0122] 服务器通过使用如下数据产生要提供给各个客户端的数据

[0123] 由标题密钥 (Kt) 加密的 (b) 块区域外部的数据，以及

[0124] 由各个块的单独块密钥（图 5 中所示）加密的 (c)k 个模式。

[0125] 服务器从图 5 的 (c) 中所示的模式 1 到 k 的 k 个模式中随机地选择块，作为在内容的每次发送中执行的处理。

[0126] 即，在内容的每次发送处理中，逐个地从模式 1 到 k 中选择由单独块密钥 Kb 加密的块 1 到 i 的加密块。

[0127] 从由图 5 的 (c) 中所示的单独块密钥 Kb(Ps,Py) 加密的加密块中逐个地选择块 1 到 i，并且将由图 5 的 (b) 中所示的标题密钥 (Kt) 加密的块区域外部的数据与所选择的块进行组合，以设置要向特定客户端提供的内容数据行。

[0128] 此外，产生的内容数据行中包括的部分块通过应用与每一个用户（客户端）对应的单独密钥（用户密钥）Ku 而被加密。

[0129] 根据处理，产生要向用户提供的内容。

[0130] 关于由在块中设置的、与每一个用户对应的单独密钥（用户密钥）Ku 加密的区域，由块密钥 Kb 加密的数据可以通过应用与用户对应的单独密钥（用户密钥）Ku 来双重地加密，或者也可以将该区域设置为仅由与每一个用户对应的单独密钥（用户密钥）Ku 加密的加密区域，而不对区域执行通过块密钥 Kb 的加密，或者在解密通过块密钥 Kb 加密的数据之后。

[0131] 图 6 示出了如下数据的配置示例。

[0132] 向用户 A 提供的内容

[0133] 向用户 B 提供的内容

[0134] 例如，图 6 中所示的向用户 A 提供的内容包括

[0135] 图 5 的 (b) 中所示的、由标题密钥 (Kt) 加密的块区域外部的数据，以及

[0136] 从图 5 的 (c) 中所示的模式 1 到 k 的 k 个模式中通过块的随机选择而选出的块 1 到 i。

[0137] 此外，由对于每一个用户各自化的、与用户 A 对应产生的用户密钥 Ku 来加密块的部分区域。

[0138] 例如，作为图中所示的要发送给用户 A 的内容而选择的块 1 是由块密钥 Kb(P2,B1) 加密的块，即图 5 的 (c) 中所示的模式 2 中的块 1。

[0139] 由块密钥 Kb(P2, B1) 加密的块的部分区域通过应用用户密钥 Ku(a) 而被加密，所述用户密钥 Ku(a) 是与用户 A 对应的、对于用户唯一的密钥。

[0140] 图中所示的以黑色填充的部分是由用户密钥 Ku(a) 加密的部分（单独加密的部分）。

[0141] 在块 1 到 i 的所有块中设置由用户密钥加密的区域（单独加密的部分）。

[0142] 同样优选的是，应用这样的配置 :关于部分块，设置由用户密钥加密的区域（单独加密的部分）。进一步优选的是，应用这样的配置 :在一个块中设置由多个用户密钥加密的区域（单独加密的部分）。

[0143] 作为图中所示的、要发送到用户 B 的内容所选择的块 1 是由块密钥 Kb(P1, B1) 加密的块，即，图 5 的 (c) 中所示的模式 1 中的块 1。

[0144] 由块密钥 Kb(P1, B1) 加密的块的部分区域通过应用用户密钥 Ku(b) 而被加密，所述用户密钥 Ku(b) 是与用户 B 对应的、对于用户唯一的密钥。

[0145] 图中所示的以黑色填充的部分是由用户密钥 Ku(b) 加密的部分。

[0146] 由用户密钥加密的区域可以改变，并且相对于每一发送处理可以是相同区域。

[0147] 优选地是，由用户密钥加密的区域包括内容的重要数据和重要场景区域。例如，将加密区域优选地设置为包括 MPEG 数据中的 I 画面的区域。

[0148] 例如，当服务器发送内容时通过随机数产生处理来产生用户密钥，并且将产生的密钥提供给用户并且存储在数据库中。

[0149] 要提供给用户的数据除了加密内容之外，还包括应用于加密内容的解密的一组加密密钥。

[0150] 例如，要关于用户 A 提供的加密密钥是如下的一组密钥：

[0151] (a) 作为对于所有用户公共的公共密钥的标题密钥

[0152] (b) 应用于要提供给用户 A 的内容中的 i 个块的解密的 i 个块密钥，以及

[0153] (c) 作为与用户 A 对应的单独密钥的用户密钥 Ku(a)。

[0154] 要提供给用户 B 的加密密钥是如下的一组密钥：

[0155] (a) 作为对于所有用户公共的公共密钥的标题密钥

[0156] (b) 应用于要提供给用户 B 的内容中的 i 个块的解密的 i 个块密钥，以及

[0157] (c) 作为与用户 B 对应的单独密钥的用户密钥 Ku(b)。

[0158] 关于 (a) 中的标题密钥 Kt，当标题共同时，向所有用户提供相同的标题密钥。

[0159] (b) 中的 i 个块密钥 Kb 根据作为提供给各个用户的内容而选择的块来产生不同的对。

[0160] (c) 中的用户密钥 Ku 根据用户而不同。

[0161] 服务器产生发送内容以及关于各个用户的一组密钥，并且将其提供给各个用户。

[0162] [3. 规定内容配置的参数]

[0163] 接着，将参照图 7 和图 8 说明设置用于规定要发送给用户的内容的配置的参数的示例。

[0164] 如图 7 所示，例如，存在如下参数，作为规定要发送的内容的参数。

[0165] a：块大小

[0166] i：块数

[0167] k：模式数

[0168] b：由用户密钥 (Ku) 单独加密的部分的大小

[0169] c：一个块中由用户密钥 (Ku) 单独加密的部分的数量

[0170] 图 8 中将示出设置这些参数的特定示例。图 8 示出了在内容具有如下条件的情况下设置参数的示例。

[0171] Video rate(视频速率) = 8Mbps

[0172] Duration(持续期) = 7200sec

[0173] Size(大小) = 7.2GB

[0174] IDR interval(IDR 间距) = 1sec

[0175] (a：块大小)

[0176] 例如，将块大小设置为 1MB。

[0177] 块大小的设置条件遵循每一个加密处理或解密处理中给定格式的规定。

[0178] 为了满足设置条件，例如设置 1Block ＝ 1Symbol 和 8Block ＝ 1Segment。

[0179] (i ＝块数)

[0180] 例如，将块数设置为每一个内容 720 个块。

[0181] 必须将块数设置为当难以再现块部分时充分地阻止用户。

[0182] 为了满足以上条件，设置约整个内容的 10％

[0183] (7200*0.1 ＝ 720sec)(720/8 ＝ 90Segment) 的块。

[0184] (k ＝模式数)

[0185] 例如，将模式数 k 设置为 32。

[0186] 优选地是，在内容的各个发送中，实现模式的不同组合。

[0187] 当模式数 k 为 32 且块数为 i 时，实现了块的 32^i 种类型的不同组合。

[0188] (b：由用户密钥 (Ku) 单独加密的部分的大小)

[0189] 例如，将由用户密钥单独加密的部分的大小设置为 16Byte。

[0190] (c：在一个块中由用户密钥 (Ku) 单独加密的部分的数量)

[0191] 例如，将在一个块中由用户密钥 (Ku) 单独加密的部分的数量设置为 8。

[0192] 必须将这些参数 b 和 c 设置在这样的水平中：其中在不解密通过用户密钥 Ku 单独加密的部分的情况下，例如，在发送之后非法地分发正常发送的内容的情况下，难以正常地观看内容，因此，优选地是，根据内容来确定这些参数。

[0193] 例如，当如图 8 所示那样设置参数时，

[0194] 在没有与每一个用户对应的单独密钥（用户密钥）的情况下不再现的内容的部分（再现时间）是 720 秒，

[0195] 由与每一个用户对应的单独密钥（用户密钥）加密的部分的总大小对于每一个内容是 92160 字节，以及

[0196] 与 k 个模式对应的块的总大小是 22.3GB。

[0197] 此外优选地是，根据要发送的内容的条件适当地设置最佳参数。

[0198] [4. 内容发送顺序]

[0199] 接下来，将参照图 9 中所示的顺序图来说明内容发送顺序的示例。

[0200] 图 9 是示出服务器与客户端之间的内容发送顺序的图。

[0201] 客户端是由用户拥有的诸如 PC 和通信终端之类的信息处理设备。

[0202] 尽管在本顺序 (sequence) 中省略了内容提供处理中包括的服务器与客户端之间的结算处理、授权处理等，但是根据需要执行这些结算处理和授权处理。

[0203] 首先，在步骤 S11，客户端请求服务器发送内容。例如，客户端向服务器发送内容指定信息，其从服务器提供的内容列表中指定特定内容。

[0204] 在步骤 S12，服务器根据内容的请求，产生用户密钥 Ku 作为与用户（客户端）对应的单独密钥。例如，服务器例如通过随机数生成来产生用户密钥 Ku。

[0205] 接着，在步骤 S13，服务器执行要在向客户端提供的内容中设置的块的选择处理，并且进一步在各个选择的块的每一个中确定由与用户对应的单独密钥（用户密钥）单独加密的部分。

[0206] 步骤 S13 中的块的选择处理通过参照图 5 说明的图 5 的 (c) 中所示的、逐个随机地从模式 1 到 k 中选择块 1 到 i 的处理来执行。

[0207] 例如，根据参照图 8 说明的参数执行所选择的块中确定由用户密钥单独加密的部分的处理，以便所述部分包括各个块中的重要场景和数据区域。

[0208] 接下来，在步骤 S14，服务器通过应用与客户端对应的单独密钥（用户密钥 Ku），对于步骤 S13 中确定的单独加密的部分执行加密处理。此外，服务器汇总执行了通过用户密钥 Ku 的加密的各个块中单独加密的部分，以被设置为一个数据文件（子块文件）。

[0209] 将每一个块设置为作为加密处理单元的子块的集合，并且还在子块的基础上执行通过与用户对应的加密密钥（用户密钥）加密的数据的部分。

[0210] 接下来，在步骤 S15，服务器执行对于客户端的数据发送。发送数据将是例如如图 9 中所示的一组如下的数据 (S15)。

[0211] (1) 块以外的公共密钥 (Kt) 加密的数据

[0212] (2) 由与用户对应的单独密钥（用户密钥）加密的部分以外的块密钥 (Kb) 的加密数据

[0213] (3) 包括由与用户对应的单独密钥（用户密钥）加密的数据的子块文件，以及

[0214] (4) 公共密钥 (Kt)、块密钥 (Kb) 和用户密钥 (Ku)。

[0215] 将以上加密的内容数据和一组密钥发送到客户端。

[0216] 服务器向客户端提供内容配置信息，其中除了以上数据之外，还记录块区域和单独加密的部分的区域信息。

[0217] 接着，在步骤 S16，服务器在数据库中登记管理信息作为发送内容信息。例如，服务器执行图 10 中所示的管理信息的登记处理。稍后将说明管理数据。

[0218] 当客户端从服务器接收加密内容和一组密钥时，客户端通过在步骤 S17 组合如下接收到的数据来重建一系列内容：

[0219] (1) 块以外的公共密钥 (Kt) 加密的数据

[0220] (2) 由与用户对应的单独密钥（用户密钥）加密的部分以外的块密钥 (Kb) 的加密数据

[0221] (3) 包括由与用户对应的单独密钥（用户密钥）加密的数据的子块文件客户端以从服务器接收到的密钥数据，即

[0222] (4) 公共密钥 (Kt)、块密钥 (Kb) 和用户密钥 (Ku)

[0223] 在客户端中的存储单元中存储内容。此外，客户端通过使用各个加密密钥执行解密处理来再现内容。

[0224] 在执行内容的解密时，执行通过参照由服务器提供的内容配置信息（即，记录块区域和单独加密的部分的区域信息的内容配置信息）切换加密密钥的解密处理。

[0225] 将参照图 10 说明作为发送内容的管理信息的、要由服务器记录的数据。

[0226] 图 10 是服务器的存储单元中保存的管理信息的数据配置示例。

[0227] 如图 10 所示，例如，管理信息包括

[0228] 发送内容信息，

[0229] 发送目的地信息，

[0230] 发送用户信息，

[0231] 发送日期信息，

[0232] 块信息，以及

[0233] 加密密钥信息（公共密钥、块密钥和与用户对应的单独密钥（用户密钥））。

[0234] 发送内容信息包括内容标题的信息、内容的 ID。

[0235] 发送目的地信息是诸如内容目的地的地址（例如，与客户端或用户对应的地址等）之类的信息。

[0236] 发送用户信息是诸如用户名、用户地址及其接触点之类的用户信息。

[0237] 发送日期信息是内容的发送日期的信息。

[0238] 块信息是关于发送内容中包括的块 1 到 i 的信息。该信息可以标识已经从哪个模式选择了相应块。

[0239] 加密密钥信息记录对于每一个提供的内容的加密处理所应用的加密密钥的信息。具体来说，该信息与如下一组密钥有关：

[0240] (a) 对于所有用户公共的标题密钥 :Kt

[0241] (b) 应用于关于用户的提供内容中的 i 个块的解密的 i 个块密钥 :Kb，以及

[0242] (c) 作为与用户对应的单独密钥的用户密钥 :Ku。

[0243] 记录以上密钥信息，以便与作为管理信息的、内容的发送目的地信息相关联。

[0244] 例如，当非法分发发送内容时，分析分发的内容中包括的块的组合，并且使用图 10 中所示的管理信息的登记信息，从而标识非法分发内容的发送目的地客户端。

[0245] 另外，例如，当出现密钥的泄露时，通过分析泄露的密钥并通过图 10 中所示的管理信息来检查密钥，可以确定哪一个客户端是密钥泄露源。

[0246] 图 10 中所示的管理信息的示例是个示例，并且并不总是需要记录所有信息。以上信息以外的信息可以存储为管理信息。

[0247] [5. 提供内容的服务器的系统示例]

[0248] 在以上实施例中，已经说明了由一个服务器执行关于客户端的所有数据发送的示例。

[0249] 在下文中，作为考虑数据发送效率的配置示例，将说明设置关于客户端执行内容提供处理的多个服务器并且各个服务器向客户端提供部分内容配置数据的处理示例。

[0250] 图 11 示出执行内容提供处理的两个服务器（第一服务器 201、第二服务器 202）以及接收内容的多个客户端（客户端 a211 到 n213）。

[0251] 如图 11 所示，第一服务器 (Web 服务器)201 向各个客户端 211 到 213 发送如下数据。

[0252] (1) 由公共密钥 (Kt) 加密的数据

[0253] (2) 由单独密钥（用户密钥）加密的部分以外的块数据（由块密钥加密的数据）

[0254] 另一方面，第二服务器 (应用服务器)202 向各个客户端 211 到 213 发送如下数据。

[0255] (3) 由与用户对应的单独密钥（用户密钥 Ku) 加密的数据

[0256] 如上所述，第一服务器 (Web 服务器)201 和第二服务器（应用服务器)202 通过分别管理作为传输内容的关于客户端的发送内容的部分来执行数据传输处理。

[0257] 产生与用户对应的单独密钥（用户密钥）的处理和应用单独密钥（用户密钥）的加密处理由第二服务器（应用服务器)202 执行，作为每一个内容发送的处理。

[0258] 第一服务器 (Web 服务器)201 不执行每一个内容发送处理中新近的数据加密处理，并执行预先在数据库中存储的数据的选择性提取，然后，向客户端提供所选择的数据。

即，在每一个发送处理中，第一服务器 202 向客户端提供如下数据。

[0259] (1) 由公共密钥 (Kt) 加密的数据

[0260] (2) 由单独密钥（用户密钥）加密的部分以外的块数据（由块密钥加密的数据）

[0261] 当应用使用两个服务器的以上配置时，可以执行内容发送处理中的负荷共享，并且可以实现高效的内容发送。

[0262] 将参照图 12 和图 13 说明如下数据的示例。

[0263] 由第一服务器 (Web 服务器）201 保存的数据

[0264] 由第二服务器（应用服务器）202 保存的数据

[0265] 首先，将参照图 12 说明由第一服务器 (Web 服务器）201 保存的数据。

[0266] 如参照图 11 说明的那样，第一服务器 (Web 服务器）201 向客户端提供如下数据。

[0267] (1) 由公共密钥 (Kt) 加密的数据

[0268] (2) 由与用户对应的单独密钥（用户密钥）加密的部分以外的块数据（由块密钥加密的数据）

[0269] 以上数据是可以预先准备的数据。关于 (2) 中所示的、由与用户对应的单独密钥（用户密钥）加密的部分以外的块数据（由块密钥加密的数据），必须确定关于每一个用户选择的块，以及在发送内容时要由与用户对应的单独密钥（用户密钥）加密的部分，然而，由块密钥加密的数据本身可以在确定作为内容发送目的地的客户端之前预先准备，并且可以存储在数据库中。

[0270] 如图 12 所示，第一服务器 (Web 服务器）201 可以在数据库中保存如下数据。

[0271] (1) 块区域外部的加密数据（由公共密钥（标题密钥 Kt) 加密的数据），以及

[0272] (2) 块区域中的加密数据（由块密钥 Kb 加密的数据）

[0273] 这些数据对应于参照图 5 说明的 (b) 和 (c) 的数据。

[0274] 第一服务器 (Web 服务器）201 可以在存储单元中保存这些数据。

[0275] 将公共密钥（标题密钥 Kt) 和块密钥 (Kb) 作为密钥数据保存。

[0276] 关于 (2) 块区域中的加密数据（由块密钥 Kb 加密的数据），在作为加密处理单元规定的子块的基础上执行通过块密钥 Kb 的加密。

[0277] 如图 12 所示，由第一服务器 (Web 服务器）201 保存的块数据可以在作为加密处理单元的子块的基础上标识。在图 12 中所示的示例中，一个块包括 n 个子块。

[0278] 由与用户对应的单独密钥（用户密钥）进行的加密也在子块的基础上执行。

[0279] 在第二服务器（应用服务器）202 中执行由与用户对应的单独密钥（用户密钥）进行的加密，并且将其提供给客户端。

[0280] 因此，第一服务器 (Web 服务器）201 向客户端提供仅包括执行通过与用户对应的单独密钥（用户密钥）进行的加密的子块区域以外的子块的块数据。

[0281] 由第一服务器 (Web 服务器）201 向客户端提供的数据是如下数据。

[0282] (1) 块区域外部的加密数据

[0283] 这是通过应用关于内容标题设置的公共密钥（标题密钥 :Kt) 来加密块以外的数据区域的数据。

[0284] (2) 块区域中的加密数据

[0285] 这是通过应用关于对应于模式 1 到 k 的 k 个模式（如参照图 5 的 (c) 所述）的各

个块 1 到 i 不同的块密钥 Kb 而加密的加密数据块，其为仅包括执行通过与用户对应的单独密钥（用户密钥）进行的加密的子块区域以外的子块的数据。

[0286] 另一方面，由第二服务器（应用服务器）202 保存的数据是图 13 中所示的数据。

[0287] 即，第二服务器保存尚未执行加密的、与各个模式（模式 1 到 k）对应的块数据的明文 (clear-text) 数据。

[0288] 由第二服务器（应用服务器）202 保存的块数据也可以如图 13 所示那样在作为加密处理的单元的子块的基础上标识。在图 13 所示的示例中，一个块包括 n 个子块。

[0289] 将说明本处理示例，作为由要在块中设置的单独密钥（用户密钥）单独加密的部分被配置为不通过块密钥 Kb 加密而是仅通过与用户对应的单独密钥（用户密钥）Ku 加密的加密数据的处理示例。也可以将单独加密的部分设置为由块密钥 Kb 和单独密钥 Ku 双重加密的部分，不限于以上状态。

[0290] 将参照图 14 说明使用两个服务器（其为第一服务器 (Web 服务器）201 和第二服务器（应用服务器）202) 提供内容的顺序 (sequence)。

[0291] 以与上面参照图 9 所述的顺序相同的方式，客户端是由用户拥有的诸如 PC 和通信终端之类的信息处理设备。尽管在本顺序中省略了内容提供处理中包括的服务器与客户端之间的结算处理、授权处理等，但是根据需要执行这些结算处理和授权处理。

[0292] 首先，在步骤 S21，客户端请求应用服务器发送内容。例如，客户端将内容指定信息发送到服务器，其从应用服务器提供的内容列表中指定特定内容。

[0293] 在步骤 S22，应用服务器根据内容的请求产生用户密钥 Ku 作为与用户（客户端）对应的单独密钥。例如，应用服务器例如通过随机数生成来产生用户密钥 Ku。

[0294] 接下来，在步骤 S23，应用服务器执行要在向客户端提供的内容中设置的块的选择处理，并进一步确定各个所选块的每一个中由与用户对应的单独密钥（用户密钥）单独加密的部分。

[0295] 步骤 S23 中块的选择处理对应于参照图 5 所述的、图 5 的 (c) 中所示的逐个随机地从模式 1 到 k 中选择块 1 到 i 的处理。

[0296] 应用服务器仅具有如参照图 13 所述的、对应于块的明文数据，而不具有由块密钥 Kb 加密的数据。

[0297] 因此，应用服务器在步骤 S23 仅确定与要提供给客户端的块对应的模式顺序。

[0298] 例如，应用服务器确定模式顺序 (2,1,k,...,5)，其指示从哪一个模式选择块 1 到 i，如下所示。

[0299] 块 1 :模式 2

[0300] 块 2 :模式 1

[0301] 块 3 :模式 k

[0302] ...

[0303] 块 i :模式 5

[0304] 然后，应用服务器关于在步骤 S23 中确定的模式顺序所对应的块，确定各个块中由单独密钥（用户密钥 :Ku) 加密的部分（单独加密的部分）。

[0305] 根据参照图 8 所述的参数，进行确定所选块中单独加密部分的处理，以便例如在各个块中包括重要场景和数据区域。

[0306] 在子块的基础上确定单独加密的部分。

[0307] 接下来，在步骤S24，应用服务器关于要由从各个块（即，作为通过应用步骤S22中产生的单独密钥（用户密钥:Ku）单独加密的部分而选择的子块）中选择的用户密钥加密的数据部分执行加密。

[0308] 如以上参照图13所述的那样，应用服务器保存块数据作为明文数据。在子块的基础上分割明文块数据，并且应用服务器加密作为通过应用在步骤S22中产生的单独密钥（用户密钥:Ku）单独加密的部分所选择的子块（明文）。

[0309] 此外，应用服务器汇总执行了通过单独密钥（用户密钥:Ku）的加密的单独加密的子块数据，以便将其设置为一个数据文件（子块文件）。

[0310] 接下来，在步骤S25，应用服务器将在步骤S24中产生的单独加密的子块数据文件（子块文件）发送到客户端。

[0311] 此外，应用服务器向客户端发送要从Web服务器向客户端提供的数据的标识信息（例如，与数据对应的URL（统一资源定位符）、地址信息等）。

[0312] 要从Web服务器向客户端提供的数据如下。

[0313] (1)块以外的由公共密钥(Kt)加密的数据，以及

[0314] (2)由与用户对应的单独密钥（用户密钥）加密的部分以外的、由块密钥(Kb)加密的数据

[0315] 应用服务器将以上数据的标识信息（例如，与数据对应的URL、地址信息等）发送到具有单独加密的子块数据文件（子块文件）的客户端。

[0316] 要从应用服务器提供到客户端的发送数据包括如下数据，例如，如如图14(S25)中所示。

[0317] (a1)由与用户对应的单独密钥（用户密钥）加密的数据

[0318] (a2)块区域以外的、由公共密钥(Kt)加密的数据的标识信息（例如，与用户对应的URL、地址信息等）

[0319] (a3)由与用户对应的单独密钥（用户密钥）单独加密的部分以外的子块的标识信息（例如，与子块区域对应的URL、地址信息等）

[0320] (a4)与用户对应的单独密钥（用户密钥）

[0321] 将以上加密数据、数据标识信息和一组密钥发送到客户端。

[0322] 应用服务器向客户端提供记录了块区域和单独加密部分的区域信息的内容配置信息。

[0323] 下一步骤S26中的处理是客户端侧的处理。

[0324] 客户端从应用服务器接收以上(a1)到(a4)的各个数据，并关于Web服务器，通过使用接收到的数据中包括的(a2)和(a3)的数据，请求从应用服务器接收到的内容以外的内容配置数据。

[0325] 即，客户端通过使用如下数据标识信息（例如，URL）来访问Web服务器，以请求与数据标识信息对应的数据的获取。

[0326] (a2)块区域以外的、由公共密钥(Kt)加密的数据的标识信息（例如，与数据对应的URL、地址信息等）

[0327] (a3)由与用户对应的单独密钥（用户密钥）单独加密的部分以外的子块的标识信

息（例如，与子块数据对应的URL、地址信息等）

[0328] 在步骤S27，Web服务器向客户端提供由客户端请求的数据。

[0329] 由Web服务器向客户端提供的数据包括如下数据，如图14(S27)中所示。

[0330] (b1)块以外的、由公共密钥（标题密钥:Kt）加密的数据

[0331] (b2)关于客户端选择的块数据中与用户对应的单独密钥（用户密钥）单独加密的部分以外的子块数据

[0332] (b3)公共密钥（标题密钥:Kt）和块密钥(Kb)

[0333] 以上数据中的(b1)和(b2)的各个数据由与从客户端接收到的各个数据对应的数据标识信息（如URL）指定。

[0334] 根据与内容对应的标题指定(b3)的公共密钥(Kt)，所述内容由从客户端接收到的数据标识信息（如，URL）中包括的数据指定。

[0335] 类似地，关于(b3)的块密钥(Kb)，选择根据以上数据中(b2)的子块数据的标识信息分析的块标识符指定的块所对应的块密钥，以便提供给客户端。

[0336] 在步骤S28，从Web服务器接收(b1)到(b3)的以上加密数据以及一组密钥的客户端基于来自应用服务器和Web服务器的接收数据来重建内容。

[0337] 即，客户端组合如下接收数据：

[0338] (1)块以外的、由公共密钥(Kt)加密的数据，

[0339] (2)由与用户（子块数据）对应的单独密钥（用户密钥）加密的部分以外的、由块密钥(Kb)加密的数据，以及

[0340] (3)包括由与用户对应的单独密钥（用户密钥）加密的数据的子块数据以重建一系列内容，并且客户端保存具有从各个服务器接收到的密钥数据的内容，即，

[0341] (4)公共密钥(Kt)、块密钥(Kb)和用户密钥(Ku)。客户端通过使用各个加密密钥执行解密处理，从而再现内容。

[0342] 在执行内容解密时，通过参照内容配置信息（其中记录了选择应用于解密的密钥所需的区域信息，如通过公共密钥加密的区域、块区域和单独加密的部分）适当地切换待应用的加密密钥来执行解密处理。

[0343] 在以上实施例中已经说明了通过使用两个服务器的内容发送处理的示例，然而，内容发送处理可以在一个设备（单元）（如，一个服务器）中执行，以及作为通过两个或更多个设备（单元）的分发处理执行。

[0344] [6.客户端中的内容再现处理]

[0345] 接下来，将参照图15说明客户端中的内容再现处理的示例。在图15中，示出了执行客户端中的内容再现处理的数据处理单元以及存储单元的配置。

[0346] 已经参照图9和图14说明了根据两个不同顺序的内容提供顺序。然而，在两个处理中，客户端从服务器接收如下数据。

[0347] (1)块以外的、由公共密钥(Kt)加密的数据，

[0348] (2)由与用户（子块数据）对应的单独密钥（用户密钥）加密的部分以外的、由块密钥(Kb)加密的数据

[0349] (3)包括由与用户对应的单独密钥（用户密钥）加密的数据的子块数据

[0350] 客户端组合以上数据以便重建一系列内容，并将具有从各个服务器接收到的密钥

数据的内容，即，

[0351] (4) 公共密钥 (Kt)、块密钥 (Kb) 和用户密钥 (Ku)，以及

[0352] (5) 内容配置信息

[0353] 存储在图 15 中所示的存储单元 501 中，并基于存储单元 501 中存储的数据来执行内容的解密和再现处理。

[0354] 客户端的数据处理单元的控制单元 502 从存储单元 501 获取内容配置信息 511。这是指示向客户端提供的内容中、包括块中的位置信息（如，块区域、单独加密的部分）等的加密数据配置的信息。即，用于确认如下各个区域以选择应用于解密的密钥所需的信息。

[0355] 由公共密钥 (Kt) 加密的区域

[0356] 由各个块密钥 (Kb) 加密的区域

[0357] 由单独密钥（用户密钥 Ku) 加密的加密区域

[0358] 如图 15 所示，客户端的控制单元 502 从存储单元 501 读取内容配置信息 511，并参照内容配置信息 511 将密钥切换信息 514 输出到加密单元 503。

[0359] 即，控制单元 502 在执行通过公共密钥 (Kt) 加密的区域的处理时，将应用公共密钥的指令输出到解密单元 503，在执行通过各个块密钥 (Kb) 加密的区域的处理时，将应用与待解密的块对应的块密钥的指令输出到解密单元 503，并且在执行通过单独密钥（用户密钥 (Ku)）加密的数据区域的处理时，将应用单独密钥的指令输出到解密单元 503。

[0360] 解密单元 503 通过应用从存储单元 501 读取的加密密钥（公共密钥、块密钥和单独密钥）513 适当地切换密钥以关于从存储单元 501 读取的加密内容 512 执行解密处理。

[0361] 将解密结果提供到解码和再现处理单元 504。解码和再现处理单元 504 通过执行给定解码处理（例如，MPEG 解码）来执行再现处理，以输出再现数据 520。

[0362] [7. 服务器中的内容产生和提供处理顺序]

[0363] 接下来，将参照图 16 和图 17 中所示的流程图说明由服务器（如，服务提供商）执行的内容的产生和提供处理顺序。

[0364] (7-1. 服务器中的内容产生处理顺序)

[0365] 首先，将参照图 16 的流程图说明服务器（如，服务提供商）中执行的内容产生处理顺序。

[0366] 在服务器的数据处理单元中执行根据图 16 的流程执行的处理。

[0367] 首先，在步骤 S101，例如，获取原始内容（如，电影）。

[0368] 接着，在步骤 S102，在原始内容中设置多个 (i 个) 块，并将其提取出。

[0369] 此外，在步骤 S103，通过应用公共密钥（标题密钥 Kt) 来加密提取的块以外的区域的数据。

[0370] 接着，在步骤 S104，将从原始内容中提取的多个 (i 个) 块设置为包括块 1 到 i 的 k 个模式。

[0371] 此外，在步骤 S105，通过应用不同的块密钥 (Kb(Px, By)) 来加密模式 1 到 k 中的块 1 到 i。

[0372] 由以上处理来产生参照图 5 说明的 (b) 和 (c) 的数据。

[0373] (7-2. 服务器中的内容提供处理顺序)

[0374] 接下来，将参照图 17 的流程图说明服务器（如，内容提供商）中执行的内容提供

处理顺序。

[0375] 如参照图 9 的顺序图和图 15 的顺序图说明的那样，对于客户端的内容提供处理可以由一个服务器执行，也可以由多个服务器执行。

[0376] 因此，图 17 的流程中所示的处理可以由一个服务器或多个服务器执行。

[0377] 在对于客户端的每一个内容发送处理中，由服务器的数据处理单元顺序地执行根据图 17 的流程执行的处理。

[0378] 首先，在步骤 S151，接收来自客户端的内容的下载请求。

[0379] 接着，在步骤 S152，产生与客户端（用户）对应的单独密钥（用户密钥 Ku）。例如，通过随机数生成处理来产生密钥。

[0380] 接着，在步骤 S153，确定要向客户端提供的块行。即，确定其中选择块 1 到 i 的模式 1 到 k 的顺序 (sequence)。

[0381] 例如，确定如下顺序（块排列信息）。

[0382] 块 1 :模式 2

[0383] 块 2 :模式 1

[0384] 块 3 :模式 k

[0385] ...

[0386] 块 i :模式 5

[0387] 确定指示从哪一个模式选择块 1 到 i 的模式顺序 (2,1, k, ...,5)（＝块排列信息）。

[0388] 接着，在步骤 S154，在各个选择块的每一个中，确定块中单独加密的部分。即，确定各个块中由单独密钥（用户密钥 :Ku) 加密的部分（单独加密的部分）。

[0389] 执行确定所选择的块中单独加密的部分的处理，以便根据例如参照图 8 所述的参数在各个块中包括重要场景和数据区域。在每一个子块（其被设置为重新分割每一个块的单元）中确定单独加密的部分。

[0390] 接着，在步骤 S155，加密由单独密钥（用户密钥 :Ku) 单独加密的部分。

[0391] 作为由单独密钥（用户密钥 :Ku) 单独加密的部分的加密处理条件，可以仅由用户密钥 Ku 来加密数据，并且数据可以由块密钥 Kb 和用户密钥 Ku 双重加密。

[0392] 接着，在步骤 S156，产生内容配置信息。内容配置信息包括当执行内容的解密时选择待应用的密钥所需的信息。

[0393] 即，内容配置信息包括能够识别如下各个密钥应用到的区域的信息。

[0394] 应用了公共密钥（标题密钥 Kt) 的区域

[0395] 应用了各个块密钥 (Kb(Px, By)) 的区域

[0396] 应用了单独密钥（用户密钥 Ku) 的区域

[0397] 接着，在步骤 S157，服务器向客户端发送数据。即，服务器向客户端提供如下数据。

[0398] (1) 由公共密钥（标题密钥 Kt) 加密的数据

[0399] (2) 由块密钥 Kb 加密的数据

[0400] (3) 由单独密钥（用户密钥 Ku) 加密的数据

[0401] (4) 公共密钥 Kt、块密钥 Kb 和单独密钥 Ku

[0402] (5) 内容配置信息

[0403] 此外，在步骤 S158，服务器产生包括向其提供内容的客户端的信息的对应数据、块排列信息（模式顺序）和加密密钥信息的管理信息。

[0404] 在步骤 S158 产生的管理信息是例如参照图 6 所述的管理信息。

[0405] 在管理信息中，通过彼此关联来记录客户端信息（如，发送目的地信息和发送用户信息）、块信息和加密密钥信息。

[0406] [8. 客户端中的内容再现顺序]

[0407] 接下来，将参照图 18 中的流程图说明由客户端进行的内容再现处理顺序。执行该处理，作为客户端设备中执行再现处理的数据处理单元的处理。

[0408] 首先，在步骤 S301，执行内容再现处理的客户端设备获取从服务器接收到的内容配置信息。即，其中记录了能够识别各个密钥的如下应用区域的信息的内容配置信息。

[0409] 公共密钥（标题密钥 Kt）的应用区域

[0410] 各个块密钥 (Kb(Px，By)) 的应用区域

[0411] 单独密钥（用户密钥 Ku）的应用区域

[0412] 接着，在步骤 S302，基于内容配置信息，获取各个加密密钥的切换位置信息。

[0413] 接着，在步骤 S103，通过根据获取的切换位置信息来切换公共密钥、块密钥和单独密钥，以顺序地解密各个加密内容。

[0414] 即，关于由公共密钥加密的数据区域执行应用公共密钥（标题密钥 Kt）的解密处理，关于由块密钥加密的数据区域执行应用块密钥 Kb(Px，By) 的解密处理，并且关于由单独密钥（用户密钥 Ku）加密的数据区域执行应用单独密钥（用户密钥 Ku）的解密处理。

[0415] 在内容配置信息中，写入指示加密区域的各个块由哪些块密钥加密的信息。

[0416] 客户端通过参照内容配置信息来确定加密区域的各个块由那些块密钥加密，以通过切换块密钥来执行解密处理。

[0417] 接着，在步骤 S304，通过对于解密内容执行解码处理（例如，MPEG 解码处理）来执行再现处理。

[0418] [9. 服务器中基于非法分发内容的源确定处理顺序]

[0419] 接着，将参照图 19 的流程图说明当发现非法分发的内容时执行的源确定处理顺序。

[0420] 例如，在作为已经执行了内容的发送的服务器提供商的服务器的数据处理单元中执行根据图 19 中所示的流程的处理。

[0421] 首先，在步骤 S501，获取非法分发的内容。

[0422] 作为非法分发的内容，例如，可以列举从网络上可由任何人访问的站点自由下载的内容、非法分发的盘中记录的拷贝内容。

[0423] 接着，在步骤 S502，通过分析非法分发的内容来分析内容中包括的块排列（模式顺序）。

[0424] 接着，在步骤 S503，通过管理信息中记录的块信息来检查从非法分发的内容获取的块排列信息，从而确定作为非法分发内容的分发源的内容发送目的地的客户端。

[0425] 管理信息指示已经在上面描述的图 10 中所示的管理信息。

[0426] 在图 19 的流程中已经仅说明了块排列的分析处理的示例，然而，要提供到客户端的加密密钥包括对于客户端唯一的一组单独密钥（用户密钥 Ku）以及对于客户端唯一的对

应于块排列的块密钥，并且当非法分发这些密钥时，通过以图 10 中所示的管理信息的登记信息检查非法分发的密钥，也可以找出非法分发的密钥的源。

[0427] [10. 各个设备的硬件配置示例]

[0428] 最后，将参照图 20 和图 21 说明执行以上处理的各个设备的硬件配置示例。

[0429] 首先，将参照图 20 说明执行内容提供处理的服务器的硬件配置示例。

[0430] CPU(中央处理单元)601 用作根据 ROM(只读存储器)602 或存储单元 608 中存储的程序执行各种处理的数据处理单元。

[0431] 例如，CPU 601 执行在以上各个特定示例中所述的加密内容的产生处理、内容的提供处理、管理信息的产生 / 记录处理等。RAM(随机存取存储器)603 适当地存储由 CPU 601 执行的程序、数据等。CPU 601、ROM 602 和 RAM 603 通过总线 604 彼此连接。

[0432] CPU 601 经由总线 604 连接到输入 / 输出接口 605。包括各种开关、键盘、鼠标、麦克风等的输入单元 606 以及包括显示器、扬声器等的输出单元 607 连接到输入 / 输出接口 605。CPU 601 响应于从输入单元 606 输入的指令执行各种处理，并且将处理结果例如输出到输出单元 607。

[0433] 连接到输入 / 输出接口 605 的存储单元 608 例如包括硬盘等，存储由 CPU601 执行的程序以及各种类型的数据。例如，记录参照图 6 所述的管理信息等。

[0434] 通信单元 609 经由网络 (如，因特网和局域网) 执行与外部设备的通信。

[0435] 接着，将参照图 22 说明执行内容的接收 / 再现处理等的客户端设备的硬件配置示例。

[0436] CPU(中央处理单元)701 用作根据 ROM(只读存储器)702 或存储单元 708 中存储的程序执行各种处理的数据处理单元。

[0437] 例如，CPU 701 执行在以上各个特定示例中所述的、关于服务器的通信处理、关于存储单元 708(硬盘等) 的来自服务器的接收数据的记录处理、来自存储单元 708(硬盘等) 的数据的再现处理。

[0438] RAM(随机存取存储器)703 适当地存储由 CPU 701 执行的程序、数据等。CPU 701、ROM 702 和 RAM 703 通过总线 704 彼此连接。

[0439] CPU 701 经由总线 704 连接到输入 / 输出接口 705。包括各种开关、键盘、鼠标、麦克风等的输入单元 706 以及包括显示器、扬声器等的输出单元 707 连接到输入 / 输出接口 705。CPU 701 响应于从输入单元 706 输入的指令执行各种处理，并且将处理结果例如输出到输出单元 707。

[0440] 连接到输入 / 输出接口 705 的存储单元 708 例如包括硬盘等，存储由 CPU701 执行的程序以及各种类型的数据。通信单元 709 经由网络 (如，因特网和局域网) 执行与外部设备的通信。

[0441] 连接到输入 / 输出接口 705 的驱动器 710 驱动可拆卸介质 711(如，磁盘、光盘、磁光盘或半导体存储器)，获取各种数据 (如，记录的内容和程序)。

[0442] 已经参照特定示例描述了本公开。然而，很明显，在不脱离本公开的要旨的范围内，本领域的技术人员可以进行修改或变更。即，已经以示例的形式公开了本公开，并且本公开不应当以限制方式解释。为了确定本公开的要旨，应当考虑所附的权利要求。

[0443] 本说明书中说明的一系列处理可以由硬件以及软件或二者的组合配置来执行。当

执行通过软件的处理时，可以将记录了处理顺序的程序安装到并入至专用硬件的计算机的存储器中以执行处理，或者可以将程序安装到可以执行各种处理的通用计算机中以执行处理。例如，可以将程序预先记录在记录介质中。除了从记录介质到计算机的安装之外，可以通过经由网络（如，LAN（局域网）和因特网）接收程序来将程序安装到记录介质（如，内部硬盘）。

[0444] 说明书中描述的各种处理不仅可以按照描述以时间顺序执行，而且可以根据执行处理的设备的处理能力或根据需要并行或单独地执行。系统是指多个设备的逻辑集合，而不限于各个设备在同一外壳中的配置。

[0445] 如上所述，根据本公开的实施例，即使当泄露加密内容的加密密钥时，也可以实现能够防止内容的完全再现的配置。

[0446] 具体来说，设置其中通过不同的块密钥来加密作为内容的配置数据的块 1 到 i 的模式 1 到 k，并且在每一个内容发送中，通过随机地选择块将具有包括不同的块 1 到 i 的块排列（模式顺序）的内容提供到客户端。将要提供给客户端的内容的块排列登记为管理信息。即使泄露了用作部分内容的加密密钥的公共密钥（标题密钥），也难以完全地再现内容。通过从非法分发的内容中获取块排列，并且以管理信息中登记的信息检查排列，还可以识别作为非法分发的内容的源的客户端。

[0447] 本公开包含与 2011 年 2 月 10 日向日本专利局提交的日本优先权专利申请 JP 2011-027300 中公开的主题有关的主题，其全部内容通过引用的方式合并在此。

[0448] 本领域的技术人员应当理解，根据设计要求和其它因素可出现各种变型、组合、部分组合和替换，只要其在所附权利要求或其等同体的范围内即可。

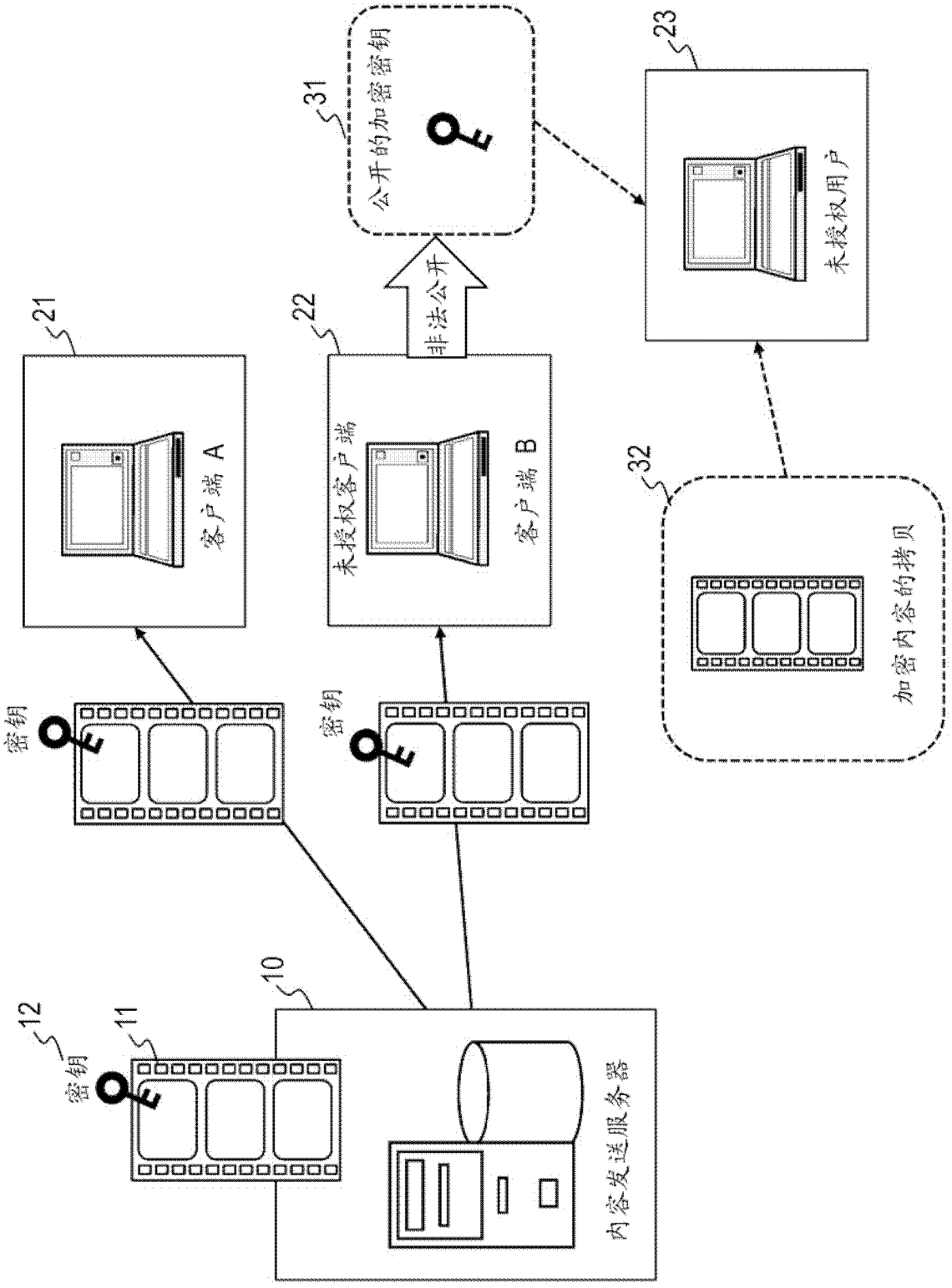

31
公开的加密钥
23
未授权用户
非法公开
21
客户端 A
22
未授权客户端
客户端 B
32
加密内容的拷贝
密钥
密钥
12
密钥
11
10
内容发送服务器

图 1

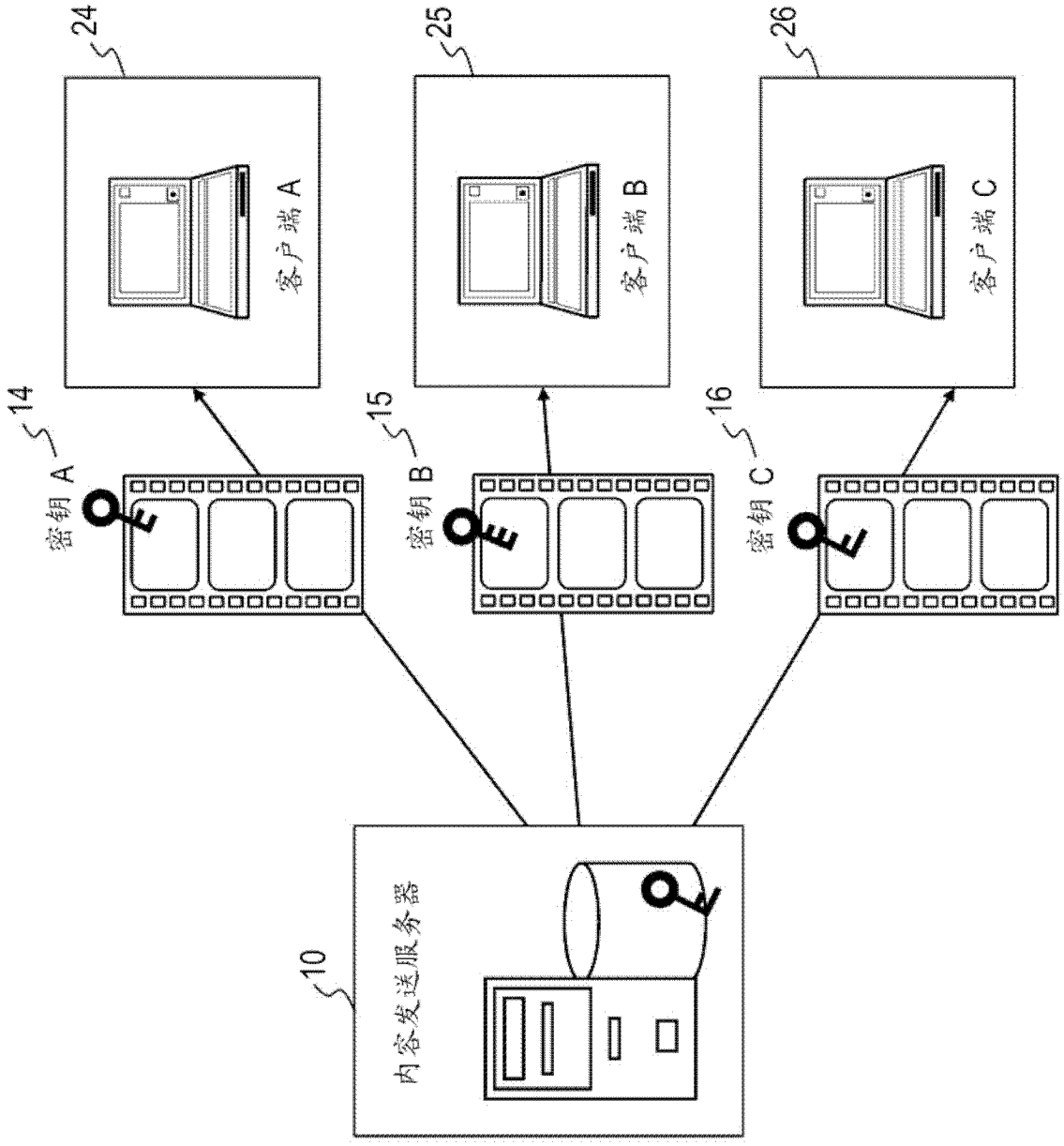


图 2

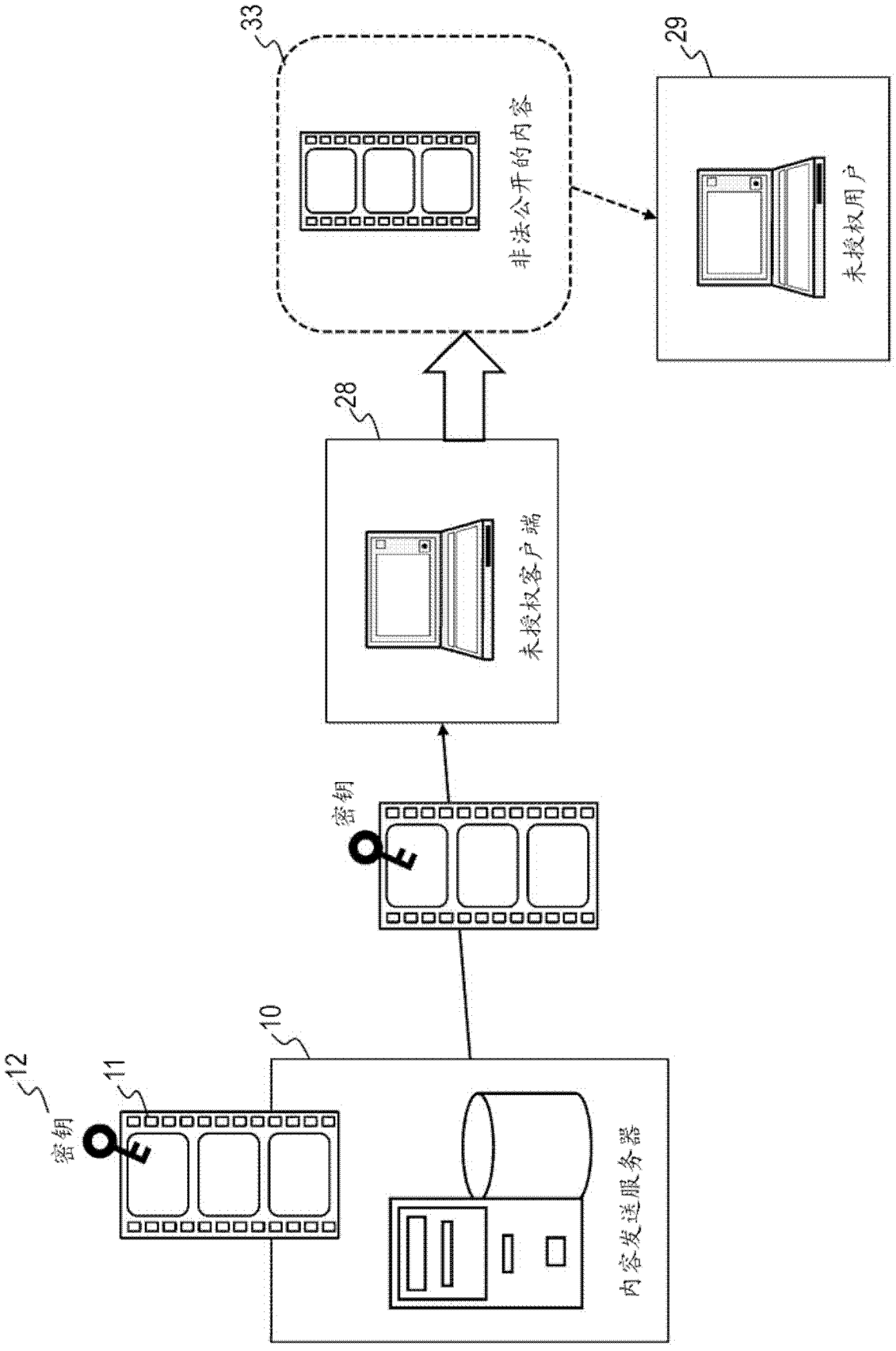


图 3

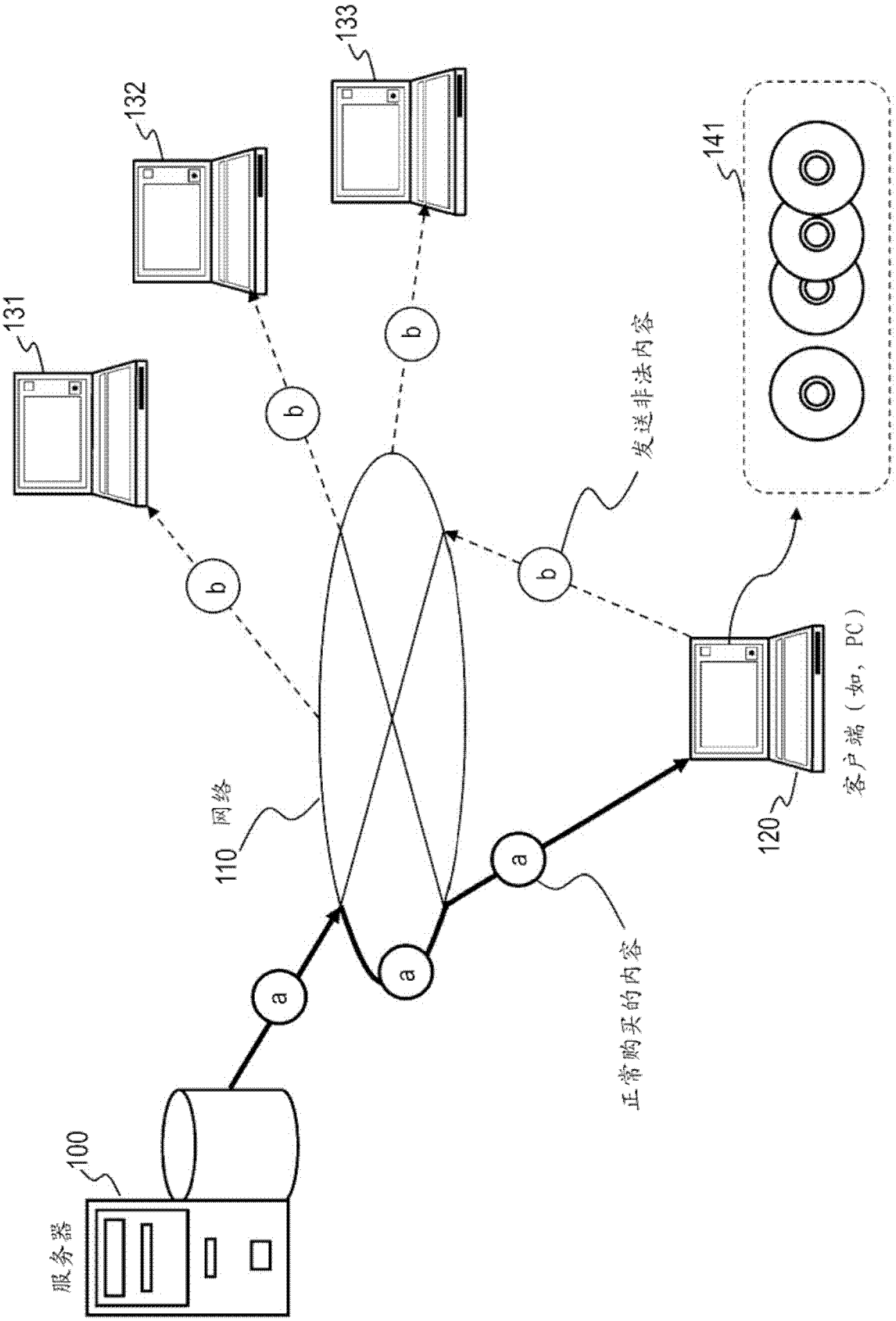


图 4

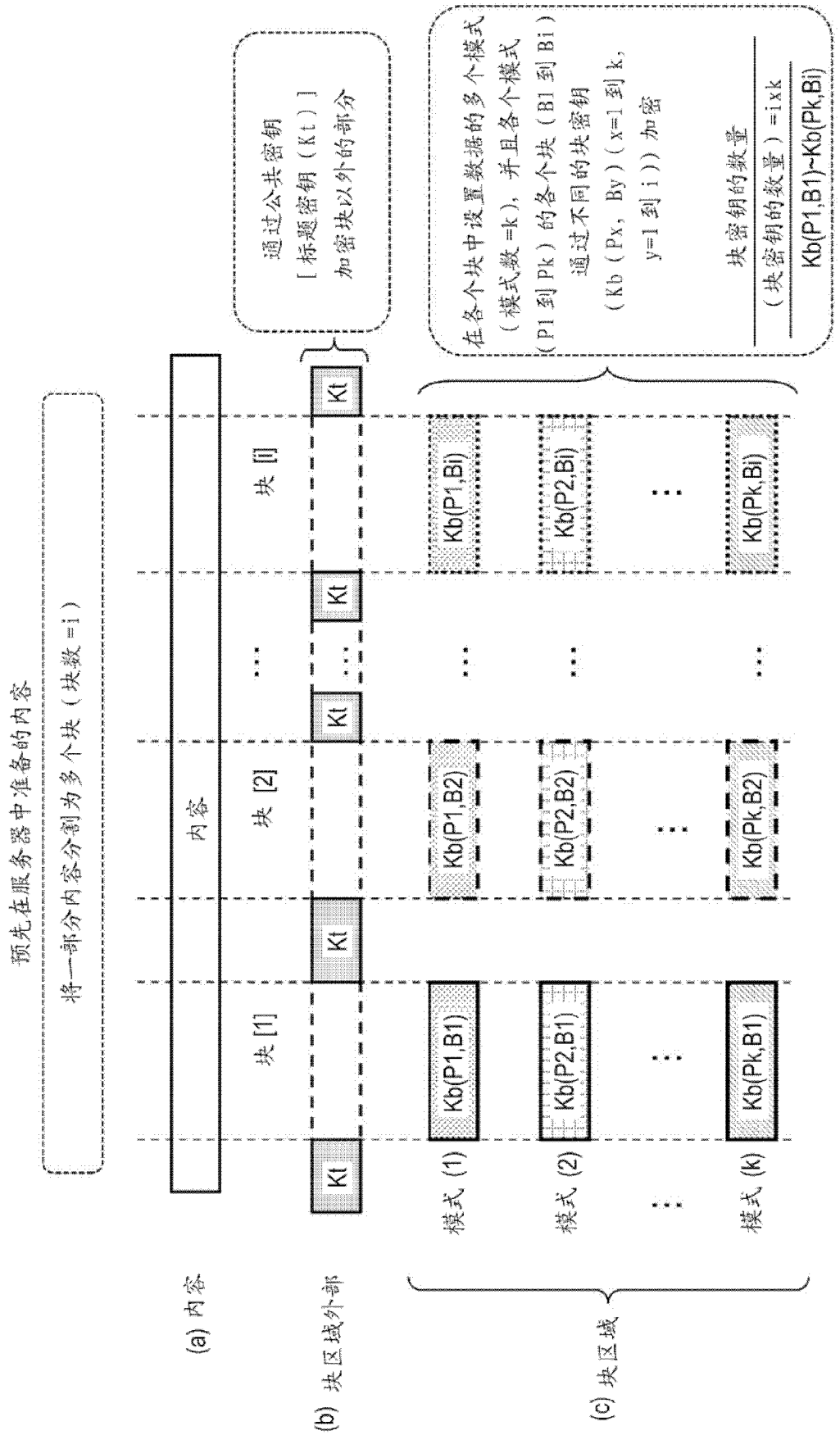

预先在服务器中准备的内容
将一部分内容分割为多个块（块数=i）
通过公共密钥
[标题密钥（Kt）]
加密块以外的部分
在各个块中设置数据的多个模式
（模式数=k），并且各个模式
（P1到Pk）的各个块（B1到Bi）
通过不同的块密钥
（Kb（Px，By）（x=1到k，
y=1到i））加密
块密钥的数量
（块密钥的数量）=ixk
Kb(P1,B1)~Kb(Pk,Bi)
(a) 内容
(b) 块区域外部
(c) 块区域
内容
块 [1]
块 [2]
块 [I]
Kt
Kb(P1,B1)
Kb(P1,B2)
Kb(P1,Bi)
Kb(P2,B1)
Kb(P2,B2)
Kb(P2,Bi)
Kb(Pk,B1)
Kb(Pk,B2)
Kb(Pk,Bi)
模式 (1)
模式 (2)
模式 (k)

图 5

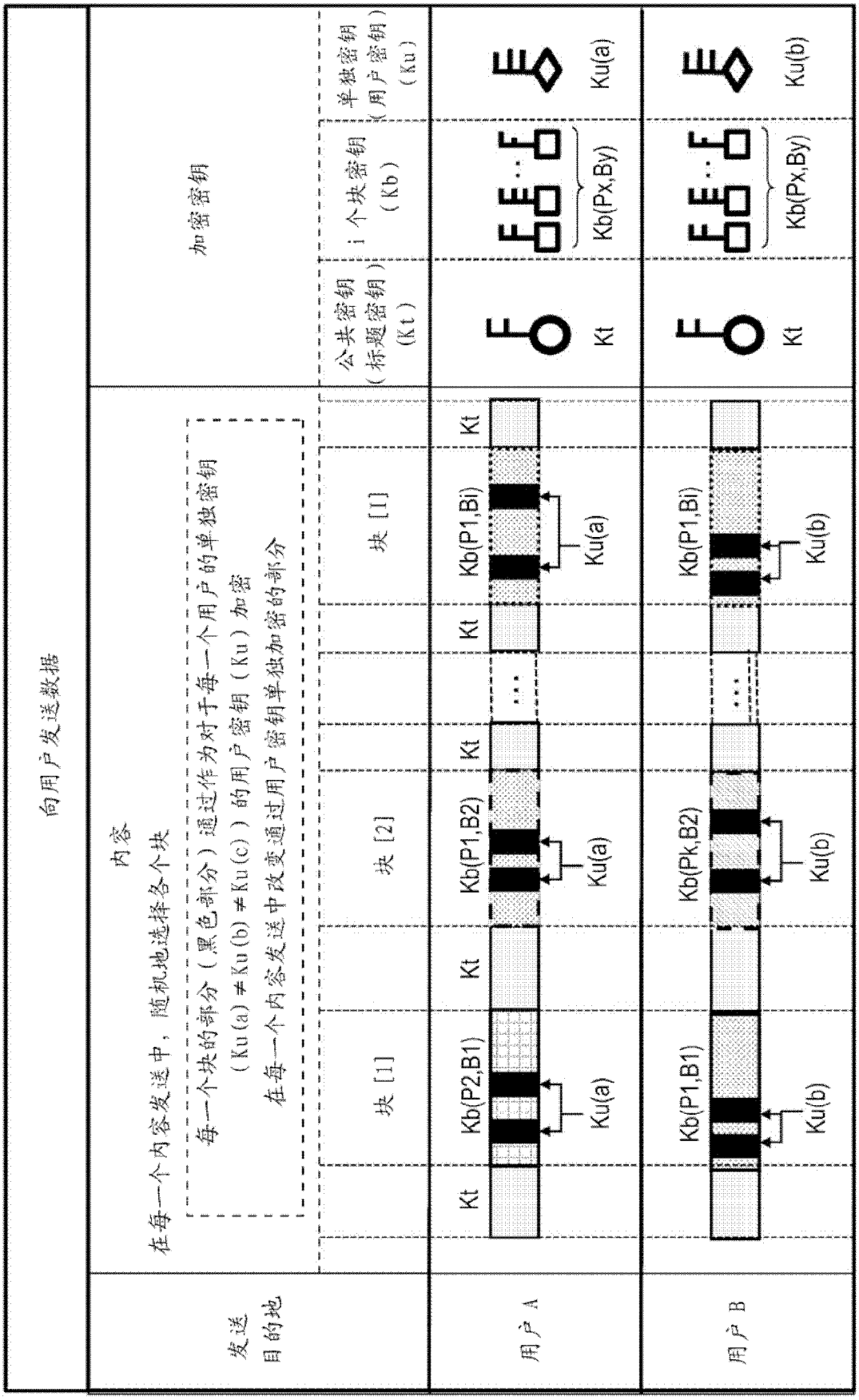

向用户发送数据
内容
在每一个内容发送中，随机地选择各个块
每一个块的部分（黑色部分）通过作为对于每一个用户的单独密钥
（Ku(a)≠Ku(b)≠Ku(c)）的用户密钥（Ku）加密
在每一个内容发送中改变通过用户密钥单独加密的部分
发送
目的地
加密密钥
公共密钥
（标题密钥）
（Kt）
i 个块密钥
（Kb）
单独密钥
（用户密钥）
（Ku）
块 [1]
块 [2]
块 [1]
用户 A
用户 B
Kt
Kb(P2,B1)
Kb(P1,B2)
Kb(P1,Bi)
Kb(P1,B1)
Kb(Pk,B2)
Kb(Px,By)
Ku(a)
Ku(b)

图 6

参数	参数内容
a	块大小
i	块数
k	模式数
b	通过用户密钥（Ku）单独加密的部分的大小
c	在一个块中通过用户密钥（Ku）单独加密的部分的数量

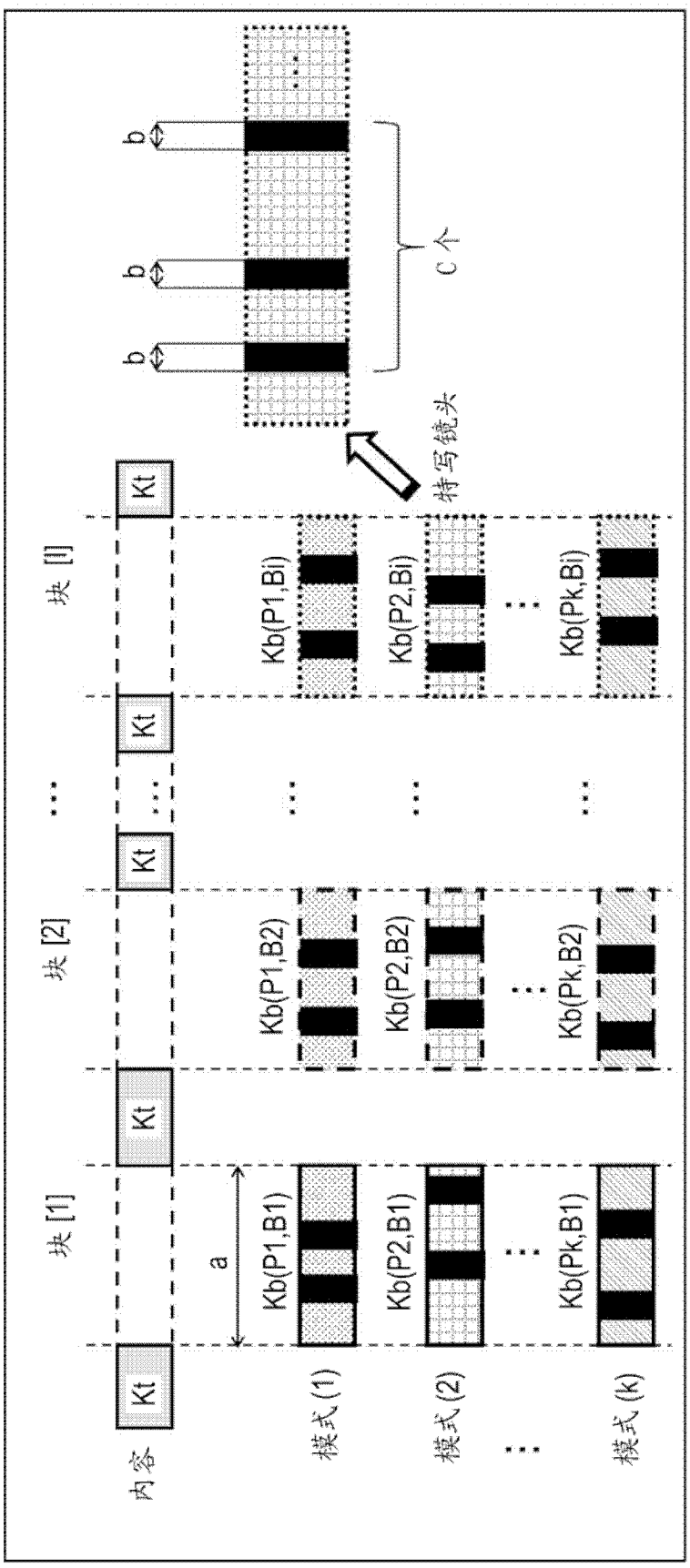


图 7

参数	设置示例（建议）	描述	参数的设置条件（要求）	满足参数的设置条件的建议措施
a	1MB (=1sec)	块大小	在每一个加密处理或解密处理中，应用遵循给定格式的规定的配置	应用 1 块 =1 码元 8 块 =1 段
i	720	块数	当难以再现块部分时，充分地阻挠用户	以块覆盖整个的 10% 7200*0.1/1=720 （720/8=90 段）
k	32	模式数	在内容的各个分发中实现模式的不同组合	准备 32 种变体
b	16 字节	单独加密的部分的大小	在不解密单独加密的部分的情况下，难以进行块部分的正常再现	高效地抹出再现所需的部分（如，IDR 画面的片头部）
c	8	一个块中单独加密的部分的数量		

内容设置示例：视频速率 =8Mbps，持续时间 =7200 秒，大小 =7.2GB，IDR 间隔 =1 秒

通过单独加密而不同的部分（再现时间）	720 秒
单独加密的部分的总大小（每一个内容）	92160 字节
认证 / 发送服务器中必须额外放入的数据大小（与各个模式对应的块数据的总和）	22.32GB

图 8

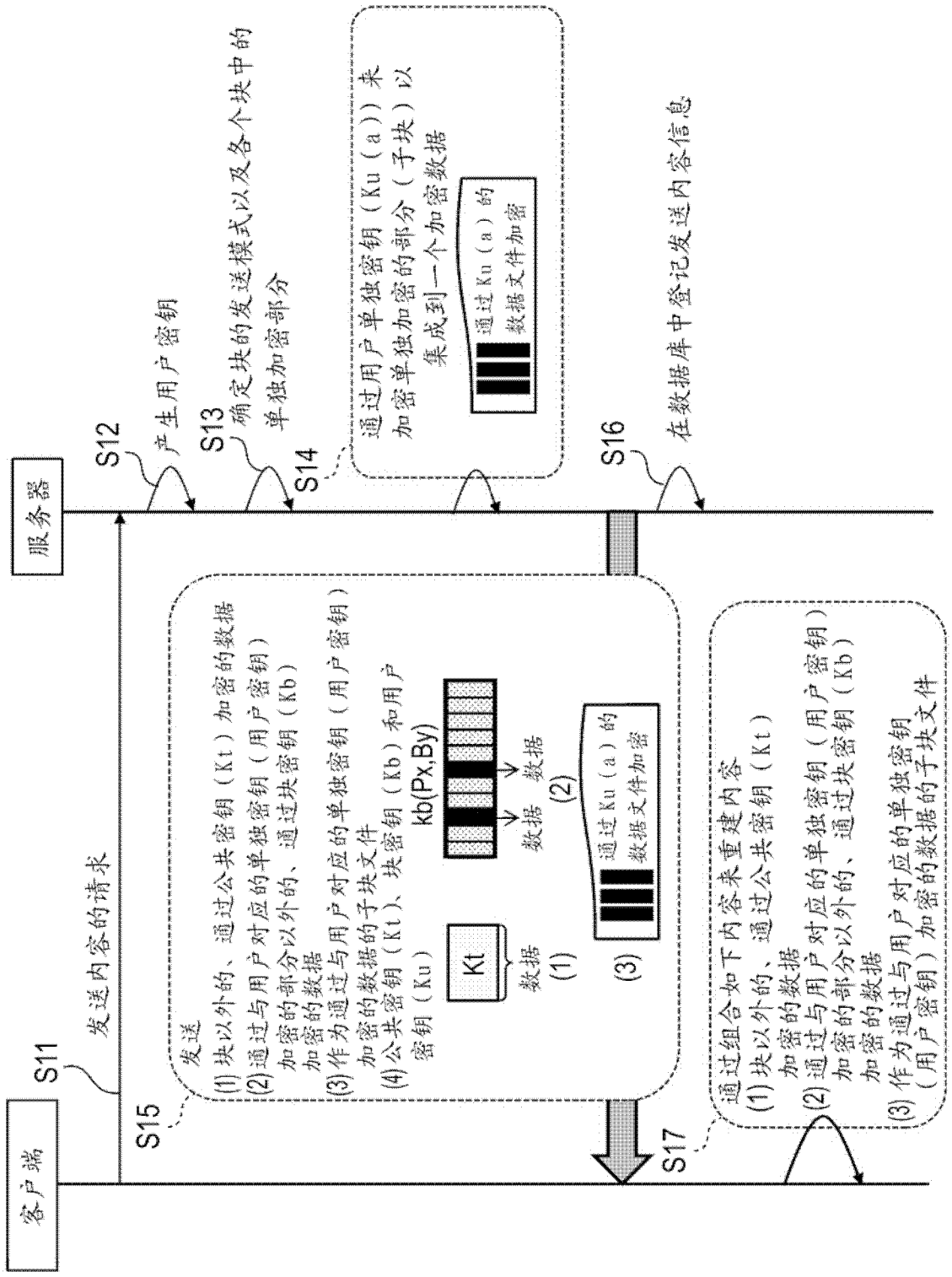

服务器
客户端
S11
发送内容的请求
S12
产生用户密钥
S13
确定块的发送模式以及各个块中的单独加密部分
S14
通过用户单独密钥（Ku（a））来加密单独加密的部分（子块）以集成到一个加密数据
通过Ku（a）的数据文件加密
S15
发送
(1)块以外的、通过公共密钥（Kt）加密的数据
(2)通过与用户对应的单独密钥（用户密钥）加密的部分以外的、通过块密钥（Kb）加密的数据
(3)作为通过与用户对应的单独密钥（用户密钥）加密的数据的子块文件
(4)公共密钥（Kt）、块密钥（Kb）和用户密钥（Ku）
Kt
数据
(1)
kb(Px,By)
数据 数据
(2)
(3)
通过Ku（a）的数据文件加密
S16
在数据库中登记发送内容信息
S17
通过组合如下内容来重建内容
(1)块以外的、通过公共密钥（Kt）加密的数据
(2)通过与用户对应的单独密钥（用户密钥）加密的部分以外的、通过块密钥（Kb）加密的数据
(3)作为通过与用户对应的单独密钥（用户密钥）加密的数据的子块文件

图 9

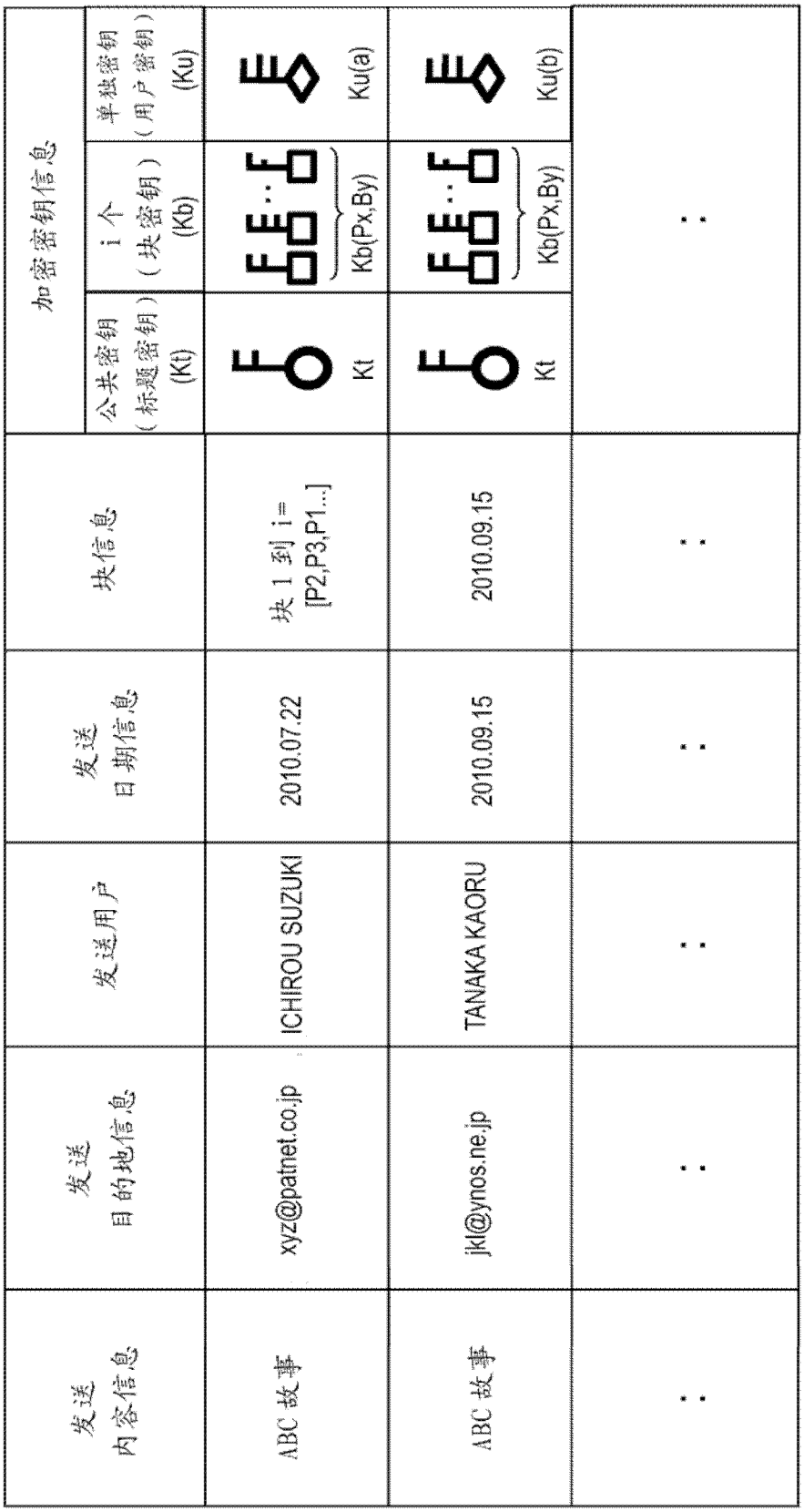

发送
内容信息
发送
目的地信息
发送用户
发送
日期信息
块信息
加密密钥信息
公共密钥
(标题密钥)
(Kt)
i 个
(块密钥)
(Kb)
单独密钥
(用户密钥)
(Ku)
ABC 故事
xyz@patnet.co.jp
ICHIROU SUZUKI
2010.07.22
块 1 到 i =
[P2,P3,P1...]
Kt
Kb(Px,By)
Ku(a)
ABC 故事
jkl@ynos.ne.jp
TANAKA KAORU
2010.09.15
2010.09.15
Kt
Kb(Px,By)
Ku(b)

图 10

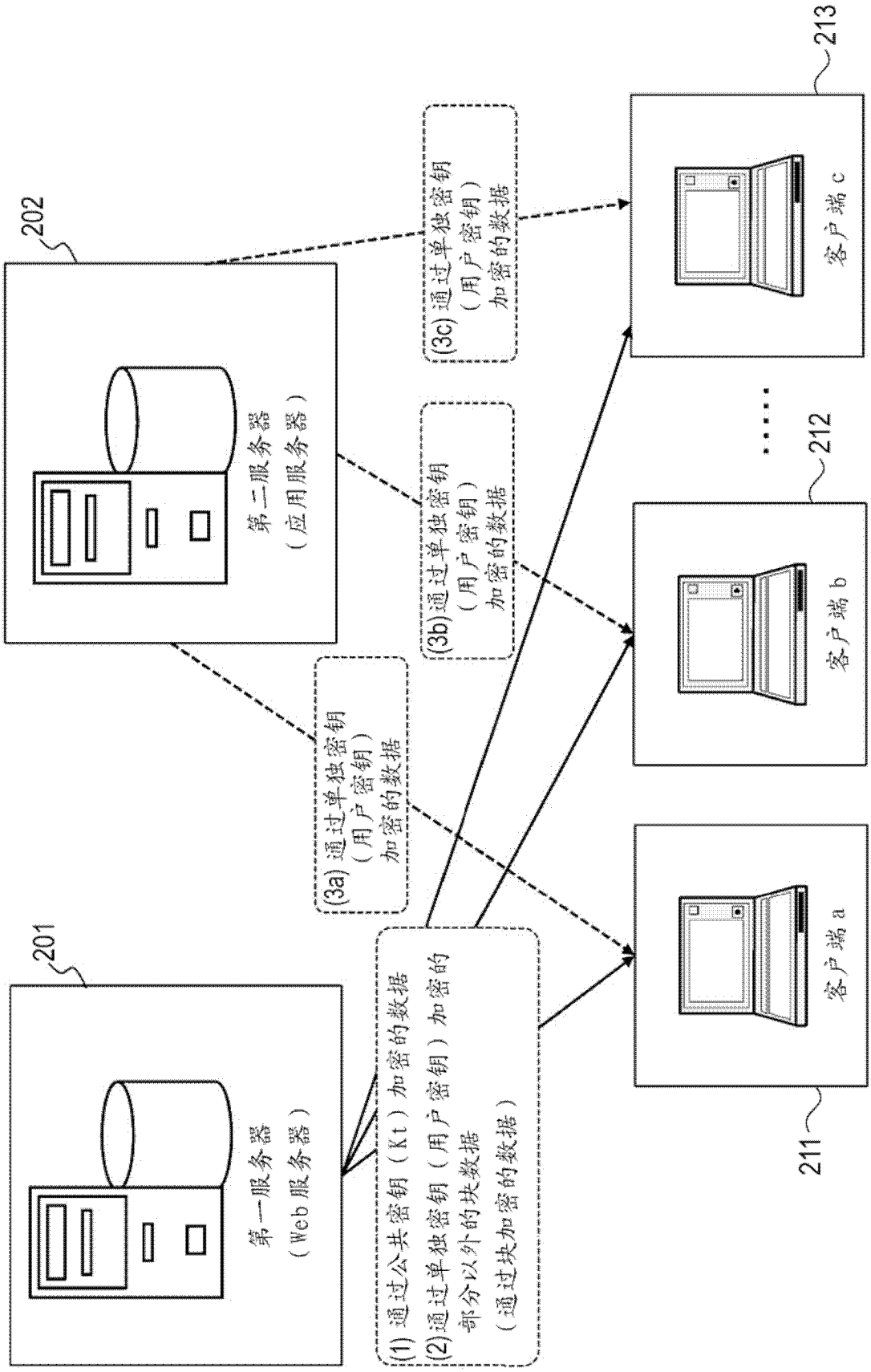

201
第一服务器
（Web 服务器）
202
第二服务器
（应用服务器）
(1) 通过公共密钥（Kt）加密的数据
(2)通过单独密钥（用户密钥）加密的
部分以外的块数据
（通过块加密的数据）
(3a) 通过单独密钥
（用户密钥）
加密的数据
(3b)通过单独密钥
（用户密钥）
加密的数据
(3c) 通过单独密钥
（用户密钥）
加密的数据
211
客户端 a
212
客户端 b
213
客户端 c

图 11

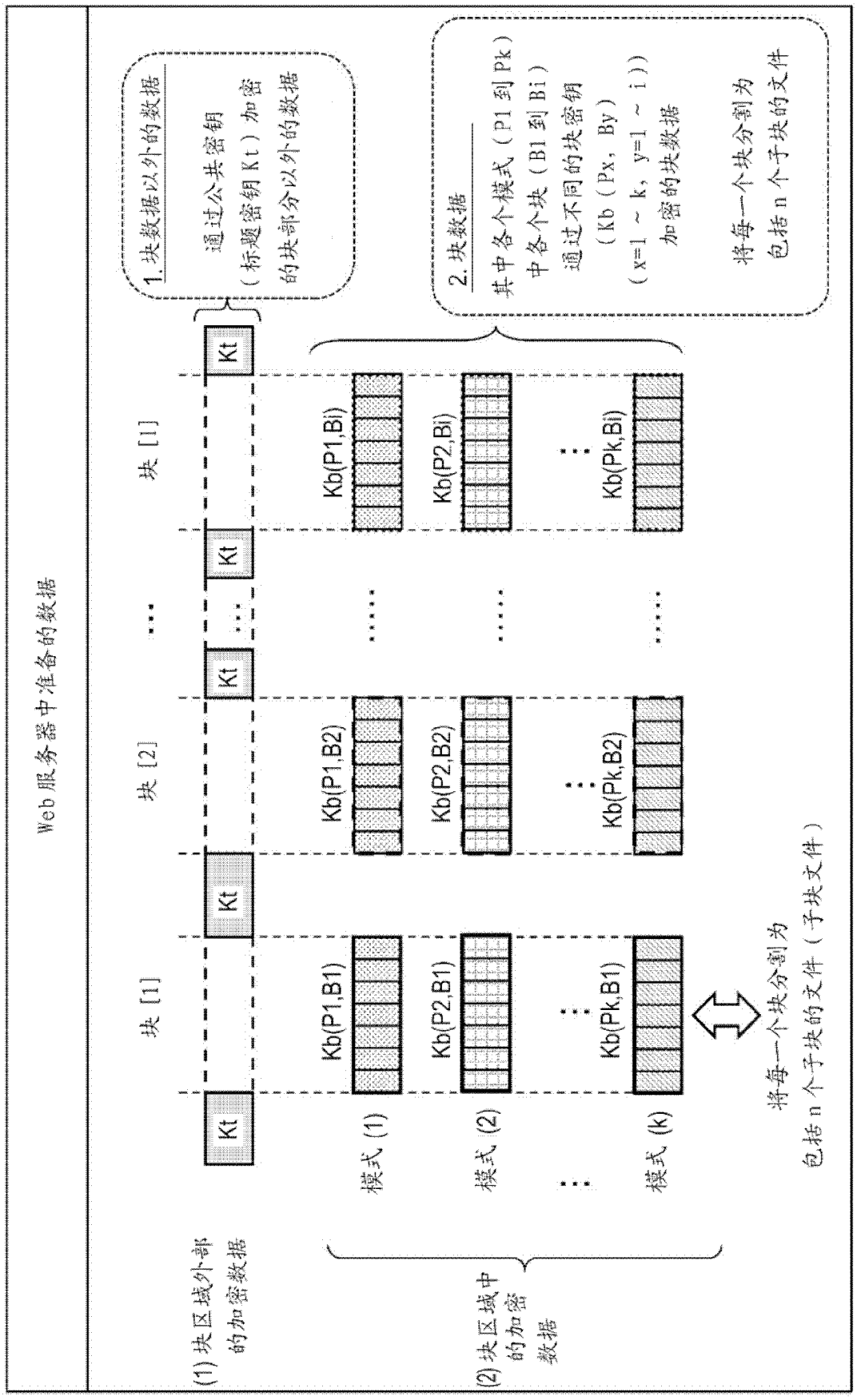

Web 服务器中准备的数据
1. 块数据以外的数据
通过公共密钥（标题密钥 Kt）加密的块部分以外的数据
2. 块数据
其中各个模式（P1 到 Pk）中各个块（B1 到 Bi）通过不同的块密钥（Kb（Px，By）（x=1 ～ k，y=1 ～ i））加密的块数据
将每一个块分割为包括 n 个子块的文件
块 [1]
块 [2]
块 [1]
Kt
Kb(P1,B1)
Kb(P2,B1)
Kb(Pk,B1)
Kb(P1,B2)
Kb(P2,B2)
Kb(Pk,B2)
Kb(P1,Bi)
Kb(P2,Bi)
Kb(Pk,Bi)
模式 (1)
模式 (2)
模式 (k)
(1) 块区域外部的加密数据
(2) 块区域中的加密数据
将每一个块分割为包括 n 个子块的文件（子块文件）

图 12

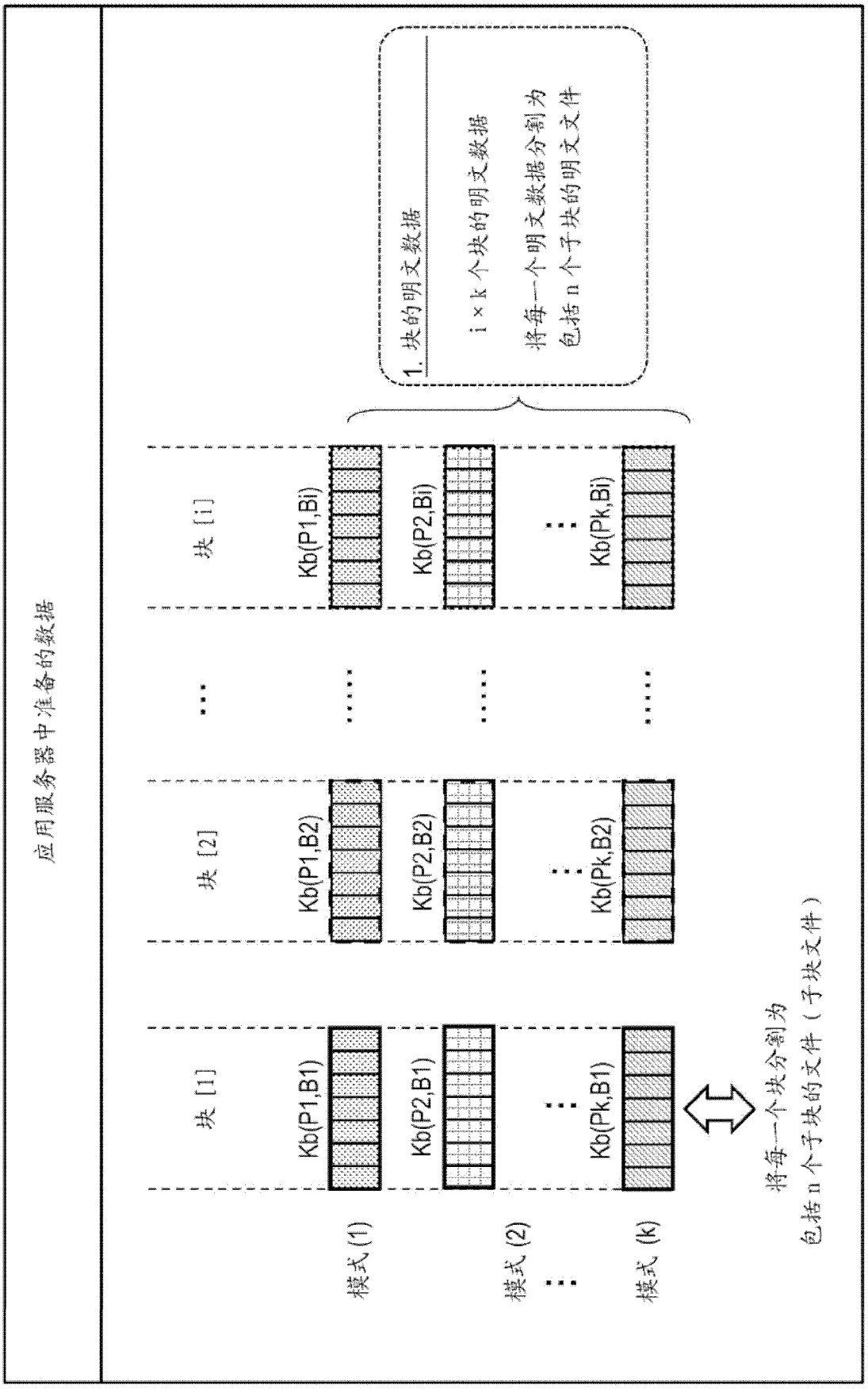

应用服务器中准备的数据
块 [1]
块 [2]
...
块 [i]
Kb(P1,B1)
Kb(P2,B1)
Kb(Pk,B1)
Kb(P1,B2)
Kb(P2,B2)
Kb(Pk,B2)
Kb(P1,Bi)
Kb(P2,Bi)
Kb(Pk,Bi)
模式 (1)
模式 (2)
模式 (k)
将每一个块分割为
包括 n 个子块的文件（子块文件）
1. 块的明文数据
i × k 个块的明文数据
将每一个明文数据分割为
包括 n 个子块的明文文件

图 13

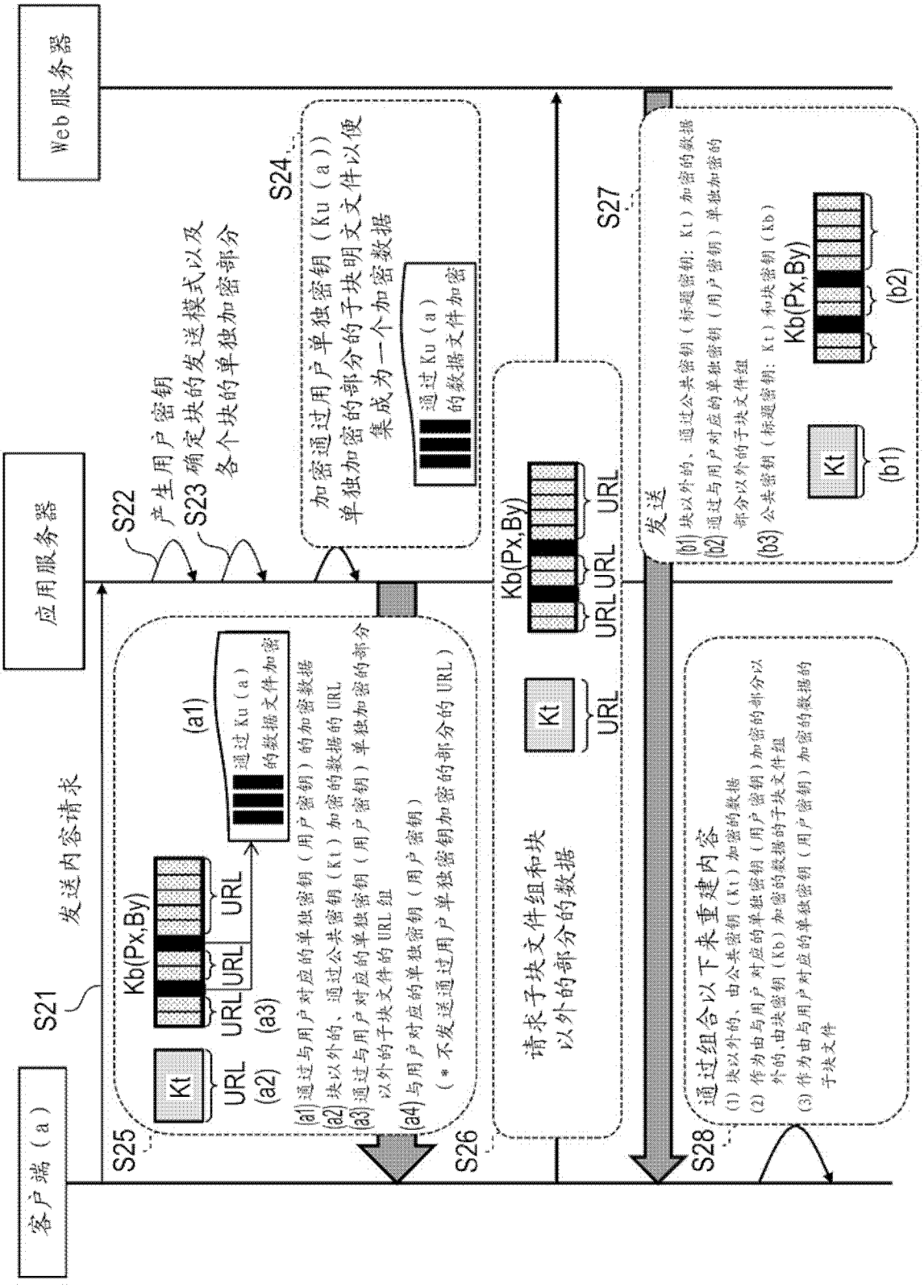

Web服务器
应用服务器
客户端（a）
发送内容请求
S21
S22
产生用户密钥
S23 确定块的发送模式以及
各个块的单独加密部分
S24
加密通过用户单独密钥（Ku（a））
单独加密的部分的子块明文文件以便
集成为一个加密数据
通过Ku（a）
的数据文件加密
S25
Kb(Px,By)
Kt
URL
URL
URL
URL
(a1)
(a2)
(a3)
通过Ku（a）
的数据文件加密
(a1)通过与用户对应的单独密钥（用户密钥）的加密数据
(a2)块以外的、通过公共密钥（Kt）加密的数据的URL
(a3)通过与用户对应的单独密钥（用户密钥）单独加密的部分
以外的子块文件的URL组
(a4)与用户对应的单独密钥（用户密钥）
（＊不发送通过用户单独密钥加密的部分的URL）
S26
请求子块文件组和块
以外的部分的数据
Kb(Px,By)
Kt
URL
URL
URL
URL
S27
发送
(b1)块以外的、通过公共密钥（标题密钥：Kt）加密的数据
(b2)通过与用户对应的单独密钥（用户密钥）单独加密的
部分以外的子块文件组
(b3)公共密钥（标题密钥：Kt）和块密钥（Kb）
Kb(Px,By)
Kt
(b1)
(b2)
S28
通过组合以下来重建内容
(1)块以外的、由公共密钥（Kt）加密的数据
(2)作为由与用户对应的单独密钥（用户密钥）加密的部分以
外的、由块密钥（Kb）加密的数据的子块文件组
(3)作为由与用户对应的单独密钥（用户密钥）加密的数据的
子块文件

图 14

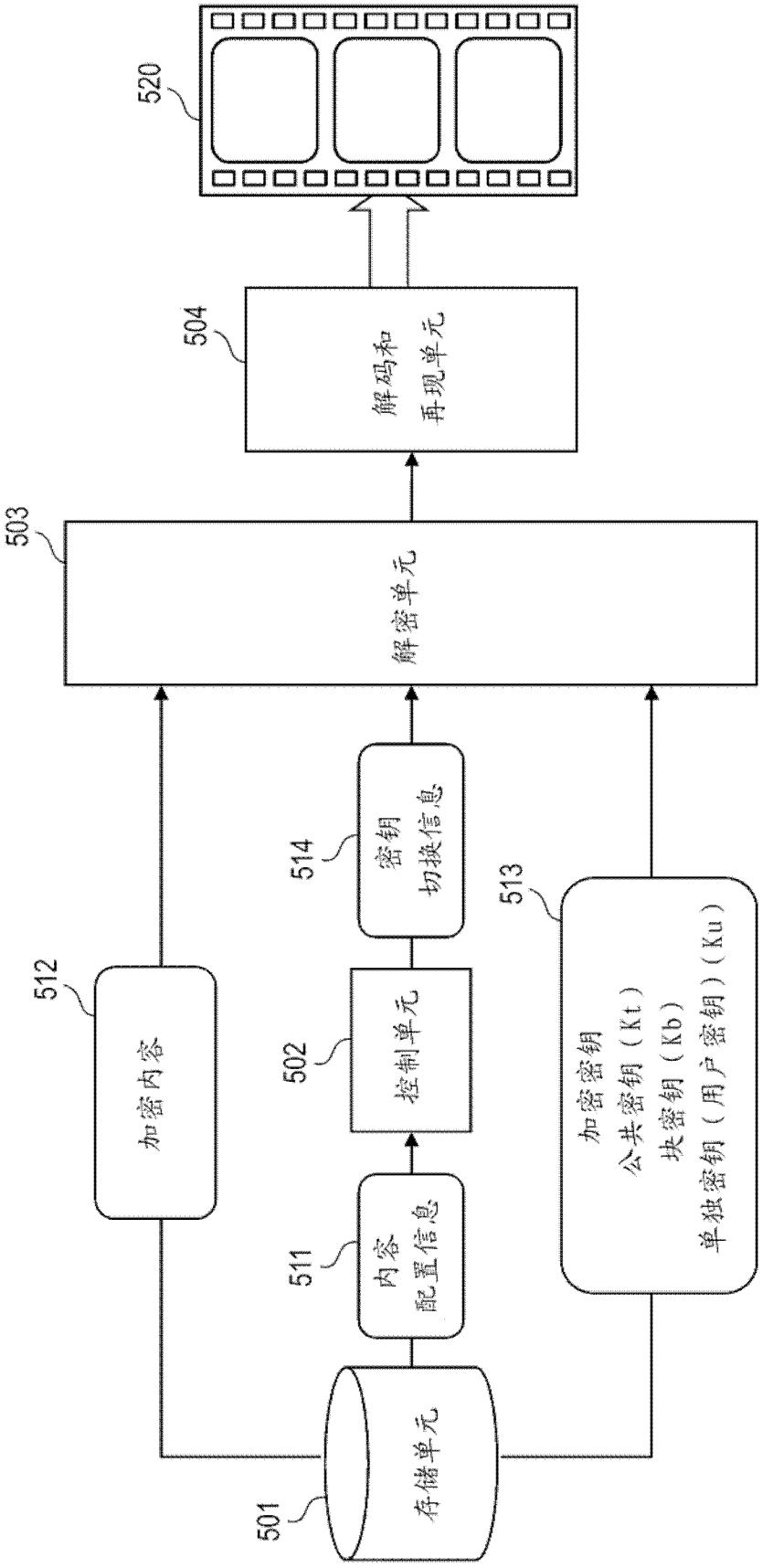

520
504
解码和
再现单元
503
解密单元
514
密钥
切换信息
513
512
加密内容
502
控制单元
加密密钥
公共密钥（Kt）
块密钥（Kb）
单独密钥（用户密钥）（Ku）
511
内容
配置信息
501
存储单元

图 15

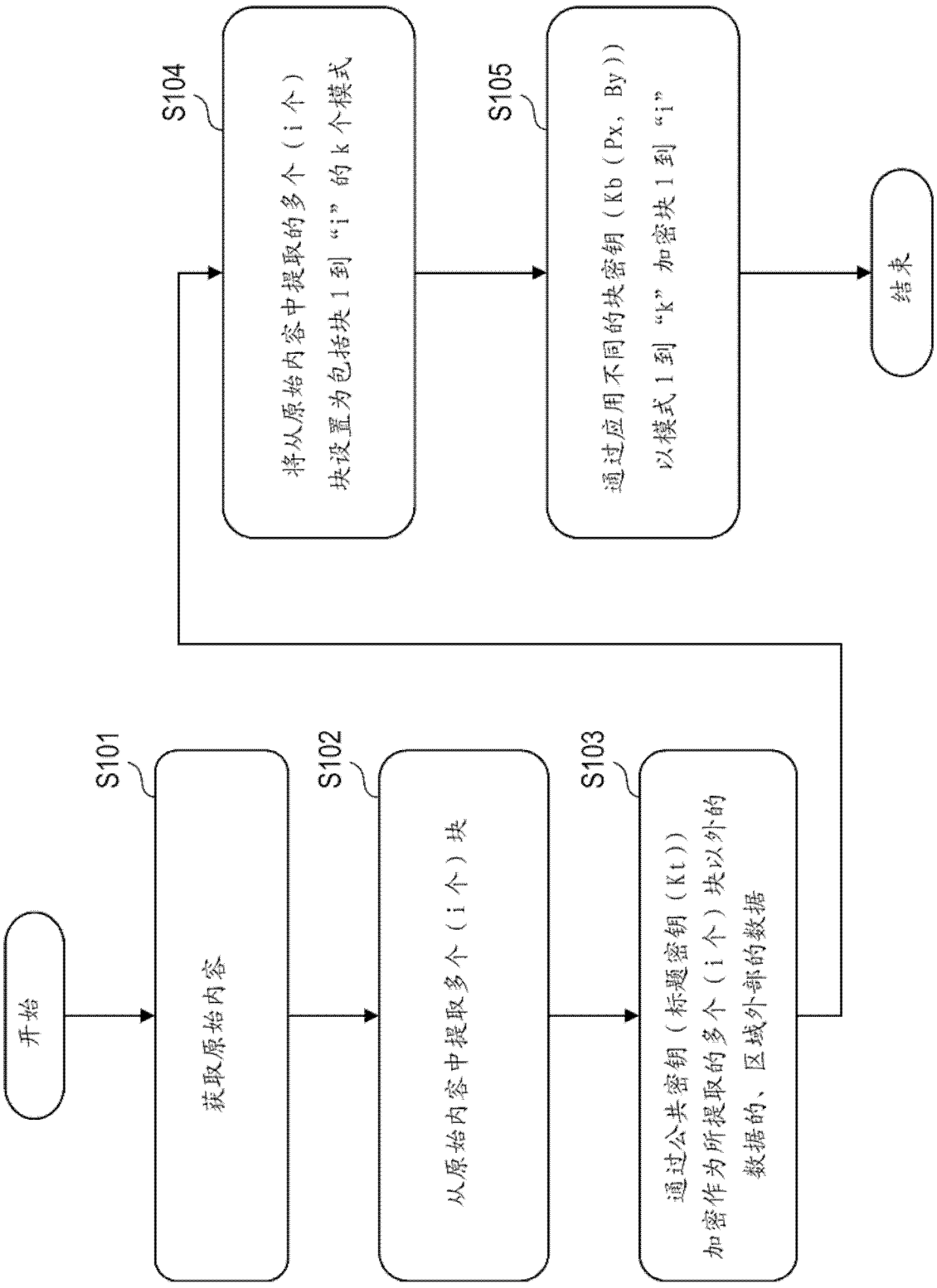

开始
S101
获取原始内容
S102
从原始内容中提取多个（i个）块
S103
通过公共密钥（标题密钥（Kt））
加密作为所提取的多个（i个）块以外的
数据的、区域外部的数据
S104
将从原始内容中提取的多个（i个）
块设置为包括块1到“i”的k个模式
S105
通过应用不同的块密钥（Kb（Px，By））
以模式1到“k”加密块1到“i”
结束

图 16

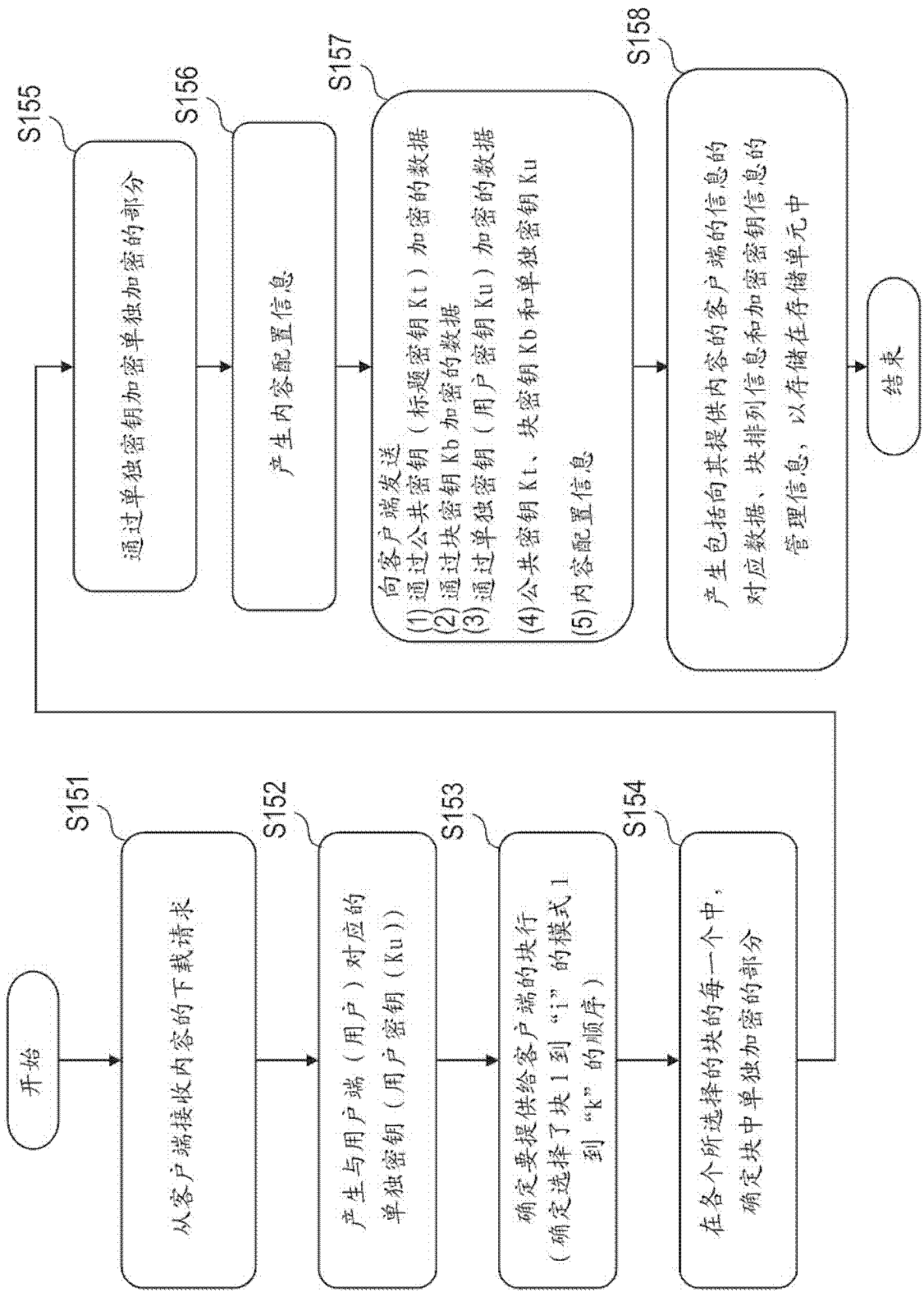

开始
S151
从客户端接收内容的下载请求
S152
产生与用户端（用户）对应的单独密钥（用户密钥（Ku））
S153
确定要提供给客户端的块行（确定选择了块1到“i”的模式1到“k”的顺序）
S154
在各个所选择的块的每一个中，确定块中单独加密的部分
S155
通过单独密钥加密单独加密的部分
S156
产生内容配置信息
S157
向客户端发送
(1)通过公共密钥（标题密钥Kt）加密的数据
(2)通过块密钥Kb加密的数据
(3)通过单独密钥（用户密钥Ku）加密的数据
(4)公共密钥Kt、块密钥Kb和单独密钥Ku
(5)内容配置信息
S158
产生包括向其提供内容的客户端的信息的对应数据、块排列信息和加密密钥信息的管理信息，以存储在存储单元中
结束

图 17

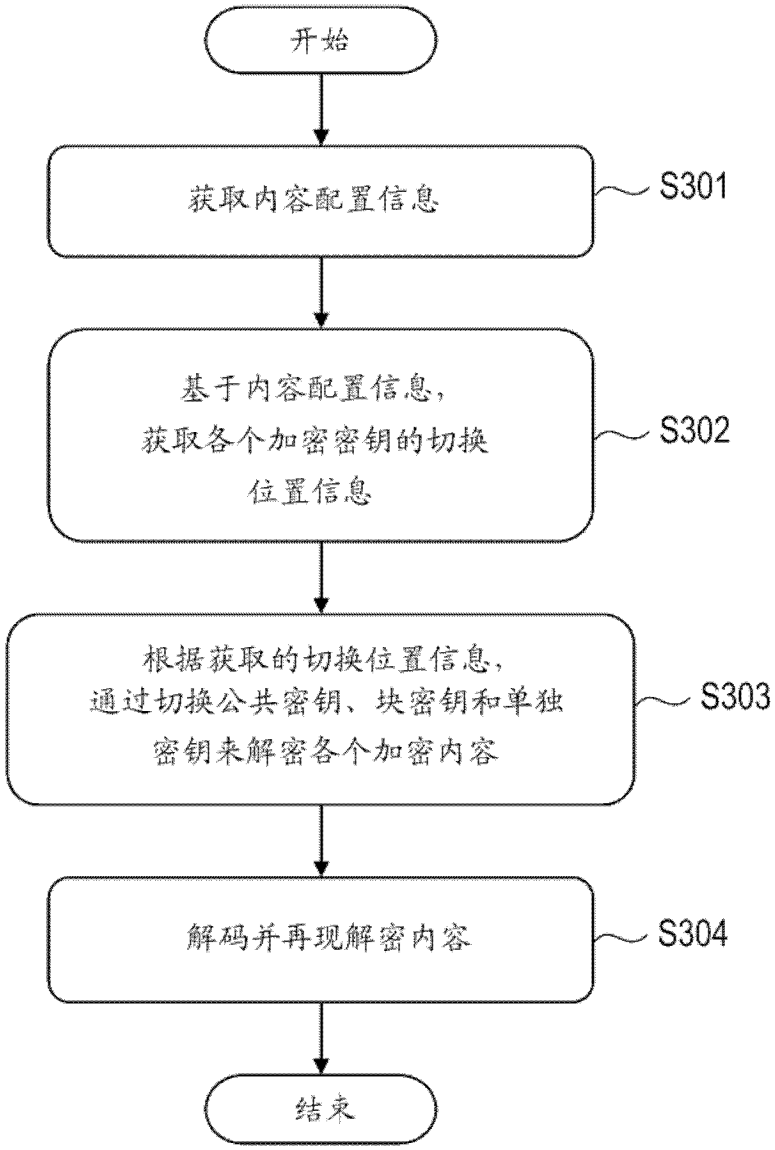

开始
获取内容配置信息
S301
基于内容配置信息，
获取各个加密密钥的切换
位置信息
S302
根据获取的切换位置信息，
通过切换公共密钥、块密钥和单独
密钥来解密各个加密内容
S303
解码并再现解密内容
S304
结束

图 18

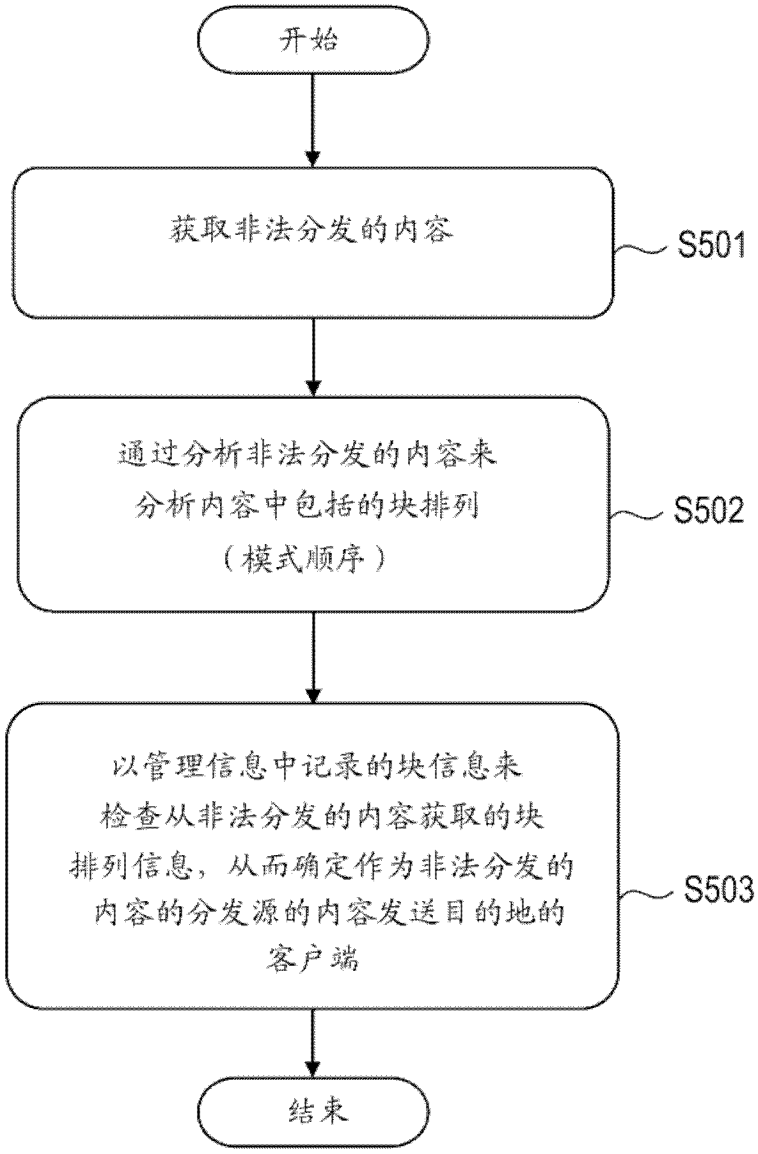

开始
获取非法分发的内容
S501
通过分析非法分发的内容来
分析内容中包括的块排列
（模式顺序）
S502
以管理信息中记录的块信息来
检查从非法分发的内容获取的块
排列信息，从而确定作为非法分发的
内容的分发源的内容发送目的地的
客户端
S503
结束

图 19

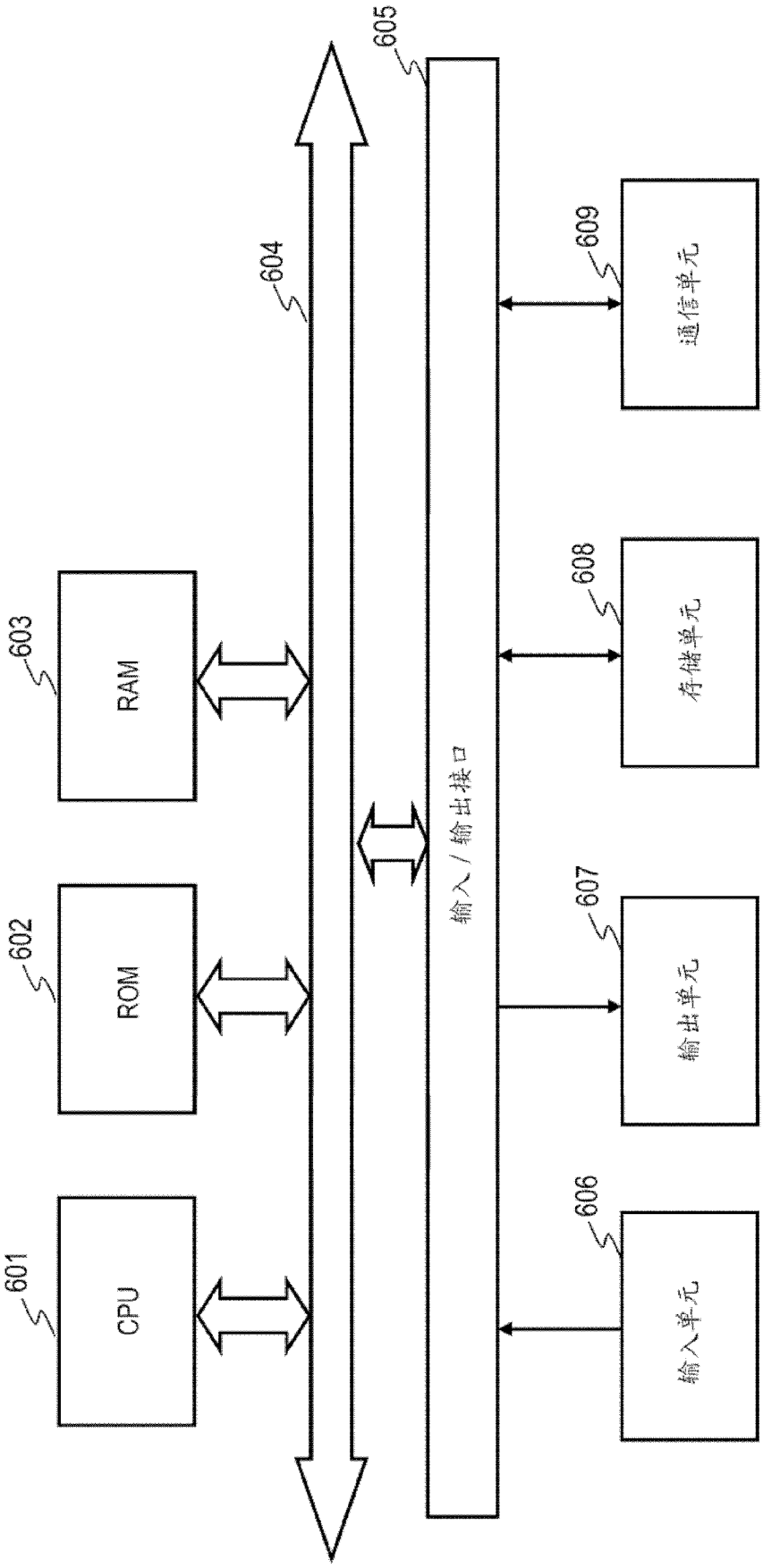

605
604
609
通信单元
608
存储单元
607
输出单元
606
输入单元
603
RAM
602
ROM
601
CPU
输入/输出接口

图 20

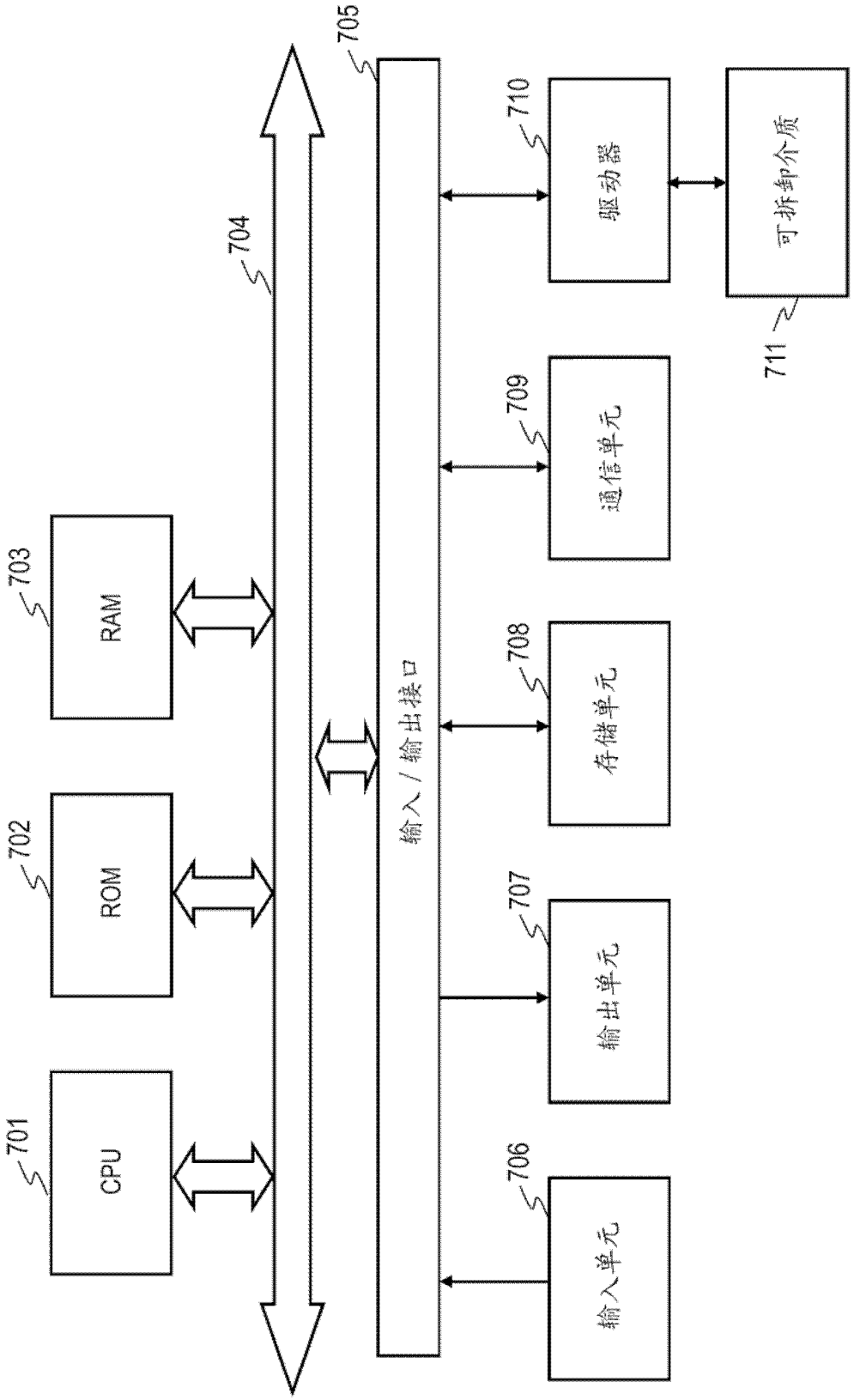

705
710
驱动器
可拆卸介质
711
704
709
通信单元
703
RAM
708
存储单元
输入 / 输出接口
702
ROM
707
输出单元
701
CPU
706
输入单元

图 21