(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 103348623 B
(45)授权公告日 2016.06.29

(21)申请号 201280006980.5
(22)申请日 2012.08.17
(30)优先权数据
61/527,854 2011.08.26 US
(85)PCT国际申请进入国家阶段日
2013.07.30
(86)PCT国际申请的申请数据
PCT/JP2012/005183 2012.08.17
(87)PCT国际申请的公布数据
WO2013/031124 JA 2013.03.07
(73)专利权人 松下电器产业株式会社
地址 日本大阪府
(72)发明人 山口高弘 布田裕一 中野稔久
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 陈萍 高迪
(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/32(2006.01)
G06F 21/62(2013.01)
(56)对比文件
CN 101803396 A,2010.08.11,
CN 101874248 A,2010.10.27,
US 2008063199 A1,2008.03.13,
US 7088822 B2,2006.08.08,
审查员 孙凯

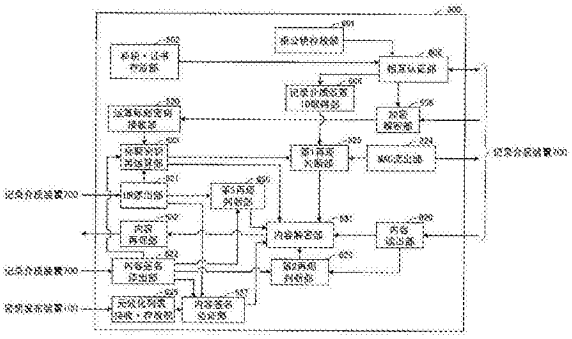
权利要求书3页 说明书28页 附图25页

(54)发明名称

终端装置、验证装置、密钥分发装置、内容再现方法及密钥分发方法

(57)摘要

终端装置(600),其特征在于,包括:读出部,从记录介质装置(700)的普通区域读出加密内容与内容签名,从记录介质装置(700)的认证区域读出利用由正规的签名装置(500)生成的内容签名变换标题密钥而得的变换标题密钥;标题密钥复原部,利用读出部所读出的内容签名对变换标题密钥进行逆变换,生成复原标题密钥;以及再现部,利用复原标题密钥,解密加密内容,再现解密而得的内容。



CN 103348623 B

1.一种终端装置,其特征在于,包括:

读出部,从记录介质装置读出加密内容与内容签名,从所述记录介质装置的被保护的区域读出变换标题密钥,该变换标题密钥通过利用由正规的签名装置生成的内容签名对标题密钥进行变换而成;

标题密钥复原部,利用读出部所读出的所述内容签名对所述变换标题密钥进行逆变换,生成复原标题密钥;以及

再现部,利用所述复原标题密钥,解密所述加密内容,再现解密而得的内容。

2.如权利要求1所述的终端装置,其特征在于,

所述变换标题密钥根据由所述正规的签名装置生成的内容签名、所述内容的利用条件以及所述标题密钥生成,

所述读出部还从所述记录介质装置读出利用条件,

所述标题密钥复原部利用所述读出部所读出的所述内容签名与所述利用条件对所述变换标题密钥进行逆变换,生成所述复原标题密钥。

3.如权利要求2所述的终端装置,其特征在于,

所述变换标题密钥通过对第1结合数据与所述标题密钥实施规定的运算来生成,该第1结合数据通过结合由所述正规的签名装置生成的内容签名以及所述利用条件而成,

所述标题密钥复原部根据所述读出部所读出的所述内容签名与读出的所述利用条件生成第2结合数据,对生成的所述第2结合数据与所述变换标题密钥实施所述规定的运算的逆运算,生成所述复原标题密钥。

4.如权利要求3所述的终端装置,其特征在于,

所述终端装置还包括内容签名验证部,该内容签名验证部判断所述读出部所读出的所述内容签名与所述变换标题密钥的生成所利用的由所述正规的签名装置生成的所述内容签名是否一致,在判断结果为不一致时,抑制所述再现部的处理。

5.如权利要求3所述的终端装置,其特征在于,

所述终端装置还包括内容验证部,该内容验证部利用所述内容签名验证所述加密内容的合法性,在判断为所述加密内容非法时,抑制所述再现部的处理。

6.如权利要求3所述的终端装置,其特征在于,

所述内容签名包括生成该内容签名的所述签名装置的识别信息,

所述终端装置还包括:

接收部,接收无效化列表,该无效化列表记载有成为无效化对象的装置的识别信息;以及

无效化确认部,利用接收的所述无效化列表确认所述签名装置是否为无效化对象,在判断为所述签名装置是无效化对象时,抑制所述再现部的处理。

7.如权利要求6所述的终端装置,其特征在于,

所述内容签名还包括第1日期信息,该第1日期信息表示所述签名装置生成该内容签名的日期,

所述无效化列表还包括第2日期信息,该第2日期信息与成为无效化对象的装置的识别信息建立对应地表示成为无效化对象的日期,

所述无效化确认部在所述签名装置的识别信息记载于所述无效化列表,并且所述第1

日期信息所表示的日期晚于所述第2日期信息所表示的日期时，判断为所述签名装置是无效化对象，

所述无效化确认部在所述签名装置的识别信息记载于所述无效化列表，并且所述第1日期信息所表示的日期早于所述第2日期信息所表示的日期时，判断为所述签名装置并非无效化对象。

8.一种验证装置，其特征在于，包括：

读出部，从记录介质装置读出加密内容与内容签名，从所述记录介质装置的被保护的区域读出变换标题密钥，该变换标题密钥通过利用由正规的签名装置生成的内容签名对标题密钥进行变换而成；以及

内容签名验证部，判断读出部所读出的所述内容签名与所述变换标题密钥的生成所利用的由所述正规的签名装置生成的所述内容签名是否一致。

9.一种密钥分发装置，其特征在于，包括：

内容保持部，保持通过标题密钥对内容进行加密而得的加密内容；

内容签名保持部，保持用于验证所述加密内容的合法性的内容签名；

标题密钥保持部，保持所述标题密钥；

密钥生成部，利用所述内容签名对所述标题密钥进行变换，生成变换标题密钥；以及

记录部，将所述加密内容、所述内容签名以及所述变换标题密钥记录于记录介质装置。

10.如权利要求9所述的密钥分发装置，其特征在于，

所述密钥分发装置还包括利用条件保持部，该利用条件保持部保持所述内容的利用条件；

所述密钥生成部根据所述内容签名、所述利用条件以及所述标题密钥生成所述变换标题密钥。

11.如权利要求10所述的密钥分发装置，其特征在于，

所述密钥生成部通过对结合数据与所述标题密钥实施规定的运算来生成所述变换标题密钥，该结合数据通过结合所述内容签名以及所述利用条件而成。

12.一种内容再现方法，在终端装置中使用，其特征在于，包括：

读出步骤，从记录介质装置读出加密内容与内容签名，从所述记录介质装置的被保护的区域读出变换标题密钥，该变换标题密钥通过利用由正规的签名装置生成的内容签名对标题密钥进行变换而成；

标题密钥复原步骤，利用所述读出步骤所读出的所述内容签名对所述变换标题密钥进行逆变换，生成复原标题密钥；以及

再现步骤，利用所述标题密钥复原步骤所复原的所述复原标题密钥，解密所述加密内容，再现解密而得的内容。

13.一种密钥分发方法，在密钥分发装置中使用，其特征在于，

在所述密钥分发装置中，保持有通过标题密钥对内容进行加密而得的加密内容、用于验证所述加密内容的合法性的内容签名、以及所述标题密钥，

所述密钥分发方法包括：

密钥生成步骤，利用所述内容签名对所述标题密钥进行变换，生成变换标题密钥；以及

记录步骤，将所述加密内容、所述内容签名以及所述变换标题密钥记录于记录介质装

置。

终端装置、验证装置、密钥分发装置、内容再现方法及密钥分发方法

技术领域

[0001] 本发明涉及一种技术，将通过网络分发的数字版权作品记录于记录介质装置，并再现记录于记录介质装置的数字版权作品。

背景技术

[0002] 最近，将电影或音乐等数字版权作品(以下，记载为“内容”。)通过网络分发的系统逐渐普及。该系统例如为如下的系统，即用户的个人电脑(以下，记载为“PC”。)从内容服务器接收内容，将接收的内容记录于用户购入的SD存储卡等。

[0003] 由于网络分发的内容为高画质以及高音质的数字数据，因此为了遏制非法拷贝等泛滥，需要版权保护对策。

[0004] 在内容的版权保护规格之一中，存在AACS(Advanced Access Content System:高级内容访问系统)。AACS为在BD(Blu-rayDisc(注册商标))中所利用的版权保护规格。在由AACS规定的版权保护技术之一中，存在“内容签名”(专利文献1)。

[0005] 内容制作方汇集分割内容而得的各部分内容的哈希值并构筑哈希列表，向值得信赖的第三方机构递交。第三方机构针对接收的哈希列表赋予数字签名，生成由哈希列表与数字签名构成的内容签名。内容制作方将内容与内容签名记录于BD，从而向用户出售。在此，内容签名利用与网络不连接的、安全能够确保的签名装置来生成。因此，签名密钥泄漏的风险低，保证了内容签名高的信赖性。

[0006] 正规的再现装置在再现时，部分地比较根据内容计算而得的哈希值与内容签名所包含的哈希列表。进而，再现装置进行内容签名所包含的数字签名的验证。据此，能够确认内容是否正规，内容是否被非法更换。再现装置在检测出内容不正规或者被非法更换时，停止内容的再现。

[0007] 在先技术文献

[0008] 专利文献

[0009] 专利文献1：日本特许第4084827号

[0010] 发明的概要

[0011] 发明要解决的问题

[0012] 当前，作为由控制器与闪速存储器构成的次时代SD存储卡所记录的内容的版权保护对策研究利用AACS。该情况下，假定由内容服务器生成内容签名。

[0013] 可是，由于内容服务器与现行的第三方机构的签名装置不同，与网络连接，因此签名密钥泄漏的风险高。存在若签名密钥泄漏，则会非法地利用泄漏的签名密钥，进行内容的非法利用的可能性。

发明内容

[0014] 于是，本发明便是鉴于上述的问题点而提出的，其目的在于提供一种终端装置、验

证装置、密钥分发装置、内容再现方法、密钥分发方法以及计算机程序，在将网络分发的内容记录于SD存储卡等记录介质装置的系统中，抑制非法利用泄漏的签名密钥的内容的非法利用。

[0015] 用于解决问题的手段

[0016] 于是，本发明的一方式的终端装置，其特征在于，包括：读出部，从记录介质装置读出加密内容与内容签名，从所述记录介质装置的被保护的区域读出变换标题密钥，该变换标题密钥利用由正规的签名装置生成的内容签名变换标题密钥而成；标题密钥复原部，利用读出部所读出的所述内容签名对所述变换标题密钥进行逆变换，生成复原标题密钥；以及再现部，利用所述复原标题密钥，解密所述加密内容，再现解密而得的内容。

[0017] 发明效果

[0018] 根据上述的构成，在所述记录介质装置的被保护的区域中，记录有变换标题密钥，该变换标题密钥利用由正规的签名装置生成的内容签名变换标题密钥而成。因此，即使进行将利用泄漏的签名密钥生成的内容签名与非法的加密内容记录于所述记录介质装置的非法行为，终端装置也无法根据从所述记录介质装置读出的变换标题密钥复原正确的标题密钥。终端装置在无法复原正确的标题密钥时，便无法正确地进行非法的加密内容的解密。因此，通过抑制终端装置的非法的加密内容的再现，能够抑制内容的非法利用。

附图说明

[0019] 图1为内容分发系统1的构成图。

[0020] 图2为密钥发布装置100的框图。

[0021] 图3为表示密钥发布装置100所生成的证书的数据构成的图。

[0022] 图4为表示密钥发布装置100所生成的无效化列表160的数据构成的图。

[0023] 图5为表示密钥发布处理的动作的流程图。

[0024] 图6为内容制作装置200的框图。

[0025] 图7为表示UR210的数据构成的图。

[0026] 图8为表示内容制作处理的动作的流程图。

[0027] 图9为内容分发装置300的框图。

[0028] 图10为用于说明内容识别信息311的生成方法的图。

[0029] 图11为表示内容分发装置的动作的流程图。

[0030] 图12为密钥分发装置400的框图。

[0031] 图13为表示内容签名510的数据构成的图。

[0032] 图14为表示处理完毕UR420以及处理完毕UR430的数据构成的图。

[0033] 图15为表示相互认证处理的动作的流程图。

[0034] 图16为表示相互认证处理的动作的流程图。

[0035] 图17为表示密钥分发处理的动作的流程图。

[0036] 图18为签名装置500的框图。

[0037] 图19为表示内容签名生成处理的动作的流程图。

[0038] 图20为终端装置600的框图。

[0039] 图21为终端装置600的框图。

[0040] 图22为表示内容记录处理的动作的流程图。

[0041] 图23为表示内容再现处理的动作的流程图。

[0042] 图24为表示内容再现处理的动作的流程图。

[0043] 图25为记录介质装置700的框图。

[0044] 图26为验证装置1600的框图。

[0045] 图27为表示附签名的内容签名1510的数据构成的框图。

具体实施方式

[0046] 在此，说明本发明的一方式即内容分发系统1。

[0047] <1.概要>

[0048] 图1为表示内容分发系统1的整体构成的图。

[0049] 内容分发系统1由密钥发布装置100、内容制作装置200、内容分发装置300、密钥分发装置400、签名装置500、终端装置600、以及记录介质装置700构成。

[0050] 密钥发布装置100为构成内容分发系统1的安全的基础的合法机构所保有的装置。密钥发布装置100针对构成内容分发系统1的各装置，生成并发布合法的私钥或公钥证书。

[0051] 内容制作装置200生成内容以及该内容的利用条件。内容制作装置200向内容分发装置300发送生成的内容，向密钥分发装置400发送生成的利用条件。

[0052] 内容分发装置300生成标题密钥，通过生成的标题密钥进行内容加密，生成加密内容。再有，内容分发装置300以加密内容为基础，生成内容识别信息。内容分发装置300向密钥分发装置400发送生成的标题密钥与内容识别信息。

[0053] 密钥分发装置400向签名装置500发送接收的内容识别信息，委托内容签名的生成。签名装置500利用签名密钥对内容识别信息实施签名，生成内容签名，向密钥分发装置400发送生成的内容签名。

[0054] 密钥分发装置400利用从签名装置500接收的内容签名与从内容制作装置200接收的利用条件，对从内容分发装置300接收的标题密钥实施规定的运算，生成运算标题密钥。密钥分发装置400将运算标题密钥通过终端装置600向记录介质装置700发送。

[0055] 终端装置600作为一例为设置于用户的自家的PC。终端装置600能够通过互联网等网络与内容分发装置300、密钥分发装置400连接。另外，在终端装置600中，能够安装SD存储卡等记录介质装置700。

[0056] 终端装置600通过网络从内容分发装置300接收加密内容，对安装的记录介质装置700写入接收的加密内容。另外，终端装置600通过网络从密钥分发装置400接收运算标题密钥、利用条件、内容签名等内容的再现所需的信息，写入记录介质装置700。此时，运算标题密钥写入记录介质装置700的被保护的区域。写入“被保护的区域”的数据能够从外部读出，但无法重写其内容。

[0057] 另外，终端装置600具有再现记录于记录介质装置700的内容的功能。此时，终端装置600利用记录于记录介质装置700的内容签名与利用条件，从运算标题密钥复原标题密钥。并且，终端装置600利用复原的标题密钥，解密被加密的内容并再现。

[0058] 在此，在保持于签名装置500的签名密钥泄漏时，存在进行如下非法行为的可能性，该非法行为是针对非法的加密内容，利用泄漏的签名密钥生成内容签名，将非法的加密

内容冒充为宛如正规的内容并记录于记录介质装置700。

[0059] 可是，如上述，在记录介质装置700的被保护的区域中，记录有运算标题密钥，该运算标题密钥是利用已由签名装置500生成的内容签名与利用条件，对标题密钥进行运算而得。

[0060] 因此，即使利用泄漏的签名密钥生成内容签名，将非法的加密内容冒充为宛如正规的内容并记录于记录介质装置700，也由于终端装置600无法从运算标题密钥复原合法的标题密钥，因而能够抑制非法的加密内容的再现。

[0061] 在以下，说明各装置的详细的构成以及各处理的动作。

[0062] <2.密钥发布装置100>

[0063] 在此，说明密钥发布装置100的细节。密钥发布装置100针对构成内容分发系统1的各装置，进行密钥发布处理，该密钥发布处理是发布合法的私钥以及公钥证书或者发布登记私钥泄漏的装置的ID而得的无效化列表的处理。

[0064] <2-1.密钥发布装置100的构成>

[0065] 图2为密钥发布装置100的功能性的构成的框图。如图2所示，密钥发布装置100由根密钥对生成部101、根密钥对存放部102、根公钥发送部103、密钥对生成部104、证书生成部105、私钥·证书存放部106、私钥·证书发送部107、无效化信息输入部108、无效化信息存放部109、签名生成部110以及无效化列表发送部111构成。

[0066] 密钥发布装置100包括未图示的处理器、RAM(Random Access Memory:随机存取存储器)、ROM(Read Only Memory:只读存储器)、以及硬盘。另外，密钥发布装置100的各功能模块作为硬件构成，或者通过处理器执行ROM或硬盘所存储的计算机程序来实现。

[0067] 根密钥对生成部101生成构成内容分发系统1的安全的根本的密钥发布装置100的根密钥对。根密钥对由根公钥以及根私钥构成。

[0068] 根密钥对存放部102存放根密钥对生成部101所生成的根密钥对。

[0069] 根公钥发送部103将存放于根密钥对存放部102的根公钥向密钥分发装置400、终端装置600以及记录介质装置700发送。根公钥在密钥分发装置400、终端装置600以及记录介质装置700验证由密钥发布装置100生成的签名时利用。

[0070] 密钥对生成部104生成密钥分发装置400、签名装置500、终端装置600以及记录介质装置700的密钥对。

[0071] 具体而言，密钥对生成部104生成密钥分发装置密钥对，该密钥分发装置密钥对由嵌入至密钥分发装置400的密钥分发装置公钥以及密钥分发装置私钥构成。另外，密钥对生成部104生成签名装置密钥对，该签名装置密钥对由嵌入至签名装置500的签名装置公钥以及签名装置私钥构成。另外，密钥对生成部104生成终端装置密钥对，该终端装置密钥对由嵌入至终端装置600的终端装置公钥以及终端装置私钥构成。另外，密钥对生成部104生成记录介质装置密钥对，该记录介质装置密钥对由嵌入至记录介质装置700的记录介质装置公钥以及记录介质装置私钥构成。

[0072] 证书生成部105生成嵌入至密钥分发装置400、签名装置500、终端装置600以及记录介质装置700的公钥证书。

[0073] 图3为表示由证书生成部105生成的公钥证书的一例的图。

[0074] 图3(a)为发布至密钥分发装置400的密钥分发装置证书120。密钥分发装置证书

120由密钥分发装置ID、密钥分发装置公钥与签名构成。密钥分发装置证书120将对作为密钥分发装置400的识别符的密钥分发装置ID附加密钥对生成部104所生成的密钥分发装置公钥而得的数据作为签名对象数据。证书生成部105通过将根私钥作为签名生成密钥并对签名对象数据实施签名验证算法从而生成签名。并且，生成由密钥分发装置ID、密钥分发装置公钥以及签名构成的密钥分发装置证书120。

[0075] 图3(b)为发布至签名装置500的签名装置证书130。图3(c)为发布至终端装置600的终端装置证书140。图3(d)为发布至记录介质装置700的记录介质装置证书150。这些公钥证书也与密钥分发装置证书120同样地生成。

[0076] 私钥·证书存放部106将密钥对生成部104所生成的各装置的私钥与证书生成部105所生成的各装置的公钥证书作为配对来存放。

[0077] 私钥·证书发送部107将存放于私钥·证书存放部106的私钥与公钥证书的配对向各装置发送。具体而言，将密钥分发装置证书120向密钥分发装置400发送，将签名装置证书130向签名装置500发送，将终端装置证书140向终端装置600发送，将记录介质装置证书150向记录介质装置700发送。

[0078] 无效化信息输入部108在能够确认经从密钥发布装置100得到私钥以及证书的发布的装置私钥泄漏，被非法利用这一事实时，接受得到被非法利用的私钥的发布的装置的装置ID的输入。另外，无效化信息输入部108接受私钥的非法利用被确认的日期的输入。

[0079] 无效化信息存放部109蓄积并存放将输入的装置ID与日期作为组的无效化信息。

[0080] 签名生成部110汇集存放于无效化信息存放部109的多条无效化信息从而生成列表，将存放于根密钥对存放部102的根私钥作为签名生成密钥，针对所生成的列表实施签名生成算法，从而生成签名。签名生成部110对列表附加签名并生成无效化列表。

[0081] 图4表示无效化列表的一例。如同图所示，无效化列表160由无效化信息区域161、162、···、163与签名区域164构成。各无效化信息区域由ID区域与撤销日期时间区域构成。作为一例，在无效化信息区域161的ID区域165中，记载有被无效化的签名装置的ID“0x201”，在撤销日期时间区域166中，记载有被无效化的日期“2011年8月15日”。在本实施方式中，通过在无效化列表包含撤销日期时间区域，能够限定于确认私钥的非法利用之后使私钥无效。另外，在确认私钥的泄漏以及非法利用时，依次追加无效化信息，更新无效化列表。

[0082] 无效化列表发送部111将签名生成部110所生成的无效化列表向签名装置400以及终端装置600发送。

[0083] <2-2.密钥发布处理的动作>

[0084] 图5为密钥发布装置100的密钥发布处理的动作的流程图。

[0085] 密钥发布装置100生成由根公钥以及根私钥构成的根密钥对(步骤S1)，存放于根密钥对存放部102。并且，根公钥发送部103向密钥分发装置400、终端装置600以及记录介质装置700发送根公钥(步骤S2)。

[0086] 密钥对生成部104生成签名装置500的密钥对(步骤S3)。证书生成部105生成签名装置证书130(步骤S4)。私钥·证书发送部107将签名装置私钥与签名装置证书130向签名装置500发送(步骤S5)。

[0087] 密钥对生成部104生成密钥分发装置400的密钥对(步骤S6)。证书生成部105生成

密钥分发装置证书120(步骤S7)。私钥·证书发送部107将密钥分发装置私钥与密钥分发装置证书120向密钥分发装置400发送(步骤S8)。

[0088] 密钥对生成部104生成终端装置600的密钥对(步骤S9)。证书生成部105生成终端装置证书140(步骤S10)。私钥·证书发送部107将终端装置私钥与终端装置证书140向制造终端装置600的装置发送(步骤S11)。

[0089] 密钥对生成部104生成记录介质装置700的密钥对(步骤S12)。证书生成部105生成记录介质装置证书150(步骤S13)。私钥·证书发送部107将记录介质装置私钥与记录介质装置证书150向制造记录介质装置700的装置发送(步骤S14)。

[0090] 无效化信息输入部108接受无效化信息(装置ID以及撤销日期时间)的输入(步骤S15)。

[0091] 签名生成部110针对由多条无效化信息构成的列表,利用根私钥生成签名(步骤S16),对列表附加签名从而生成无效化列表。

[0092] 无效化列表发送部111将所生成的无效化列表向签名装置400以及终端装置600发送。

[0093] <3.内容制作装置200>

[0094] 在此,说明内容制作装置200的细节。内容制作装置200进行生成并加密内容的内容制作处理。

[0095] <3-1.内容制作装置200的构成>

[0096] 图6为表示内容制作装置200的功能性的构成的框图。如图6所示,内容制作装置200由素材存放部201、编辑部202、内容存放部203、内容登记部204、UR输入部205、UR存放部206以及UR登记部207构成。

[0097] 内容制作装置200包括未图示的处理器、RAM、ROM、以及硬盘。另外,内容制作装置200的各功能模块作为硬件构成,或者通过处理器执行ROM或硬盘所存储的计算机程序来实现。

[0098] 素材存放部201存放大量的素材数据(电影等视频数据以及音频数据)。

[0099] 编辑部202组合存放于素材存放部201的大量的素材数据来制作电影等内容。

[0100] 内容存放部203存放由编辑部202制作的内容。

[0101] 内容登记部204将存放于内容存放部203的内容登记至内容分发装置300。

[0102] UR输入部205包括键盘或鼠标等输入设备。UR输入部205通过由内容制作方操作输入设备,接受内容的可再现次数或可否移动等内容的利用所涉及的条件即Usage Rule(使用规则,以下,记载为"UR"。)的输入。

[0103] UR存放部206存放UR输入部205所接受的UR。

[0104] 图7表示UR的数据构造。如同图所示,UR210由输出控制信息区域211与其他信息区域212构成。在输出控制信息区域211中,例如记载有可再现期间、再现开始日期时间、再现结束日期时间、可再现次数、目录输出可否信息、移动可否信息、可移动次数等有关再现或移动的控制信息。

[0105] 在其他信息区域212中,例如记载有记录有内容服务器的URL、内容制作方的名称以及住所、内容版权方的名称以及住所等有关再现或移动的控制信息以外的信息。

[0106] UR登记部207将存放于UR登记部206的UR登记至密钥分发装置400。

[0107] <3-2.内容制作处理的动作>

[0108] 图8为表示内容制作装置200的内容制作处理的动作的流程图。

[0109] 编辑部202组合存放于素材存放部201的素材数据来生成电影等内容(步骤S21)。所生成的内容存放于内容存放部203。

[0110] 内容登记部204向内容分发装置300发送(步骤S22)。

[0111] 接着,UR输入部205从内容制作方接受UR的输入(步骤S23)。所输入的UR存放于UR存放部206。

[0112] UR登记部207将UR向内容分发装置400发送(步骤S24)。

[0113] <4.内容分发装置300>

[0114] 在此,说明内容分发装置300的细节。内容分发装置300从内容制作装置200接收内容,通过标题密钥对接收的内容进行加密。另外,内容分发装置300进行内容分发处理,该内容分发处理是通过网络向所连接的终端装置600分发内容的处理。

[0115] <4-1.内容分发装置300的构成>

[0116] 图9为表示内容分发装置300的功能性的构成的框图。如图9所示,内容分发装置300由内容接收部301、标题密钥生成部302、加密部303、内容存放部304、内容识别信息生成部305、标题密钥·内容识别信息发送部306、分发委托接收部307以及内容分发部308构成。

[0117] 内容分发装置300包括未图示的处理器、RAM、ROM、以及硬盘。另外,内容分发装置300的各功能模块作为硬件构成,或者通过处理器执行ROM或硬盘所存储的计算机程序来实现。

[0118] 内容接收部301从内容制作装置200接收内容。

[0119] 标题密钥生成部302生成作为用于加密内容的加密密钥的标题密钥。作为一例,标题密钥为128位的随机数。

[0120] 加密部303将标题密钥用作加密密钥,对内容实施加密算法E来进行加密,生成加密内容。在以下,尤其只要没有注释,将通过标题密钥加密的状态的内容简单地记载为“内容”。另外,加密算法D的一例为AES(Advanced Encryption Standard:高级加密标准)。

[0121] 内容存放部304存放由加密部303加密而得的内容。

[0122] 内容识别信息生成部305生成内容识别信息,该内容识别信息是从存放于内容存放部304的内容中,唯一地识别该内容的信息。

[0123] 图10为用于说明内容识别信息的生成方法的图。如图10所示,内容识别信息生成部305将内容310分割为N个部分内容。并且,运算各部分内容的哈希值。内容识别信息生成部305将记载这N个哈希值的哈希表作为内容识别信息311。

[0124] 标题密钥·内容识别信息发送部306将由标题密钥生成部302生成的标题密钥、由内容识别信息生成部305生成的内容识别信息向密钥分发装置400发送。

[0125] 分发委托接收部307在从终端装置600接收分发委托数据时,对内容分发部308指示内容的分发。

[0126] 内容分发部308在被分发委托接收部307指示内容的分发时,从内容存放部304检索分发委托数据所指定的内容。在发现所对应的内容时,从内容存放部3024读出内容,并向终端装置600分发。另外,分发委托数据包含用于指定内容的信息,内容分发部308能够以分发委托数据为基础,检索所分发的内容。

[0127] <4-2.内容分发处理的动作>

[0128] 图11为表示内容分发装置300的内容分发处理的动作的流程图。

[0129] 内容接收部301从内容制作装置200接收内容(步骤S31),将接收的内容向加密部303输出。

[0130] 标题密钥生成部302生成标题密钥(步骤S32),将所生成的标题密钥向加密部303以及标题密钥·内容识别信息发送部306输出。

[0131] 加密部303通过标题密钥加密内容,生成加密内容(步骤S33)。加密部303将加密的内容存放于内容存放部304(步骤S34)。

[0132] 内容识别信息生成部305根据由加密部303加密的内容生成内容识别信息(步骤S35),将所生成的内容识别信息向标题密钥·内容识别信息发送部306输出。

[0133] 标题密钥·内容识别信息发送部306将标题密钥与内容识别信息向密钥分发装置400发送(步骤S36)。

[0134] 分发委托接收部307从终端装置600接收分发委托数据(步骤S37)。分发委托接收部307对内容分发部308指示内容的分发。

[0135] 内容分发部308以分发委托数据为基础,从内容存放部304检索内容(步骤S38)。在发现所对应的内容时,内容分发部308将内容分发至委托方的终端装置600(步骤S39)。在未能发现所对应的内容时,内容分发部308对委托方的终端装置600通知未能发现之意亦可。

[0136] <5.密钥分发装置400>

[0137] 在此,说明密钥分发装置400的细节。密钥分发装置400进行密钥分发处理,该密钥分发处理是将内容的再现所需的标题密钥、UR、内容签名等通过终端装置600向记录介质装置700发送的处理。

[0138] <5-1.密钥分发装置400的构成>

[0139] 图12为表示密钥分发装置400的功能性的构成的框图。如图12所示,密钥分发装置400由根公钥接收部401、根公钥存放部402、私钥·证书接收部403、私钥·证书存放部404、标题密钥·内容识别信息接收部405、内容识别信息发送部406、UR接收部407、内容签名接收部408、无效化列表接收部409、UR处理部410、标题密钥运算部411、相互认证部412、加密解密部413、记录介质装置ID接收部414以及MAC运算部415构成。

[0140] 密钥分发装置400包括未图示的处理器、RAM、ROM、以及硬盘。另外,密钥分发装置400的各功能模块作为硬件构成,或者通过处理器执行ROM或硬盘所存储的计算机程序来实现。

[0141] 根公钥接收部401从密钥发布装置100接收根公钥。

[0142] 根公钥存放部402存放根公钥接收部401所接收的根公钥。

[0143] 私钥·证书接收部403从密钥发布装置100接收密钥分发装置私钥以及密钥分发装置证书。

[0144] 私钥·证书存放部404存放私钥·证书接收部403所接收的密钥分发装置私钥以及密钥分发装置证书。

[0145] 标题密钥·内容识别信息接收部405从内容分发装置300接收标题密钥与内容识别信息。

[0146] 内容识别信息发送部406将从内容分发装置300接收的内容识别信息向签名装置

500发送。这是为了从签名装置500得到对内容识别信息的签名赋予。

[0147] UR接收部407从内容制作装置200接收UR。

[0148] 内容签名接收部408从签名装置500接收内容签名。内容签名为赋予了针对内容识别信息的签名装置500的签名的数据。

[0149] 内容签名接收部408在从签名装置500接收内容签名时，利用保持于无效化列表接收部409的无效化列表，判断所接收的内容签名是有效还是无效。在判断所接收的内容签名无效时，密钥分发装置400结束处理。在判断所接收的内容签名有效时，内容签名接收部408将所接收的内容签名向UR处理部410输出。再有，内容签名接收部408将所接收的内容签名向终端装置600发送。

[0150] 图13表示内容签名的一例。如同图所示，内容签名510由内容识别信息区域511、签名数据区域512、签名日期时间区域513以及签名装置证书区域514构成。

[0151] 在内容识别信息区域511中，记录有内容识别信息发送部406向签名装置500发送的内容识别信息311。在签名数据区域512中，记载有针对内容识别信息区域511所记载的内容识别信息311，签名装置500利用签名装置私钥生成的签名数据。在签名日期时间区域513中，记载有签名装置500所签名的日期时间。在签名装置证书区域514中，记载有签名装置证书130(图3)。

[0152] 无效化列表接收部409从密钥发布装置100接收无效化列表，并保持于内部。

[0153] UR处理部410利用内容签名接收部408所接收的内容签名，对UR接收部407所接收的UR追加数据，生成处理完毕UR。UR处理部410将所生成的处理完毕UR输出至标题密钥运算部411。再有，UR处理部410将所生成的处理完毕UR向终端装置600发送。

[0154] 利用图14，说明处理完毕UR的具体例。

[0155] 图14(a)所示的处理完毕UR420由UR210与内容签名确定信息区域421构成。UR210如在图7说明了的，由输出控制信息区域211以及其他的信息区域212构成。内容签名确定信息区域421是为了存放内容签名、内容签名整体的哈希值、内容识别信息的哈希值、内容识别信息的一部分等能够唯一地确定内容的信息的区域。

[0156] 图14(b)所示的处理完毕UR430由UR210、签名数据区域431、签名日期时间区域432以及内容签名哈希值区域433构成。UR210如在图7说明了的，由输出控制信息区域211以及其他的信息区域212构成。签名数据区域431、签名日期时间区域432以及内容签名哈希值区域433为对处理完毕UR420的内容签名确定信息区域421进行具体化而得的区域。在签名数据区域431中，记载有内容签名510的签名数据区域512所记载的签名数据。在签名日期时间区域432中，记载有内容签名510的签名日期时间区域513所记载的日期时间。在内容签名哈希值区域433中，记载有针对内容签名510的整体的哈希值。另外，UR处理部410算出针对内容签名510的整体的哈希值。在以下，UR处理部410作为生成图14(b)所示的处理完毕UR430的处理部来说明。

[0157] 标题密钥运算部411从标题密钥·内容识别信息接收部405取得标题密钥，从UR处理部410取得处理完毕UR。并且，标题密钥运算部411计算处理完毕UR的哈希值。标题密钥运算部411进行利用处理完毕UR的哈希值与标题密钥的能够可逆运算的运算，从而生成作为本发明所涉及的变换标题密钥的运算标题密钥。在此作为一例，标题密钥运算部411通过计算处理完毕UR的哈希值与标题密钥的异或(XOR)，生成运算标题密钥(XORed(异或后的)标

题密钥)。由标题密钥运算部411生成的运算标题密钥向加密解密部413传递,在加密解密部413中,通过与记录介质装置700共有的共通密钥加密之后发送。

[0158] 相互认证部412利用在与终端装置600之间以素因子分解的复杂性为基础的密钥交换方式的Difiee-Hellman方式、或以椭圆曲线上的离散对数问题为基础的密钥交换方式的EC-DH(Eliptic Curve Difiee-Hellman)方式等进行相互认证,彼此共有共通密钥。另外,同样地,相互认证部412与记录介质装置700进行相互认证,在与记录介质装置700之间彼此共有共通密钥。

[0159] 加密解密部413利用与终端装置600共有的共通密钥,对在与终端装置600之间收发的数据进行加密或者解密。另外,加密解密部413利用与记录介质装置700共有的共通密钥,加密由标题密钥运算部411生成的运算标题密钥,发送至记录介质装置700。

[0160] 记录介质装置ID接收部414从终端装置600经由加密解密部413接收记录介质装置ID,该记录介质装置ID用于识别作为内容的写入目的地的记录介质装置。另外,所谓"经由加密解密部413"是指加密解密部413接收通过共通密钥加密而得的记录介质装置ID,在向记录介质装置ID接收部414输出之前,将所加密的记录介质装置ID利用共通密钥来解密。

[0161] MAC运算部415根据标题密钥·内容识别信息接收部405所接收的标题密钥与记录介质装置ID接收部414所接收的记录介质装置ID运算MAC(Message Authentication Code:报文认证码)。作为一例,MAC运算部415通过将标题密钥用作认证报文,将记录介质装置ID用作密钥,实施MAC生成算法,由此生成用于验证标题密钥的完整性的MAC。MAC运算部415将所生成的MAC向终端装置600发送。

[0162] 在本实施方式中,MAC用作用于将记录介质装置700所记录的内容以及标题密钥与记录介质装置700建立对应(介质绑定)的信息。即,对记录介质装置700写入根据标题密钥与记录介质装置ID生成的MAC,从而通过在内容的再现时验证MAC,能够判定要再现的内容是否为正规地记录于记录介质装置700的内容。在对与记录介质装置ID不同的其他的记录介质装置非法拷贝内容时,终端装置600为在内容的再现时MAC的验证失败,无法再现非法拷贝的内容的构造。

[0163] <5-2.相互认证处理的动作>

[0164] 在此,利用图15以及图16的流程图,说明相互认证部412所执行的相互认证处理的一例。在此,作为一例,说明在密钥分发装置400以及记录介质装置700之间执行的相互认证处理。

[0165] 密钥分发装置400的相互认证部412生成160位的随机值Hn(Host nonce:主随机数)(步骤S41)。另外,在此,为了利用密钥长度为160位的EC-DSA(Eliptic Curve-Digital Signature Algorithm:Eliptic曲线数字签名算法),而生成160位的随机值,但在利用其他算法时,不言自明的是,在此所生成的随机值并非160位。

[0166] 相互认证部412对在步骤S41生成的160位的随机值Hn连结存放于私钥·证书存放部404的密钥分发装置证书。将之作为挑战数据(challenge data)向记录介质装置700发送(步骤S42)。另外,在图13中,将密钥分发装置证书记载为"Hcert(Host Certificate:主证书)"。此外,"||"为表示数据的连结的记号。

[0167] 记录介质装置700在从密钥分发装置400接收挑战数据时,利用根公钥进行在步骤S42所接收的挑战数据所包含的密钥分发装置证书Hcert的验证处理(步骤S43)。在密钥分

发装置证书Hcert的验证处理失败时(在步骤S44为否),记录介质装置700停止处理。在密钥分发装置证书Hcert的验证处理成功时(在步骤S44为是),记录介质装置700生成160位的随机值Mn(Media nonce:介质随机数)(步骤S45)。

[0168] 记录介质装置700对由步骤S45生成的160位的随机值Mn连结记录介质装置证书。将之作为挑战数据(challenge data)向密钥分发装置置400发送(步骤S46)。另外,在图13中,将记录介质装置证书记载为"Mcert(Media Certificate):介质证书)"。

[0169] 密钥分发装置400在从记录介质装置700接收挑战数据时,利用根公钥进行在步骤S46所接收的挑战数据所包含的记录介质装置证书Mcert的验证处理(步骤S47)。在记录介质装置证书Mcert的验证处理失败时(在步骤S48为否),密钥分发装置400停止处理。在记录介质装置证书Mcert的验证处理成功时(在步骤S48为是),密钥分发装置400的相互认证部412向步骤S53行进。

[0170] 记录介质装置700在步骤S46发送挑战数据之后,生成160位的随机值Mk(Media Key:介质密钥)(步骤S49)。另外,在利用EC-DH之外的其他算法时,在步骤S49生成的随机值不限于160位。

[0171] 记录介质装置700针对在步骤S49生成的随机值Mk,利用作为在本系统中事先确定的椭圆加密的参数的基点G,计算Mv=Mk·G(步骤S50)。

[0172] 再有,记录介质装置700针对Hn||Mv利用记录介质装置私钥(Mpriv)来生成数字签名(Sign(Mpriv,Hn||Mv))(步骤51),该Hn||Mv为连结在步骤S42所接收的挑战数据所包含的的Hn与在步骤S50算出的Mv而得的数据。

[0173] 记录介质装置700将连结在步骤S50算出的Mv与在步骤S51生成的数字签名Sign(Mpriv,Hn||Mv)而得的数据作为响应数据,向密钥分发装置400发送(步骤S52)。

[0174] 密钥分发装置400的相互认证部412从记录介质装置700接收响应数据。相互认证部412进行所接收的响应数据所包含的数字签名Sign(Mpriv,Hn||Mv)的验证(步骤S53)。具体而言,相互认证部412从响应数据提取Mv,对连结在步骤S41生成的Hn与Mv而得的数据,利用记录介质装置证书Mcert所包含的记录介质装置公钥,验证数字签名。

[0175] 在数字签名的验证失败时(在步骤S54为否),密钥分发装置400停止处理。在数字签名的验证成功时(在步骤S54为是),相互认证部412生成160位的随机值Hk(Host Key:主密钥)(步骤S55)。

[0176] 相互认证部412针对在步骤S55生成的随机值Hk,利用作为在本系统中事先确定的椭圆加密的参数的基点G,计算Hv=Hk·G(步骤S56)。

[0177] 再有,相互认证部412针对Mn||Hv利用密钥分发装置私钥(Hpriv)来生成数字签名(Sign(Hpriv,Mn||Hv))(步骤57),该Mn||Hv为连结在步骤S46所接收的挑战数据所包含的的Mn与在步骤S56算出的Hv而得的数据。

[0178] 相互认证部412将连结在步骤S56算出的Hv与在步骤S57生成的数字签名Sign(Hpriv,Mn||Hv)而得的数据作为响应数据,向记录介质装置700发送(步骤S58)。

[0179] 记录介质装置700从密钥分发装置400接收响应数据。记录介质装置700进行所接收的响应数据所包含的数字签名Sign(Hpriv,Mn||Hv)的验证(步骤S59)。具体而言,记录介质装置700从响应数据提取Hv,对连结在步骤S45生成的Mn与Hv而得的数据,利用密钥分发装置400的公钥证书Hcert所包含的密钥分发装置公钥,验证数字签名。

[0180] 在数字签名的验证失败时(在步骤S60为否),记录介质装置700停止处理。在数字签名的验证成功时(在步骤S60为是),记录介质装置700根据在步骤S49生成的随机值Mk与在步骤S58所接收的响应数据所包含的Hv计算BK＝Mk・Hv,生成共通密钥BK(Bus Key:总线密钥)(步骤S61)。

[0181] 另一方面,密钥分发装置400的相互认证部412根据在步骤S55生成的随机值Hk与在步骤S52所接收的响应数据所包含的Mv计算BK＝Hk・Mv,生成共通密钥BK(步骤S62)。

[0182] 通过进行以上的处理,密钥分发装置400与记录介质装置700能够确认相互的合法性,共有终端装置600无法知晓的共通密钥BK。并且,密钥分发装置400与记录介质装置700确立利用共通密钥BK的安全的通道(会话),不会被终端装置600知晓地安全收发通信数据。

[0183] 在此,说明了在密钥分发装置400以及记录介质装置700之间执行的相互认证处理,但在密钥分发装置400以及终端装置600之间执行的相互认证处理、以及在终端装置600以及记录介质装置700之间执行的相互认证处理的过程也与之同样。另外,在此所示的相互认证处理的过程为一例,利用其他方式亦可。

[0184] <5-3.密钥分发处理的动作>

[0185] 图17为密钥分发装置400的密钥分发处理的动作的流程图。

[0186] 密钥分发装置400在密钥分发处理之前,从密钥发布装置100接收根公钥、密钥分发装置私钥、密钥分发装置证书120以及无效化列表160,并存放。另外,密钥分发装置400从内容制作装置200接收UR210,并存放。

[0187] 以下的处理在密钥分发装置400从终端装置600或者记录介质装置700接受标题密钥的发送要求时执行。

[0188] 标题密钥・内容识别信息接收部405从内容分发装置300接收标题密钥与内容识别信息311(步骤S71)。

[0189] 内容识别信息发送部406将在步骤71接收的内容识别信息311向签名装置500发送(步骤S72)。

[0190] 内容签名接收部408从签名装置500接收内容签名510(步骤S73)。在此接收的内容签名510为对在步骤S72向签名装置500发送的内容识别信息311赋予签名装置500的签名数据而得到的数据。

[0191] 内容签名接收部408进行在步骤S73接收的内容签名510的验证(步骤S74)。具体而言,内容签名接收部408从所接收的内容签名510所包含的签名装置证书130提取签名装置ID。并且,内容签名接收部408对照已保持于无效化列表接收部409的无效化列表160,判断签名装置ID是否记载于无效化列表。

[0192] 在签名装置ID记载于无效化列表160时,即,在签名装置500为撤销对象时,内容签名接收部408判断所接收的内容签名为无效(在步骤S74为失败),密钥分发装置400结束处理。

[0193] 在签名装置ID未记载于无效化列表160时,即,在签名装置500并非撤销对象时,内容签名接收部408判断所接收的内容签名510为有效(在步骤S74为成功),向UR处理部410输出,进而向终端装置600发送。

[0194] UR处理部410利用UR接收部407已接收并保持的UR210与从内容签名接收部408接受的内容签名510,生成处理完毕UR430(步骤S75)。

[0195] 具体而言，UR处理部410计算内容签名510的整体的哈希值。并且，UR处理部410将内容签名510的签名数据区域512所记载的数据、签名日期时间区域513所记载的数据、以及计算而得的哈希值追加至UR210，生成处理完毕UR430。

[0196] UR处理部410将所生成的处理完毕UR430向标题密钥运算部411输出。

[0197] 标题密钥运算部411若接收处理完毕UR430，则计算接受的处理完毕UR430的哈希值(步骤S76)。再有，标题密钥运算部411从标题密钥·内容识别信息接收部405接受标题密钥。标题密钥运算部411通过计算处理完毕UR430的哈希值与标题密钥的异或(XOR)，生成运算标题密钥(步骤S77)。

[0198] 相互认证部412与终端装置600以及记录介质装置700的各装置进行相互认证(步骤S78)。在步骤S78的相互认证处理中，相互认证部412确认终端装置600的合法性，在与终端装置600之间共有共通密钥BK1。同样地，相互认证部412确认记录介质装置700的合法性，在与记录介质装置700之间共有共通密钥BK2。

[0199] 加密解密部413将在步骤S77生成的运算标题密钥通过共通密钥BK2加密，向记录介质装置700发送(步骤S79)。

[0200] 接着，加密解密部413从终端装置600接收通过共通密钥BK1加密的记录介质装置ID(步骤S73)，通过共通密钥BK1解密(步骤S80)。加密解密部413将所解密的记录介质装置ID向记录介质装置ID接收部414输出。并且，记录介质装置ID接收部414将所接受的记录介质装置ID向MAC运算部415输出。

[0201] MAC运算部415从标题密钥·内容识别信息接收部405接受标题密钥。另外，MAC运算部415从记录介质装置ID接收部414接受记录介质装置ID。MAC运算部415根据标题密钥与记录介质装置ID运算MAC(步骤S81)。MAC运算部415将MAC向终端装置600发送(步骤S82)。

[0202] 接着，UR处理部410将处理完毕UR430向终端装置600发送(步骤S83)。最后，内容签名接收部408将内容签名向终端装置600发送(步骤S84)。

[0203] <6.签名装置500>

[0204] 在此，说明签名装置500的细节。签名装置500进行内容签名生成处理，该内容签名生成处理是从密钥分发装置400接收内容识别信息，针对内容识别信息通过合法的签名密钥实施签名从而生成内容签名，将所生成的内容签名送回密钥分发装置400的处理。

[0205] <6-1.签名装置500的构成>

[0206] 图18为表示签名装置500的功能性的构成的框图。如同图18所示，签名装置500由私钥·证书接收部501、私钥·证书存放部502、内容识别信息接收部503、签名部504以及内容签名发送部505构成。

[0207] 签名装置500包括未图示的处理器、RAM、ROM、以及硬盘。另外，另外，500的各功能模块作为硬件构成，或者通过处理器执行ROM或硬盘所存储的计算机程序来实现。

[0208] 私钥·证书接收部501从密钥发布装置100接收签名装置私钥以及签名装置证书。

[0209] 私钥·证书存放部502存放签名装置私钥以及签名装置证书。

[0210] 内容识别信息接收部503从密钥分发装置400接收内容识别信息。

[0211] 签名部504将计量日期时间的时钟保持于内部。签名部504从内容识别信息接收部503接受内容识别信息，对接受的内容识别信息附加签名数据等从而生成内容签名。签名部504将所生成的内容签名向内容签名发送部505输出。

[0212] 内容签名发送部505从签名部504接受内容签名，将所接受的内容签名向作为内容识别信息的发送方的密钥分发装置400发送。

[0213] <6-2.内容签名生成处理的动作>

[0214] 图19为签名装置500的内容签名生成处理的动作的流程图。

[0215] 签名装置500在内容签名生成处理之前，从密钥发布装置100接收签名装置私钥以及签名装置证书130，并存放。

[0216] 内容识别信息接收部503从密钥分发装置400接收内容识别信息311(步骤S91)。

[0217] 签名部504通过针对内容识别信息311将签名装置私钥用作签名密钥，实施签名生成算法S，据此生成签名数据(步骤92)。签名生成算法S的一例为DSA(Digital Signature Algorithm:数字签名算法)。

[0218] 签名部504将在步骤S91接收的内容识别信息311记载于内容识别信息区域511，将在步骤S92生成的签名数据记载于签名数据区域512。

[0219] 接着，签名装置500从保持于内部的时钟取得当前的日期时间，将当前的日期时间记载于签名日期时间区域513(步骤S93)。

[0220] 最后，签名装置500对签名装置证书区域514记载签名装置证书130，生成内容签名510(步骤S94)。

[0221] 内容签名发送部505将在步骤94生成的内容签名510向密钥分发装置400发送(步骤S95)。

[0222] <7.终端装置600>

[0223] 在此，说明终端装置600的细节。

[0224] 终端装置600为包括处理器、ROM、RAM、硬盘、作为输入设备的键盘以及鼠标、作为显示设备的显示器、用于供记录介质装置700插入的卡插槽、以及网络连接单元等的PC。在ROM、RAM或者硬盘中记录有计算机程序，终端装置600的一部分的功能能够通过处理器执行计算机程序来实现。

[0225] 终端装置600通过互联网或数字广播等网络，从内容分发装置300接收内容，另外，从密钥分发装置400接收内容签名、UR、MAC以及运算标题密钥。终端装置600进行内容记录处理，该内容记录处理是将所接收的内容等记录于记录介质装置700的处理。

[0226] 另外，终端装置600进行内容再现处理，该内容再现处理是从记录有内容、内容签名、UR、MAC、以及运算标题密钥的记录介质装置700读出内容并再现的处理。

[0227] <7-1.终端装置600的构成>

[0228] 图20以及图21为表示终端装置600的功能性的构成的框图。

[0229] 在此，图20表示终端装置600进行内容记录处理时的功能的构成。图21表示终端装置600进行内容再现处理时的功能性的构成。

[0230] 如图20以及图21所示，终端装置600由根公钥存放部601、私钥·证书存放部602、内容接收部603、内容写入部604、相互认证部605、记录介质装置ID取得部606、记录介质装置ID发送部607、加密解密部608、MAC·UR·内容签名接收部609、MAC·UR·内容签名写入部610、运算标题密钥传输部611、运算标题密钥接收部620、UR读出部621、内容签名读出部622、标题密钥再运算部623、MAC读出部624、第1再现判断部625、无效化列表接收·存放部626、内容签名验证部627、内容读出部628、第2再现判断部629、第3再现判断部630、内容解

密部631、以及内容再现部632构成。

[0231] 根公钥存放部601存放由密钥发布装置100生成的根公钥。

[0232] 私钥·证书存放部602存放由密钥发布装置100生成的终端装置私钥以及终端装置证书140。

[0233] 另外，根公钥、终端装置私钥以及终端装置证书140在终端装置600的制造时，由制造终端装置600的装置嵌入至终端装置600。

[0234] 内容接收部603从内容分发装置300接收内容。

[0235] 内容写入部604将内容接收部603所接收的内容写入至记录介质装置700的普通区域。

[0236] 相互认证部605与密钥分发装置400进行相互认证，确认密钥分发装置400的合法性，在与密钥分发装置400之间彼此共有共通密钥BK1。另外，相互认证部605与记录介质装置700进行相互认证，确认记录介质装置700的合法性，在与记录介质装置700之间彼此共有共通密钥BK3。有关相互认证处理，已利用图15以及图16说明了，因此在此省略说明。

[0237] 记录介质装置ID取得部606在内容记录处理中，从在相互认证部605的相互认证处理的途中接收的记录介质装置证书150取得记录介质装置ID，将所取得的记录介质装置ID向记录介质装置ID发送部607输出。

[0238] 记录介质装置ID取得部606在内容再现处理中，从在相互认证部605的相互认证处理的途中接收的记录介质装置证书150取得记录介质装置ID，将所取得的记录介质装置ID向第1再现判断部625输出。

[0239] 记录介质装置ID发送部607从记录介质装置ID取得部606接受记录介质装置ID，将所接受的记录介质装置ID经由加密解密部608向密钥分发装置400发送。

[0240] 加密解密部608利用与密钥分发装置400共有的共通密钥BK1，对在与密钥分发装置400之间收发的数据进行加密或者解密。同样地，加密解密部608利用与记录介质装置700共有的共通密钥BK3，对在与记录介质装置700之间收发的数据进行加密或者解密。

[0241] MAC·UR·内容签名接收部609从密钥分发装置400接收处理完毕UR430以及内容签名510。在此接收的MAC为根据标题密钥与记录介质装置ID运算而得的MAC，该标题密钥是内容写入部604写入记录介质装置700的内容的加密所利用的密钥，该记录介质装置ID是记录介质装置ID发送部607向密钥分发装置400发送的ID。MAC·UR·内容签名接收部609将所接收的MAC、处理完毕UR430以及内容签名510向MAC·UR·内容签名写入部610输出。

[0242] MAC·UR·内容签名写入部610从MAC·UR·内容签名接收部609接受处理完毕UR430以及内容签名510，将所接受的MAC、处理完毕UR430以及内容签名510写入至记录介质装置700的普通区域。

[0243] 运算标题密钥传输部611传输在与密钥分发装置400和记录介质装置700之间接收的通信数据。在此传输的通信数据具体而言是利用密钥分发装置400与记录介质装置700在相互认证中共有的共通密钥BK2加密而得的加密运算标题密钥。

[0244] 若密钥分发装置400与记录介质装置700经相互认证确立会话，则运算标题密钥传输部611针对在会话上发送而来的通信数据，除了通知通信的开始或通信的结束等的控制数据之外，不会判断其内容或者变更数据，单纯地只进行传输。另外，由于终端装置600并不知晓密钥分发装置400与记录介质装置700所共有的共通密钥BK2的值，因此无法对加密运

算标题密钥进行解密。

[0245] 运算标题密钥接收部620在内容的再现处理时，从记录介质装置700经由加密解密部608接收根据作为再现对象的内容的加密所利用的标题密钥生成的运算标题密钥。运算标题密钥接收部620将所接收的运算标题密钥向标题密钥再运算部623输出。

[0246] UR读出部621从记录介质装置700读出作为再现对象的内容所对应的处理完毕UR430。UR读出部621将所读出的处理完毕UR430向标题密钥再运算部623、内容签名验证部627以及第3再现判断部630输出。

[0247] 内容签名读出部622从记录介质装置700读出作为再现对象的内容所对应的内容签名510。内容签名读出部622将所读出的内容签名510向标题密钥再运算部623、内容签名验证部627、第2再现判断部629以及第3再现判断部630输出。

[0248] 标题密钥再运算部623从UR读出部621接受处理完毕UR430，从运算标题密钥接收部620接受运算标题密钥，从内容签名读出部622接受内容签名510。标题密钥再运算部623执行利用这些信息的运算，生成标题密钥。标题密钥再运算部623将生成的标题密钥向第1再现判断部625以及内容解密部631输出。

[0249] 另外，标题密钥再运算部623所执行的运算相当于密钥分发装置400的标题密钥运算部411所执行的运算的逆运算。因此，只要处理完毕UR以及内容签名510合法，标题密钥再运算部623能够复原标题密钥运算部411所生成的标题密钥。

[0250] MAC读出部624从记录介质装置700读出作为再现对象的内容所对应的MAC。MAC读出部624将所读出的MAC向第1再现判断部625输出。

[0251] 第1再现判断部625从标题密钥再运算部623接受标题密钥，从记录介质装置ID取得部606接受记录介质装置ID，从MAC读出部624接受MAC。第1再现判断部625根据接受的标题密钥与记录介质识别ID运算MAC。并且，第1再现判断部625判断运算而得的MAC与MAC读出部624从记录介质装置700读出的MAC是否一致。在两MAC未一致时，第1再现判断部625向内容解密部631输出解密中止的指示。

[0252] 无效化列表接收·存放部626从密钥发布装置100接收无效化列表160，并保持于内部。

[0253] 内容签名验证部627对照无效化列表160，确认生成从内容签名读出部622接受的内容签名的签名装置500是否为撤销对象。在签名装置500为撤销对象时，内容签名验证部627向内容解密部631输出解密中止的指示。

[0254] 另外，内容签名验证部627确认从UR读出部621接受的处理完毕UR430的签名数据区域431所记载的签名数据与内容签名510的签名数据区域512所记载的签名数据是否一致。在未一致时，内容签名验证部627向内容解密部631输出解密中止的指示。

[0255] 内容读出部628从记录介质装置700读出作为再现对象的内容。内容读出部628将所读出的内容向第2再现判断部629以及内容解密部631输出。

[0256] 第2再现判断部629从内容签名读出部622接受内容签名510，从内容读出部628接受内容。第2再现判断部629利用内容签名510确认内容的合法性。在判断内容非法时，第2再现判断部629向内容解密部631输出解密中止的指示。

[0257] 第3再现判断部630从UR读出部621接受处理完毕UR430，从内容签名读出部622接受内容签名510。第3再现判断部630计算内容签名510整体的哈希值，确认计算而得的哈希

值与处理完毕UR430的内容签名哈希值区域433所记载的哈希值是否一致。在哈希值未一致时，第3再现判断部630向内容解密部631输出解密中止的指示。

[0258] 内容解密部631从标题密钥再运算部623接受由标题密钥再运算部623复原的标题密钥，从内容读出部628接受内容。内容解密部631将标题密钥用作解密密钥，对内容实施解密算法D，从而解密内容。解密算法D为将由加密算法E加密而得的加密文解密为明文的算法。内容解密部631将所解密的内容向内容再现部632输出。

[0259] 另外，内容解密部631在从第1再现判断部625、内容签名验证部627、第2再现判断部629或者第3再现判断部630接受表示解密中止的信号时，中止内容的解密。

[0260] 内容再现部632接受并解码由内容解密部631解密而得的内容。并且，内容再现部632向未图示的显示设备输出解码而得的内容。

[0261] <7-2.内容记录处理的动作>

[0262] 图22为表示终端装置600的内容记录处理的动作的流程图。

[0263] 另外，在终端装置600中，事先存放有根公钥、终端装置私钥以及终端装置证书140。

[0264] 相互认证部605与记录介质装置700进行相互认证，确认记录介质装置700的合法性。记录介质装置ID取得部606从在相互认证处理的途中接收的记录介质装置证书150取得记录介质装置ID(步骤S101)。

[0265] 内容接收部603从内容分发装置300接收内容(步骤S102)。内容写入部604将在步骤S102接收的内容写入至记录介质装置700(步骤S103)。

[0266] 接着，相互认证部605与密钥分发装置400进行相互认证，确认密钥分发装置400的合法性，在与密钥分发装置400之间共有共通密钥BK1(步骤S104)。加密解密部608将在步骤S101取得的记录介质装置ID通过共通密钥BK1加密，向密钥分发装置400发送(步骤S105)。

[0267] 接着，MAC·UR·内容签名接收部609从密钥分发装置400接收MAC(步骤S106)，MAC·UR·内容签名写入部610将所接收的MAC写入至记录介质装置700(步骤S107)。

[0268] 另外，MAC·UR·内容签名接收部609从密钥分发装置400接收处理完毕UR430(步骤S108)，MAC·UR·内容签名写入部610将所接收的处理完毕UR430写入至记录介质装置700(步骤S109)。

[0269] 另外，MAC·UR·内容签名接收部609从密钥分发装置400接收内容签名510(步骤S110)，MAC·UR·内容签名写入部610将所接收的内容签名510写入至记录介质装置700(步骤S111)。

[0270] 接着，运算标题密钥传输部611将从密钥分发装置400接收的运算标题密钥向记录介质装置700传输(步骤S112)。另外，在步骤S112传输的运算标题密钥通过终端装置600无法知晓的在密钥分发装置400以及记录介质装置700之间共有的共通密钥BK3加密。

[0271] <7-3.内容再现处理的动作>

[0272] 图23为表示终端装置600的内容再现处理的动作的流程图。另外，记录介质装置700经上述的内容记录处理，已存放了内容、运算标题密钥、MAC、处理完毕UR、内容签名等。

[0273] 相互认证部605在与记录介质装置700之间进行相互认证处理，生成共通密钥BK3。另外，记录介质装置ID取得部606从在相互认证处理的途中接收的记录介质装置证书150取得记录介质装置ID(步骤S201)。记录介质装置ID取得部606将所取得的记录介质装置ID向

第1再现判断部625输出。

[0274] 接着，加密解密部608从记录介质装置700接收通过共通密钥BK3加密而得的运算标题密钥，利用共通密钥BK3来解密(步骤S202)。加密解密部608将所解密的运算标题密钥向运算标题密钥接收部620输出。运算标题密钥接收部620接收运算标题密钥，向标题密钥再运算部623输出。

[0275] 接着，UR读出部621从记录介质装置700读出处理完毕UR430，将所读出的处理完毕UR430向标题密钥再运算部623以及第3再现判断部630输出。内容签名读出部622从记录介质装置700读出内容签名510，将读出的内容签名510向标题密钥再运算部623、内容签名验证部627、第2再现判断部629以及第3再现判断部630输出。MAC读出部624从记录介质装置700读出MAC，将读出的MAC向第1再现判断部625输出(步骤S203)。

[0276] 标题密钥再运算部623计算处理完毕UR430的哈希值(步骤S205)。并且，标题密钥再运算部623根据处理完毕UR430的哈希值与运算标题密钥进行异或(XOR)的运算，生成标题密钥(步骤S206)。标题密钥再运算部623将算出的标题密钥向第1再现判断部625以及内容解密部631输出。

[0277] 接着，第1再现判断部625根据标题密钥与记录介质装置ID运算MAC(步骤S207)。第1再现判断部625判断在步骤S207算出的MAC与在步骤S203从记录介质装置700读出的MAC是否一致。

[0278] 在两MAC未一致时(在步骤S208为否)，第1再现判断部625向内容解密部631输出解密中止的指示。并且，终端装置600结束内容再现处理。

[0279] 在两MAC一致时(在步骤S208为是)，内容签名验证部627从内容签名510的签名装置证书区域514所记载的签名装置证书130提取签名装置ID(步骤S209)。内容签名验证部627确认在无效化列表接收·存放部626所存放的无效化列表160中，是否记载有在步骤S209提取的签名装置ID(步骤S210)。

[0280] 在无效化列表160中未记载有签名装置ID时(在步骤S211为否)，向步骤S215行进。在无效化列表160中记载有签名装置ID时(在步骤S211为是)，内容签名验证部627从内容签名510的签名日期时间区域513提取签名日期时间(步骤S212)。内容签名验证部627确认在无效化列表160内与签名装置ID建立对应地记载的撤销日期时间(步骤S213)。

[0281] 在撤销日期时间早于签名日期时间时(在步骤S214为是)，内容签名验证部627向内容解密部631输出解密中止的指示。并且，终端装置600结束内容再现处理。另外，在本实施方式中，在撤销日期时间与签名日期时间相同时，也设为内容签名验证部627向内容解密部631输出解密中止的指示。

[0282] 在撤销日期时间晚于签名日期时间时(在步骤S214为否)，内容读出部628从记录介质装置700读出内容(步骤S215)。内容读出部628将所读出的内容向第2再现判断部629以及内容解密部631输出。

[0283] 第2再现判断部628将从内容读出部628接受的内容分割为N个部分内容。并且，选择任意7个部分内容，计算选择的部分内容的哈希值。

[0284] 第2再现判断部629从由内容签名读出部622接受的内容签名510所包含的内容识别信息(哈希表)311中，读出选择的7个部分内容所对应的哈希值。并且，通过比较计算而得的哈希值与从内容识别信息311读出的哈希值，验证从记录介质装置700读出的内容是否为

合法的内容(步骤S216)。

[0285] 在7个哈希值之中至少1个未一致时(在步骤S217为失败),第2再现判断部629向内容解密部631输出解密中止的指示。并且,终端装置600结束内容再现处理。

[0286] 在7个哈希值全都一致时(在步骤S217为成功),第2再现判断部629从内容识别信息311读出根据从记录介质装置700读出的内容算出的7个哈希值之外的哈希值(N-7个哈希值)。第2再现判断部629组合从内容识别信息311读出的(N-7)个哈希值与根据内容算出的7个哈希值,生成验证用哈希表。

[0287] 第2再现判断部629从内容签名510的签名装置证书区域514提取签名装置公钥。第2再现判断部629通过将签名装置公钥用作验证密钥,对验证用哈希表实施签名验证算法V从而生成验证数据。签名验证算法V为验证由签名生成算法S生成的签名数据的算法。

[0288] 第2再现判断部629确认生成的验证数据与内容签名510的签名数据区域512所记载的签名数据是否一致(步骤S218)。

[0289] 在验证数据与签名数据未一致时(在步骤S219为失败),第2再现判断部629向内容解密部631输出解密中止的指示。并且,终端装置600结束内容再现处理。

[0290] 在验证数据与签名数据一致时(在步骤S219为成功),第3再现判断部630确认从记录介质装置700读出的处理完毕UR430是否为利用正规的内容签名510加工而成。

[0291] 具体而言,第3再现判断部630计算内容签名510的哈希值(步骤S220),比较计算而得的哈希值与处理完毕UR430的内容签名哈希值区域433所记载的哈希值(步骤S221)。

[0292] 在哈希值未一致时(在步骤S222为否),第3再现判断部630向内容解密部631输出解密中止的指示。并且,终端装置600结束内容再现处理。

[0293] 在哈希值一致时(在步骤S222为是),内容解密部631将标题密钥用作解密密钥,对内容实施解密算法D,从而解密内容(步骤S223)。

[0294] 内容再现部632解码内容并输出至显示设备(步骤S224)。

[0295] <8.记录介质装置700>

[0296] 在此,说明记录介质装置700的细节。记录介质装置700为安装于终端装置600并利用的SD存储卡。

[0297] <8-1.记录介质装置700的构成>

[0298] 图25为表示记录介质装置700的功能性的构成的框图。

[0299] 如图25所示,记录介质装置700由控制器701与存储部702构成。

[0300] 控制器701为由控制器制造商制造而得的LSI设备,安全地保护内部处理,从外部无法读出信息。

[0301] 存储部702为由闪存制造商制造而得的闪速存储器。对存储部702的数据的写入、以及从存储部702的数据的读出通过控制器701进行。具体而言,存储部702包括系统区域706、认证区域707以及普通区域708。系统区域706为只从控制器701能够访问(数据的读出以及写入),而从控制器701的外部无法访问的区域。认证区域707是为了访问而经由控制器701的认证处理所需的区域。普通区域708是无需认证处理,就能够经由控制器701从外部自由访问的区域。

[0302] 控制器701包括相互认证部703、加密解密部704以及读出写入部705。

[0303] 相互认证部703在与密钥分发装置400之间进行相互认证,彼此共有共通密钥BK2。

另外，相互认证部703在与终端装置600之间进行相互认证，彼此共有共通密钥BK3。有关相互认证处理以及密钥交换处理，已利用图15以及图16说明了，因此在此说明省略。

[0304] 加密解密部704利用与密钥分发装置400共有的共通密钥BK2，对在与密钥分发装置400之间收发的数据进行加密或者解密。同样地，加密解密部704利用与终端装置600共有的共通密钥BK3，对在与终端装置600之间收发的数据进行加密或者解密。

[0305] 具体而言，在内容的记录时，加密解密部704通过终端装置600的运算标题密钥传输部611接收从密钥分发装置400发送的加密运算标题密钥。并且，加密解密部704解密所接收的加密运算标题密钥，写入至存储部702。

[0306] 另外，在内容的再现时，加密解密部704读出存放于存储部702的运算标题密钥并加密，向终端装置600发送。

[0307] 读出写入部705进行从普通区域708的数据的读出、以及对普通区域708的数据的写入。

[0308] 系统区域706包括私钥·证书存放部711以及根公钥存放部712。

[0309] 私钥·证书存放部711存放由密钥发布装置100生成的记录介质装置私钥以及记录介质装置证书150。

[0310] 根公钥存放部712存放由密钥发布装置100生成的根公钥。

[0311] 另外，根公钥、记录介质装置私钥以及记录介质装置证书在记录介质装置700的制造时，由制造记录介质装置700的装置嵌入至存储部702。

[0312] 认证区域707包括运算标题密钥存放部713，在内部存放运算标题密钥。如上所述，为了访问认证区域707，控制器701的认证处理是必需的。因此，运算标题密钥的写入以及读出必须通过相互认证部703以及加密解密部704进行。

[0313] 普通区域708包括内容存放部714、内容签名存放部715、UR存放部716以及MAC存放部717。

[0314] 内容存放部714存放内容。内容签名存放部715存放内容签名510。UR存放部716存放处理完毕UR430。MAC存放部717存放MAC。

[0315] 另外，有关内容、内容签名510、处理完毕UR430以及MAC，在内容记录时，读出写入部705从终端装置600接收，由读出写入部705分别写入至内容存放部714、内容签名存放部715、UR存放部716以及MAC存放部717。

[0316] 另外，有关内容、内容签名510、处理完毕UR430以及MAC，在内容再现时，接受来自终端装置600的读出要求，由读出写入部705分别从内容存放部714、内容签名存放部715、UR存放部716以及MAC存放部717读出。并且，向终端装置600发送。

[0317] <9.变形例>

[0318] 以上，说明了本发明的实施方式，但也能够如以下变形例示的内容分发系统，本发明不限于如所述的实施方式那样的内容分发系统是毋庸置疑的。

[0319] (1)在所述的实施方式中，密钥分发装置400与签名装置500为两个独立的装置，但通过一个装置实现亦可。

[0320] (2)在所述的实施方式中，内容制作装置200与内容分发装置300为两个独立的装置，但通过一个装置实现亦可。

[0321] 另外，如图9所示的内容分发装置300所包含的标题密钥生成部302、加密部303、内

容识别信息生成部305以及标题密钥·内容识别信息发送部306并非内容分发装置300，而是包含于内容制作装置200，这些功能模块的功能通过内容制作装置200来实现的构成亦可。

[0322] (3)在所述的实施方式中，将SD存储卡用于具体例说明了记录介质装置700。但是，记录介质装置700不限于SD存储卡。记录介质装置700为由如HDD那样的存储设备与控制LSI构成的设备亦可。另外，记录介质装置700不限于如SD存储卡那样的插拔式的设备。由内置于便携式电话机、eBook、NetBook等的内置型存储器与控制LSI构成的设备亦可。

[0323] (4)另外，在所述的实施方式中，将PC用作具体例说明了记录终端装置600。但是，终端装置600不限于PC。例如，终端装置600为智能电话、平板电脑终端等便携终端亦可。例如，终端装置600为设置于便利店等店铺的所谓KIOSK终端亦可。另外，终端装置600为接收数字电视广播的接收装置亦可。终端装置600为至少能够与互联网或电视广播网等网络连接的机器，具有通过网络取得内容、标题密钥、内容签名、UR等，并记录至记录介质装置700的功能即可。

[0324] (5)在所述的实施方式中，终端装置600具有在与记录介质装置700进行相互认证的途中，取得记录介质装置ID的构成。可是，记录介质装置ID的取得方法不限于此。

[0325] 例如，在记录介质装置700的认证区域707中，存放有用于唯一地识别记录介质装置700的记录介质装置ID亦可。此时，终端装置600与记录介质装置700进行相互认证，共有共通密钥BK3之后，从记录介质装置700接收通过共通密钥BK3加密记录介质装置ID而得的加密记录介质装置ID。终端装置600为通过共通密钥BK3解密所接收的加密记录介质装置ID，取得记录介质装置ID的构成亦可。

[0326] (6)另外，对在所述的实施方式中说明了的相互认证处理，追加以下的处理亦可。

[0327] 密钥分发装置400、终端装置600以及记录介质装置700事先从密钥发布装置100取得记载有暴露私钥的装置(撤销的装置)的装置ID的无效化列表160。并且，各装置从在相互认证处理的途中接收的对方装置的公钥证书提取装置ID，判断提取的装置ID是否记载于无效化列表。在从公钥证书提取的装置ID记载于无效化列表时，即，在对方装置被撤销时，中断相互认证处理。

[0328] (7)利用图26说明作为所述的终端装置600的变形例的验证装置1600。如图26所示，验证装置1600由根公钥存放部601、私钥·证书存放部602、相互认证部605、记录介质装置ID取得部606、加密解密部608、运算标题密钥接收部620、UR读出部621、内容签名读出部622、标题密钥再运算部623、MAC读出部624、第1判断部1625、无效化列表接收·存放部626、内容签名验证部627以及第3判断部1630构成。在此，针对与终端装置600所包含的构成要素具有相同功能的构成要素，赋予与图20以及图21所示的符号相同的符号。

[0329] 验证装置1600并不具有与内容的解密以及内容的再现有关的功能。

[0330] 第1判断部1625与第1再现判断部625同样地，从标题密钥再运算部623接受标题密钥，从记录介质装置ID取得部606接受记录介质装置ID，从MAC读出部624接受MAC。第1判断部1625根据接受的标题密钥与记录介质识别ID运算MAC。并且，第1判断部1625判断运算而得的MAC与MAC读出部624从记录介质装置700读出的MAC是否一致。第1判断部1625输出判断结果。

[0331] 第3判断部1630与第3再现判断部630同样地，从UR读出部621接受处理完毕UR430，

从内容签名读出部622接受内容签名。第3判断部1630计算内容签名整体的哈希值，确认计算而得的哈希值与处理完毕UR430的内容签名哈希值区域所记载的哈希值是否一致。第3判断部1630输出判断结果。

[0332] 如此，并不具有与内容的解密以及内容的再现有关的功能的验证装置也包含于本发明的一方式。

[0333] 另外，本发明的一方式的验证装置也可构成为，包括：读出部，从记录介质装置读出加密内容与内容签名，从所述记录介质装置的被保护的区域读出变换标题密钥，该变换标题密钥利用由正规的签名装置生成的内容签名变换标题密钥而成；内容签名验证部，判断读出部所读出的所述内容签名与由所述变换标题密钥的生成所利用的所述正规的签名装置生成的所述内容签名是否一致。

[0334] 在此，所述验证装置的所述内容签名验证部向外部输出判断结果亦可。并且，所述验证装置与接收从所述内容签名验证部输出的所述判断结果并根据所接收的判断结果进行处理的控制装置连接亦可。具体而言，所述控制装置根据所接收的判断结果，进行加密内容的解密或加密内容的移动等。即，在内容签名不一致时，所述控制装置并不进行加密内容的解密或加密内容的移动等，只在内容签名一致时，进行加密内容的解密或加密内容的移动等。

[0335] (8)所述的实施方式中的密钥分发装置400的内容签名接收部408如以下进行从签名装置500接收的内容签名510的验证亦可。

[0336] 内容签名接收部408对照保持于无效化列表接收部409的无效化列表160，判断签名装置ID是否记载于无效化列表。在签名装置ID记载于无效化列表160时，内容签名接收部408比较内容签名510所记载的签名日期时间与无效化列表所记载的撤销日期时间。在内容签名510所记载的签名日期时间晚于无效化列表160所记载的撤销日期时间时，内容签名接收部408将内容签名510判断为无效。

[0337] 在内容签名510所记载的签名日期时间早于无效化列表160所记载的撤销日期时间时，内容签名接收部408进而确认内容签名510的签名日期时间是否大幅度地偏离接收内容签名510的日期时间。

[0338] 作为一例，确认在签名日期时间与当前日期时间之间是否存在48小时以上的差距。在确认的结果是在签名日期时间与当前日期时间之间存在48小时以上的差距时，内容签名接收部408将所接收的内容签名510判断为无效。

[0339] (9)在所述的实施方式中，UR处理部410计算内容签名接收部408所接收的内容签名510的哈希值，对UE接收部407所接收的UR210追加内容签名510的哈希值。

[0340] 密钥分发装置400例如如以下变形所述的构成亦可。

[0341] 密钥分发装置400为代替UR处理部410而包括追加签名部的构成的亦可。追加签名部根据内容签名接收部408所接收的内容签名510，生成图27所示的附签名的内容签名1510。

[0342] 追加签名部针对内容签名510(连结内容识别信息区域511、签名数据区域512、签名日期时间区域513以及签名装置证书区域514所记载的数据而得的数据)，将私钥·证书存放部404所存放的密钥分发装置私钥用作签名密钥并实施签名生成算法，生成签名数据。并且，追加签名部将生成的签名数据记载于附签名的内容签名1510的基于密钥分发装置的

私钥的签名数据区域1511。进而，追加签名部将私钥·证书存放部404所存放的密钥分发装置证书120记载于密钥分发装置证书区域1512。

[0343] 如此，追加签名部修正内容签名接收部408所接收的内容签名510，并生成附签名的内容签名1510。密钥分发装置400代替将内容签名510向终端装置600发送，将由追加签名部生成的附签名的内容签名1510向终端装置600发送。

[0344] 终端装置600在从密钥分发装置400接收附签名的内容签名1510时，记录于记录介质装置700的普通区域708。

[0345] 在代替处理完毕UR，利用附签名的内容签名1510时，终端装置600在内容再现处理时，并不进行所述的第3再现判断部630的判断处理。取而代之，第2再现判断部629追加并进行以下的处理。

[0346] 第2再现判断部629针对连结内容识别信息区域511、签名数据区域512、签名日期时间区域513以及签名装置证书区域514所记载的数据而得的数据，将密钥分发装置证书区域1512所记载的密钥分发装置证书120所包含的密钥分发装置公钥用作验证密钥并实施签名验证算法，生成验证数据。第2再现判断部629确认生成的验证数据与基于密钥分发装置的私钥的签名数据区域1511所记载的签名数据是否一致。

[0347] 在签名验证成功时，终端装置600继续内容再现处理。在签名验证失败时，第2再现判断部629向内容解密部631输出解密中止的指示。并且，终端装置600结束内容再现处理。

[0348] (10)在所述的实施方式中，终端装置600的第1再现判断部625利用基于记录介质装置700的ID生成的MAC，判断内容的再现可否。但是，再现可否的判断所利用的信息不限于MAC。例如，利用对运算标题密钥与记录介质装置的识别信息进行XOR(异或)而得的信息亦可。另外，利用对运算标题密钥与记录介质装置的识别信息的哈希值进行XOR(异或)而得的信息亦可。另外，例如，利用对记录介质装置700的识别信息赋予密钥发布装置100的签名而得的信息亦可。此时，终端装置600通过计算XOR，进行签名验证，能够判断内容的再现可否。

[0349] (11)在所述的实施方式中，终端装置600的第2再现判断部629具有从N个部分内容选择任意7个部分内容，计算选择的7个部分内容的哈希值的构成。通过该构成，能够削减第2再现判断部629的计算量。

[0350] 但是，第2再现判断部628为了提高内容的合法性验证的精度，也可为根据多于7个的部分内容计算哈希值的构成。另外，第2再现判断部629为了进一步削减计算量，也可为根据少于7个的部分内容计算哈希值的构成。

[0351] (12)在所述的实施方式中，终端装置600的第3再现判断部630具有计算内容签名510的哈希值，比较计算而得的哈希值与处理完毕UR的内容签名哈希值区域所记载的哈希值的构成。

[0352] 但是，该构成为一例。第3再现判断部630能够确认用于确定内容签名510的信息被正确地嵌入至处理完毕UR430即可。

[0353] 例如，第3再现判断部630为确认UR读出部621所读出的处理完毕UR430的签名数据区域431所记载的签名数据与内容签名读出部622所读出的内容签名510的签名数据区域512所记载的签名数据是否一致的构成亦可。

[0354] (13)在所述的实施方式中，第1再现判断部625、内容签名验证部627、第2再现判断部629以及第3再现判断部630具有根据判断结果，针对内容解密部631，输出解密中止的指

示的构成。但是，该构成为一例。为了抑制内容的再现，第1再现判断部625、内容签名验证部627、第2再现判断部629以及第3再现判断部630根据判断结果，针对内容再现部632，输出解码中止的指示亦可。另外，第1再现判断部625根据判断结果，对内容读出部628输出读出中止的指示亦可。

[0355] (14)在所述的实施方式中，记载为内容的一例为由视频数据以及音频数据构成的电影。但是，内容不限于电影是不言自明的。内容为JPEG数据等静止图像、计算机程序、计算机游戏、不含视频数据的音乐内容、文本数据等亦可。

[0356] (15)也能够将控制程序记录至记录介质，或者能够通过各种通道等流通分发，该控制程序由用于使密钥分发装置以及诊断装置的处理器、以及与该处理器连接的各种电路执行在实施方式所示的密钥分发处理以及内容再现处理的机器语言或者高级语言的程序代码构成。在如此的记录介质中，存在IC卡、硬盘、光盘、软盘、ROM、闪速存储器等。流通、分发的控制程序通过存放于可由处理器读出的内存等以供利用，该处理器通过执行该控制程序实现所述的实施方式所示的各功能。另外，处理器除了直接执行控制程序之外，通过编译来执行或者由解释器来执行亦可。

[0357] (16)在实施方式所示的各装置的各功能构成要素(作为一例，根公钥存放部601、私钥·证书存放部602、内容接收部603、内容写入部604、相互认证部605、记录介质装置ID取得部606、记录介质装置ID发送部607、加密解密部608、MAC·UR·内容签名接收部609、MAC·UR·内容签名写入部610、运算标题密钥传输部611、运算标题密钥接收部620、UR读出部621、内容签名读出部622、标题密钥再运算部623、MAC读出部624、第1再现判断部625、无效化列表接收·存放部626、内容签名验证部627、内容读出部628、第2再现判断部629、第3再现判断部630、内容解密部631、以及内容再现部632等)通过执行该功能的电路来实现亦可，通过由1或者多个处理器执行程序来实现亦可。另外，在实施方式所示的密钥分发装置以及终端装置构成为IC、LSI之外的集成电路的封装亦可。该封装装配至各种装置以供利用，据此，各种装置实现如在所述的实施方式所示的各功能。

[0358] (17)对所述的实施方式以及所述的变形例进行适宜组合亦可。

[0359] <10.补充>

[0360] 以下，进一步说明作为本发明的一方式的终端装置、验证装置、密钥分发装置的构成以及其变形例和效果。

[0361] (a)本发明的一方式的终端装置，其特征在于，包括：读出部，从记录介质装置读出加密内容与内容签名，从所述记录介质装置的被保护的区域读出变换标题密钥，该变换标题密钥利用由正规的签名装置生成的内容签名变换标题密钥而成；标题密钥复原部，利用读出部所读出的所述内容签名对所述变换标题密钥进行逆变换，生成复原标题密钥；以及再现部，利用所述复原标题密钥，解密所述加密内容，再现解密而得的内容。

[0362] 根据该构成，在所述记录介质装置的被保护的区域中，记录有变换标题密钥，该变换标题密钥利用由正规的签名装置生成的内容签名变换标题密钥而成。因此，即使进行将利用泄漏的签名密钥生成的内容签名与非法的加密内容记录于所述记录介质装置的非法行为，终端装置也无法根据从所述记录介质装置读出的变换标题密钥复原合法的标题密钥。终端装置在无法复原正确的标题密钥时，便无法正确地进行非法的加密内容的解密。因此，通过抑制终端装置的非法的加密内容的再现，能够抑制内容的非法利用。

[0363] 另外，由于即使发布如在终端装置侧无法再现的非法内容，也毫无意义，因此存在能够抑制非法利用泄漏的签名密钥，将非法的加密内容冒充为宛如正规的内容并记录于记录介质装置的非法行为本身的可能性。

[0364] (b)在此，其特征在于，所述变换标题密钥通过由所述正规的签名装置生成的内容签名、所述内容的利用条件、以及所述标题密钥生成，所述读出部还从所述记录介质装置读出利用条件；所述标题密钥复原部利用所述读出部所读出的所述内容签名与所述利用条件对所述变换标题密钥进行逆变换，生成所述复原标题密钥。

[0365] 根据该构成，在非法的用户对记录介质装置记录非法的利用条件时，终端装置无法从变换标题密钥复原正确的标题密钥。因此，通过抑制终端装置的非法的加密内容的再现，能够抑制内容的非法利用。

[0366] (c)在此，其特征在于，所述变换标题密钥通过对结合由所述正规的签名装置生成的内容签名以及所述利用条件而得的第1结合数据与所述标题密钥实施规定的运算来生成；所述标题密钥复原部根据所述读出部所读出的所述内容签名与所述读出的利用条件生成第2结合数据，对所生成的所述第2结合数据与所述变换标题密钥实施所述规定的运算的逆运算，从而生成所述复原标题密钥。

[0367] 根据该构成，非法的用户记录至记录介质装置的利用条件以及内容签名与正规的利用条件以及内容签名只要有1位不同，终端装置便无法从变换标题密钥复原正确的标题密钥。因此，由于抑制终端装置的非法的加密内容的再现，能够抑制内容的非法利用。

[0368] (c)在此，其特征在于，所述终端装置还包括内容签名验证部(实施方式的第3再现判断部630)，该内容签名验证部判断所述读出部所读出的所述内容签名与所述变换标题密钥的生成所利用的由所述正规的签名装置生成的所述内容签名是否一致，在判断结果为不一致时，抑制所述再现部的处理。

[0369] 在记录介质装置所记录的内容签名与正规的内容签名不同时，记录介质装置所记录的加密内容为非法内容的可能性高。因此，通过包括所述的构成，能够抑制非法的内容的再现。

[0370] 另外，在通过终端装置再现非法内容时，存在产生用户无法预期的再现错误的可能性。假如用户并不知晓记录介质装置所记录的内容为非法内容时，若在终端装置产生再现错误则可预想用户混乱的情形。因此，通过包括所述的构成，抑制非法的内容的再现，能够事先排除在终端装置产生再现错误的可能性。

[0371] (e)在此，其特征在于，所述终端装置还包括内容验证部(实施方式的第2再现判断部629)，该内容验证部利用所述内容签名验证所述加密内容的合法性，在判断为所述加密内容非法时，抑制所述再现部的处理。

[0372] 根据该构成，在记录介质装置所记录的加密内容与内容签名不匹配时，能够抑制内容的再现。

[0373] (c)在此，其特征在于，所述内容签名还包括生成该内容签名的所述签名装置的识别信息，所述终端装置还包括：接收部，接收记载有成为无效化对象的装置的识别信息的无效化列表；以及无效化确认部(实施方式的内容签名验证部627)，该无效化确认部利用所接收的所述无效化列表确认所述签名装置是否无效化对象，在判断所述签名装置为无效化对象时，抑制所述再现部的处理。

[0374] 根据该构成，即使进行将利用泄漏的签名密钥生成的内容签名与非法的加密内容记录于所述记录介质装置的非法行为，也由于抑制赋予利用泄漏的私钥生成的内容签名的内容的再现，因此能够抑制内容的非法利用。

[0375] (g)在此，其特征在于，所述内容签名还包括表示所述签名装置生成该内容签名的日期的第1日期信息，所述无效化列表还包括与成为无效化对象的装置的识别信息建立对应地表示成为无效化对象的日期的第2日期信息，所述无效化确认部在所述签名装置的识别信息记载于所述无效化列表，并且，所述第1日期信息所表示的日期晚于所述第2日期信息所表示的日期时，判断所述签名装置为无效化对象，在所述签名装置的识别信息记载于所述无效化列表，并且，所述第1日期信息所表示的日期早于所述第2日期信息所表示的日期时，判断所述签名装置并非无效化对象。

[0376] 根据该构成，终端装置的再现部能够再现被赋予了在签名装置的私钥泄漏之前生成的内容签名的内容。因此，能够保护正规地下载内容的用户的权利。

[0377] (h)本发明的一方式的验证装置，其特征在于，包括：读出部，从记录介质装置读出加密内容与内容签名，从所述记录介质装置的被保护的区域读出变换标题密钥，该变换标题密钥利用由正规的签名装置生成的内容签名变换标题密钥而成；以及内容签名验证部(实施方式的第3判断部1630)，判断读出部所读出的所述内容签名与所述变换标题密钥的生成所利用的由所述正规的签名装置生成的所述内容签名是否一致。

[0378] 根据该构成，存在在进行利用泄漏的签名密钥，根据非法的加密内容生成内容签名，将该内容签名与非法的加密内容记录于所述记录介质装置的非法行为时，通过所述内容签名验证部的验证判断为不一致，并不执行之后的处理的可能性。因此，由于抑制利用非法的加密内容的处理，能够抑制内容的非法利用。

[0379] (i)本发明的一方式的密钥分发装置，其特征在于，包括：内容保持部，保持通过标题密钥加密内容而得的加密内容；内容签名保持部，保持用于验证所述加密内容的合法性的内容签名；标题密钥保持部，保持所述标题密钥；密钥生成部，利用所述内容签名变换所述标题密钥，生成变换标题密钥；以及记录部，将所述加密内容、所述内容签名、所述变换标题密钥记录于记录介质装置。

[0380] 根据该构成，即使进行将利用泄漏的签名密钥生成的内容签名与非法的加密内容记录于所述记录介质装置的非法行为，在再现加密内容的终端装置中，也无法根据从所述记录介质装置读出的变换标题密钥复原正确的标题密钥。终端装置在无法复原正确的标题密钥时，便无法正确地进行非法的加密内容的解密。因此，通过抑制终端装置的非法的加密内容的再现，能够抑制内容的非法利用。

[0381] (j)在此，其特征在于，所述密钥分发装置还包括：利用条件保持部，保持所述内容的利用条件；所述密钥生成部根据所述内容签名、所述利用条件以及所述标题密钥生成所述变换标题密钥。

[0382] 根据该构成，在非法的用户对记录介质装置记录非法的利用条件时，再现加密内容的终端装置无法从变换标题密钥复原正确的标题密钥。因此，通过抑制终端装置的非法的加密内容的再现，能够抑制内容的非法利用。

[0383] (k)在此，其特征在于，所述密钥生成部通过对结合由所述内容签名以及所述利用条件而得的结合数据与所述标题密钥实施规定的运算来生成所述变换标题密钥。

[0384] 根据该构成，非法的用户记录至记录介质装置的利用条件以及内容签名与正规的利用条件以及内容签名只要有1位不同，终端装置便无法从变换标题密钥复原正确的标题密钥。因此，由于抑制终端装置的非法的加密内容的再现，能够抑制内容的非法利用。

[0385] 工业实用性

[0386] 本发明能够用作以下技术：在制造以及出售将网络分发的内容、内容签名、UR、标题密钥等记录于SD存储卡等记录介质装置的终端装置中，即使进行将利用泄漏的签名密钥生成的内容签名与非法的加密内容记录于所述记录介质装置的非法行为，也能够抑制终端装置的非法的加密内容的再现。

[0387] 标记说明

[0388] 1 内容分发系统；

[0389] 100 密钥发布装置；

[0390] 200 内容制作装置；

[0391] 300 内容分发装置；

[0392] 400 密钥分发装置；

[0393] 401 根公钥接收部；

[0394] 402 根公钥存放部；

[0395] 403 私钥·证书接收部；

[0396] 404 私钥·证书存放部；

[0397] 405 标题密钥·内容识别信息接收部；

[0398] 406 内容识别信息发送部；

[0399] 407 UR接收部；

[0400] 408 内容签名接收部；

[0401] 409 无效化列表接收部；

[0402] 410 UR处理部；

[0403] 411 标题密钥运算部；

[0404] 412 相互认证部；

[0405] 413 加密解密部；

[0406] 414 记录介质装置ID接收部；

[0407] 415 MAC运算部；

[0408] 500 签名装置；

[0409] 501 私钥·证书接收部；

[0410] 502 私钥·证书存放部；

[0411] 503 内容识别信息接收部；

[0412] 504 签名部；

[0413] 505 内容签名发送部；

[0414] 600 终端装置；

[0415] 601 根公钥存放部；

[0416] 602 私钥·证书存放部；

[0417] 603 内容接收部；

[0418] 604 内容写入部；

[0419] 605 相互认证部；

[0420] 606 记录介质装置ID取得部；

[0421] 607 记录介质装置ID发送部；

[0422] 608 加密解密部；

[0423] 609 MAC·UR·内容签名接收部；

[0424] 610 MAC·UR·内容签名写入部；

[0425] 611 运算标题密钥传输部；

[0426] 620 运算标题密钥接收部；

[0427] 621 UR读出部；

[0428] 622 内容签名读出部；

[0429] 623 标题密钥再运算部；

[0430] 624 MAC读出部；

[0431] 625 第1再现判断部；

[0432] 626 无效化列表接收·存放部；

[0433] 627 内容签名验证部；

[0434] 628 内容读出部；

[0435] 629 第2再现判断部；

[0436] 630 第3再现判断部；

[0437] 631 内容解密部；

[0438] 632 内容再现部；

[0439] 700 记录介质装置；

[0440] 1600 验证装置。

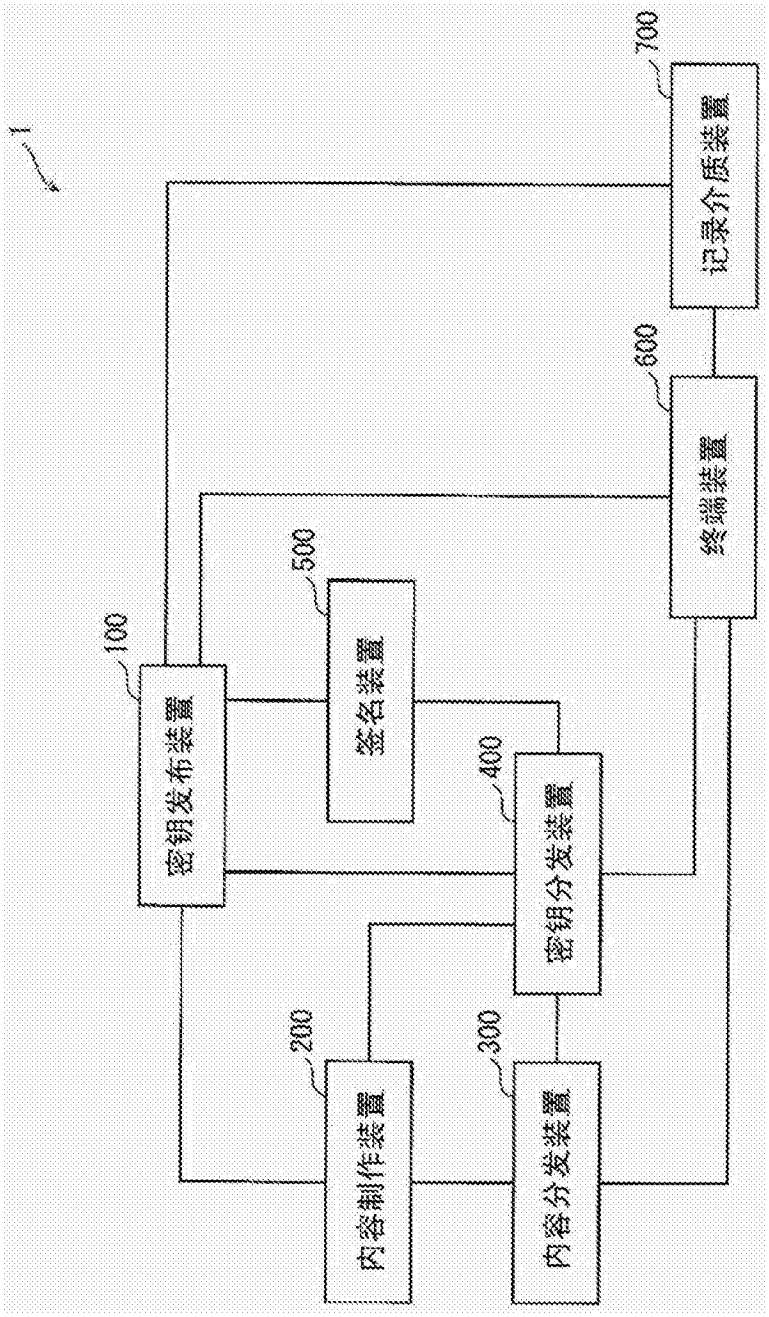

1
700
记录介质装置
600
终端装置
500
签名装置
100
密钥发布装置
400
密钥分发装置
200
内容制作装置
300
内容分发装置

图1

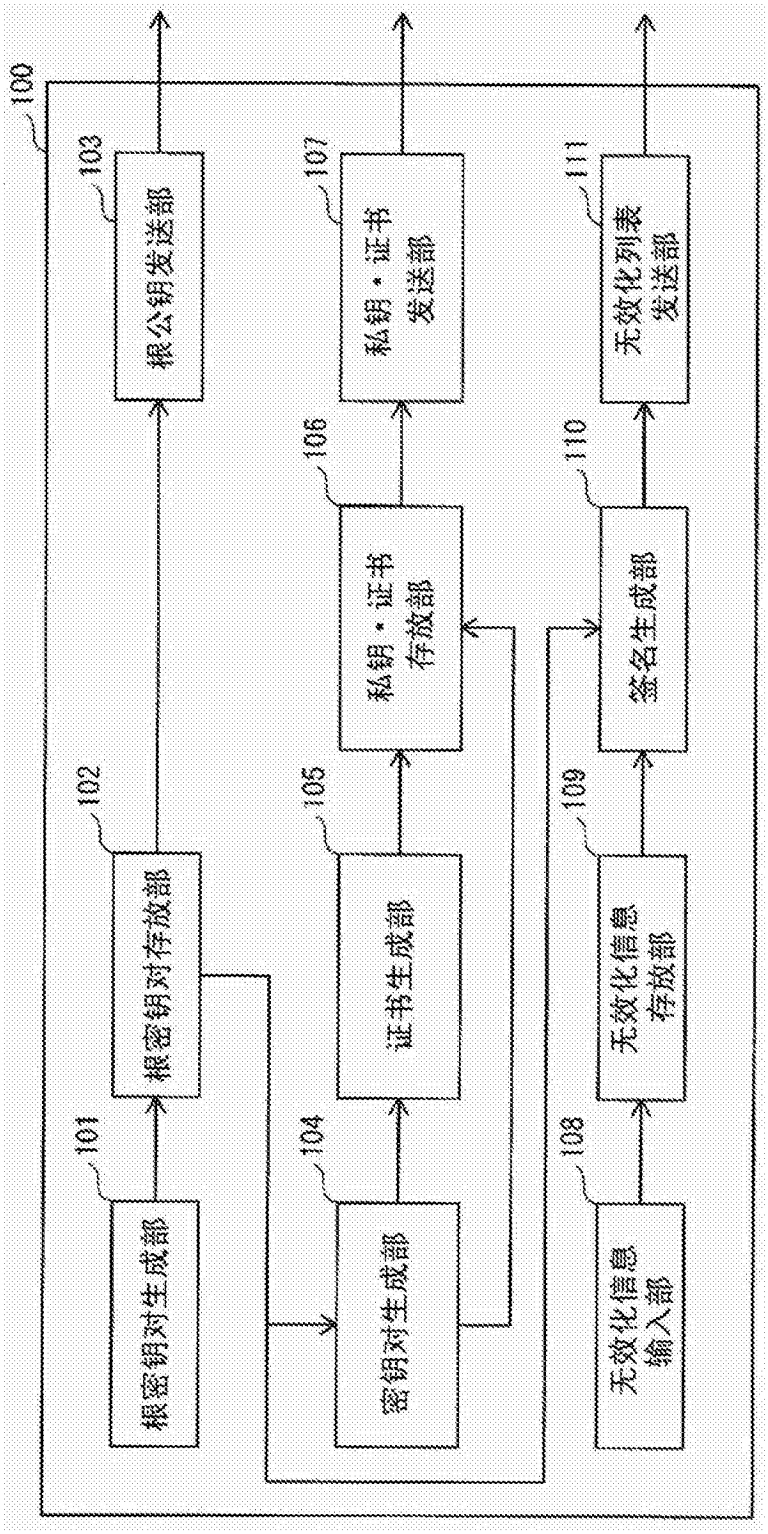

100
101
根密钥对生成部
102
根密钥对存放部
103
根公钥发送部
104
密钥对生成部
105
证书生成部
106
私钥·证书
存放部
107
私钥·证书
发送部
108
无效化信息
输入部
109
无效化信息
存放部
110
签名生成部
111
无效化列表
发送部

图2

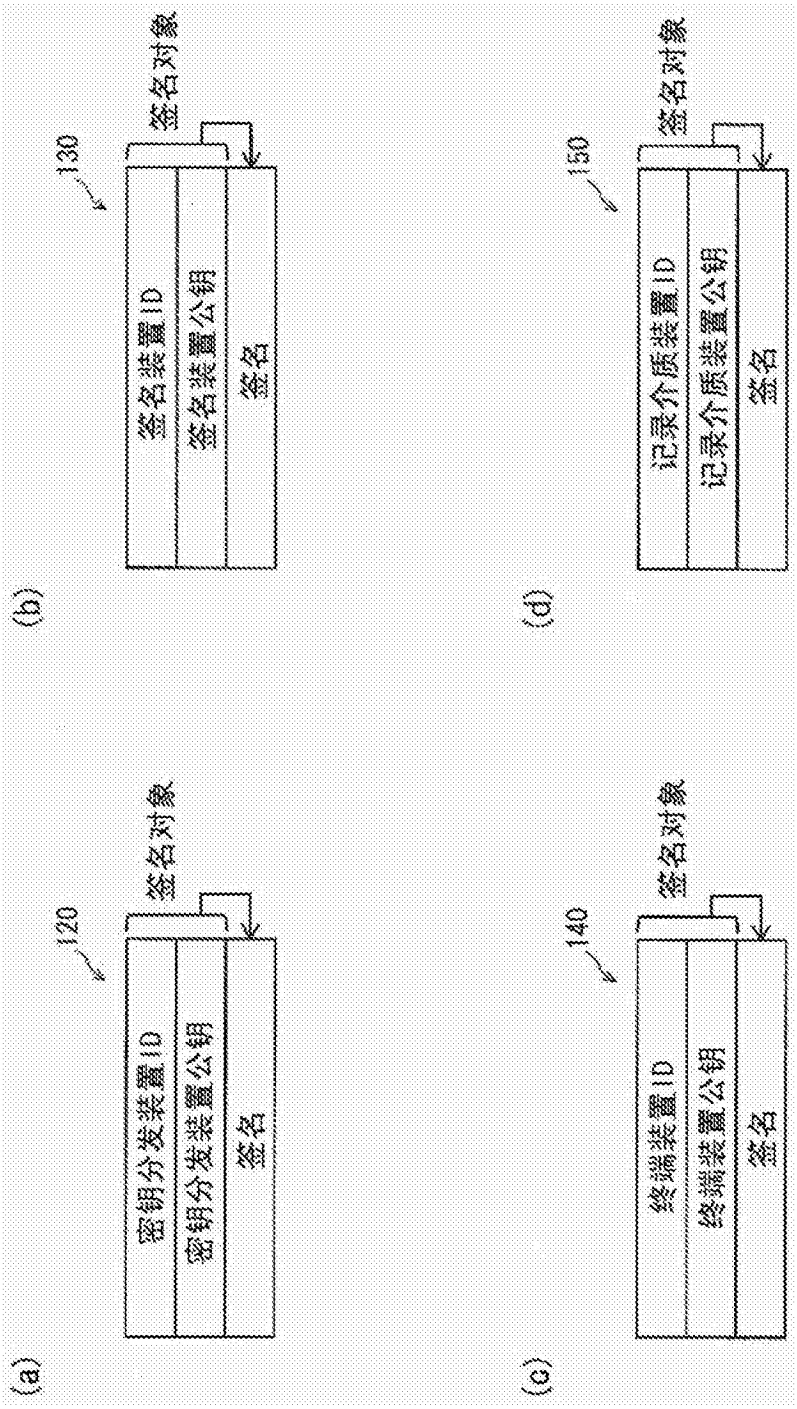

(a)
120
密钥分发装置ID
密钥分发装置公钥
签名
签名对象
(b)
130
签名装置ID
签名装置公钥
签名
签名对象
(c)
140
终端装置ID
终端装置公钥
签名
签名对象
(d)
150
记录介质装置ID
记录介质装置公钥
签名
签名对象

图3

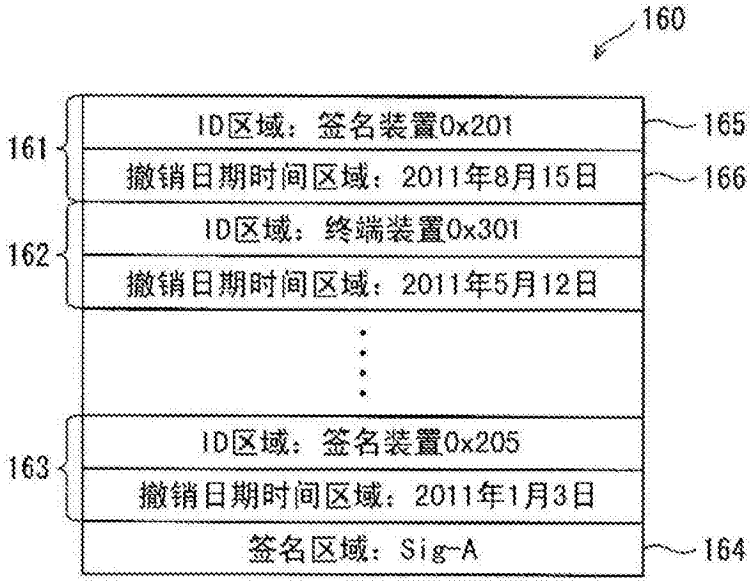

160
161
162
163
ID区域：签名装置0x201
165
撤销日期时间区域：2011年8月15日
166
ID区域：终端装置0x301
撤销日期时间区域：2011年5月12日
ID区域：签名装置0x205
撤销日期时间区域：2011年1月3日
签名区域：Sig-A
164

图4

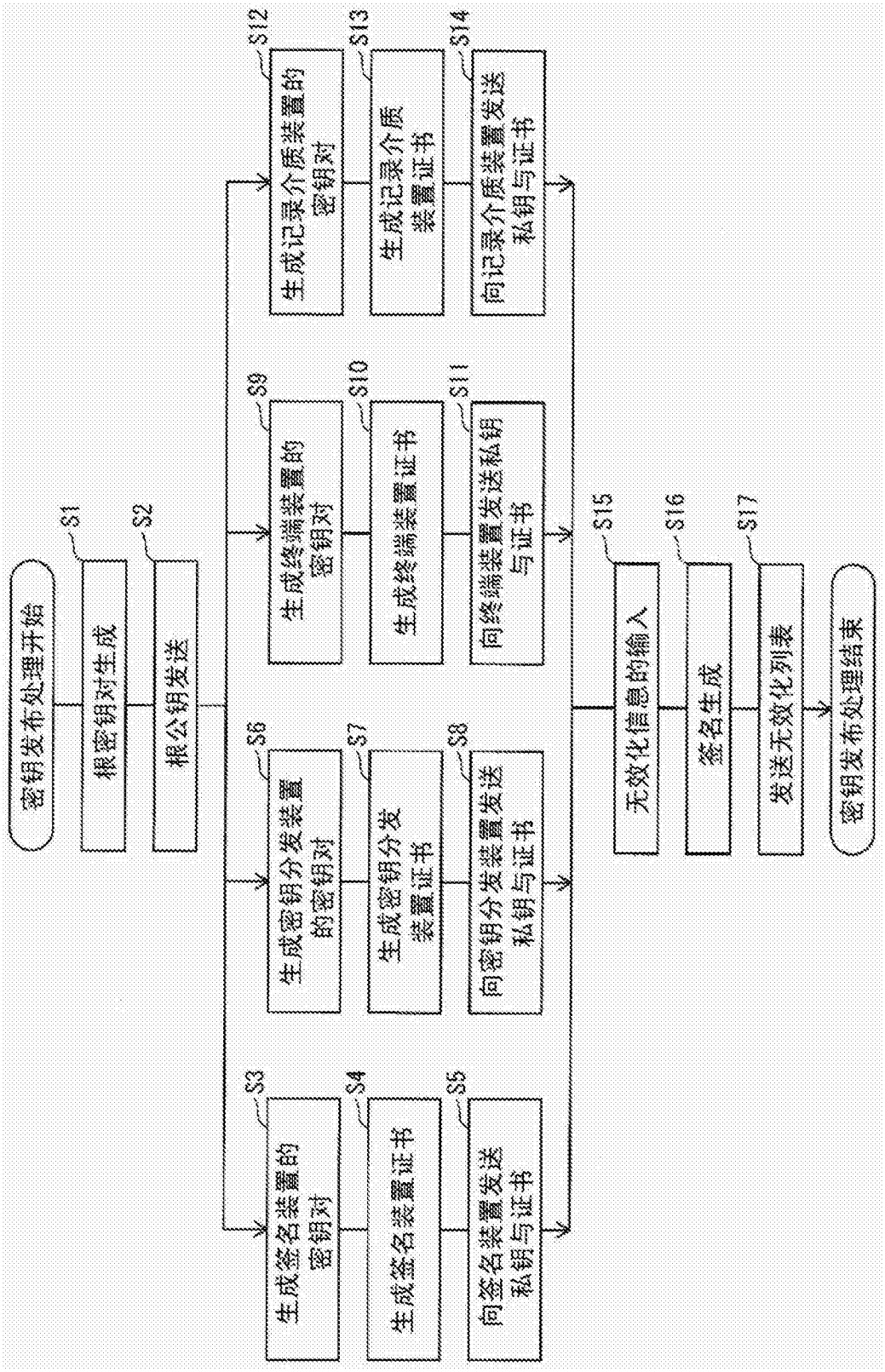

密钥发布处理开始
S1
根密钥对生成
S2
根公钥发送
S3
生成签名装置的密钥对
S4
生成签名装置证书
S5
向签名装置发送私钥与证书
S6
生成密钥分发装置的密钥对
S7
生成密钥分发装置证书
S8
向密钥分发装置发送私钥与证书
S9
生成终端装置的密钥对
S10
生成终端装置证书
S11
向终端装置发送私钥与证书
S12
生成记录介质装置的密钥对
S13
生成记录介质装置证书
S14
向记录介质装置发送私钥与证书
S15
无效化信息的输入
S16
签名生成
S17
发送无效化列表
密钥发布处理结束

图5

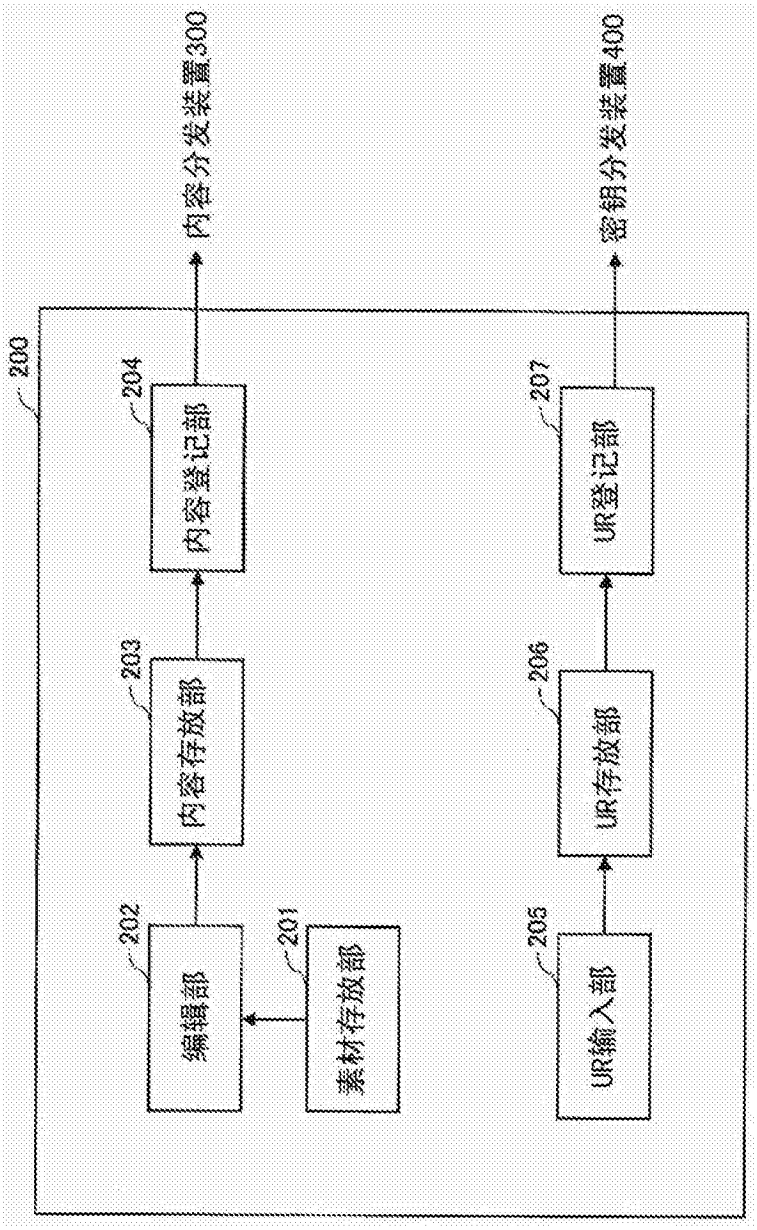

内容分发装置300
密钥分发装置400
200
204
内容登记部
207
UR登记部
203
内容存放部
206
UR存放部
202
编辑部
201
素材存放部
205
UR输入部

图6

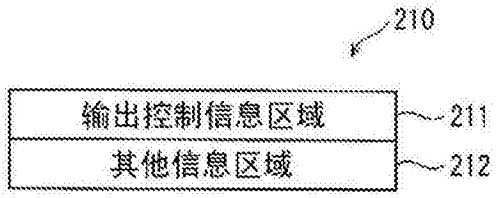

210
输出控制信息区域
211
其他信息区域
212

图7

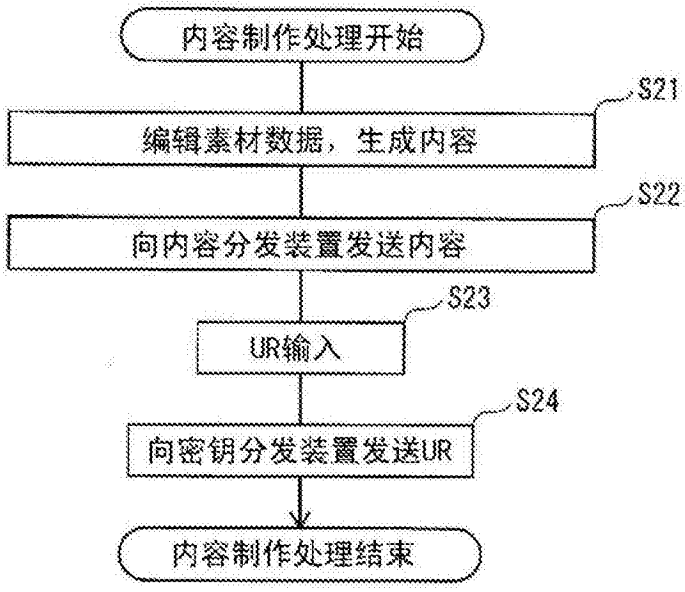

内容制作处理开始
S21
编辑素材数据，生成内容
S22
向内容分发装置发送内容
S23
UR输入
S24
向密钥分发装置发送UR
内容制作处理结束

图8

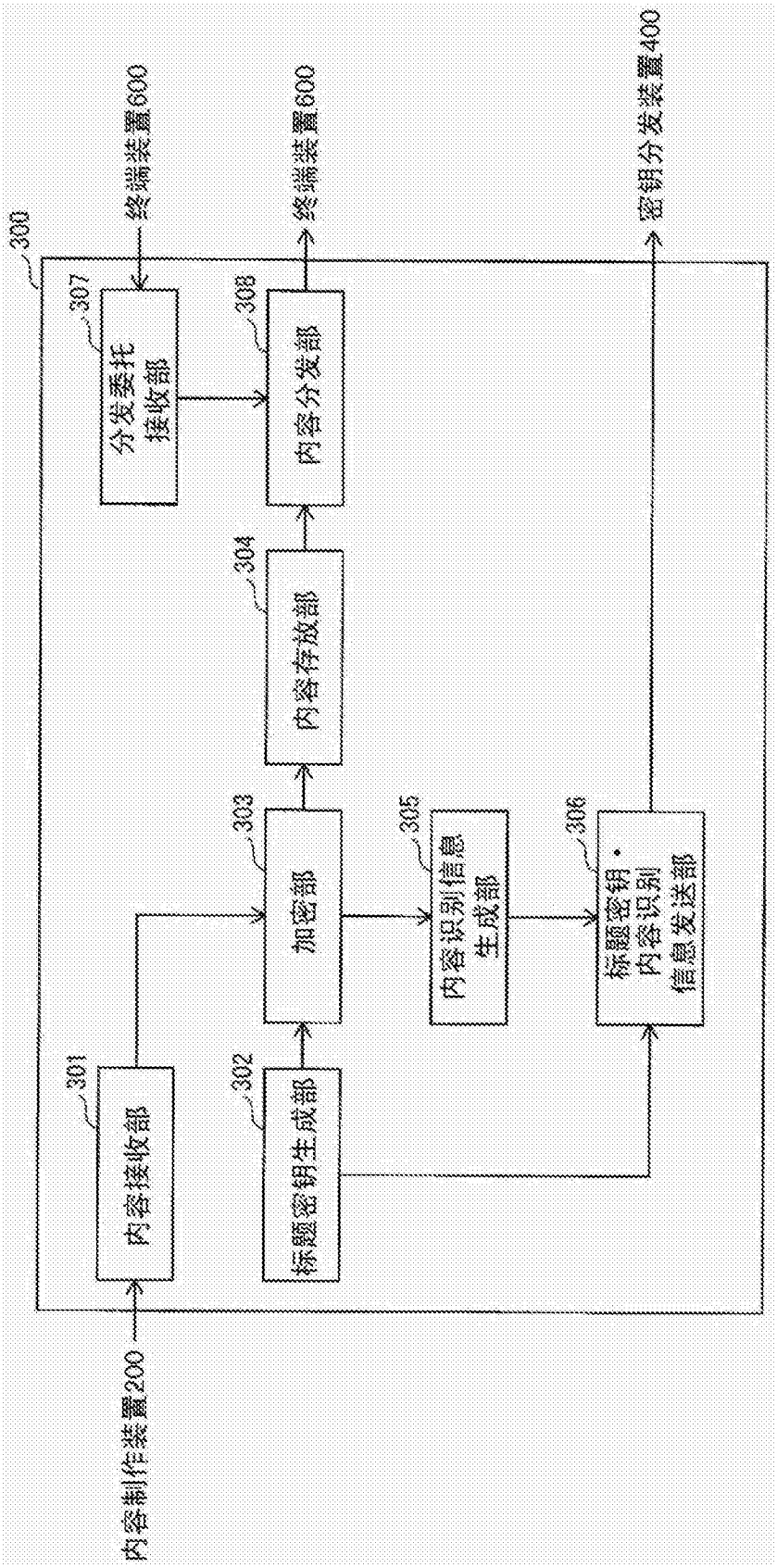

300
内容制作装置200
301
内容接收部
302
标题密钥生成部
303
加密部
304
内容存放部
305
内容识别信息生成部
306
标题密钥·内容识别信息发送部
307
分发委托接收部
308
内容分发部
终端装置600
终端装置600
密钥分发装置400

图9

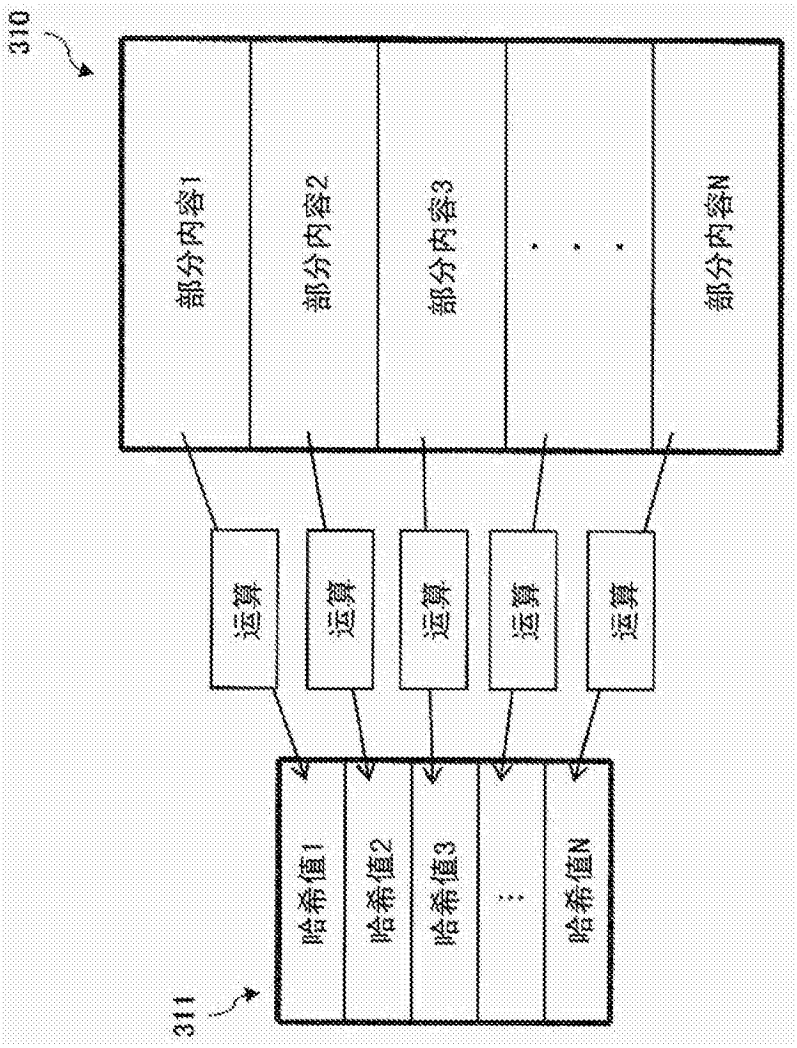

310
部分内容1
部分内容2
部分内容3
部分内容N
运算
运算
运算
运算
运算
哈希值1
哈希值2
哈希值3
哈希值N
311

图10

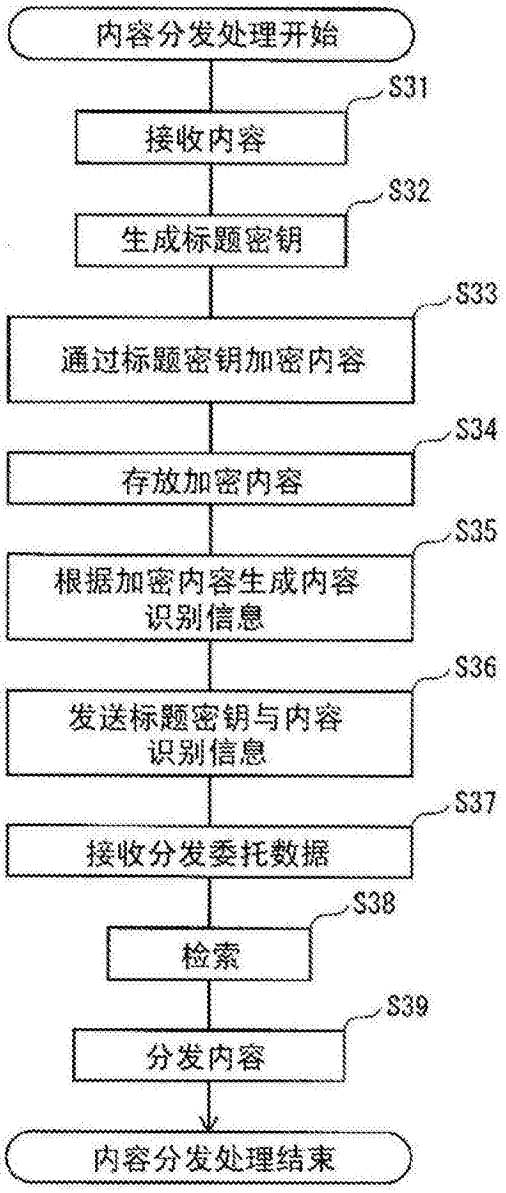

内容分发处理开始
S31
接收内容
S32
生成标题密钥
S33
通过标题密钥加密内容
S34
存放加密内容
S35
根据加密内容生成内容识别信息
S36
发送标题密钥与内容识别信息
S37
接收分发委托数据
S38
检索
S39
分发内容
内容分发处理结束

图11

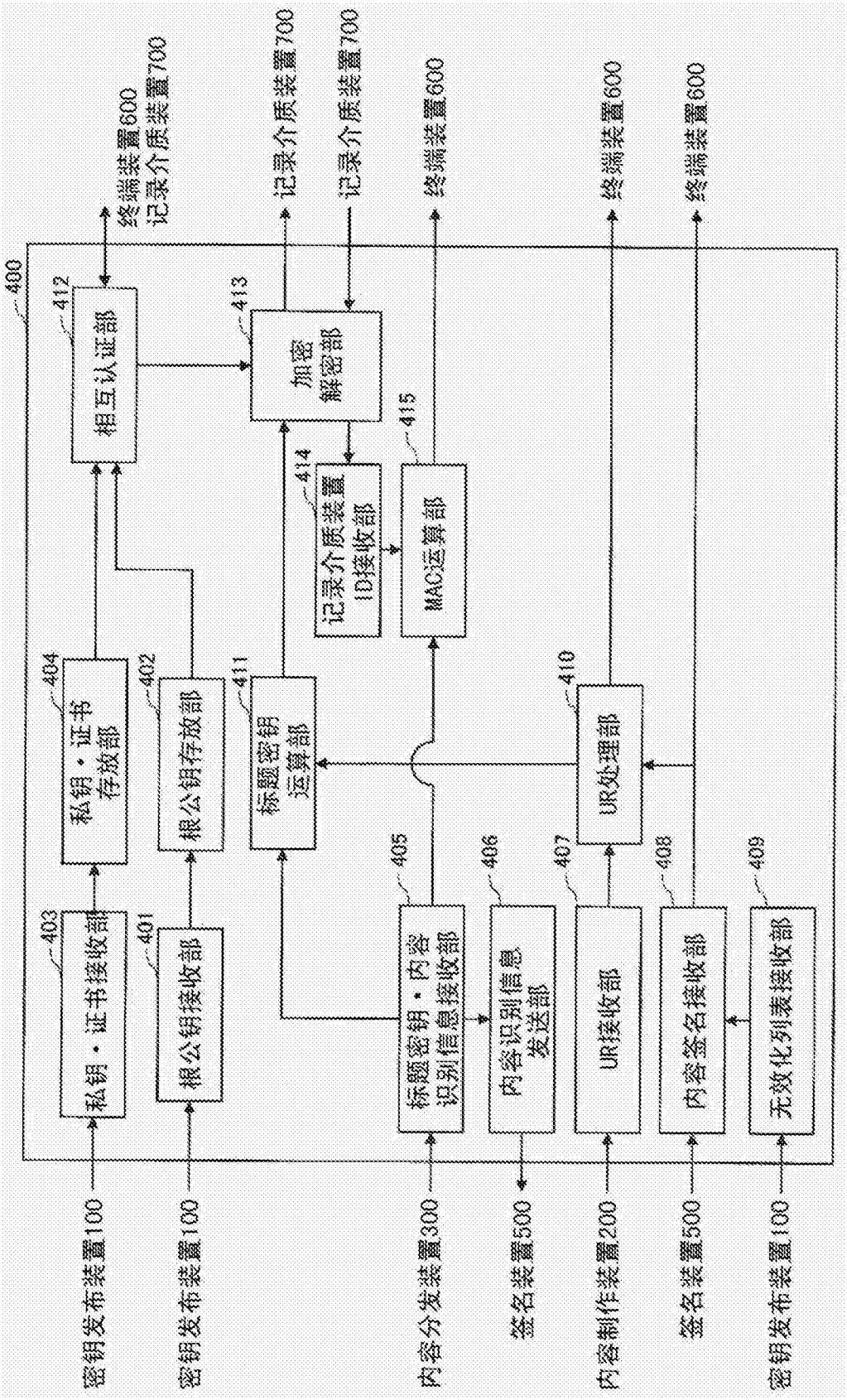

400
密钥发布装置100
密钥发布装置100
内容分发装置300
签名装置500
内容制作装置200
签名装置500
密钥发布装置100
私钥·证书接收部
403
根公钥接收部
401
私钥·证书存放部
404
根公钥存放部
402
标题密钥运算部
411
标题密钥·内容识别信息接收部
405
内容识别信息发送部
406
UR接收部
407
UR处理部
410
内容签名接收部
408
无效化列表接收部
409
记录介质装置ID接收部
414
MAC运算部
415
相互认证部
412
加密解密部
413
终端装置600
记录介质装置700
记录介质装置700
终端装置600
终端装置600
终端装置600

图12

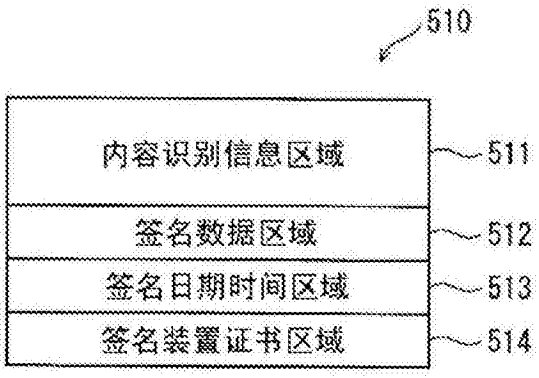

510
内容识别信息区域
511
签名数据区域
512
签名日期时间区域
513
签名装置证书区域
514

图13

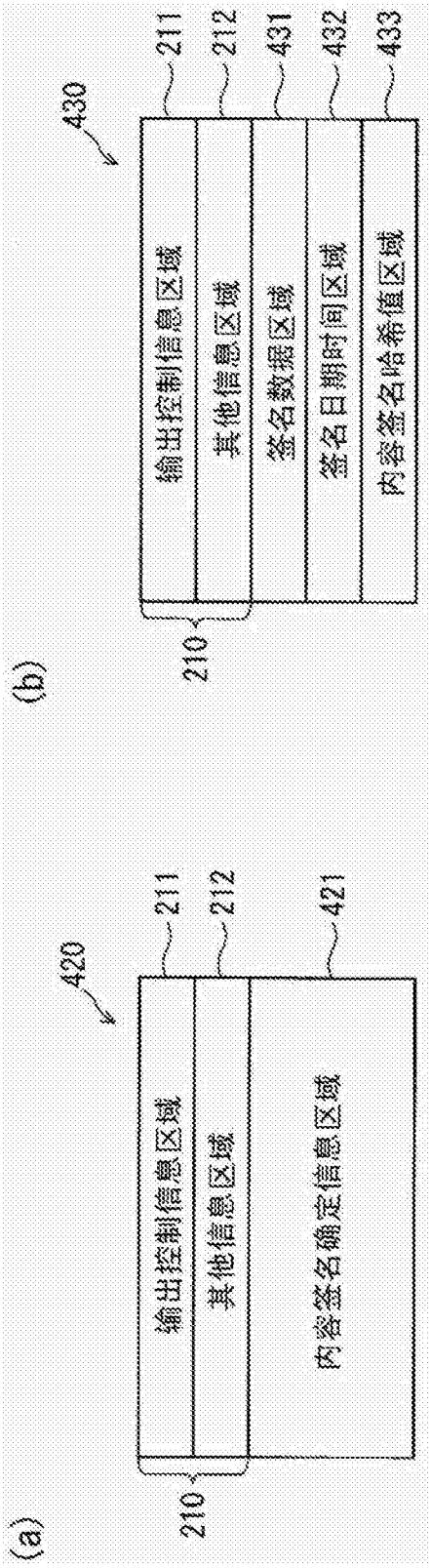

(b)
430
211
212
431
432
433
输出控制信息区域
其他信息区域
签名数据区域
签名日期时间区域
内容签名哈希值区域
210
(a)
420
211
212
421
输出控制信息区域
其他信息区域
内容签名确定信息区域
210

图14

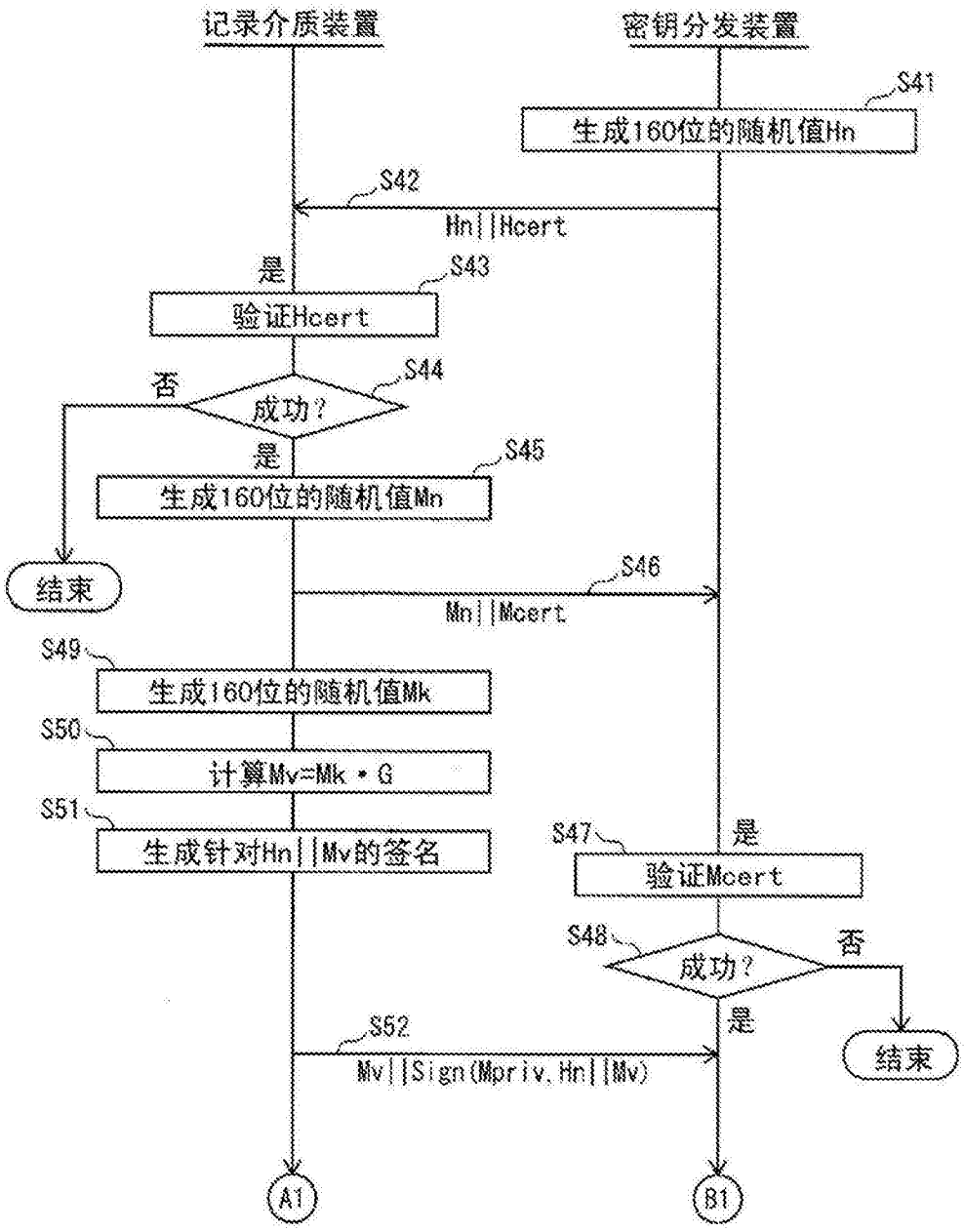

记录介质装置
密钥分发装置
S41
生成160位的随机值Hn
S42
Hn||Hcert
是
S43
验证Hcert
否
S44
成功？
是
S45
生成160位的随机值Mn
结束
S46
Mn||Mcert
S49
生成160位的随机值Mk
S50
计算Mv=Mk * G
S51
生成针对Hn||Mv的签名
S47
是
验证Mcert
S48
成功？
否
是
结束
S52
Mv||Sign(Mpriv,Hn||Mv)
A1
B1

图15

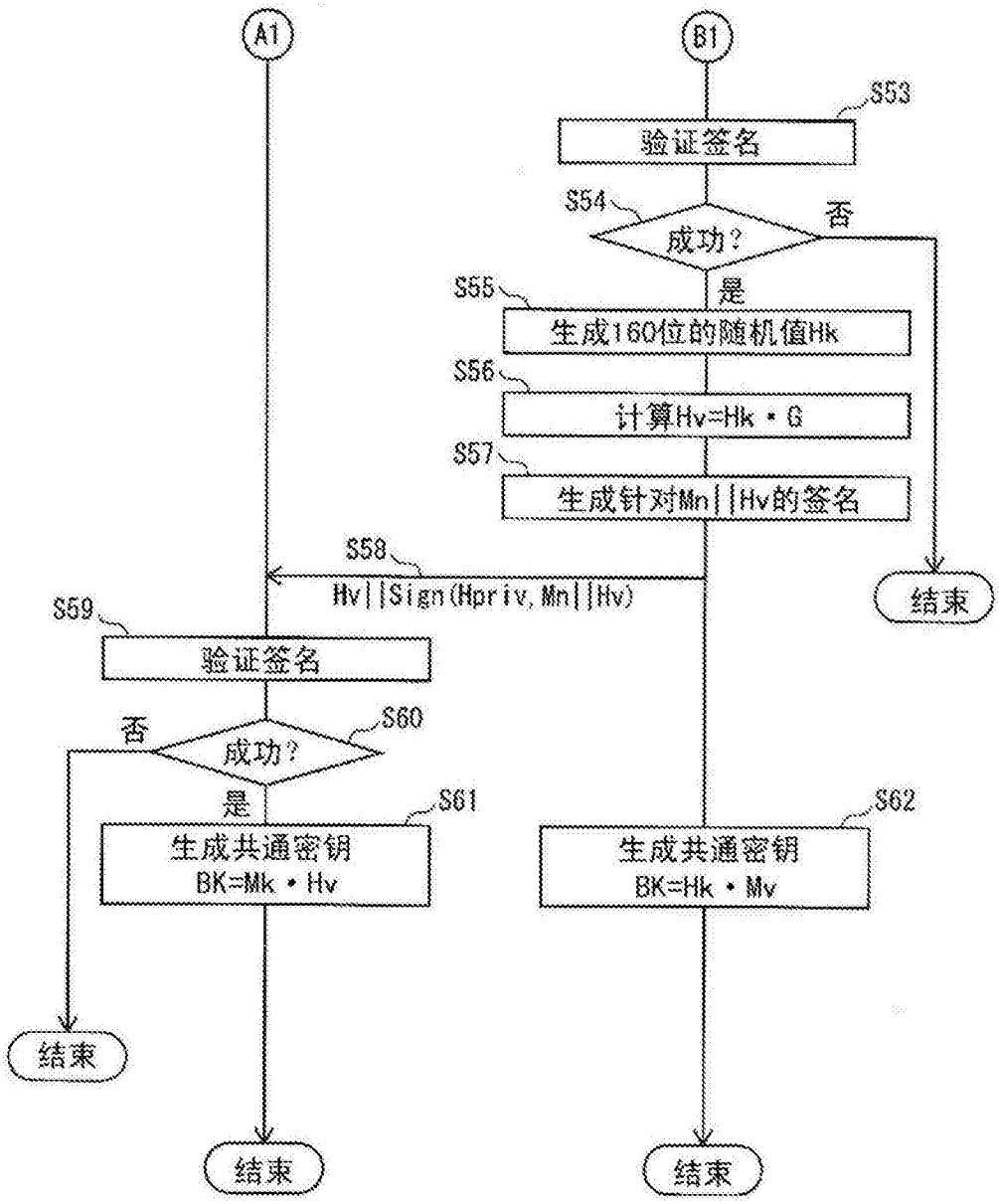

A1
B1
S53
验证签名
S54
成功？
否
是
S55
生成160位的随机值Hk
S56
计算Hv=Hk・G
S57
生成针对Mn||Hv的签名
S58
Hv||Sign(Hpriv,Mn||Hv)
结束
S59
验证签名
S60
成功？
否
是
S61
生成共通密钥
BK=Mk・Hv
S62
生成共通密钥
BK=Hk・Mv
结束
结束
结束

图16

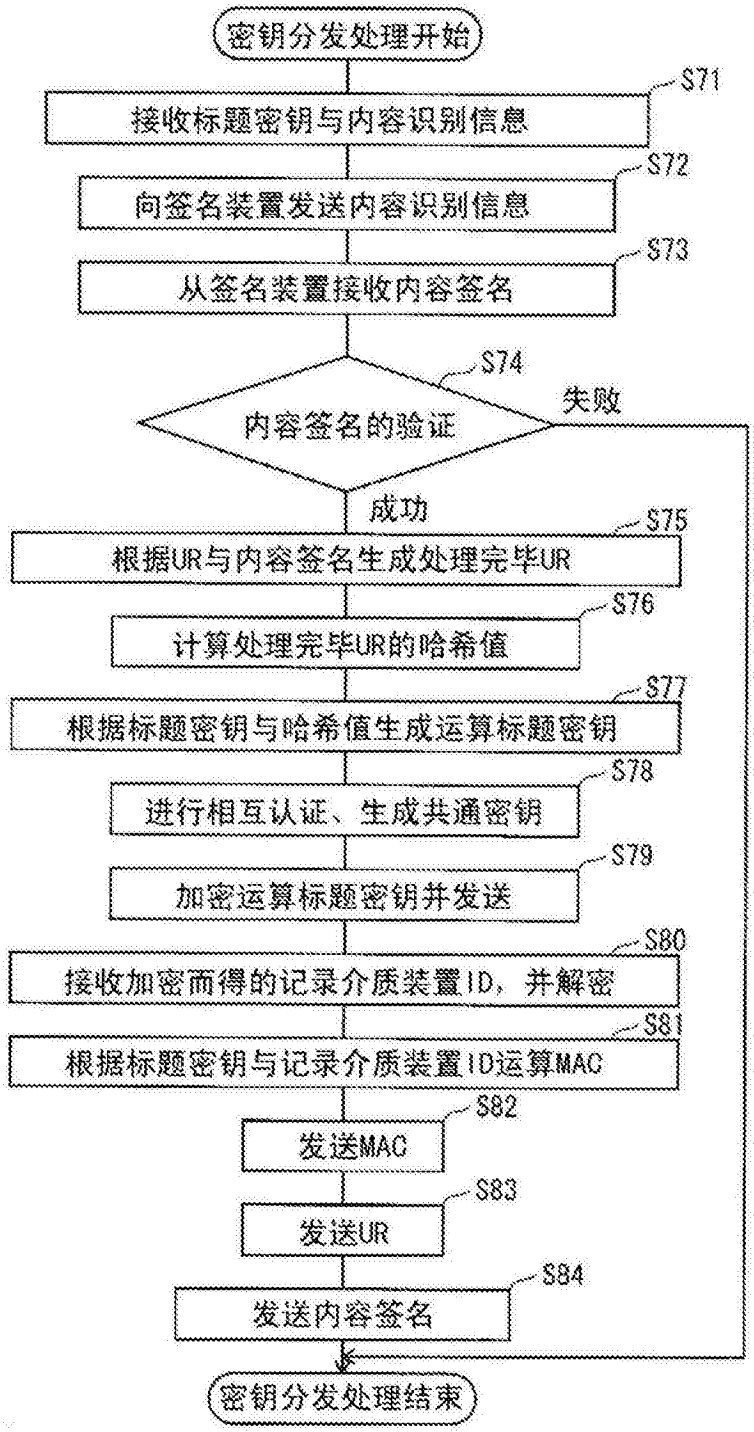

密钥分发处理开始
S71
接收标题密钥与内容识别信息
S72
向签名装置发送内容识别信息
S73
从签名装置接收内容签名
S74
内容签名的验证
失败
成功
S75
根据UR与内容签名生成处理完毕UR
S76
计算处理完毕UR的哈希值
S77
根据标题密钥与哈希值生成运算标题密钥
S78
进行相互认证、生成共通密钥
S79
加密运算标题密钥并发送
S80
接收加密而得的记录介质装置ID，并解密
S81
根据标题密钥与记录介质装置ID运算MAC
S82
发送MAC
S83
发送UR
S84
发送内容签名
密钥分发处理结束

图17

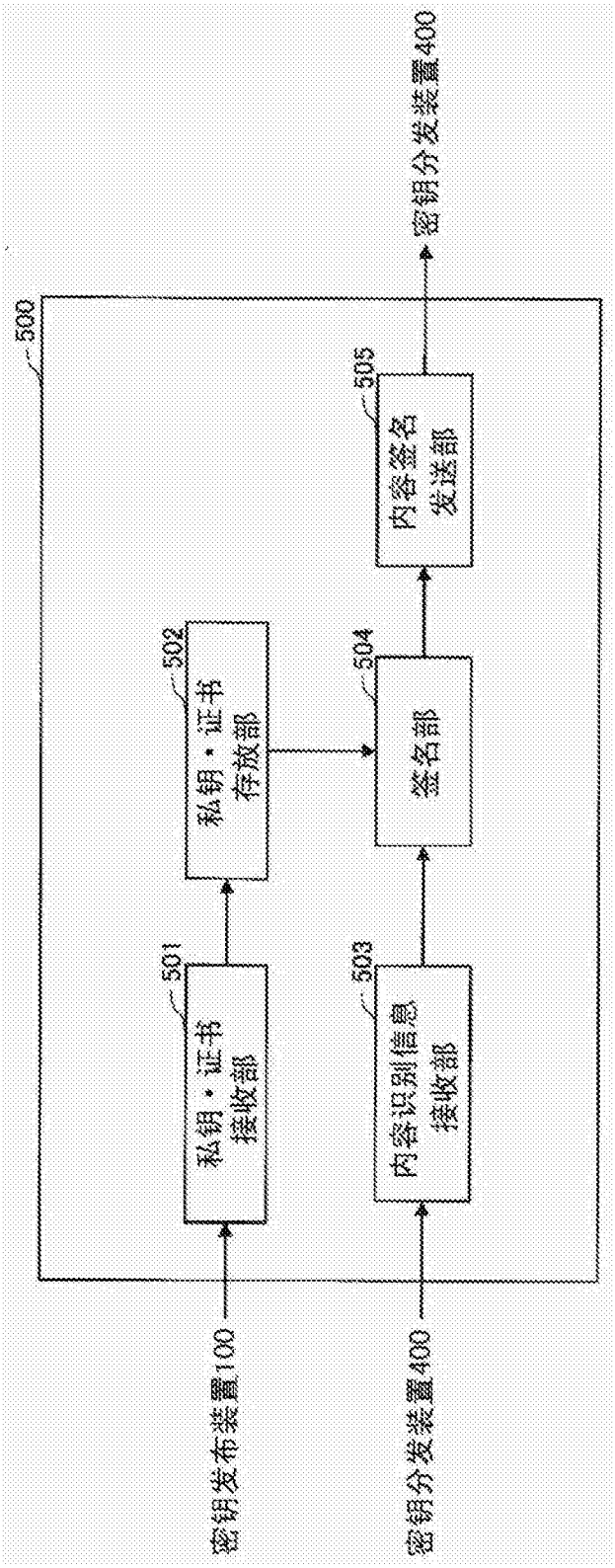

密钥发布装置100
密钥分发装置400
500
501
私钥·证书
接收部
502
私钥·证书
存放部
503
内容识别信息
接收部
504
签名部
505
内容签名
发送部
密钥分发装置400

图18

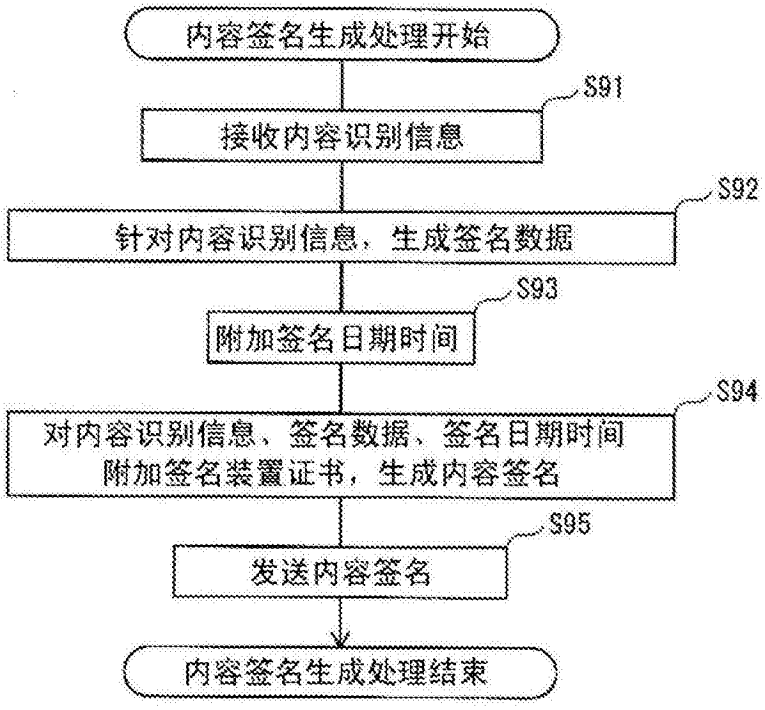

内容签名生成处理开始
S91
接收内容识别信息
S92
针对内容识别信息，生成签名数据
S93
附加签名日期时间
S94
对内容识别信息、签名数据、签名日期时间
附加签名装置证书，生成内容签名
S95
发送内容签名
内容签名生成处理结束

图19

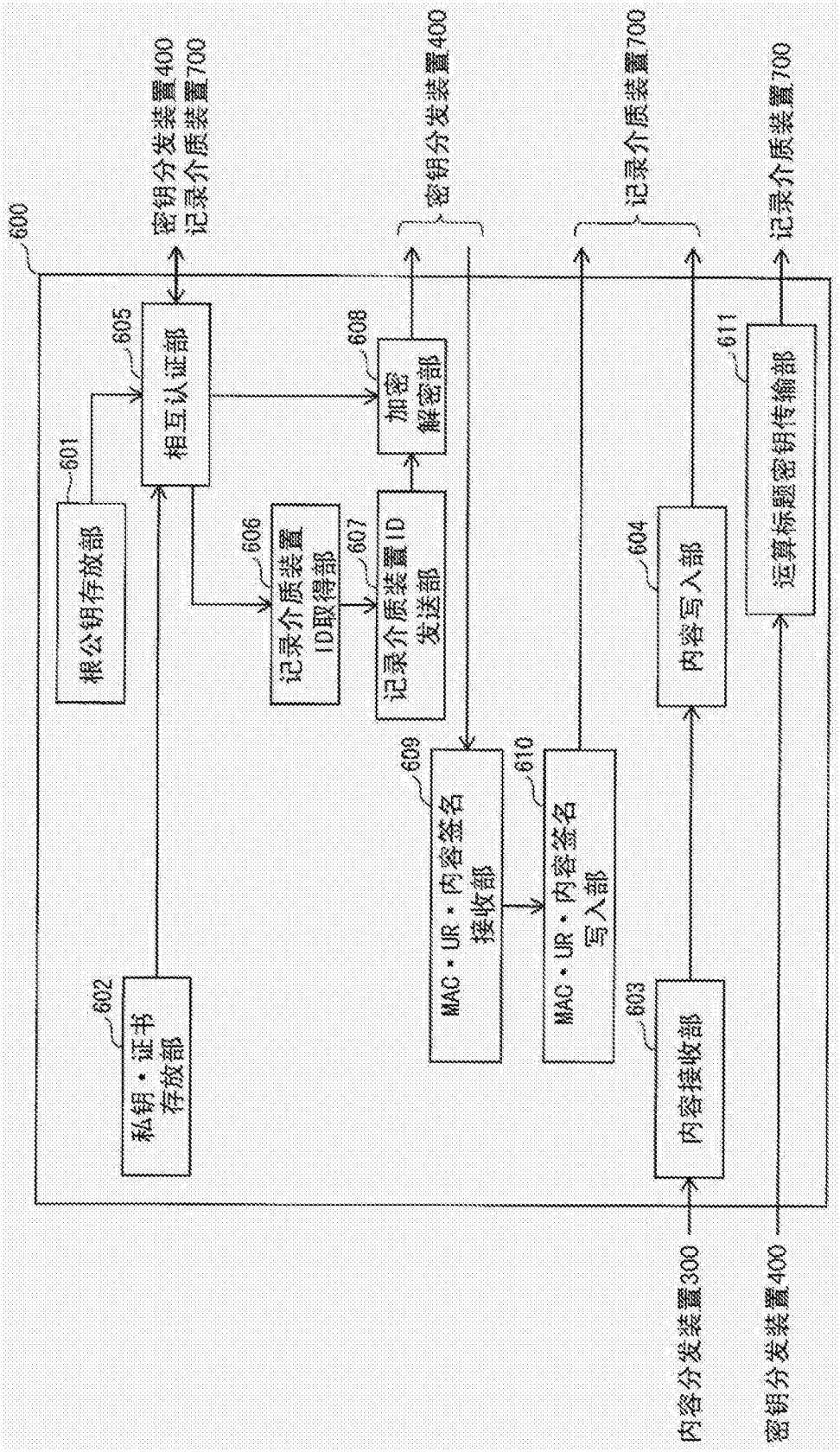

600
密钥分发装置400
记录介质装置700
密钥分发装置400
记录介质装置700
记录介质装置700
605
相互认证部
608
加密
解密部
611
运算标题密钥传输部
601
根公钥存放部
606
记录介质装置
ID取得部
607
记录介质装置ID
发送部
604
内容写入部
609
MAC・UR・内容签名
接收部
610
MAC・UR・内容签名
写入部
602
私钥・证书
存放部
603
内容接收部
内容分发装置300
密钥分发装置400

图20

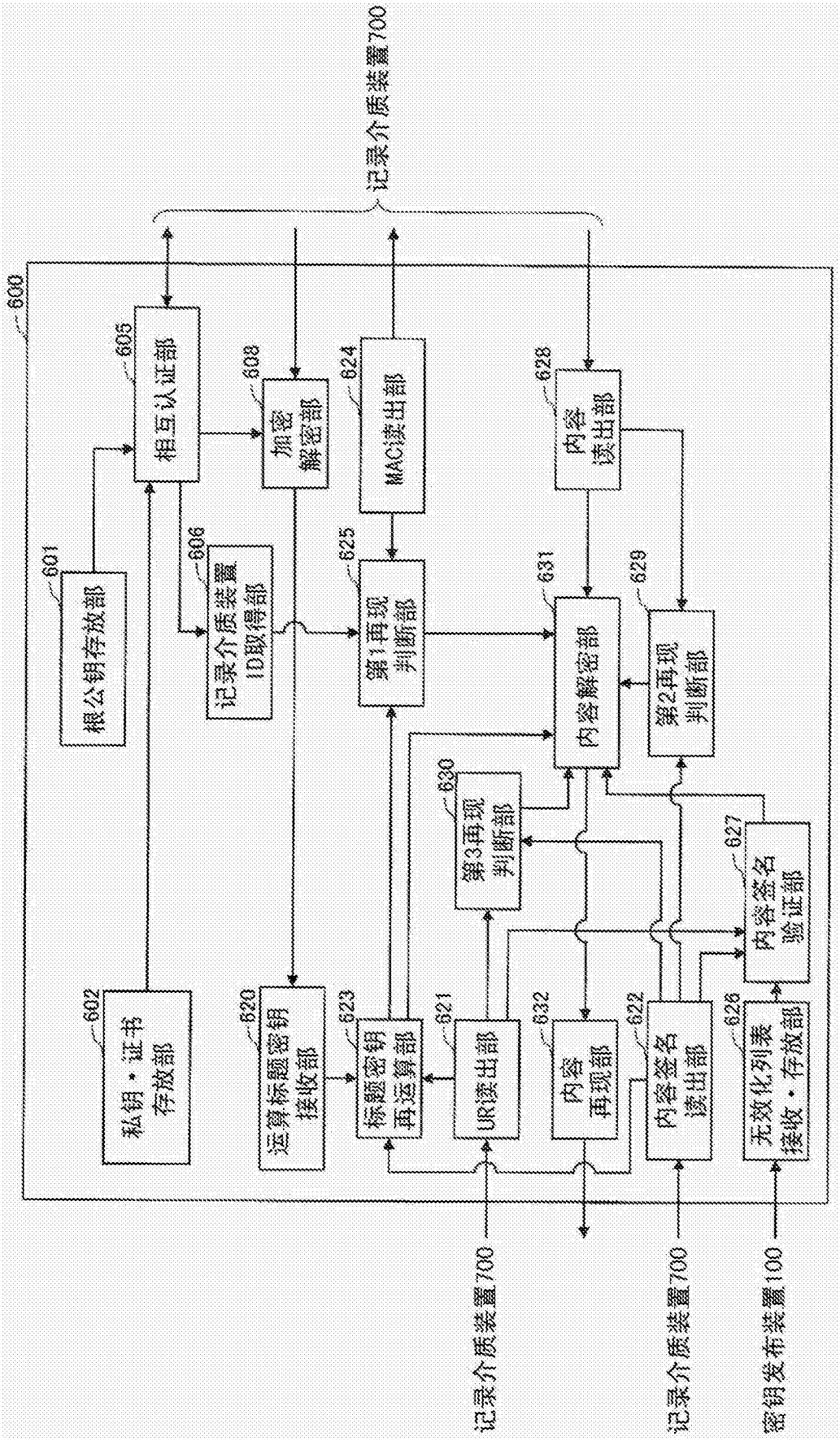

记录介质装置700
600
605
相互认证部
608
加密
解密部
624
MAC读出部
628
内容
读出部
601
根公钥存放部
606
记录介质装置
ID取得部
625
第1再现
判断部
631
内容解密部
629
第2再现
判断部
620
第3再现
判断部
627
内容签名
验证部
602
私钥·证书
存放部
620
运算标题密钥
接收部
623
标题密钥
再运算部
621
UR读出部
632
内容
再现部
622
内容签名
读出部
626
无效化列表
接收·存放部
记录介质装置700
记录介质装置700
密钥发布装置100

图21

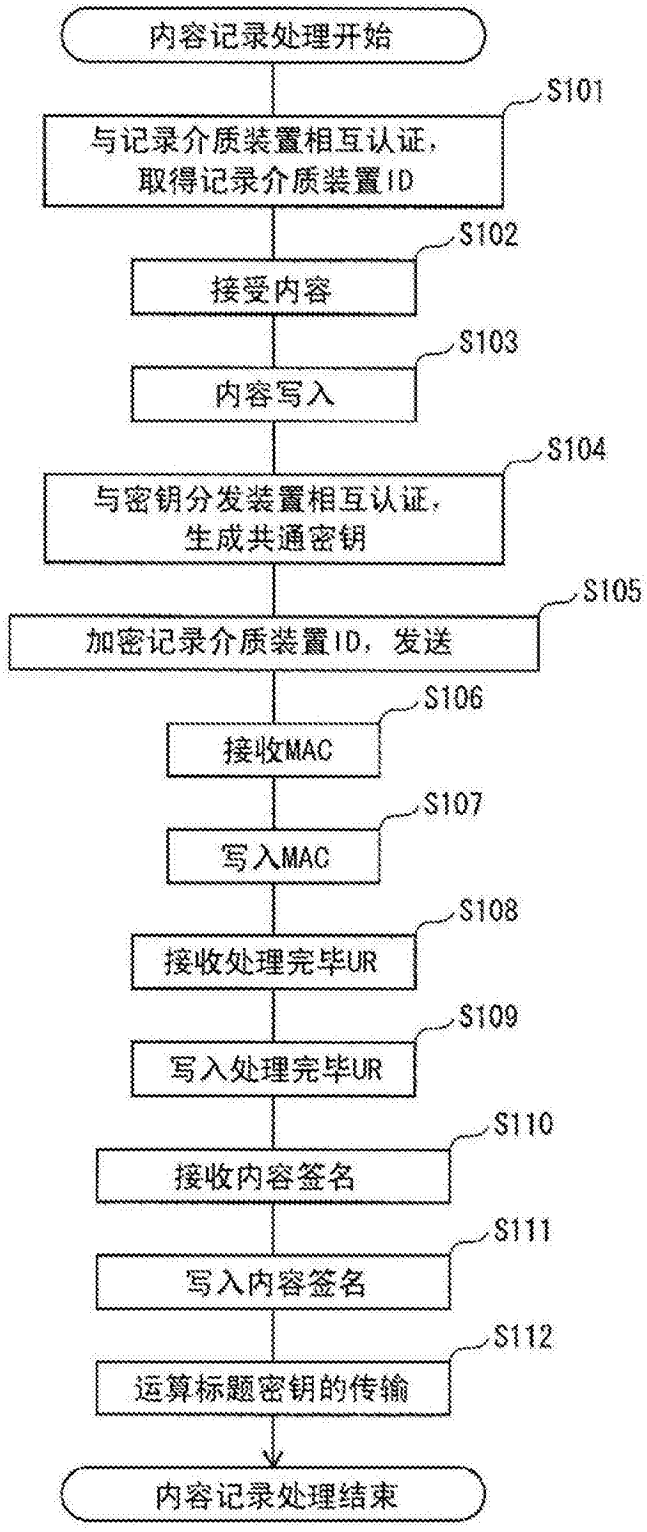

内容记录处理开始
S101
与记录介质装置相互认证，
取得记录介质装置ID
S102
接受内容
S103
内容写入
S104
与密钥分发装置相互认证，
生成共通密钥
S105
加密记录介质装置ID，发送
S106
接收MAC
S107
写入MAC
S108
接收处理完毕UR
S109
写入处理完毕UR
S110
接收内容签名
S111
写入内容签名
S112
运算标题密钥的传输
内容记录处理结束

图22

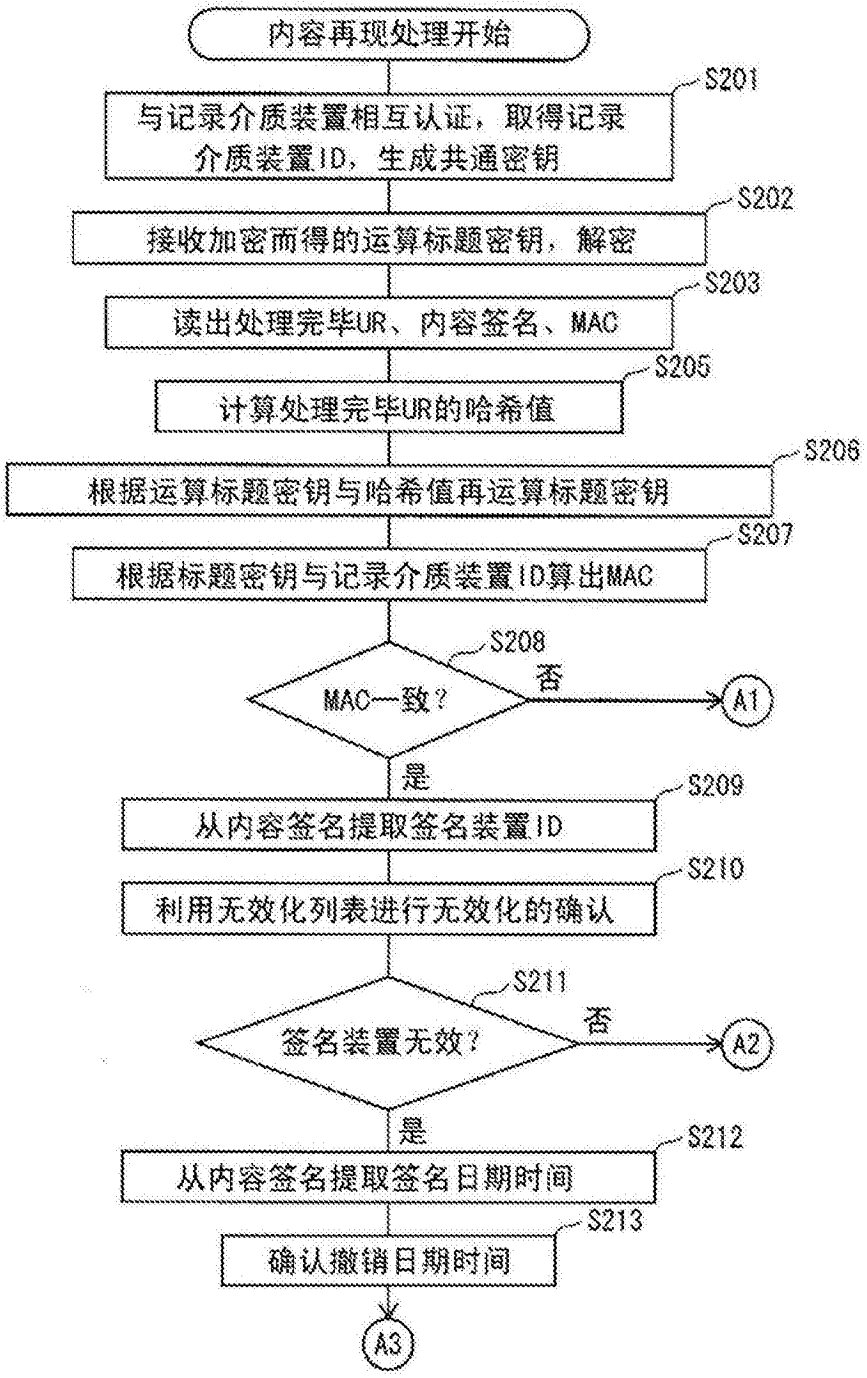

内容再现处理开始
S201
与记录介质装置相互认证，取得记录介质装置ID，生成共通密钥
S202
接收加密而得的运算标题密钥，解密
S203
读出处理完毕UR、内容签名、MAC
S205
计算处理完毕UR的哈希值
S206
根据运算标题密钥与哈希值再运算标题密钥
S207
根据标题密钥与记录介质装置ID算出MAC
S208
MAC一致？
否
A1
是
S209
从内容签名提取签名装置ID
S210
利用无效化列表进行无效化的确认
S211
签名装置无效？
否
A2
是
S212
从内容签名提取签名日期时间
S213
确认撤销日期时间
A3

图23

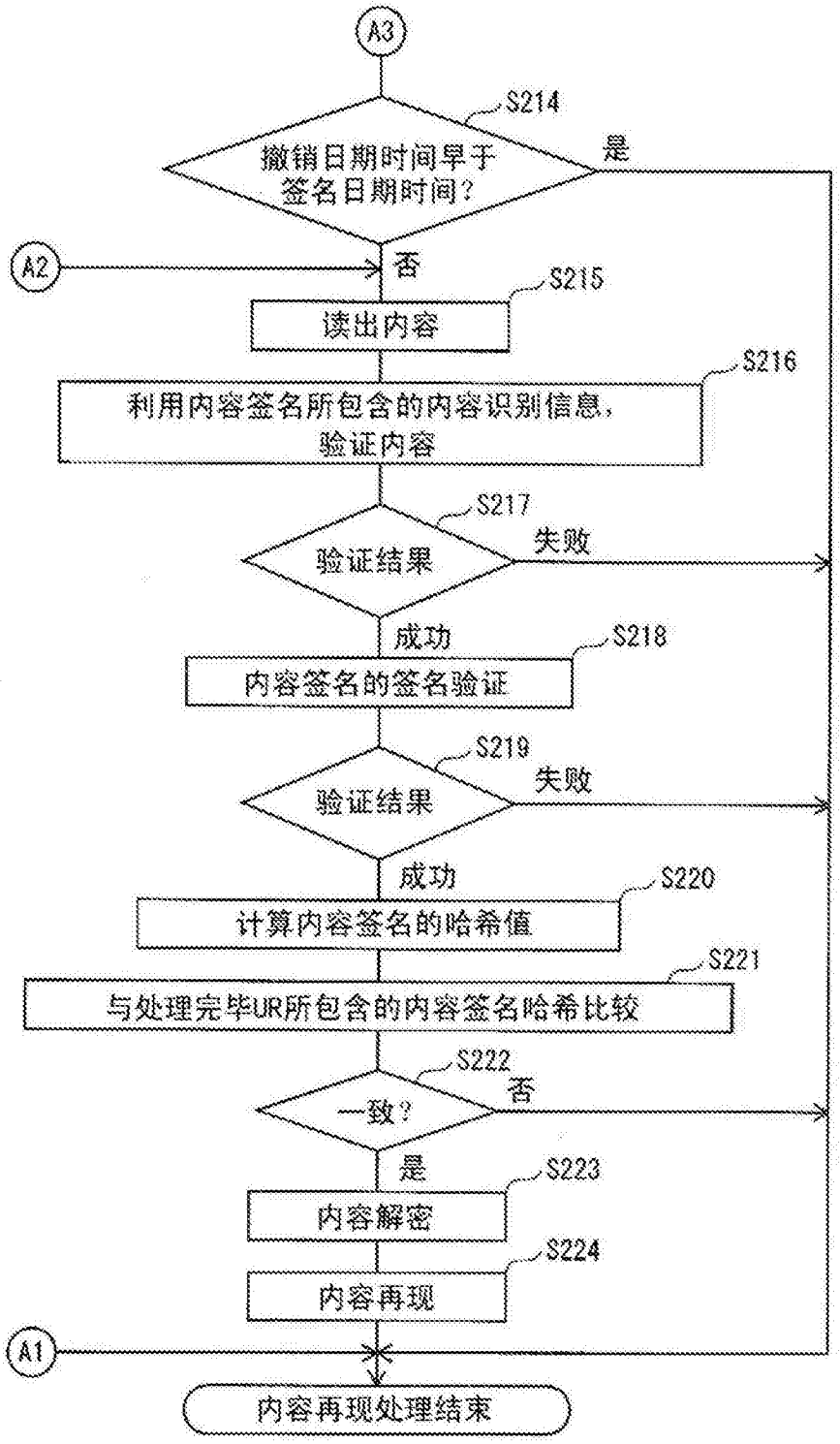

A3
S214
撤销日期时间早于
签名日期时间?
是
A2
否
S215
读出内容
S216
利用内容签名所包含的内容识别信息,
验证内容
S217
验证结果
失败
成功
S218
内容签名的签名验证
S219
验证结果
失败
成功
S220
计算内容签名的哈希值
S221
与处理完毕UR所包含的内容签名哈希比较
S222
一致?
否
是
S223
内容解密
S224
内容再现
A1
内容再现处理结束

图24

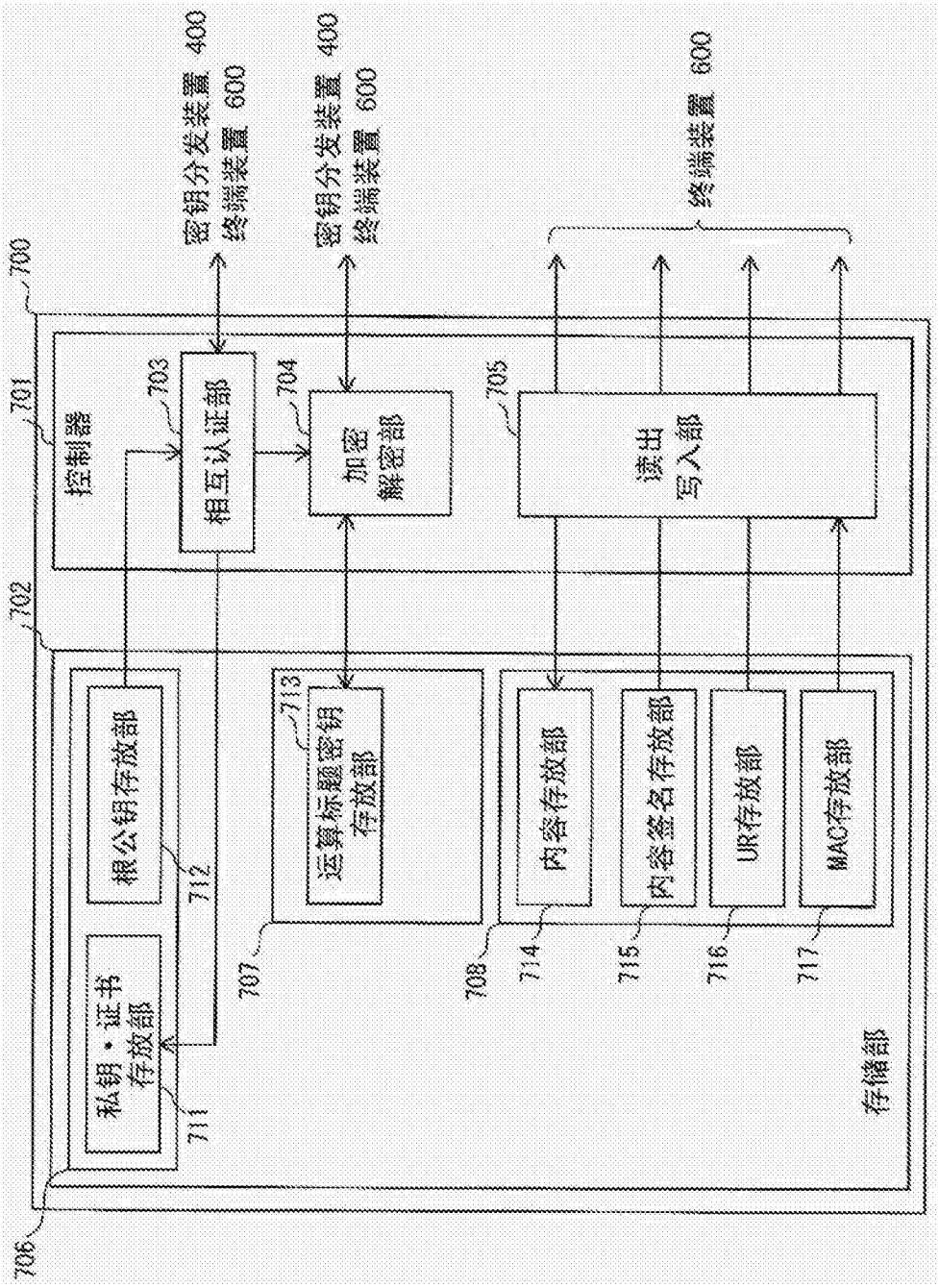

密钥分发装置 400
终端装置 600
密钥分发装置 400
终端装置 600
终端装置 600
700
701
控制器
703
相互认证部
704
加密
解密部
705
读出
写入部
702
根公钥存放部
712
私钥·证书
存放部
711
713
运算标题密钥
存放部
707
内容存放部
708
714
内容签名存放部
715
UR存放部
716
MAC存放部
717
存储部
706

图25

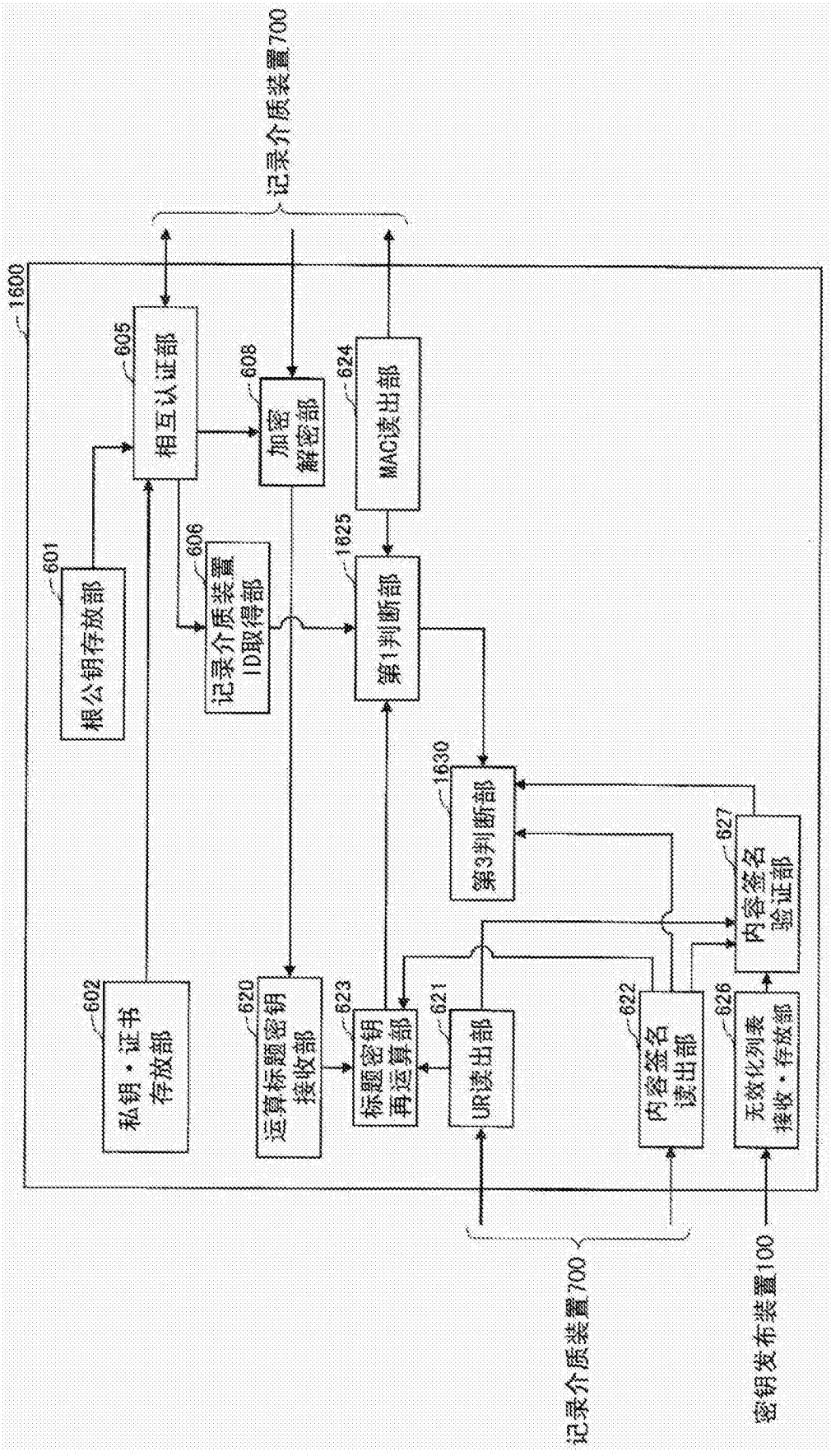

记录介质装置700
1600
相互认证部
605
加密解密部
608
MAC读出部
624
根公钥存放部
601
记录介质装置ID取得部
606
第1判断部
1625
第3判断部
1630
内容签名验证部
627
私钥·证书存放部
602
运算标题密钥接收部
620
标题密钥再运算部
623
UR读出部
621
内容签名读出部
622
无效化列表接收·存放部
626
记录介质装置700
密钥发布装置100

图26

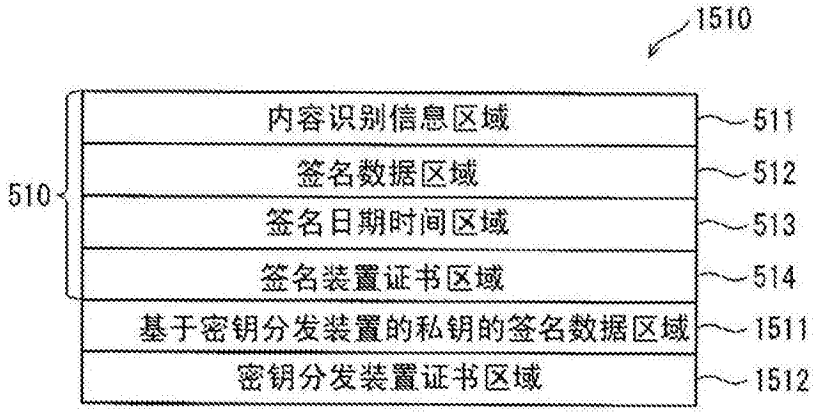

1510
内容识别信息区域
511
签名数据区域
512
510
签名日期时间区域
513
签名装置证书区域
514
基于密钥分发装置的私钥的签名数据区域
1511
密钥分发装置证书区域
1512

图27