



(12) 发明专利申请

(10) 申请公布号 CN 102224704 A

(43) 申请公布日 2011. 10. 19

(21) 申请号 200980140460. 1

(74) 专利代理机构 永新专利商标代理有限公司
72002

(22) 申请日 2009. 11. 12

代理人 陈萍

(30) 优先权数据

2008-290528 2008. 11. 13 JP

(51) Int. Cl.

H04L 9/06 (2006. 01)

(85) PCT申请进入国家阶段日

H04L 9/14 (2006. 01)

2011. 04. 13

(86) PCT申请的申请数据

PCT/JP2009/006033 2009. 11. 12

(87) PCT申请的公布数据

W02010/055658 JA 2010. 05. 20

(71) 申请人 松下电器产业株式会社

地址 日本大阪府

(72) 发明人 兵藤昌彦 岩田彻 栗木悟

佐野正宏

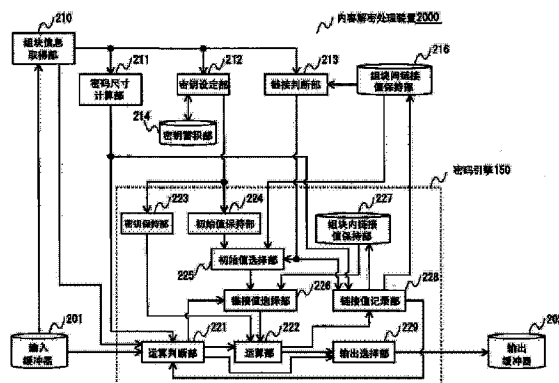
权利要求书 2 页 说明书 35 页 附图 29 页

(54) 发明名称

内容解密处理装置、内容解密处理方法及集成电路

(57) 摘要

内容解密处理装置 (2000) 将对组块的末尾的密码块进行解密时计算出的链接值与内容类型和帧序号建立关联地存储至组块间链接值保持部 (216), 在对组块的开头的密码块进行解密的情况下, 当组块间链接值保持部 (216) 中存在与该组块的内容类型和帧序号相对应地存储着的链接值时, 采用与该组块的内容类型和帧序号相对应地存储在组块间链接值保持部 (216) 的链接值, 对组块的开头的密码块进行解密, 从而即使进行解密的数据流为在属于第 1 种密码帧的密码组块之间存在有属于第 2 种密码帧的密码组块的数据结构, 也能够正确地对数据流进行解密。



1. 一种内容解密处理装置,对数据流进行解密,上述数据流如下形成,即:分类为多个种类的帧分别以链接密码块方式、且以包含多个由链接的密码块列构成的组块的形态被加密,并分割多个密码帧中的各个密码帧,以属于第1种密码帧的密码组块和属于第2种密码帧的密码组块混杂存在的方式,进行流线化而形成,该内容解密处理装置的特征在于,具有:

解密部,利用链接值,依次对上述数据流中包含的密码块进行解密,每当对密码块进行解密时,计算新的链接值;

链接值保持部,用于将密码帧的识别信息和链接值建立关联地存储;以及

链接值记录部,在通过上述解密部对组块的末尾的密码块进行了解密的情况下,将通过上述解密部进行了解密的密码块所属的密码帧的识别信息与该进行了解密的密码块在被解密时通过上述解密部算出的链接值建立关联地记录至上述链接值保持部;

上述解密部参照上述链接值保持部,在要解密的密码块是组块的开头的密码块的情况下,当已对上述要解密的密码块所属的密码帧的一部分进行了解密时,作为对该密码块进行解密时使用的链接值,使用该密码帧的密码块之中的最后解密的密码块在被解密时计算出的链接值。

2. 如权利要求1记载的内容解密处理装置,其特征在于,

上述链接值保持部包括组块内链接值保持部,该组块内链接值保持部用于存储链接值;

在通过上述解密部对密码块进行了解密的情况下,当对不是组块的末尾的密码块进行了解密时,上述链接值记录部用上述解密部所计算出的链接值覆盖至上述组块内链接值保持部中存储着的链接值并记录;

在要解密的密码块不是组块的开头的密码块的情况下,上述解密部利用上述组块内链接值保持部中记录着的链接值,对密码块进行解密。

3. 如权利要求1记载的内容解密处理装置,其特征在于,

上述链接值记录部在将密码帧的识别信息与链接值建立关联地记录至上述链接值保持部的情况下,按每种密码帧,将表示密码帧的信息和链接值覆盖并记录至上述链接值保持部。

4. 如权利要求1记载的内容解密处理装置,其特征在于,还具备:

数据赋予部,在作为上述解密部的解密对象的密码块小于规定的比特数的情况下,对该密码块赋予赋予数据,以使该密码块成为上述规定的比特数;

解密数据保持部,用于存储通过上述解密部进行了解密的密码块;以及

解密数据记录部,将通过上述解密部进行了解密的密码块的一部分记录至上述解密数据保持部;

在作为上述解密部的解密对象的密码块小于上述规定的比特数的情况下,上述数据赋予部对作为上述解密对象的密码块赋予赋予数据,生成上述规定的比特数的合成密码块,上述解密部替代上述解密对象的密码块而解密上述合成密码块,上述解密数据记录部将通过上述解密部进行了解密的合成密码块之中的、除了通过上述解密部对上述数据赋予部所赋予的赋予数据的部分进行解密从而得到的部分以外的部分,记录至上述解密数据保持部。

5. 一种内容解密处理方法,使内容解密处理装置对数据流进行解密,该内容解密处理装置具备用于将密码帧的识别信息与链接值建立关联地存储的链接值保持部,上述数据流如下形成,即:分类为多个种类的帧分别以链接密码块方式、且以包含多个由链接的密码块列构成的组块的形态被加密,并分割多个密码帧中的各个密码帧,以属于第1种密码帧的密码组块和属于第2种密码帧的密码组块混杂存在的方式,进行流线化而形成,该内容解密处理方法的特征在于,具有:

解密步骤,上述内容解密处理装置的解密部利用链接值,依次对上述数据流中包含的密码块进行解密,每当对密码块进行解密时,计算新的链接值;以及

链接值记录步骤,上述内容解密处理装置的链接值记录部在通过上述解密部对组块的末尾的密码块进行了解密的情况下,将通过上述解密步骤进行了解密的密码块所属的密码帧的识别信息与该进行了解密的密码块在被解密时通过上述解密部算出的链接值建立关联地记录至上述链接值保持部;

上述解密步骤参照上述链接值保持部,在要解密的密码块是组块的开头的密码块的情况下,当已对上述要解密的密码块所属的密码帧的一部分进行了解密时,作为对该密码块进行解密时使用的链接值,使用该密码帧的密码块之中的最后解密的密码块在被解密时计算出的链接值。

6. 一种集成电路,对数据流进行解密,上述数据流如下形成,即:分类为多个种类的帧分别以链接密码块方式、且以包含多个由链接的密码块列构成的组块的形态被加密,并分割多个密码帧中的各个密码帧,以属于第1种密码帧的密码组块和属于第2种密码帧的密码组块混杂存在的方式,进行流线化而形成,该集成电路的特征在于,具有:

解密部,利用链接值,依次对上述数据流中包含的密码块进行解密,每当对密码块进行解密时,计算新的链接值;

链接值保持部,用于将密码帧的识别信息和链接值建立关联地存储;以及

链接值记录部,在通过上述解密部对组块的末尾的密码块进行了解密的情况下,将通过上述解密部进行了解密的密码块所属的密码帧的识别信息与该进行了解密的密码块在被解密时通过上述解密部算出的链接值建立关联地记录至上述链接值保持部;

上述解密部参照上述链接值保持部,在要解密的密码块是组块的开头的密码块的情况下,当已对上述要解密的密码块所属的密码帧的一部分进行了解密时,作为对该密码块进行解密时使用的链接值,使用该密码帧的密码块之中的最后解密的密码块在被解密时计算出的链接值。

内容解密处理装置、内容解密处理方法及集成电路

技术领域

[0001] 本发明涉及内容解密处理装置,对通过密码链接块(暗号連鎖ブロック, ciphertext block chaining)方式而加密了的密码数据进行解密。

背景技术

[0002] 为了防止对经由信息通信网络而进行通信的数字数据、蓄积在光盘等介质中的数字数据等的不正当利用,经常对这些数字数据进行加密使其成为密码数据,从而使第三者无法直接使用。

[0003] 作为对数字数据进行加密的方式之一,有所谓的密码链接块方式,即,将密码对象数据分割为多个明文块(平文ブロック)来进行加密,使得前一个明文块的加密不对其下一个明文块的加密带来影响,从而链接式地对各明文块进行密码处理。

[0004] 在密码链接块方式中,各明文块利用对在前一个明文块的加密时使用的链接值进行规定的运算处理从而得到的链接值,进行加密。

[0005] 通过该密码链接块方式而加密后的密码数据,以通过加密明文块而得的密码块按加密顺序排列而构成。

[0006] 在密码链接块方式中,各密码块利用对在前一个密码块的解密时使用的链接值进行规定的运算处理而得的链接值,进行解密。

[0007] 作为对通过密码链接块方式而加密了的密码数据进行解密的技术,例如提出了以下等技术:对密码块解密时,与密码块的解密处理并行地生成下一个密码块的解密所需的链接值,从而使下一个密码块的解密开始时刻提前(参照专利文献1)。

[0008] 现有技术文献

[0009] 专利文献

[0010] 专利文献1:特开2000-295212号公报

发明概要

[0011] 发明所要解决的问题

[0012] 另一方面,作为将由视频帧构成的视频数据流与由音频帧构成的音频数据流作为一个数据流来处理的手法,有将视频数据流与音频数据流分割复用而成为一个新数据流的手法。

[0013] 在这样的手法中,分割复用前的视频数据流与音频数据流是分别按每帧以密码链接块方式而被加密的数据流的情况下,分割复用后的数据流中,在进行着密码链接的密码块列(例如加密后的视频帧的密码块列)之间,有时会存在与其密码帧独立地进行了密码链接的密码块列(例如加密后的音频帧的密码块列)。

[0014] 对这样的数据流进行解密的内容解密处理装置,需要能够对如下解密对象的数据流进行解密,该数据流具有如下数据结构:在与属于第1种密码帧(例如加密后的视频帧)的链接的密码块列(以下称作“密码组块”)之间存在属于第2种密码帧(例如加密后的音

频帧)的密码组块。

[0015] 但是,当对密码块进行解密时,在具有利用仅对数据流上的前一个密码块的解密时所使用的链接值进行规定的运算处理从而得到的链接值来对密码块进行解密的结构的内容解密处理装置中,无法解密这样的数据流。

发明内容

[0016] 因此,本发明目的在于提供一种内容解密处理装置,即使解密的数据流是在属于第1种密码帧的密码组块之间存在属于第2种密码帧的密码组块这样的数据结构的数据流,也能够按数据流的密码块顺序来解密该数据流。

[0017] 解决问题所采用的手段

[0018] 为了解决上述技术问题,本发明的内容解密处理装置对流线化而成的数据流进行解密,上述数据流是通过如下方式得到的数据流,即:以密码块链接方式并以包含多个由进行链接的密码块列构成的组块的形态,对分类为多个种类的帧各自进行加密,并分别分割多个密码帧,以使得属于第1种密码帧的密码组块和属于第2种密码帧的密码组块混杂存在,该内容解密处理装置的特征在于,具有:解密部,利用链接值,依次对上述数据流中包含的密码块进行解密,每当对密码块进行解密,就计算新的链接值;链接值保持部,用于将密码帧的识别信息和链接值建立关联地进行存储;以及链接值记录部,在通过上述解密部对组块的末尾的密码块进行了解密的情况下,将通过上述解密部而解密的密码块所属的密码帧的识别信息与在该解密的密码块的解密时通过上述解密部算出的链接值建立关联地记录到上述链接值保持部;上述解密部参照上述链接值保持部,在进行解密的密码块是组块的开头的密码块的情况下,当已对上述进行解密的密码块所属的密码帧的一部分进行了解密时,作为对该密码块进行解密时使用的链接值,采用该密码帧的密码块中最后解密的密码块的解密时计算出的链接值。

[0019] 发明效果

[0020] 具备上述结构的本发明的内容解密处理装置中,链接值记录部在通过上述解密部对组块的末尾的密码块进行了解密的情况下,将通过上述解密部而解密的密码块所属的密码帧的识别信息与在该解密的密码块的解密时通过上述解密部算出的链接值建立关联地记录到上述链接值保持部,解密部参照上述链接值保持部,在进行解密的密码块是组块的开头的密码块的情况下,当已对上述进行解密的密码块所属的密码帧的一部分进行了解密时,作为对该密码块进行解密时使用的链接值,采用该密码帧的密码块中最后解密的密码块的解密时计算出的链接值,因此,具有如下效果,即:即使进行解密的数据流为在属于第1种密码帧的密码组块之间存在有属于第2种密码帧的密码组块的数据结构,也能够正确地对数据流进行解密。

[0021] 此外,例如,即使是以下解密处理装置,即:依次从数据流中仅提取所有属于第1种密码帧的密码组块并依次对提取出的密码组块进行解密,并且依次从数据流中仅提取所有第2种密码帧并与第1种密码帧的解密独立地依次对提取出的第2种密码帧进行解密,也能够正确地对数据流进行解密,但是,该解密处理装置需要从数据流整体中按类别地分离并提取所有密码帧的工序,并且,需要用于按类别地暂时存储所提取出的密码块的存储区域。

[0022] 与此相反,具备上述结构的本发明的内容解密处理装置中,不需要按类别地提取所有密码帧的工序,此外,不需要用于按类别地存储所提取出的密码帧的存储区域。

[0023] 此外,也可以具有如下特征:上述链接值保持部包含用于存储链接值的组块内链接值保持部,在通过上述解密部对密码块进行了解密的情况下,当对不是组块的末尾的密码块进行了解密时,上述链接值记录部用上述解密部所计算出的链接值对上述组块内链接值保持部中存储着的链接值进行覆盖并记录,上述解密部在进行解密的密码块不是组块的开头的密码块的情况下,利用上述组块内链接值保持部中记录着的链接值,对密码块进行解密。

[0024] 通过采用这样的结构,组块内链接值保持部仅覆盖并存储链接值,因此具有如下效果,即:提供一种内容解密处理装置,将组块内链接值保持部所需要的存储容量限定为存储 1 个链接值所需要的存储容量。

[0025] 此外,也可以具有如下特征:在将密码帧的识别信息和链接值建立关联地向上述链接值保持部中记录的情况下,上述链接值记录部按每种密码帧,将表示密码帧的信息和链接值覆盖并记录到上述链接值保持部。

[0026] 通过采用这样的结构,链接值保持部按每种密码帧来覆盖并记录表示密码帧的信息和链接值,因此具有如下效果,即:提供一种内容解密处理装置,能够将链接值保持部所需要的存储容量限定为,按每种密码帧来关联地存储表示 1 个密码帧的信息、及 1 个链接值所需要的存储容量。

[0027] 此外,也可以还具备:数据赋予部,在作为上述解密部的解密对象的密码块小于规定的比特数的情况下,将赋予数据赋予到该密码块,以使该密码块成为上述规定的比特数;解密数据保持部,用于存储上述解密部所解密的密码块;以及解密数据记录部,将上述解密部所解密的密码块的一部分记录到上述解密数据保持部;在作为上述解密部的解密对象的密码块小于上述规定的比特数的情况下,上述数据赋予部将赋予数据赋予到作为上述解密对象的密码块,生成上述规定的比特数的合成密码块,上述解密部替代上述解密对象的密码块而解密上述合成密码块,上述解密数据记录部将从上述解密部所解密的合成密码块中、除了通过上述解密部对上述数据赋予部所赋予的赋予数据的部分进行解密从而得到的部分以外的部分,记录到上述解密数据保持部。

[0028] 这里,所谓规定的比特数,是指解密部能够解密的密码块的比特数。

[0029] 通过采用这样的结构,即使在作为解密对象的密码块的一部分比特缺失而成为小于规定的比特数的密码块的情况下,将赋予数据赋予到密码块,从而解密部对成为规定的比特数的合成密码块进行解密,将从解密的合成密码块中、除了通过对赋予数据的部分进行解密而得到的部分以外的部分记录到解密数据保持部,因此具有如下效果,即:提供一种内容解密处理装置,即使是小于规定的比特数的密码块,也能够对该密码块进行解密并记录到解密数据保持部。

附图说明

[0030] 图 1 是表示再生机 1000 的模块结构的模块图。

[0031] 图 2 是表示内容的数据结构的数据结构图。

[0032] 图 3 是表示组块 310 的数据结构的数据结构图。

- [0033] 图 4 是表示内容解密处理装置 2000 的功能结构的模块图。
- [0034] 图 5 是表示密钥蓄积部 214 所保持的信息的图。
- [0035] 图 6 是表示组块间链接值保持部 216 所保持的信息的图。
- [0036] 图 7 是表示运算部 222 的功能结构的模块图。
- [0037] 图 8 是内容解密处理装置 2000 的内容解密动作的流程图。
- [0038] 图 9 是表示组块 1050 的数据结构的数据结构图。
- [0039] 图 10 是表示内容头所包含的信息的图。
- [0040] 图 11 是表示内容解密处理装置 3000 的功能结构的模块图。
- [0041] 图 12 是内容解密处理装置 3000 的内容解密动作的流程图。
- [0042] 图 13 是表示内容数据的数据结构的数据结构图。
- [0043] 图 14 是表示内容解密处理装置 4000 的功能结构的模块图。
- [0044] 图 15 是表示组块间链接值保持部 1316 所保持的信息的图。
- [0045] 图 16 是表示密码块的前半部缺失的情况下,前处理部 1301、运算部 222 与后处理部 1302 所进行的处理的动作的图。
- [0046] 图 17 是表示密码块的后半部缺失的情况下,前处理部 1301、运算部 222 与后处理部 1302 所进行的处理的动作的图。
- [0047] 图 18 是表示密码块中没有缺失的情况下,前处理部 1301、运算部 222 与后处理部 1302 所进行的处理的动作的图。
- [0048] 图 19 是内容解密处理装置 4000 的内容解密动作的流程图之一。
- [0049] 图 20 是内容解密处理装置 4000 的内容解密动作的流程图之二。
- [0050] 图 21 是表示组块 2250 的数据结构的数据结构图。
- [0051] 图 22 是表示内容解密处理装置 5000 的功能结构的模块图。
- [0052] 图 23 是表示密钥蓄积部 2114 所保持的信息的图。
- [0053] 图 24 是内容解密处理装置 5000 的内容解密动作的流程图。
- [0054] 图 25 是表示内容解密处理装置 6000 的功能结构的模块图。
- [0055] 图 26 是表示帧序号蓄积部 2522 所保持的信息的图。
- [0056] 图 27 是表示密码信息蓄积部 2530 所保持的信息的图。
- [0057] 图 28 是内容解密处理装置 6000 的内容解密动作的流程图之一。
- [0058] 图 29 是内容解密处理装置 6000 的内容解密动作的流程图之二。
- [0059] 图 30 是表示再生机 1000 的硬件结构的模块图。

具体实施方式

- [0060] (实施方式 1)
- [0061] 以下,作为本发明的内容解密处理装置的一个实施方式,说明对以密码链接块方式被加密了的内容进行解密的内容解密处理装置。
- [0062] 这里,被加密了的内容是指如下内容:分别按每帧,以密码链接块方式,对由视频帧构成的视频数据流和由音频帧构成的音频数据流加密,对加密后的视频数据流和加密后的音频数据流进行分割复用而成为一个新数据流。
- [0063] 即使解密对象的数据流的数据结构为如下数据结构,该内容解密处理装置也能够

正确的解密数据流,上述数据结构为:在与属于第1种密码帧(例如加密后的视频帧)的链接的密码块列所构成的密码组块之间,存在属于第2种密码帧(例如加密后的音频帧)的密码块列所构成的密码组块。

[0064] 下面,参照附图说明本实施方式的内容解密处理装置的结构。

[0065] (结构)

[0066] (再生机 1000)

[0067] 图 1 是表示具备本实施方式的内容解密处理装置 2000 的再生机 1000 的模块结构的模块图。

[0068] 再生机 1000 是个人计算机,由 CPU(Central Processing Unit:中央运算处理装置)模块 110、存储器模块 120、周边设备模块 130、总线 140、密码引擎 150、AV 解码器 160 构成。

[0069] CPU 模块 110 由 CPUA111 与 CPUB112 这 2 个 CPU 构成。

[0070] CPUA111 与 CPUB112 与总线 140 连接,通过执行存储器模块 120 存储的程序,从而利用存储器模块 120、周边设备模块 130、密码引擎 150、AV 解码器 160,实现从记录介质读出加密后的数据流的功能、对加密后的数据流进行解密的功能、对编码后的数据流进行解码的功能等。

[0071] CPUA111 与 CPUB112 相互协调且并行地动作,从而实现上述功能。

[0072] 存储器模块 120 由 ROM(Read Only Memory)121 与 RAM(Random Access Memory)122 构成。

[0073] ROM121 与总线 140 连接,存储有:规定 CPUA111 的动作的程序、规定 CPUB112 的动作的程序、CPUA111 与 CPUB112 所利用的数据。

[0074] RAM122 与总线 140 连接,暂时存储随着 CPUA111 与 CPUB112 执行程序而产生的数据,还暂时存储从周边设备模块 130 读取的数据。

[0075] 周边设备模块 130 由硬盘装置 131、硬盘装置接口 141、读取写入装置 132、读取写入装置接口 142、输出装置 133、输出装置接口 143、输入装置 134、输入装置接口 144、通信装置 135 构成。

[0076] 密码引擎 150 是具有对加密后的数据进行解密的功能的 DSP(Digital Signal Processor,数字信号处理器),由 CPUA111 与 CPU112B 控制,与总线 140 连接。

[0077] AV 解码器 160 是对编码后的视频数据及音频数据进行解码的 DSP,由 CPUA111 与 CPU112B 控制,具有 MPEG(Moving Picture Experts Group,动态图像专家组)2 解码功能、MPEG4 解码功能、MPEG4-AVC 解码功能。

[0078] 再生机 1000 中,通过由输出装置 133 输出 AV 解码器 160 解码后的结果,从而对内容进行再生。

[0079] 硬盘装置 131 由 CPUA111 与 CPU112B 控制,具有向内置的硬盘写入内容的功能、以及读取在内置的硬盘中写入的内容的功能,经由硬盘装置接口 141 而与总线 140 连接。

[0080] 硬盘装置接口 141 用于对硬盘装置 131 与总线 140 之间的信号的交换(やりとり)进行中介。

[0081] 读取写入装置 132 由 CPUA111 与 CPU112B 控制,具有向外部记录介质 137 写入内容的功能、以及读取在外部记录介质 137 中写入的内容的功能,经由读取写入装置接口 142

而与总线 140 连接。

[0082] 这里,外部记录介质 137 是 DVD(Digital Versatile Disc)、DVD-R、DVD-RAM、BD(Blu-ray disc,蓝光光盘)、BD-R、BD-RE 等,读取写入装置 132 能够对这些 DVD、DVD-R、BD、BD-R、BD-RE 等写入、读取数据。

[0083] 读取写入装置接口 142 用于对读取写入装置 132 与总线 140 之间的信号的交换进行中介。

[0084] 通信装置 135 具有通过外部传送媒体 136 而取得内容的功能,与总线 140 连接,从外部的内容服务器、互联网上的内容提供站点等取得内容。

[0085] 这里,外部传送媒体 136 是光通信线路、电话通信线路、广播波等,通信装置 135 能够接收来自这些光通信线路、电话通信线路、广播波等的信号。

[0086] 通信装置 135 取得的内容被写入外部记录介质 137、硬盘装置 131 中内置的硬盘、或 RAM122。

[0087] 输出装置 133 是输出影像与声音的装置,具有输出由 AV 解码器 160 解码后的视频信号及音频信号的功能,经由输出装置接口 143 而与总线 140 连接,由 LCD(Liquid Crystal Display,液晶显示器)与扬声器构成。

[0088] 输出装置接口 143 用于对输出装置 133 与总线 140 之间的信号的交换进行中介。

[0089] 输入装置 134 由接受用户的操作的键盘及鼠标构成,具有接受用户对再生机 1000 的操作命令的功能,经由输入装置接口 144 而与总线 140 连接。

[0090] 输入装置接口 144 用于对输入装置 134 与总线 140 之间的信号的交换进行中介。

[0091] 总线 140 与 CPUA111、CPUB112、ROM121、RAM122、密码引擎 150、AV 解码器 160、通信装置 135、硬盘装置接口 141、读取装置接口 142、输出装置接口 143 以及输入装置接口 144 连接,用于在连接的各构成要素间进行数据通信。

[0092] 如上构成的再生机 1000 通过由 CPUA111 及 CPUB112 执行存储在 ROM121 或 RAM122 中的程序,来执行对写入到外部记录介质 137、硬盘装置 131 的内置硬盘、或 RAM122 中的内容的再生处理。

[0093] (内容的数据结构)

[0094] 图 2 是表示本实施方式 1 的内容解密处理装置 2000 所解密的内容 300 的数据结构的数据结构图。

[0095] 内容 300 由如下部分构成:分割复用将对影像进行编码而得的视频流被加密而成的视频 ES(Elementary Stream)、对日语的声音进行编码而得的音频流被加密而成的音频 1ES、以及对英语的声音进行编码而得的音频流被加密而成的音频 2ES 分割复用从而成为连续的 1 个流的内容数据 302;以及包含与内容 300 相关的信息的内容头 301。

[0096] 这里,被加密了的视频 ES 是对于以 MPEG4-AVC 方式进行了编码的影像数据将 1 个画面的图像数据即视频帧分别以密码链接块方式加密,从而得到的流数据。

[0097] 密码链接以各视频帧单位而结束,在相互不同的视频帧中密码链接不继续。

[0098] 此外,对进行链接的密码块的开头密码块进行解密时使用的链接值即初始值、以及对各密码块进行解密时使用的密钥,在全部视频帧中共通。

[0099] 这里,被加密了的音频 1ES、音频 2ES 是将以 MPEG4-AVC 方式对声音数据进行编码而得的各个音频帧、通过密码链接块方式加密而得的流数据。

[0100] 密码链接以各音频帧单位而结束,在相互不同的音频帧中密码链接不继续。

[0101] 此外,虽然初始值与密钥在属于被加密了的音频 1ES 的所有音频帧中共通,并且在属于被加密了的音频 2ES 的所有音频帧中共通,但属于被加密了的音频 1ES 的音频帧的初始值与密钥,不同于属于被加密了的音频 2ES 的音频帧的初始值与密钥。

[0102] 内容数据 302 的数据结构成为许多的组块 310 连续的结构,各组块 310 进一步由组块头 311、组块数据 312、填充(padding)313 构成。

[0103] 图 3 是表示组块 310 的数据结构的数据结构图。

[0104] 组块头 311 是未加密的固定长数据,由包含表示组块的尺寸的信息的组块尺寸 401、包含表示组块所属的内容类型的信息的内容类型 402、包含表示组块所属的帧序号的信息的帧序号 403、包含表示解码所使用的信息的解码用头信息 404、包含表示组块数据的尺寸的信息的组块数据尺寸 405 构成。

[0105] 这里,内容类型是视频、音频 1、音频 2 中的某一种,若内容类型为视频,则表示属于被加密了的视频 ES,若内容类型为音频 1,则表示属于被加密了的音频 1ES,若内容类型为音频 2,则表示属于被加密了的音频 2ES。

[0106] 此外,组块头 311 的构成要素、即组块尺寸 401、内容类型 402、帧序号 403、解码用头信息 404,其各自的位长与出现顺序是固定的。

[0107] 组块数据 312 是由按密码链接的顺序排列的密码块 411 ~ 413 构成的密码块列。

[0108] 例如,采用 AES(Advanced Encryption Standard,高级加密标准)密码方式的情况下,密码块是在 CTR 模式下被链接加密了的密码链接的单位,位长是 128 位。

[0109] 这里,密码块是通过对 128 比特的明文、以及利用 128 比特的密钥并通过 AES 密码方式等将 128 比特的链接值加密从而得到的 128 比特的密码链接值,按每比特来取异而生成的,各密码块是通过对视频帧、音频 1 帧、音频 2 帧中的某个帧进行加密而得的。

[0110] 填充 313 是未加密的数据,是用于调整组块 310 的数据尺寸而附加的数据。

[0111] (内容解密处理装置 2000)

[0112] 图 4 是表示利用再生机 1000 而功能性地实现的、内容解密处理装置 2000 的功能结构的模块图。

[0113] 内容解密处理装置 2000 对由 CPUA111 与 CPUB112 按照存储器模块 120 所存储的程序利用存储器模块 120、周边设备模块 130、总线 140、密码引擎 150 等而被加密了的内容进行解密处理,将解密的内容输出到 AV 解码器 160。

[0114] 内容解密处理装置 2000 由暂时保持解密对象的组块的输入缓冲器 201、暂时保持被解密的组块的输出缓冲器 202、存储密钥与初始值的密钥蓄积部 214、存储跨越组块之间的链接值的组块间链接值保持部 216、从组块头 311 取得信息的组块信息取得部 210、计算组块数据 312 的开始地址和填充 313 的开始地址的密码尺寸计算部 211、向密码引擎 150 输出密钥和初始值的密钥设定部 212、判断密码链接是否跨越组块之间而继续的链接判断部 213、以及密码引擎 150 构成。

[0115] 输入缓冲器 201 是用于暂时存储密码引擎 150 所解密的内容的一部分的存储区域,作为存储器模块 120 的一部分而被安装。

[0116] 输入缓冲器 201 所存储的单位是内容头 301 或组块 310 的单位,通过 CPUA111 和 CPUB112,按照内容 300 的数据顺序,对上次存储的内容的一部分进行覆盖。

[0117] 输出缓冲器 202 是用于将密码引擎 150 所解密的内容的一部分在向 AV 解码器 160 输出之前进行暂时存储的存储区域,作为存储器模块 120 的一部分而被安装。

[0118] 组块信息取得部 120 具有如下功能:取得输入缓冲器 201 保持的组块的开始地址,并且,从组块头 311 取得组块尺寸 401、组块数据尺寸 405、内容类型 402 与帧序号 403,向密码尺寸计算部 211 输出组块的开始地址、组块尺寸 401、与组块数据尺寸 405,向密钥设定部 212 输出内容类型 402,向链接判断部 213 输出内容类型 402、帧序号 403。

[0119] 组块信息取得部 210 具有如下功能:若通过 CPUA111 或 CPUB112 写入内容头 301,则向密码引擎 150 输出表示输入缓冲器 201 保持的数据是内容头 307 的内容头信号。

[0120] 密码尺寸计算部 211 具有如下功能:若从组块信息取得部 210 输入组块的开始地址、组块尺寸 401 与组块数据尺寸 405,则计算组块数据 312 的开始地址、填充 313 的开始地址、组块的结束地址、与组块数据 312 所含有的密码块的个数,并向密码引擎 150 输出。

[0121] 组块数据 312 的开始地址通过对组块的开始地址和固定长的组块头 311 的尺寸进行加法运算而被算出,填充 313 的开始地址通过对组块头 311 的开始地址加上组块数据尺寸 405 而被算出,组块的结束地址通过对组块的开始地址与组块尺寸 401 进行加法运算而被算出,密码块的个数通过用组块数据尺寸 405 除以密码块的单位比特数即 128 而被算出。

[0122] 密钥蓄积部 214 是用于将内容类型、密钥与初始值建立关联地进行存储的存储区域,作为存储器模块 120 的一部分而被安装。

[0123] 图 5 是表示密钥蓄积部 214 所存储的信息的图。

[0124] 如图 5 所示,密钥蓄积部 214 将解密时使用的密钥 502、初始值 503,与各个内容类型 402 对应起来而预先存储。

[0125] 密钥 502 的比特数是 128 比特,初始值 503 的比特数是 128 比特。

[0126] 这里,初始值是指,在对通过密码链接块方式加密了的密码块进行解密的情况下,对链接开头的密码块解密时使用的链接值。

[0127] 密钥设定部 212 具有如下功能:将来自组块信息取得部 210 的内容类型 402 作为输入,从密钥蓄积部 214 读出与输入的内容类型 402 对应地存储的密钥 502 和初始值 503,并向密码引擎 150 输出。

[0128] 组块间链接值保持部 216 是用于将内容类型、帧序号与链接值对应地存储的存储区域,作为存储器模块 120 的一部分而被安装。

[0129] 图 6 是表示组块间链接值保持部 216 所存储的信息的图。

[0130] 如图 6 所示,组块间链接值保持部 216 将帧序号 602、链接值 603,与各个内容类型 402 对应起来进行存储。

[0131] 这里所存储的帧序号 602 是对应的内容类型 402 中最后被解密的帧的帧序号,链接值 603 是属于帧序号 602 的最后被解密的组块的最后的密码块被解密时所算出的链接值。

[0132] 链接值 603 的比特数是 128 比特。

[0133] 另外,帧序号 602 与链接值 603 二者的组,按每个内容类型 402 通过密码引擎 150 而被覆盖。

[0134] 链接判断部 213 具有如下功能:若从组块信息取得部 210 输入内容类型 402 与帧序号 403 二者的组合,则调查从组块信息取得部 210 输入的内容类型 402 与帧序号 403 二

者的组合是否被建立关联地存储在组块间链接值保持部 216 中,在存储了的情况下,判断为输入缓冲器 201 所保持的组块为密码链接继续中,在未存储的情况下,判断为输入缓冲器 201 所保持的组块不为密码链接继续中。

[0135] 链接判断部 213 还具有如下功能:向密码引擎输出内容类型 402 和帧序号 403,此外,在判断为是密码链接继续中的情况下,向密码引擎 150 输出表示是密码链接继续中的密码链接信号,在判断为不是链接继续中的情况下,向密码引擎 150 输出表示是密码链接结束的密码结束信号。

[0136] 密码引擎 150 具有如下功能:根据来自组块信息取得部 210 的内容头信号,来自密码尺寸计算部 211 的组块数据 312 的开始地址、填充 313 的开始地址、组块的结束地址、组块数据 312 中所包含的密码块的个数,来自密钥设定部 212 的密钥 502 和初始值 503,来自链接判断部 213 的内容类型 402、帧序号 403、密码链接信号或密码结束信号,来读出输入缓冲器 201 所保持的组块,对读出的组块进行解密,将解密的组块写入输出缓冲器 202。

[0137] 密码引擎 150 包括:运算判断部 221,将组块数据 312 从输入缓冲器 201 所保持的组块读出并输出到运算部;运算部 222,以密码块单位对组块数据 312 进行解密;密钥保持部 223,存储密钥;初期值保持部 224,存储初期值;初期值选择部 225,选择初期值或链接值中的某一个;链接值选择部 226,选择运算部使用的链接值;组块内链接值保持部 227,用于存储链接值;链接值记录部 228,将运算部 222 输出的链接值记录到组块内链接值保持部 227 或组块间链接值保持部 216;以及输出选择部 229,将由运算部 222 以密码块单位进行了解密的组块数据,写入到输出缓冲器 202。

[0138] 运算判断部 221 具有如下功能:利用从密码尺寸计算部 211 输出的组块的开始地址、组块数据 312 的开始地址、填充 313 的开始地址与组块的结束地址,从输入缓冲器 201 所保持的组块读出组块头 311 和填充 313 并输出到输出选择部 229,读出组块数据 312 并以密码块单位输出到运算部 222,输出到运算部 222 的密码块是组块数据的开头的密码块时,向链接值选择部 226 输出初始值选择信号,输出到运算部 222 的密码块不是组块数据的开头的密码块时,向链接值选择部 226 输出链接值选择信号。

[0139] 另外,采用组块数据的开始地址来判断是否是组块数据的开头的密码块。

[0140] 这里,向运算部 222 输出组块数据的开头的密码块的定时为,从密码尺寸计算部 211 输入了组块数据 312 的开始地址的定时,而向运算部 222 输出组块数据的开头的密码块以外的密码块的定时为,从链接值记录部 228 接收到密码块请求信号的定时。

[0141] 此外,具有如下功能:从组块信息取得部 210 输入了内容头信号的情况下,将输入缓冲器 201 所保持的内容头 301 读出并输出到输出选择部 229。

[0142] 密钥保持部 223 具有如下功能:每当从密钥设定部 212 输入密钥,就覆盖至自身存储的密钥,不断向运算部 222 输出所存储的密钥。

[0143] 初期值保持部 224 具有如下功能:每当从密钥设定部 212 输入初始值,就覆盖自身存储的初始值,不断向初期值选择部输出所存储的初始值。

[0144] 初期值选择部 225 具有如下功能:若从链接判断部 213 接收密码链接继续信号与内容类型 402 二者的组,则从组块间链接值保持部 216 读出与接收到的内容类型 402 建立关联地存储的链接值并输出到链接值选择部 226,若从链接判断部 213 接收表示密码链接结束这一情况的信号,则将初期值保持部 224 所保持的初始值读出并输出到链接值选择部

226。

[0145] 组块内链接值保持部 227 是用于存储通过链接值记录部 228 覆盖的链接值的存储区域。

[0146] 链接值选择部 226 具有如下功能：在从运算判断部 221 接收到初始值选择信号的情况下，向运算部 222 输出从初始值选择部 225 输出的初始值或链接值，在从运算判断部 221 接收到链接值选择信号的情况下，读出组块内链接值保持部 227 所保持的链接值并将其向运算部 222 输出。

[0147] 链接值记录部 228 具有如下功能：输入密码尺寸计算部 211 输出的密码块的个数，链接判断部 213 输出的内容类型、帧序号，以及运算部 222 输出的链接值，若输入运算部 222 输出的链接值，则将输入的链接值记录到组块间链接值保持部 216 或组块内链接值保持部 227 中的某一个。

[0148] 链接值记录部 228 具有如下功能：在从运算部 222 输入的链接值为运算部 222 对组块的末尾的密码块进行解密时输出的链接值的情况下，将所输入的链接值与从链接判断部 213 输入的内容类型和帧序号建立关联并覆盖记录到组块间链接值保持部 216，在从运算部 222 输入的链接值不为运算部 222 对组块的末尾的密码块进行解密时输出的链接值的情况下，将所输入的链接值覆盖记录到组块内链接值保持部 217，向运算判断部 221 输出密码块请求信号。

[0149] 链接值记录部 228 具备链接值数计数器，该链接值数计数器计测所输入的链接值的个数，以用来判断从运算部 222 所输入的链接值是否是在对组块的末尾的密码块进行解密时所输出的链接值。

[0150] 每当从密码尺寸计算部 211 输入密码块的个数，该链接值数计数器就被复位。

[0151] 链接值记录部 228，在从运算部 222 输入了链接值的情况下，对链接值计数器计测的链接值数加 1 使其成为新的链接值数，当该新的链接值数未达到从密码尺寸计算部 211 输入的密码块的个数时，判断为不是在对组块的末尾的密码块进行解密时输出的链接值，当链接值数计数器计测的链接值的个数与从密码尺寸计算部 211 输入的密码块的个数相等时，判断为是在对组块的末尾的密码块进行解密时输出的链接值。

[0152] 输出选择部 229 具有向输出缓冲器 202 写入从运算判断部 221 输出的组块头 311、填充 313、以解密的密码块单位从运算部 222 输出的解密的密码块、内容头 301 的功能。

[0153] 运算部 222 具有如下功能：利用密钥保持部 223 所保持的密钥、和从链接值选择部 226 输出的初始值或链接值，以密码链接块方式解密从运算判断部 221 输出的密码块，并且在解密时计算并输出下一个链接值。

[0154] 图 7 是表示运算部 222 的功能结构的模块图。

[0155] 运算部 222 包括：AES 密码电路 701，加密所输入的链接值并输出密码链接值；增量器 (incrementer) 703，根据所输入的链接值，制作在对下一个密码块进行解密时使用的链接值；以及异电路 702，输出根据密码块与密码链接值而被解密的密码块、即明文。运算部 222 具有对以 CTR 模式而链接加密了的密码块进行解密的功能。

[0156] AES 密码电路 701 对于 128 比特的链接值，采用 128 比特的密钥、以 AES 密码方式来制作 128 比特的密码链接值，将其输出到异电路 702。

[0157] 增量器 703 具有如下功能：从输入的链接值中，对下位 32 比特的部分增加 1 而计

算下一个链接值。

[0158] 这里,当被增量的下位 32 比特的部分发生上溢时,仅下位 32 比特的部分成为 0×00 ,而上位 96 比特不受影响。

[0159] 异电路 702 具有如下功能:输出从 AES 密码电路 701 输出的 128 比特的密码链接值与从运算判断部 221 输出的 128 比特的密码块的每个比特的异。

[0160] 如上构成的内容解密处理装置 2000,将密码引擎 150 对组块的末尾的密码块进行解密时计算出的链接值,与内容类型和帧序号建立关联地存储到组块间链接值保持部 216。

[0161] 此外,内容解密处理装置 2000 在密码引擎 150 对组块的开头的密码块进行解密的情况下,当组块间链接值保持部 216 中存在与该组块的内容类型及帧序号对应地存储的链接值时,判断为该组块为链接继续的状态,利用与该组块的内容类型及帧序号对应地存储在组块间链接值保持部 216 中的链接值,对组块的开头的密码块进行解密,当组块间链接值保持部 216 中没有与该组块的内容类型及帧序号对应地存储的链接值时,判断为该组块不为链接继续的状态,利用与该组块的内容类型对应的初始值对组块的开头的密码块进行解密。

[0162] 并且,内容解密处理装置 2000,在密码引擎 150 对组块的开头的密码块以外的密码块进行解密的情况下,利用组块内链接值保持部 227 保持的链接值对密码块进行解密。

[0163] 下面利用附图详细说明内容解密处理装置 2000 的动作。

[0164] (动作)

[0165] 若再生机 1000 开始内容的再生处理,则 CPUA111 或 CPUB112 对于写入到外部记录介质 137、硬盘装置 131 的内置硬盘、或 RAM122 的解密对象的内容,首先将内容头 301 写入输入缓冲器 201。

[0166] 之后 CPUA111 或 CPUB112,从内容数据的最初的组块到最后的组块,依次将组块写入输入缓冲器 201。

[0167] 若内容头 301 被写入输入缓冲器 201,则内容解密处理装置 2000 开始内容解密处理。

[0168] 图 8 是内容解密处理装置 2000 所进行的内容解密处理的流程图。

[0169] 若内容解密处理装置 2000 开始内容解密处理,则组块信息取得部 210 输出内容头信号,运算判断部 221 接收所输出的内容头信号。

[0170] 运算判断部 221 若接收内容头信号,则从输入缓冲器 201 读出内容头 301 并输出到输出选择部 229,输出选择部 229 将接收到的内容头 301 写入输出缓冲器 202。

[0171] 若通过 CPUA111 或 CPUB112 向输入缓冲器 201 写入组块,则组块信息取得部 210 取得输入缓冲器 201 保持的组块的开始地址,并且从组块头 311 取得组块尺寸 401、组块数据尺寸 405、内容类型 402 与帧序号 403(步骤 S800),向密码尺寸计算部 211 输出组块的开始地址、组块尺寸 401 与组块数据尺寸 405,向密钥设定部 212 输出内容类型 402,向链接判断部 213 输出内容类型 402 与帧序号 403。

[0172] 密码尺寸计算部 211 若从组块信息取得部 210 输入组块的开始地址、组块尺寸 401 与组块数据尺寸 405,则计算填充 313 的开始地址、组块的结束地址与组块数据 312 所包含的密码块的个数(步骤 S805),向运算判断部 221 输出组块的开始地址、填充 313 的开始地址与组块的结束地址,向链接值记录部 228 输出密码块的个数。

[0173] 链接值记录部 228 若从密码尺寸计算部 211 输入密码块的个数,则使链接值计数器计测的链接值的个数复位。

[0174] 运算判断部 221 若从密码尺寸计算部 211 接收组块的开始地址、填充 313 的开始地址与组块的结束地址,则从输入缓冲器读出组块头 311 和填充 313 并输出到输出选择部 229,输出选择部 229 向输出缓冲器 202 写入所输入的组块头 311 和填充 313(步骤 S810),向链接值选择部 226 输出初始值选择信号。

[0175] 密钥设定部 212 若从组块信息取得部 210 输入内容类型 402,则读出在密钥蓄积部 214 中与输入的内容类型 402 建立关联地存储的密钥 502 和初始值 503,向密钥保持部 223 输出所读出的密钥 502,向初始值保持部 224 输出所读出的初始值 503,密钥蓄积部 214 覆盖并存储所输入的密钥,初始值保持部 224 覆盖并存储所输入的初始值(步骤 S815)。

[0176] 链接判断部 213 若从组块信息取得部 210 输入内容类型 402 与帧序号 403,则为了判断输入缓冲器 201 所保持的组块是否为密码链接继续中,调查输入的内容类型 402 与帧序号 403 的组合是否被建立关联地存储在组块间链接值保持部 216 中(步骤 S820),在已存储的情况下,判断为输入缓冲器 201 所保持的组块为密码链接继续中(步骤 S820:是),向链接值记录部 228 输出内容类型 402 与帧序号 403,向初始值选择部 225 输出密码链接信号与内容类型 402。

[0177] 初始值选择部 225 若从链接判断部 213 接收密码链接继续信号与内容类型 402 这二者的组,则从组块间链接值保持部 216 读出与接收到的内容类型 402 建立关联地存储的链接值并输出到链接值选择部 226。

[0178] 链接值选择部 226 由于已从运算判断部 221 接收初期值选择信号,因此从初始值选择部 225 选择所输入的链接值,并输出到运算部 222(步骤 S825)。

[0179] 在步骤 S820 中,在输入的内容类型 402 和帧序号 403 的组合没有被建立关联地存储在组块间链接值保持部 216 中的情况下,判断为输入缓冲器 201 所保持的组块不为密码链接继续中(步骤 S820:否),向链接值记录部 228 输出内容类型 402 和帧序号 403,向初始值选择部 225 输出密码结束信号。

[0180] 初始值选择部 225 若从链接判断部 213 接收密码链接结束信号,则读出初始值保持部 224 所保持的初始值并输出到链接值选择部 226。

[0181] 链接值选择部 226 由于已从运算判断部 221 接收到初始值选择信号,因此,若从初始值选择部 225 输入初始值,则将输入的初始值作为运算部 222 所使用的链接值而输出到运算部 222(步骤 S830)。

[0182] 若步骤 S825 或步骤 S830 的处理结束,则运算部 222 从运算判断部 221 接收密码组块的开头的密码块。

[0183] 运算部 222 利用密钥保持部 223 中记录的密钥、以及从链接值选择部输出的链接值,将接收到的密码块解密后输出到输出选择部 229,将解密时计算出的下一个链接值输出到链接值记录部 228(步骤 S835)。

[0184] 运算部 222 所进行的密码块的解密及下一个链接值的计算,通过如下 3 个处理而实现:(1)AES 密码电路 701 利用密钥对链接值加密而制作密码链接值;(2)异电路 702 按每比特来对制作出的密码链接值及密码块取异,从而对密码块进行解密;(3)增量器 703 仅对输入的链接值中、下位 32 比特的部分增加 1 从而计算下一个链接值。

[0185] 输出选择部 229 若从运算部 222 输入解密的密码块,则向输出缓冲器 202 写入所输入的解密的密码块。

[0186] 链接值记录部 228 若从运算部 222 输入链接值,则对链接值数计数器所计测的链接值数加 1 而作为新的链接值数,通过对该新的链接值数和从密码尺寸计算部输入的密码块的个数进行比较,从而判断从运算部 222 输入的链接值是否是运算部 222 对组块的末尾的密码块进行解密时输出的链接值(步骤 S840)。

[0187] 在步骤 S840 中,当新的链接值数未达到从密码尺寸计算部 211 输入的密码块的个数时,判断为所输入的链接值不是对组块的末尾的密码块进行解密时输出的链接值(步骤 S840:是),将从运算部 222 输入的链接值覆盖并记录到组块内链接值保持部(步骤 S845),链接值记录部 228 向运算判断部 221 输出密码块请求信号。

[0188] 运算判断部 221 若从链接值记录部 228 接收密码块请求信号,则向运算部 222 输出下一个密码块,向链接值选择部 226 输出链接值选择信号,若链接值选择部 226 接收链接值选择信号,则读出组块内链接值保持部 227 保持的链接值并输出到运算部 222(步骤 S850)。

[0189] 若步骤 S850 的处理结束,则再次开始步骤 S835 的处理。

[0190] 在步骤 S840 中,当新的链接值数与从密码尺寸计算部 211 输入的密码块的个数相等时,判断为所输入的链接值是对组块的末尾的密码块进行解密时输出的链接值(步骤 S840:否),将从运算部 222 输入的链接值,与从链接判断部 213 输入的内容类型和帧序号建立关联,覆盖并记录到组块间链接值保持部 216(步骤 S855)。

[0191] 若步骤 S855 的处理结束,则到 CPUA111 或 CPUB112 向输入缓冲器 201 写入后续的组块为止,内容解密处理装置 2000 待机(步骤 S865)。

[0192] CPUA111 或 CPUB112 在规定时间、例如 1ms 的期间向输入缓冲器 201 写入了后续的组块的情况下(步骤 S870:是),再次开始步骤 S800 的处理。

[0193] CPUA111 或 CPUB112 没有在规定时间、例如 1ms 的期间向输入缓冲器 201 写入后续的组块的情况下(步骤 S870:否),判断为内容数据 302 中不存在后续的组块,内容解密处理装置 2000 结束内容解密处理。

[0194] (具体动作)

[0195] 作为例子,对以下情况进行说明:在内容类型为视频且帧序号为 10 的第 1 组块,与同样地内容类型为视频且帧序号为 10、并与第 1 组块连续的组块即第 2 组块之间,存在内容类型为音频 1 且帧序号为 5 的第 3 组块的情况下,内容解密处理装置 2000 能够采用正确的链接值对第 2 帧的开头的密码块进行正确地解密。

[0196] 若运算部 222 对第 1 组块的末尾的密码块进行解密,则链接值记录部 228 将从运算部 222 输入的链接值、例如 0×00001111 ,与从链接判断部 213 输入的代表视频的内容类型和表示 10 的帧序号建立关联,覆盖并记录到组块间链接值保持部 216(步骤 S865)。

[0197] 之后,内容解密处理装置 2000 对第 3 组块进行解密,对第 3 组块进行解密之后,开始第 2 组块的解密。

[0198] 若第 2 组块被写入输入缓冲器 201,则组块信息取得部 210 取得表示视频的内容类型和表示 10 的帧序号(步骤 S800),并输出到链接判断部 213。

[0199] 链接判断部 213 调查表示视频的内容类型和表示 10 的帧序号这二者的组合是否

被建立关联地存储在组块间链接值保持部 216 中 (步骤 S820), 由于可知表示视频的内容类型和表示 10 的帧序号这二者的组合已与链接值 0×00001111 建立关联地进行了存储, 因此判断为第 2 组块为密码链接继续中 (步骤 S820 : 是), 输出密码链接信号与表示视频的内容类型。

[0200] 初始值选择部 225 若接收密码链接信号与表示视频的内容类型, 则从组块间链接值保持部 216 读出与表示视频的内容类型建立关联地存储的链接值 0×00001111 , 并输出到链接值选择部 226, 链接值选择部 226 向运算部 222 输出该链接值 0×00001111 。

[0201] 由此, 运算部 222 利用该链接值 0×00001111 、即对第 1 组块的末尾的密码块进行解密时计算出的链接值, 对第 2 组块的开头的密码块进行解密, 从而正确地对第 2 组块的开头的密码块进行解密。

[0202] (实施方式 2)

[0203] 下面, 作为本发明的内容解密处理装置的一个实施方式, 说明对以密码块链接方式进行了加密的内容进行解密的内容解密处理装置。

[0204] 本实施方式 2 的内容解密处理装置是对实施方式 1 所说明的内容解密处理装置 2000 进行了变形的装置, 能够解密作为对实施方式 1 的内容解密处理装置 2000 的解密对象、即内容 300 所包含的组块 310 的组块头 311 的一部分和内容头 301 进行了变形的数据格式的内容。

[0205] 本实施方式 2 的内容解密处理装置是如下变形的实施方式, 即: 对实施方式 1 所说明的内容解密处理装置 2000 的一部分、即组块信息取得部 210 进行变形, 并且新具备了内容头解析部和场 (field) 信息蓄积部, 与内容解密处理装置 2000 同样地, 在实施方式 1 的再生机 1000 上来实现。

[0206] 下面, 省略与实施方式 1 中说明的内容没有变更点的部分的说明, 而以变更点为中心进行说明。

[0207] (结构)

[0208] (内容的数据结构)

[0209] 本实施方式 2 的内容解密处理装置 3000 所解密的内容, 是对实施方式 1 的内容 300 进行如下变形的内容, 即: 使与实施方式 1 的组块头 311 中存在的 content type 402 和帧序号 403 对应的信息存在于内容头中。

[0210] 图 9 是表示构成作为本实施方式 2 的内容解密处理装置 3000 的解密对象的内容的、组块 1050 的数据结构的结构图。

[0211] 组块 1050 由组块头 1015、组块数据 1010 和填充 1020 构成。

[0212] 组块头 1015 是未加密的数据, 由包含表示组块的尺寸的信息的组块尺寸 1001、包含表示在解码中使用的信息的解码用头信息 1004、以及包含表示组块数据的尺寸的信息的组块数据尺寸 1005 构成, 组块尺寸 1001、解码用头信息 1004、以及组块数据尺寸 1005 各自的位长和出现顺序是固定的。组块数据 1010 与实施方式 1 的组块数据 312 同样, 填充 2230 与实施方式 1 的填充 313 同样。

[0213] 图 10 是表示构成本实施方式 2 的内容的内容头所包含的信息的结构图。

[0214] 内容头对于内容所包含的全部组块 1050, 按组块 1050 的排列顺序, 将每个组块 1050 的开始地址 1101、content type 1102、以及帧序号 1103 对应起来进行保持。

[0215] 内容类型 1102 与实施方式 1 的内容类型 402 同样,帧序号 1103 与实施方式 1 的帧序号 602 同样。

[0216] (内容解密处理装置 3000)

[0217] 图 11 是表示内容解密处理装置 3000 的功能结构的模块图。

[0218] 内容解密处理装置 3000 相对于实施方式 1 的内容解密处理装置 2000,将组块信息取得部 210 变形为组块信息取得部 910,并新追加了场信息蓄积部 920 和内容头解析部 930。

[0219] 场信息蓄积部 920 是存储区域,用于将内容头所保持的、每个组块 1050 的开始地址 1101、内容类型 1102 和帧序号 1103 对应起来存储,作为存储器模块 120 的一部分而被安装。

[0220] 内容头解析部 930 具有如下功能:从输入缓冲器 201 保持的内容头,读出按每个组块而建立对应的开始地址 1101、内容类型 1102、帧序号 1103 的所有的组,将读出的开始地址 1101、内容类型 1102、帧序号 1103 的所有的组对应起来记录至场信息蓄积部 920。

[0221] 组块信息取得部 910 具有如下功能:取得输入缓冲器 201 保持的组块的开始地址,并且从组块头 1015 取得组块尺寸 1001 与组块数据尺寸 1005,并且从场信息蓄积部 920 取得与输入缓冲器 201 保持的组块对应的内容类型 1102 及帧序号 1103,向密码尺寸计算部 211 输出组块的开始地址、组块尺寸 1001 与组块数据尺寸 1005,向密钥设定部 212 输出内容类型 1102,向链接判断部 213 输出内容类型 1102 与帧序号 1103。

[0222] 组块信息取得部 910 具有如下功能:若通过 CPUA111 或 CPUB112 写入内容头,则向密码引擎 950 输出表示输入缓冲器 201 保持的数据是内容头这一情况的内容头信号。

[0223] 下面,参照附图详细说明如上结构的内容解密处理装置 3000 的动作。

[0224] (动作)

[0225] 若再生机 1000 开始内容的再生处理,则 CPUA111 或 CPUB112,对于写入到外部记录介质 137、硬盘装置 131 的内置硬盘、或 RAM122 的解密对象的内容,首先将内容头写入输入缓冲器 201。

[0226] 之后 CPUA111 或 CPUB112,从内容数据的最初的组块到最后的组块,依次将组块写入输入缓冲器 201。

[0227] 若内容头被写入输入缓冲器 201,则内容解密处理装置 3000 开始内容解密处理。

[0228] 图 12 是内容解密处理装置 3000 所进行的内容解密处理的流程图。

[0229] 若内容解密处理装置 3000 开始内容解密处理,则组块信息取得部 910 输出内容头信号,运算判断部 221 接收所输出的内容头信号。

[0230] 并且,内容头解析部 930 从输入缓冲器 201 保持的内容头,读出按每个组块而建立对应的开始地址 1101、内容类型 1102、帧序号 1103 的所有的组,将读出的开始地址 1101、内容类型 1102、帧序号 1103 的所有的组对应起来记录至场信息蓄积部 920(步骤 S1200)。

[0231] 运算判断部 221 若接收内容头信号,则从输入缓冲器 201 读出内容头并输出到输出选择部 229,输出选择部 229 将接收到的内容头写入输出缓冲器 202。

[0232] 若通过 CPUA111 或 CPUB112 向输入缓冲器 201 写入组块,则组块信息取得部 910 取得输入缓冲器 201 保持的组块的开始地址,并且从组块头 1015 取得组块尺寸 1001 与组块数据尺寸 1005(步骤 S1202),此外,从场信息蓄积部 920 取得与输入缓冲器 201 保持的组

块对应的内容类型 1102 及帧序号 1103, 向密码尺寸计算部 211 输出组块的开始地址、组块尺寸 1001 与组块数据尺寸 1005, 向密钥设定部 212 输出内容类型 1102, 向链接判断部 213 输出内容类型 1102 与帧序号 1103。

[0233] 之后, 步骤 S1205 到步骤 S1265 的处理与实施方式 1 的内容解密处理装置 2000 的动作中的步骤 S805 到步骤 S865 的处理相同, 因此省略说明。

[0234] 另外, 步骤 S1205 与步骤 S805 对应, 步骤 S1210 与步骤 S810 对应, 步骤 S1215 与步骤 S815 对应, 步骤 S1220 与步骤 S820 对应, 步骤 S1225 与步骤 S825 对应, 步骤 S1230 与步骤 S830 对应, 步骤 S1235 与步骤 S835 对应, 步骤 S1240 与步骤 S840 对应, 步骤 S1245 与步骤 S845 对应, 步骤 S1250 与步骤 S850 对应, 步骤 S1255 与步骤 S855 对应, 步骤 S1265 与步骤 S865 对应。

[0235] 在步骤 S1265 中, 从内容解密处理装置 3000 开始待机起, 在规定期间、例如 1ms 的期间, 通过 CPUA111 或 CPUB112 向输入缓冲器 201 写入了后续的组块的情况下 (步骤 S1270 : 是), 再次开始步骤 S1202 的处理。

[0236] 在规定期间、例如 1ms 的期间, 没有通过 CPUA111 或 CPUB112 向输入缓冲器 201 写入后续的组块的情况下 (步骤 S1270 : 否), 判断为内容数据 302 中不存在后续的组块, 内容解密处理装置 3000 结束内容解密处理。

[0237] (实施方式 3)

[0238] 下面, 作为本发明的内容解密处理装置的一个实施方式, 说明对以密码块链接方式进行了加密的内容进行解密的内容解密处理装置。

[0239] 本实施方式 3 的内容解密处理装置是对实施方式 1 所说明的内容解密处理装置 2000 进行了变形的装置, 能够解密成为如下数据格式的内容, 该数据格式允许构成解密的内容的密码块构成为分割至连续 2 个组块。

[0240] 本实施方式 3 的内容解密处理装置, 对在实施方式 1 中说明的内容解密处理装置 2000 的一部分、即组块信息取得部 210、组块间链接值保持部 216、链接值记录部 228 进行变形, 并且新具备有尾数处理控制部 1300、前处理部 1301 和后处理部 1302, 本实施方式 3 的内容解密处理装置在将实施方式 1 的再生机 1000 的密码引擎 150 替换为将密码引擎 150 的一部分变形而得到的密码引擎 950 后的再生机上实现。

[0241] 下面, 省略与实施方式 1 中说明的内容没有变更点的部分的说明, 而以变更点为中心进行说明。

[0242] (结构)

[0243] (内容的数据结构)

[0244] 本实施方式 3 的内容解密处理装置 4000 所解密的内容为如下变形后的数据格式, 即: 构成为将实施方式 1 的密码块分割至连续 2 个组块。

[0245] 图 13(a) 是表示作为内容解密处理装置 4000 的解密对象的内容中的、内容数据的一部分的数据结构的图, 图 13(b) 是对图 13(a) 的一部分进行了放大的图。

[0246] 加密后的帧 1410 的内容类型为视频且帧序号为 j, 被分割为组块 1430、组块 1440 和组块 1460 这 3 个帧。

[0247] 加密后的帧 1420 的内容类型为音频 1 且帧序号为 k, 被分割为组块 1450 和组块 1470 这 2 个帧。

[0248] 加密后的视频帧 1410 由 8 个密码块 1401 ~ 1408 构成,它们之中,密码块 1401 和密码块 1402 包含于组块 1430,密码块 1404 和密码块 1405 包含于组块 1440,密码块 1407 和密码块 1408 包含于组块 1460。

[0249] 密码块 1403 被分割为前半部分和后半部分,前半部分包含于组块 1430,后半部分包含于组块 1440。

[0250] 密码块 1404 被分割为前半部分和后半部分,前半部分包含于组块 1440,后半部分包含于组块 1460。

[0251] 如上所述,作为内容解密处理装置 4000 的解密对象的内容中的内容数据,构成密码块允许被分割至连续 2 个组块。

[0252] (内容解密处理装置 4000)

[0253] 图 14 是表示内容解密处理装置 4000 的功能结构的模块图。

[0254] 内容解密处理装置 4000 相对于实施方式 1 的内容解密处理装置 2000,将组块信息取得部 210 变形为组块信息取得部 1310,将组块间链接值保持部 216 变形为组块间链接值保持部 1316,将链接值记录部 228 变形为链接值记录部 1328,并新追加了尾数处理控制部 1300、前处理部 1301 和后处理部 1302。

[0255] 组块信息取得部 1310 具有如下功能:取得输入缓冲器 201 保持的组块的开始地址,并且从组块头 311 取得组块尺寸 401、组块数据尺寸 405、内容类型 402 和帧序号 403,向密码尺寸计算部 211 输出组块的开始地址、组块尺寸 401 与组块数据尺寸 405,向密钥设定部 212 输出内容类型 402,向链接判断部 213 和尾数处理控制部 1300 输出内容类型 402 与帧序号 403。

[0256] 组块信息取得部 1310 具有如下功能:若通过 CPUA111 或 CPUB112 写入内容头 301,则向密码引擎 1350 输出表示输入缓冲器 201 保持的数据是内容头 301 这一情况的内容头信号。

[0257] 组块间链接值保持部 1316 是用于将内容类型、帧序号、链接值、组块的末尾的密码块的尺寸即尾数数据尺寸建立关联地存储的存储区域,作为存储器模块 120 的一部分而被安装。

[0258] 图 15 是表示组块间链接值保持部 1316 所存储的信息的图。

[0259] 如图 15 所示,组块间链接值保持部 1316 将内容类型 1801 分别与帧序号 1802、链接值 1803、尾数数据尺寸 1804 对应起来进行存储。

[0260] 这里所存储的帧序号 1802 是对应的内容类型 1801 中最后被解密的帧的帧序号,链接值 1803 是属于帧序号 602 的最后被解密的组块的末尾的密码块被解密时所算出的链接值,尾数数据尺寸 1804 是属于帧序号 602 的最后被解密的组块的末尾的密码块的尺寸。

[0261] 另外,帧序号 1802、链接值 1803、尾数数据尺寸 1804 这三者的组,通过密码引擎 150 按每个内容类型 1801 覆盖。

[0262] 尾数处理控制部 1300 具有如下功能:若从组块信息取得部 1310 接收内容类型 402 和帧序号 403,则读出与接收到的内容类型 402 和帧序号 403 二者的组对应地存储在组块间链接值保持部 1316 中的尾数数据尺寸 1804,计算存储在输入缓冲器 201 中的组块的开头的密码块的尺寸和末尾的密码块的尺寸,利用前处理部 1301、运算部 222 和后处理部 1302 执行尾数处理,向链接值记录部 1328 输出末尾的密码块的尺寸。

[0263] 稍后利用附图说明该尾数处理。

[0264] 通过从密码块的单位比特数即 128 中减去从组块间链接值保持部 1316 读出的尾数数据尺寸 1804, 来计算组块的开头的密码块的尺寸, 对于组块的末尾的密码块的尺寸, 将其计算为, 对从密码尺寸计算部 1311 输出的组块数据尺寸 405 和从组块间链接值保持部 1316 读出的尾数数据尺寸 1804 进行加法运算, 并用加法运算结果除以密码块的单位比特数即 128 所得到的余数。

[0265] 前处理部 1301 具有如下功能: 在从尾数处理控制部 1300 接收到的开头的密码块的尺寸未达到 128 比特的情况下, 若从运算判断部 221 接收输入缓冲器 201 保持的组块的开头的密码块, 则将开头的密码块的尺寸与 128 比特之差的比特数的 0 赋予至接收到的密码块的开头, 制作 128 比特的合成密码块, 使制作出的合成密码块代替从运算判断部 221 接收到的密码块而输出到运算部 222。

[0266] 此外, 前处理部 1301 具有如下功能: 在从尾数处理控制部 1300 接收到的末尾的密码块的尺寸未达到 128 比特的情况下, 若从运算判断部 221 接收输入缓冲器 201 保持的组块的末尾的密码块, 则将小于 128 比特的比特数量的 0 赋予至接收到的密码块的末尾, 制作 128 比特的合成密码块, 使制作出的合成密码块代替从运算判断部 221 接收到的密码块而输出到运算部 222。

[0267] 后处理部 1302 具有如下功能: 在从尾数处理控制部 1300 接收到的开头的密码块的尺寸未达到 128 比特的情况下, 若从运算部 222 接收通过对输入缓冲器 201 保持的组块的开头的密码块进行解密而得到的解密的密码块, 则将开头的密码块的尺寸与 128 比特之差的比特数的 00 从密码块的开头去除, 制作合成明文, 使制作出的合成明文代替从运算判断部 221 接收到的解密的密码块而输出到输出选择部 229。

[0268] 此外, 后处理部 1302 具有如下功能: 在从尾数处理控制部 1300 接收到的末尾的密码块的尺寸未达到 128 比特的情况下, 若从运算部 222 接收通过对输入缓冲器 201 保持的组块的末尾的密码块进行解密而得到的解密的密码块, 则将小于 128 比特的比特数从密码块的末尾去除, 制作合成明文, 使制作出的合成明文代替从运算判断部 221 接收到的解密的密码块而输出到输出选择部 229。

[0269] 链接值记录部 1328 具有如下功能: 输入密码尺寸计算部 1311 输出的密码块的个数, 链接判断部 213 输出的内容类型、帧序号, 运算部 222 输出的链接值, 以及尾数处理控制部 1300 输出的末尾的密码块的尺寸, 若输入运算部 222 输出的链接值, 则将输入的链接值记录到组块间链接值保持部 1316 或组块内链接值保持部 227 中的某一个。

[0270] 链接值记录部 1328 具有如下功能: 在从运算部 222 输入的链接值为运算部 222 对组块的末尾的密码块进行解密时输出的链接值的情况下, 将所输入的链接值与从链接判断部 213 输入的内容类型、帧序号和尾数数据尺寸建立关联并覆盖记录到组块间链接值保持部 1316, 在从运算部 222 输入的链接值不为运算部 222 对组块的末尾的密码块进行解密时输出的链接值的情况下, 将所输入的链接值覆盖记录到组块内链接值保持部 227, 向运算判断部 221 输出密码块请求信号。

[0271] 另外, 链接值记录部 1328 具有如下功能: 在从运算部 222 输入的链接值为运算部 222 对组块的末尾的密码块进行解密时输出的链接值的情况下, 且在尾数数据尺寸未达到 128 比特的情况下, 将覆盖记录到组块间链接值保持部 1316 的链接值作为上一次从运算部

222 输入的链接值。

[0272] 这里,所谓写入组块间链接值保持部 1316 的尾数数据尺寸,是指从尾数处理控制部 1300 输入的末尾的密码块的尺寸。

[0273] 链接值记录部 1328 具备链接值数计数器,该链接值数计数器计测所输入的链接值的个数,以用来判断从运算部 222 所输入的链接值是否是在对组块的末尾的密码块进行解密时所输出的链接值。

[0274] 每当从密码尺寸计算部 1311 输入密码块的个数,该链接值数计数器就被复位。

[0275] 链接值记录部 1328 在从运算部 222 输入了链接值的情况下,对链接值计数器计测的链接值数加 1 使其成为新的链接值数,当该新的链接值数未达到从密码尺寸计算部 211 输入的密码块的个数时,判断为不是在对组块的末尾的密码块进行解密时输出的链接值,当链接值数计数器计测的链接值的个数与从密码尺寸计算部 211 输入的密码块的个数相等时,判断为是在对组块的末尾的密码块进行解密时输出的链接值。

[0276] 密码引擎 1350 是如下结构:相对于实施方式 1 的密码引擎 150,将组块间链接值保持部 216 变形为 1316,将链接值记录部 228 变形为链接值记录部 1328,并新追加了尾数处理控制部 1300、前处理部 1301 和后处理部 1302。

[0277] (尾数处理)

[0278] 下面,利用附图,说明尾数处理控制部 1300 利用前处理部 1301、运算部 222 和后处理部 1302 所进行的尾数处理。

[0279] 图 16 是表示密码块的前半部缺失的情况下,前处理部 1301、运算部 222 与后处理部 1302 所进行的处理的动作的图。

[0280] 前处理部 1301 在从尾数处理控制部 1300 接收到的开头的密码块的尺寸未达到 128 比特的情况下,若从运算判断部 221 接收输入缓冲器 201 保持的组块的开头的密码块,则判断为接收到的密码块 1501 的开头的比特缺失了开头的密码块的尺寸与 128 比特之差的比特数,将缺失的比特数由 0 构成的补足数据 1502 赋予接收到的密码块 1501,制作 128 比特的合成密码块。

[0281] 前处理部 1301 用制作出的密码块代替从运算判断部 221 接收到的密码块而输出到运算部 222。

[0282] 运算部 222 通过对输入的 128 比特的密码块与 128 比特的密码链接值按每比特求异,从而制作解密的密码块,将制作出的解密的密码块输出到后处理部 1302。

[0283] 后处理部 1302 在从尾数处理控制部 1300 接收到的开头的密码块的尺寸未达到 128 比特的情况下,若从运算部 222 接收对输入缓冲器 201 保持的开头的密码块进行解密的密码块,则判断为对于接收到的解密的密码块的开头的比特而言,开头的密码块的尺寸与 128 比特之差的比特数是不需要的比特,将不需要的比特从密码块的开头去除,从而制作合成明文,用制作出的合成明文代替从运算判断部 221 接收到的解密的密码块而输出到输出选择部 229。

[0284] 图 17 是表示密码块的后半部缺失的情况下,前处理部 1301、运算部 222 与后处理部 1302 所进行的处理的动作的图。

[0285] 前处理部 1301,在从尾数处理控制部 1300 接收到的末尾的密码块的尺寸未达到 128 比特的情况下,若从运算判断部 221 接收输入缓冲器 201 保持的组块的末尾的密码块,

则判断为接收到的密码块 1501 的末尾的比特缺失了末尾的密码块的尺寸与 128 比特之差的比特数,将缺失的比特数由 0 构成的补足数据 1502 赋予接收到的密码块 1501,制作 128 比特的合成密码块。

[0286] 前处理部 1301 用制作出的密码块代替从运算判断部 221 接收到的密码块而输出到运算部 222。

[0287] 运算部 222 通过对输入的 128 比特的密码块与 128 比特的密码链接值按每比特求异,从而制作解密的密码块,将制作出的解密的密码块输出到后处理部 1302。

[0288] 后处理部 1302 在从尾数处理控制部 1300 接收到的末尾的密码块的尺寸未达到 128 比特的情况下,若从运算部 222 接收对输入缓冲器 201 保持的组块的末尾的密码块进行解密的密码块,则判断为对于接收到的解密的密码块的末尾的比特而言,末尾的密码块的尺寸与 128 比特之差的比特数是不需要的比特,将不需要的比特从密码块的末尾去除,从而制作合成明文,用制作出的合成明文代替从运算判断部 221 接收到的解密的密码块而输出到输出选择部 229。

[0289] 图 18 是表示密码块中没有缺失的情况下,前处理部 1301、运算部 222 与后处理部 1302 所进行的处理的动作的图。

[0290] 前处理部 1301, (1) 在从尾数处理控制部 1300 接收到的开头的密码块的尺寸为 128 比特的情况下,当从运算判断部 221 接收输入缓冲器 201 保持的组块的开头的密码块时;(2) 在从尾数处理控制部 1300 接收到的末尾的密码块的尺寸为 128 比特的情况下,当从运算判断部 221 接收输入缓冲器 201 保持的组块的末尾的密码块时;(3) 当从运算判断部 221 接收输入缓冲器 201 保持的组块的开头与末尾的密码块之外的密码块时;判断为接收到的密码块没有缺失,将接收到的密码块原样地输出到运算部 222。

[0291] 运算部 222 通过对输入的 128 比特的密码块与 128 比特的密码链接值按每比特求异,从而制作解密的密码块,将制作出的解密的密码块输出到后处理部 1302。

[0292] 后处理部 1302, (1) 在从尾数处理控制部 1300 接收到的开头的密码块的尺寸为 128 比特的情况下,当从运算部 222 接收对输入缓冲器 201 保持的组块的开头的密码块进行解密的密码块时;(2) 在从尾数处理控制部 1300 接收到的末尾的密码块的尺寸为 128 比特的情况下,当从运算部 222 接收对输入缓冲器 201 保持的组块的末尾的密码块进行解密的密码块时;(3) 当从运算判断部 221 接收输入缓冲器 201 保持的组块的开头与末尾的密码块之外的密码块时;判断为接收到的解密的密码块没有缺失,将接收到的解密的密码块原样输出到输出选择部 229。

[0293] 下面,利用附图来详细说明如上结构的内容解密处理装置 4000 的动作。

[0294] (动作)

[0295] 若再生机开始内容的再生处理,则 CPUA111 或 CPUB112 对于写入到外部记录介质 137、硬盘装置 131 的内置硬盘、或 RAM122 的解密对象的内容,首先将内容头 301 写入输入缓冲器 201。

[0296] 之后 CPUA111 或 CPUB112,从内容数据的最初的组块到最后的组块,依次将组块写入输入缓冲器 201。

[0297] 若内容头被写入输入缓冲器 201,则内容解密处理装置 3000 开始内容解密处理。

[0298] 图 19、图 20 是内容解密处理装置 4000 所进行的内容解密处理的流程图。

[0299] 若内容解密处理装置 4000 开始内容解密处理,则组块信息取得部 910 输出内容头信号,运算判断部 221 接收所输出的内容头信号。

[0300] 运算判断部 221 若接收内容头信号,则从输入缓冲器 201 读出内容头 301 并输出到输出选择部 229,输出选择部 229 将接收到的内容头 301 写入输出缓冲器 202。

[0301] 若通过 CPUA111 或 CPUB112 向输入缓冲器 201 写入组块,则组块信息取得部 1310 取得输入缓冲器 201 保持的组块的开始地址,并且从组块头 311 取得组块尺寸 401、组块数据尺寸 405、内容类型 402 与帧序号 403 (步骤 S1900),向密码尺寸计算部 211 输出组块的开始地址、组块尺寸 401 与组块数据尺寸 405,向密钥设定部 212 输出内容类型 402,向链接判断部 213 和尾数处理控制部 1300 输出帧序号 403。

[0302] 密码尺寸计算部 1311 若从组块信息取得部 210 输入组块的开始地址、组块尺寸 401 与组块数据尺寸 405,则计算填充 313 的开始地址、组块的结束地址与组块数据 312 所包含的密码块的个数 (步骤 S1910),向运算判断部 221 输出组块的开始地址、填充 313 的开始地址与组块的结束地址,向链接值记录部 1328 输出密码块的个数。

[0303] 链接值记录部 1328 若从密码尺寸计算部 211 输入密码块的个数,则使链接值计数器计测的链接值的个数复位。

[0304] 运算判断部 221 若从密码尺寸计算部 1311 接收组块的开始地址、填充 313 的开始地址与组块的结束地址,则从输入缓冲器读出组块头 311 和填充 313 并输出到输出选择部 229,输出选择部 229 向输出缓冲器 202 写入所输入的组块头 311 和填充 313 (步骤 S1920),向链接值选择部 226 输出初始值选择信号。

[0305] 密钥设定部 212 若从组块信息取得部 1310 输入内容类型 402,则读出在密钥蓄积部 214 中与输入的内容类型 402 建立关联地存储的密钥 502 和初始值 503,向密钥保持部 223 输出所读出的密钥 502,向初始值保持部 224 输出所读出的初始值,密钥蓄积部 214 覆盖并存储被输入的密钥,初始值保持部 224 覆盖并存储被输入的初始值 (步骤 S1930)。

[0306] 尾数处理控制部 1300 若从组块信息取得部 1310 接收内容类型 402 和帧序号 403,则读出与接收到的内容类型 402 和帧序号 403 二者的组对应地存储在组块间链接值保持部 1316 中的尾数数据尺寸 1804,计算存储在输入缓冲器 201 中的组块的开头的密码块的尺寸和末尾的密码块的尺寸 (步骤 S1935),将计算出的开头的密码块的尺寸输出到前处理部 1301 与后处理部 1302,将计算出的末尾的密码块的尺寸输出到链接值记录部 1328。

[0307] 链接判断部 213 若从组块信息取得部 1310 输入内容类型 402 与帧序号 403,则为了判断输入缓冲器 201 所保持的组块是否为密码链接继续中,调查所输入的内容类型 402 与帧序号 403 的组合是否被建立关联地存储在组块间链接值保持部 1316 中 (步骤 S1940),在已存储的情况下,判断为输入缓冲器 201 所保持的组块为密码链接继续中 (步骤 S1940 : 是),向链接值记录部 1328 输出内容类型 402 与帧序号 403,向初始值选择部 225 输出密码链接信号与内容类型 402。

[0308] 初始值选择部 225 若从链接判断部 213 接收密码链接继续信号与内容类型 402 这二者的组,则从组块间链接值保持部 1316 读出与接收到的内容类型 402 建立关联地存储的链接值并输出到链接值选择部 226。

[0309] 链接值选择部 226 由于已从运算判断部 221 接收初期值选择信号,因此从初始值选择部 225 选择所输入的链接值,并输出到运算部 222 (步骤 S1950)。

[0310] 接着,运算判断部 221 读出在输入缓冲器 201 中存储的密码组块的开头的密码块,并输出到前处理部 1301。

[0311] 前处理部 1301 为了判断密码块是否被分割而判断从尾数处理控制部 1300 接收到的开头的密码块的尺寸是否未达到 128 比特(步骤 S1970),在未达到 128 比特的情况下,判断为密码块被分割(步骤 S1970:是),将小于 128 比特的比特数量的 0 赋予接收到的密码块的开头,从而制作 128 比特的合成密码块,用制作出的合成密码块代替从运算判断部 221 接收到的密码块而输出到运算部 222。

[0312] 在步骤 S1940 中,在输入的内容类型 402 和帧序号 403 的组合没有被建立关联地存储在组块间链接值保持部 1316 中的情况下,判断为输入缓冲器 201 所保持的组块不为密码链接继续中(步骤 S1940:否),向链接值记录部 228 输出内容类型 402 和帧序号 403,向初始值选择部 225 输出密码结束信号。

[0313] 初始值选择部 225 若从链接判断部 213 接收密码链接结束信号,则读出初始值保持部 224 所保持的初始值并输出到链接值选择部 226。

[0314] 链接值选择部 226 由于已从运算判断部 221 接收到初始值选择信号,因此,若从初始值选择部 225 输入初始值,则将输入的初始值作为运算部 222 所使用的链接值而输出到运算部 222(步骤 S1960)。

[0315] 接着,运算判断部 221 读出在输入缓冲器 201 中存储的密码组块的开头的密码块并输出到前处理部 1301,前处理部 1301 将接收到的密码块原样地输出到运算部 222。

[0316] 若步骤 S1980 或步骤 S1960 的处理结束,则运算部 222 从前处理部 1301 接收密码组块的开头的密码块。

[0317] 运算部 222 利用密钥保持部 223 中记录的密钥、以及从链接值选择部输出的链接值,将接收到的密码块解密后输出到后处理部 1302,将解密时计算出的下一个链接值输出到链接值记录部 228(步骤 S2000)。

[0318] 后处理部 1302,(1) 在从尾数处理控制部 1300 接收到的开头的密码块的尺寸未达到 128 比特的情况下,当从运算部 222 接收到通过对输入缓冲器 201 保持的组块的开头的密码块进行解密从而得到的解密的密码块时;(2) 在从尾数处理控制部 1300 接收到的末尾的密码块的尺寸未达到 128 比特的情况下,当从运算部 222 接收到通过对输入缓冲器 201 保持的组块的末尾的密码块进行解密从而得到的解密的密码块时;判断为,接收到的解密的密码块,是对通过前处理部 1301 赋予了补足数据的密码块进行解密的密码块(步骤 S2000:是),制作将接收到的解密的密码块的、与所赋予的补足数据对应的部分去除后的合成明文,用制作出的合成明文代替从运算判断部 221 接收到的解密的密码块地输出到输出选择部 229(步骤 S2010)。

[0319] 后处理部 1302(1) 在从尾数处理控制部 1300 接收到的开头的密码块的尺寸为 128 比特的情况下;(2) 在从尾数处理控制部 1300 接收到的末尾的密码块的尺寸为 128 比特的情况下;(3) 在从尾数处理控制部 1300 接收到的开头的密码块的尺寸未达到 128 比特的情况下,且当从运算部 222 接收到通过对输入缓冲器 201 保持的组块的开头的密码块与末尾的密码块以外的密码块进行解密从而得到的解密的密码块时,判断为,接收到的解密的密码块,是对未通过前处理部 1301 赋予补足数据的密码块进行解密的密码块(步骤 S2000:否),将接收到的解密的密码块原样地输出到输出选择部 229。

[0320] 步骤 S2010 或步骤 S2005:若“否”的处理结束,则输出选择部 229 从后处理部 1302 接收解密的密码块。

[0321] 输出选择部 229 若从运算部 222 输入解密的密码块,则向输出缓冲器 202 写入所输入的解密的密码块。

[0322] 链接值记录部 228 若从运算部 222 输入链接值,则对链接值数计数器所计测的链接值数加 1 而作为新的链接值数,通过对该新的链接值数和从密码尺寸计算部输入的密码块的个数进行比较,从而判断从运算部 222 输入的链接值是否是运算部 222 对组块的末尾的密码块进行解密时输出的链接值(步骤 S2015)。

[0323] 在步骤 S2015 中,当新的链接值数未达到从密码尺寸计算部 211 输入的密码块的个数时,判断为所输入的链接值不是对组块的末尾的密码块进行解密时输出的链接值(步骤 S2015:是),将从运算部 222 输入的链接值覆盖并记录到组块内链接值保持部(步骤 S2020),链接值记录部 228 向运算判断部 221 输出密码块请求信号。

[0324] 运算判断部 221 若从链接值记录部 228 接收密码块请求信号,则向前处理部 1301 输出下一个密码块,向链接值选择部 226 输出链接值选择信号。

[0325] 前处理部 1301 在从尾数处理控制部 1300 接收到的末尾的密码块的尺寸未达到 128 比特的情况下,当从运算判断部 221 接收到输入缓冲器 201 保持的组块的末尾的密码块时,判断为后续的密码块被分割(步骤 S2025:是),将小于 128 比特的比特数量的 0 赋予接收到的密码块的开头,从而制作 128 比特的合成密码块(步骤 S2030),用制作出的合成密码块代替从运算判断部 221 接收到的密码块而输出到运算部 222。

[0326] 前处理部 1301 在从尾数处理控制部 1300 接收到的末尾的密码块的尺寸为 128 比特的情况下,或是在从运算判断部 221 接收到输入缓冲器 201 保持的组块的末尾的密码块以外的密码块的情况下,判断为后续的密码块没有被分割(步骤 S2025:否),将从运算判断部 221 接收到的密码块原样地输出到运算部 222。

[0327] 链接值选择部 226 若接收链接值选择信号,则读出组块内链接值保持部 227 保持的链接值并输入到运算部 222(步骤 S2035)。

[0328] 若步骤 S2035 的处理结束,则再次开始步骤 S2000 的处理。

[0329] 在步骤 S2015 中,当新的链接值数与从密码尺寸计算部 211 输入的密码块的个数相等时,判断为所输入的链接值是对组块的末尾的密码块进行解密时输出的链接值(步骤 S2015:否),在尾数数据尺寸为 128 比特时,将从运算部 222 输入的链接值,与从链接判断部 213 输入的内容类型、帧序号和尾数数据尺寸建立关联,覆盖并记录到组块间链接值保持部 1316,在尾数数据尺寸未达到 128 比特时,作为覆盖并记录到组块间链接值保持部 1316 的链接值,记录上一次从运算部 222 输入的链接值(步骤 S2040)。

[0330] 若步骤 S2040 的处理结束,则到 CPUA111 或 CPUB112 向输入缓冲器 201 写入后续的组块为止,内容解密处理装置 4000 待机(步骤 S2050)。

[0331] CPUA111 或 CPUB112 在规定时间、例如 1ms 的期间向输入缓冲器 201 写入了后续的组块的情况下(步骤 S2055:是),再次开始步骤 S1900 的处理。

[0332] CPUA111 或 CPUB112 没有在规定时间、例如 1ms 的期间向输入缓冲器 201 写入后续的组块的情况下(步骤 S2055:否),判断为内容数据 302 中不存在后续的组块,内容解密处理装置 2000 结束内容解密处理。

[0333] (实施方式 4)

[0334] 下面,作为本发明的内容解密处理装置的一个实施方式,说明对以密码块链接方式进行了加密的内容进行解密的内容解密处理装置。

[0335] 本实施方式 2 的内容解密处理装置,对作为实施方式 1 的内容解密处理装置 2000 的解密对象的内容所包含的组块 310 的组块头 311 的一部分进行了变形,是对实施方式 1 所说明的内容解密处理装置 2000 进行变形后的装置,以能够解密在组块头中含有密钥信息和初始值信息的数据格式的内容。

[0336] 本实施方式 4 的内容解密处理装置是进行如下变形的方式,即:对在实施方式 1 中说明的内容解密处理装置 2000 的一部分、即组块信息取得部 210、密钥蓄积部 214 和密钥设定部 212 进行变形,并且新具备有密钥生成部,本实施方式 4 的内容解密处理装置与内容解密处理装置 2000 同样地,在实施方式 1 的再生机 1000 的基础上实现。

[0337] 下面,省略与实施方式 1 中说明的内容没有变更点的部分的说明,而以变更点为中心进行说明。

[0338] (结构)

[0339] (内容的数据结构)

[0340] 本实施方式 4 的内容解密处理装置 5000 所解密的内容,是对实施方式 1 的内容 300 进行了如下变形的内容,即:对实施方式 1 的组块头 311 新加入密钥信息 2205、初始值信息 2206。

[0341] 图 21 是表示构成作为本实施方式 4 的内容解密处理装置 3000 的解密对象的内容的、组块 2250 的数据结构的结构图。

[0342] 组块 2250 由组块头 1015、组块数据 1010 和填充 1020 构成。

[0343] 组块头 2200 是未加密的数据,包括:包含表示组块的尺寸的信息的组块尺寸 2201;包含表示内容类型的信息的内容类型 2202;包含表示帧序号的信息的帧序号 2203;包含表示在解码中使用的信息的解码用头信息 2204;用于生成密钥的密钥信息 2205;用于生成初期值的初期值信息 2206;以及包含表示组块数据的尺寸的信息的组块数据尺寸 2207。

[0344] 其中,组块尺寸 2201、内容类型 2202、帧序号 2203、解码用头信息 2204、以及组块数据尺寸 2207 分别与实施方式 1 的组块尺寸 401、内容类型 402、帧序号 403、解码用头信息 404、以及组块数据尺寸 405 同样。

[0345] 此外,作为组块头 2200 的结构要素的、组块尺寸 2201、内容类型 2202、帧序号 2203、解码用头信息 2204、密钥信息 2205、初始值信息 2206 以及组块数据尺寸 2207,它们各自的位长和出现顺序是固定的。

[0346] 这里,密钥信息 2205 用于生成密钥,该密钥用于对包含密钥信息 2205 自身的组块所属于的密码帧进行解密,初始值信息 2206 用于生成初始值,该初始值用于对包含初始值信息 2206 自身的组块所属于的密码帧进行解密。

[0347] (内容解密处理装置 5000)

[0348] 图 22 是表示内容解密处理装置 5000 的功能结构的模块图。

[0349] 内容解密处理装置 5000 相对于实施方式 1 的内容解密处理装置 2000,将组块信息取得部 210 变形为组块信息取得部 2110,将密钥蓄积部 214 变形为密钥蓄积部 2114,将密

钥设定部 212 变形为密钥设定部 2112,并新追加了密钥生成部 2101。

[0350] 组块信息取得部 2110 具有如下功能:取得输入缓冲器 201 保持的组块的开始地址,并且从组块头 2200 取得组块尺寸 2201、组块数据尺寸 2207、内容类型 2202、帧序号 2203、密钥信息 2205 和初始值信息 2206,向密码尺寸计算部 211 输出组块的开始地址、组块尺寸 2201 与组块数据尺寸 2207,向密钥设定部 212 和链接判断部 213 输出内容类型 2202 和帧序号 2203,向密钥生成部 2101 输出内容类型 2202、帧序号 2203、密钥信息 2205 和初始值信息 2206。

[0351] 组块信息取得部 2110 具有如下功能:若通过 CPUA111 或 CPUB112 写入内容头 301,则向密码引擎 150 输出表示输入缓冲器 201 保持的数据是内容头 301 这一情况的内容头信号。

[0352] 密钥生成部 2101 若从组块信息取得部 2110 接收内容类型 2202、帧序号 2203、密钥信息 2205 和初始值信息 2206,则根据接收到的密钥信息 2205 制作密钥,根据接收到的初始值信息 2206 制作初始值,并将接收到的内容类型 2202、接收到的帧序号 2203、生成的密钥、生成的初始值建立关联地记录到密钥蓄积部 2114。

[0353] 此外,密钥生成部 2101 具有如下功能:在密钥信息 2205 被加密的情况下进行解密,在初始值信息 2206 被加密的情况下进行解密。

[0354] 密钥蓄积部 2114 是用于将内容类型、帧序号、密钥、初始值建立关联地进行存储的存储区域,作为存储器模块 120 的一部分而被安装。

[0355] 图 23 是表示密钥蓄积部 2114 所存储的信息的图。

[0356] 如图 23 所示,密钥蓄积部 2114 建立关联地存储有内容类型 2300、帧序号 2301、密钥 2302、初始值 2303。

[0357] 密钥设定部 2112 具有如下功能:若输入来自组块信息取得部 2110 的内容类型 2202 和帧序号 2203,则从密钥蓄积部 2114 读出与所输入的内容类型 2202 和帧序号 2203 的组建立关联地存储的密钥 2302 和初始值 2303,并输出到密码引擎 150。

[0358] 下面,参照附图详细说明如上结构的内容解密处理装置 5000 的动作。

[0359] (动作)

[0360] 若再生机 1000 开始内容的再生处理,则 CPUA111 或 CPUB112 对于写入到外部记录介质 137、硬盘装置 131 的内置硬盘、或 RAM122 的解密对象的内容,首先将内容头写入输入缓冲器 201。

[0361] 之后 CPUA111 或 CPUB112 从内容数据的最初的组块到最后的组块,依次将组块写入输入缓冲器 201。

[0362] 若内容头被写入输入缓冲器 201,则内容解密处理装置 5000 开始内容解密处理。

[0363] 图 24 是内容解密处理装置 2000 所进行的内容解密处理的流程图。

[0364] 若内容解密处理装置 5000 开始内容解密处理,则组块信息取得部 2110 输出内容头信号,运算判断部 221 接收所输出的内容头信号。

[0365] 运算判断部 221 若接收内容头信号,则从输入缓冲器 201 读出内容头并输出到输出选择部 229,输出选择部 229 将接收到的内容头写入输出缓冲器 202。

[0366] 若通过 CPUA111 或 CPUB112 向输入缓冲器 201 写入组块,则组块信息取得部 2110 取得输入缓冲器 201 保持的组块的开始地址,并且从组块头 2200 取得组块尺寸 2201、组

块数据尺寸 2207、内容类型 2202、帧序号 2203、密钥信息 2205 和初始值信息 2206 (步骤 S2400), 向密码尺寸计算部 211 输出组块的开始地址、组块尺寸 2201 与组块数据尺寸 2207, 向密钥设定部 2112 和链接判断部 213 输出内容类型 2202 和帧序号 2203, 向密钥生成部 2101 输出内容类型 2202、帧序号 2203、密钥信息 2205 和初始值信息 2206。

[0367] 密钥生成部 2101 若从组块信息取得部 2110 接收内容类型 2202、帧序号 203、密钥信息 2205 和初始值信息 2206, 则根据接收到的密钥信息 2205 制作密钥, 根据接收到的初始值信息 2206 制作初始值, 并将接收到的内容类型 2202、接收到的帧序号 2203、生成的密钥、生成的初始值建立关联地记录到密钥蓄积部 2114 (步骤 S2402)。

[0368] 密码尺寸计算部 211 若从组块信息取得部 210 输入组块的开始地址、组块尺寸 2201 与组块数据尺寸 2207, 则计算填充 2230 的开始地址、组块的结束地址与组块数据 2220 所包含的密码块的个数 (步骤 S2405), 向运算判断部 221 输出组块的开始地址、填充 2230 的开始地址与组块的结束地址, 向链接值记录部 228 输出密码块的个数。

[0369] 链接值记录部 228 若从密码尺寸计算部 211 输入密码块的个数, 则使链接值计数器计测的链接值的个数复位。

[0370] 运算判断部 221 若从密码尺寸计算部 211 接收组块的开始地址、填充 2230 的开始地址与组块的结束地址, 则从输入缓冲器读出组块头 2200 和填充 2230 并输出到输出选择部 229, 输出选择部 229 向输出缓冲器 202 写入所输入的组块头 2200 和填充 2230 (步骤 S2410), 向链接值选择部 226 输出初始值选择信号。

[0371] 密钥设定部 2112 若从组块信息取得部 210 输入内容类型 2202 和帧序号 2203, 则读出在密钥蓄积部 214 中与输入的内容类型 2202 和帧序号 2203 的组建立关联地存储的密钥 2302 和初始值 2303, 向密钥保持部 223 输出所读出的密钥 2302, 向初始值保持部 224 输出所读出的初始值 2303, 密钥蓄积部 214 覆盖并存储被输入的密钥, 初始值保持部 224 覆盖并存储被输入的初始值 (步骤 S2415)。

[0372] 之后, 步骤 S2420 到步骤 S2465 的处理与实施方式 1 的内容解密处理装置 2000 的动作中的步骤 S820 到步骤 S865 的处理相同, 因此省略说明。

[0373] 另外, 步骤 S2420 与步骤 S820 对应, 步骤 S2425 与步骤 S825 对应, 步骤 S2430 与步骤 S830 对应, 步骤 S2435 与步骤 S835 对应, 步骤 S2440 与步骤 S840 对应, 步骤 S2445 与步骤 S845 对应, 步骤 S2450 与步骤 S850 对应, 步骤 S2455 与步骤 S855 对应, 步骤 S2465 与步骤 S865 对应。

[0374] 在步骤 S2465 中, 从内容解密处理装置 5000 开始待机起, 在规定期间、例如 1ms 的期间, 通过 CPUA111 或 CPUB112 向输入缓冲器 201 写入了后续的组块的情况下 (步骤 S2470 : 是), 再次开始步骤 S2400 的处理。

[0375] 在规定期间、例如 1ms 的期间, 没有通过 CPUA111 或 CPUB112 向输入缓冲器 201 写入后续的组块的情况下 (步骤 S2470 : 否), 判断为内容数据 302 中不存在后续的组块, 内容解密处理装置 5000 结束内容解密处理。

[0376] (实施方式 5)

[0377] 下面, 作为本发明的内容解密处理装置的一个实施方式, 说明对以密码块链接方式进行了加密的内容进行解密的内容解密处理装置。

[0378] 本实施方式 5 的内容解密处理装置是对与作为实施方式 1 的内容解密处理装置

2000 的解密对象的内容格式相同的内容进行解密的内容解密处理装置,是对实施方式 1 所说明的内容解密处理装置 2000 进行了如下变形的装置,即:由第 1 处理部和第 2 处理部构成,该第 1 处理部从解密对象的内容读出并记录所有组块的组块头的信息,该第 2 处理部利用在第 1 处理部中存储的组块头的信息对内容进行解密。

[0379] 本实施方式 5 的内容解密处理装置是进行了如下变形的装置,即:对在实施方式 1 中说明的内容解密处理装置 2000 的一部分、即组块信息取得部 210、密码尺寸计算部 211、链接判断部 213、密钥设定部 212、运算判断部 221、初始值选择部 225 和链接值记录部 228 进行变形,并且具备密码信息蓄积部和帧序号蓄积部,本实施方式 5 的内容解密处理装置,是在将实施方式 1 的再生机 1000 的密码引擎 150 替换为将密码引擎 150 的一部分变形而得到的密码引擎 2250 后的再生机上实现的。

[0380] 下面,省略与实施方式 1 中说明的内容没有变更点的部分的说明,而以变更点为中心进行说明。

[0381] (结构)

[0382] (内容解密处理装置 6000)

[0383] 图 25 是表示内容解密处理装置 6000 的功能结构的模块图。

[0384] 内容解密处理装置 6000 相对于实施方式 1 的内容解密处理装置 2000,将组块信息取得部 210 变形为组块信息取得部 2510,将密码尺寸计算部 211 变形为密码尺寸计算部 2511,将链接值判断部 213 变形为链接值判断部 2413,将密钥设定部 212 变形为密钥设定部 2512,将运算判断部 221 变形为运算判断部 2521,将初始值选择部 225 变形为初始值选择部 2525,将链接值记录部 228 变形为链接值记录部 2528,并追加了密码信息蓄积部 2530 和帧序号蓄积部 2522。

[0385] 组块信息取得部 2510 具有如下功能:取得输入缓冲器 201 保持的组块的开始地址,并且从组块头 311 取得组块尺寸 401、组块数据尺寸 405、内容类型 402 和帧序号 403,向密码尺寸计算部 211 输出组块的开始地址、组块尺寸 401 与组块数据尺寸 405,向链接判断部 213 输出内容类型 402 与帧序号 403,并将内容类型 402 和帧序号 403 建立关联地记录到密码信息蓄积部 2530。

[0386] 密码尺寸计算部 2511 具有如下功能:若从组块信息取得部 210 输入组块的开始地址、组块尺寸 401 与组块数据尺寸 405,则计算组块数据 312 的开始地址、填充 313 的开始地址、组块的结束地址、以及组块数据 312 所含有的密码块的个数,将计算出的组块数据的开始地址、填充的开始地址、组块的结束地址以及密码块的个数,与通过组块信息取得部 2510 记录在密码信息蓄积部 2530 中的内容类型与帧序号的组建立关联地进行记录。

[0387] 组块数据 312 的开始地址通过将组块的开始地址和固定长的组块头 311 的尺寸相加而被算出,填充 313 的开始地址通过将组块头 311 的开始地址与组块数据尺寸 405 相加而被算出,组块的结束地址通过将组块的开始地址与组块尺寸 401 相加而被算出,密码块的个数通过用组块数据尺寸 405 除以密码块的单位比特数即 128 而被算出。

[0388] 帧序号蓄积部 2522 是用于将内容类型与帧序号建立关联地进行存储的存储区域,作为存储器模块 120 的一部分而被安装。

[0389] 图 26 是表示帧序号蓄积部 2522 所存储的信息的图。

[0390] 如图 26 所示,帧序号蓄积部 2522 中,与视频、音频 1、音频 2 这 3 个内容类型 2701

分别对应地存储有帧序号 2702。

[0391] 这里所存储的帧序号 2702 是,在内容类型 2701 的每个内容类型中由组块信息取得部 2510 取得的帧序号中最新的帧序号。

[0392] 链接判断部 2513 具有如下功能:若从组块信息取得部 2510 输入内容类型 402 与帧序号 403 二者的组合,则调查从组块信息取得部 2510 输入的内容类型 402 与帧序号 403 二者的组合是否被建立关联地存储在帧序号蓄积部 2522 中,在存储了的情况下,判断为输入缓冲器 201 所保持的组块为密码链接继续中,在未存储的情况下,判断为输入缓冲器 201 所保持的组块不为密码链接继续中。

[0393] 链接判断部 2513 具有如下功能:在判断为是密码链接继续中的情况下,将密码链接中这一情况,与通过组块信息取得部 2510 所记录的内容类型和帧序号的组建立关联地记录到密码信息蓄积部 2530,在判断为不是链接继续中的情况下,对帧序号蓄积部 2522 中存储的、与从组块信息取得部 2510 输入的内容类型相同的内容类型 2701 的帧序号 2702 进行更新,并将密码链接结束这一情况,与通过组块信息取得部 2510 所记录的内容类型和帧序号的组建立关联地记录到密码信息蓄积部 2530。

[0394] 密码信息蓄积部 2530 是用于存储的存储区域,将构成解密对象的内容的所有组块的开始地址、内容类型、帧序号、组块数据开始地址、密码块数、填充开始地址、组块结束地址、有无链接建立对应并按组块的顺序进行存储,作为存储器模块 120 的一部分而被安装。

[0395] 图 27 是表示密码信息蓄积部 2530 所存储的信息的图。

[0396] 如图 27 所示,密码信息蓄积部 2530 按解密对象的内容的组块的顺序存储有各组块的开始地址 2601、内容类型 2602、帧序号 2603、组块数据开始地址 2604、密码块数 2605、填充开始地址 2606、组块结束地址 2607 和有无链接 2608。

[0397] 密钥设定部 2512 具有如下功能:从密码信息蓄积部 2530,按组块的顺序依次读出内容类型 2602,从密钥蓄积部 214 读出与读出的内容类型 2602 关联地存储着的密钥 502 和初始值 503,并向密码引擎 150 输出。

[0398] 运算判断部 2521 具有如下功能:根据密码信息蓄积部 2530,按组块的顺序依次利用组块的开始地址 2601、组块数据开始地址 2604、填充开始地址 2606、组块结束地址 2607,从输入缓冲器 201 保持的组块,读出组块头 311 和填充 313 并输出到输出选择部 229,读出组块数据 312 并以密码块单位输出到运算部 222,在输出到运算部 222 的密码块是组块数据的开头的密码块的情况下,将初始值选择信号输出到链接值选择部 226,在输出到运算部 222 的密码块不是组块数据的开头的密码块的情况下,将链接值选择信号输出到链接值选择部 226。

[0399] 另外,利用组块数据的开始地址,判断是否是组块数据的开头的密码块。

[0400] 初始值选择部 2525 具有如下功能:从密码信息蓄积部 2530 按组块的顺序依次读出有无链接 2608 和内容类型 2602 的组,在读出的有无链接 2608 表示是链接中的情况下,从组块间链接值保持部 216 读出与读出的内容类型 2602 关联地存储着的链接值并输出到链接值选择部 226,在读出的有无链接 2608 不表示是链接中的情况下,读出初始值保持部 224 保持着的初始值并输出到链接值选择部 226。

[0401] 链接值记录部 2528 具有如下功能:从密码信息蓄积部 2530 按组块的顺序依次读

出密码块数 2605、内容类型 2602 和帧序号 2603,在输入了运算部 222 输出的链接值的情况下,将所输入的链接值记录到组块间链接值保持部 216 或组块内链接值保持部 227 中的某一个。

[0402] 链接值记录部 2528 具有如下功能:在从运算部 222 输入的链接值是运算部 222 对组块的末尾的密码块进行解密时输出的链接值的情况下,将所输入的链接值与从密码信息蓄积部 2530 读出的内容类型 2602 和帧序号 2603 建立关联地覆盖并记录到组块间链接值保持部 216,在从运算部 222 输入的链接值不是运算部 222 对组块的末尾的密码块进行解密时输出的链接值的情况下,将所输入的链接值覆盖并记录到组块内链接值保持部 227,并向运算判断部 2521 输出密码块请求信号。

[0403] 链接值记录部 228 具备链接值数计数器,该链接值数计数器计测所输入的链接值的个数,以用来判断从运算部 222 所输入的链接值是否是在对组块的末尾的密码块进行解密时所输出的链接值。

[0404] 每当从密码信息蓄积部 2530 读出密码块数 2605,该链接值数计数器就被复位。

[0405] 链接值记录部 228,在从运算部 222 输入了链接值的情况下,对链接值计数器计测的链接值数加 1 使其成为新的链接值数,当该新的链接值数未达到从密码尺寸计算部 211 输入的密码块的个数时,判断为不是在对组块的末尾的密码块进行解密时输出的链接值,当链接值数计数器计测的链接值的个数与从密码尺寸计算部 211 输入的密码块的个数相等时,判断为是在对组块的末尾的密码块进行解密时输出的链接值。

[0406] 密码引擎 2550 对实施方式 1 的密码引擎 150 进行了如下变形:将运算判断部 221 变形为运算判断部 2521,将初始值选择部 225 变形为初始值选择部 2525,将链接值记录部 228 变形为链接值记录部 2528。

[0407] 第 1 处理部 2501 由组块信息取得部 2510、密码尺寸计算部 2511、链接判断部 2513、密码信息蓄积部 2530 和帧序号蓄积部 2522 构成,通过 CPUA111 进行控制。

[0408] 第 1 处理部 2501 从内容所含有的所有组块的组块头,按组块的顺序取得内容的解密所需要的信息,进行向密码信息蓄积部 2530 蓄积的组块数据蓄积处理。

[0409] 第 2 处理部 2502 由密钥设定部 2512、密钥蓄积部 214、组块间链接值保持部 216 和密码引擎 2550 构成,通过 CPUB112 来进行控制。

[0410] 第 2 处理部 2502 从第 1 处理部的密码信息蓄积部 2530 读出内容的解密所需要的信息,进行对内容进行解密的内容解密处理。

[0411] 下面,参照附图详细说明如上结构的内容解密处理装置 6000 的动作。

[0412] (动作)

[0413] 若再生机 1000 开始内容的再生处理,则 CPUA111 或 CPUB112 对于写入到外部记录介质 137、硬盘装置 131 的内置硬盘、或 RAM122 的解密对象的内容,首先将内容头 301 写入输入缓冲器 201。

[0414] 之后 CPUA111 或 CPUB112,从内容数据的最初的组块到最后的组块,依次将组块写入输入缓冲器 201。

[0415] 若内容头 301 被写入输入缓冲器 201,则内容解密处理装置 6000 的第 1 处理部 2501 从内容所含有的组块的组块头,按组块的顺序取得内容的解密所需要的信息,并蓄积到密码信息蓄积部 2530。

[0416] 若第 1 处理部 2501 结束组块数据蓄积处理,则 CPUA111 或 CPUB112 再次将内容头 301 写入输入缓冲器 201,之后,从内容数据的最初的组块到最后的组块,依次将组块写入输入缓冲器 201。

[0417] 若内容头 301 第二次被写入输入缓冲器,则内容解密处理装置 6000 的第 2 处理部 2502 开始内容解密处理。

[0418] 图 28 和图 29 是内容解密处理装置 6000 所进行的内容解密处理的流程图。

[0419] 若内容解密处理装置 6000 的第 1 处理部 2501 开始组块头的信息读取处理,则组块信息取得部 2510 输出内容头信号,运算判断部 2521 接收所输出的内容头信号。

[0420] 运算判断部 2521 若接收内容头信号,则从输入缓冲器 201 读出内容头 301 并输出到输出选择部 229,输出选择部 229 将接收到的内容头 301 写入输出缓冲器 202。

[0421] 若通过 CPUA111 或 CPUB112 向输入缓冲器 201 写入组块,则组块信息取得部 2510 取得输入缓冲器 201 保持的组块的开始地址,并且从组块头 311 取得组块尺寸 401、组块数据尺寸 405、内容类型 402 与帧序号 403 (步骤 S2800),向密码尺寸计算部 2511 输出组块的开始地址、组块尺寸 401 与组块数据尺寸 405,向链接判断部 2513 输出内容类型 402 与帧序号 403,将内容类型 402 与帧序号 403 建立关联地记录到密码信息蓄积部 2530。

[0422] 密码尺寸计算部 2511 若输入来自组块信息取得部 2510 的组块的开始地址、组块尺寸 401 与组块数据尺寸 405,则计算组块数据 312 的开始地址、填充 313 的开始地址、组块的结束地址与组块数据 312 所包含的密码块的个数 (步骤 S2810)。

[0423] 链接判断部 2513 调查从组块信息取得部 2510 输入的内容类型 402 与帧序号 403 的组合是否被建立关联地存储在帧序号蓄积部 2522 中 (步骤 S2820),在未存储的情况下,对帧序号蓄积部 2522 中存储的、与从组块信息取得部 2510 输入的内容类型相同的内容类型 2701 的帧序号 2702 进行更新。

[0424] 密码尺寸计算部 2511 将计算出的组块数据的开始地址、填充的开始地址、组块的结束地址以及密码块的个数,与通过组块信息取得部 2510 记录在密码信息蓄积部 2530 中的内容类型与帧序号的组建立关联地进行记录,链接判断部 2513 在步骤 S2820 中为已记录的情况下,将密码链接中这一情况,与通过组块信息取得部 2510 所记录的内容类型和帧序号的组建立关联地记录到密码信息蓄积部 2530,在未记录的情况下,并将密码链接结束这一情况,与通过组块信息取得部 2510 所记录的内容类型和帧序号的组建立关联地记录到密码信息蓄积部 2530 (步骤 S2840)。

[0425] 若步骤 S2840 的处理结束,则到 CPUA111 或 CPUB112 向输入缓冲器 201 写入后续的组块为止,内容解密处理装置 2000 待机 (步骤 S2850)。

[0426] CPUA111 或 CPUB112 在规定时间、例如 1ms 的期间向输入缓冲器 201 写入了后续的组块的情况下 (步骤 S2850 :是),再次开始步骤 S800 的处理。

[0427] CPUA111 或 CPUB112 没有在规定时间、例如 1ms 的期间向输入缓冲器 201 写入后续的组块的情况下 (步骤 S2850 :否),判断为内容数据 302 中不存在后续的组块,第 1 处理部 2501 结束组块数据蓄积处理。

[0428] 若第 1 处理部 2501 结束组块数据蓄积处理,则 CPUA111 或 CPUB112 再次将内容头 301 写入输入缓冲器 201,之后,从内容数据的最初的组块到最后的组块,依次将组块写入输入缓冲器 201。

[0429] 若内容头 301 第二次被写入输入缓冲器,则内容解密处理装置 6000 的第 2 处理部 2502 开始内容解密处理。

[0430] 若内容解密处理装置 2000 开始内容解密处理,则运算判断部 2521 从输入缓冲器 201 读出内容头 301 并输出到输出选择部 229,输出选择部 229 将接收到的内容头 301 写入输出缓冲器 202。

[0431] 若通过 CPUA111 或 CPUB112 向输入缓冲器 201 写入组块,则运算判断部 2521 从密码信息蓄积部 2530 读出与所写入的组块对应的开始地址 2601、填充开始地址 2606 和组块结束地址 2607,密钥设定部 2512 从密码信息蓄积部 2530 读出与所写入的组块对应的内容类型 2602,初始值选择部 2525 从密码信息蓄积部 2530 读出与所写入的组块对应的有无链接 2608 和内容类型 2602,链接值记录部 2528 从密码信息蓄积部 2530 读出与所写入的组块对应的密码块数 2605、内容类型 2602 和帧序号 2603,并使链接值数计数器计测的链接值数复位(步骤 S2900)。

[0432] 运算判断部 2521 若从密码信息蓄积部 2530 读出开始地址 2601、填充开始地址 2606、组块结束地址 2607,则从输入缓冲器读出组块头 311 和填充 313 并输出到输出选择部 229,输出选择部 229 将所输入的组块头 311 和填充 313 写入输出缓冲器 202(步骤 S2910),并向链接值选择部 226 输出初期值选择信号。

[0433] 密钥设定部 2512 若从密码信息蓄积部 2530 输入内容类型 2602,则读出在密钥蓄积部 214 中与所输入的内容类型 2602 关联地存储着的密钥 502 和初始值 503,向密钥保持部 223 输出所读出的密钥 502,向初始值保持部 224 输出所读出的初始值 503,密钥蓄积部 214 覆盖并存储所输入的密钥,初始值保持部 224 覆盖并存储所输入的初始值(步骤 S2915)。

[0434] 初始值选择部 2525 若从密码信息蓄积部 2530 按组块的顺序依次读出有无链接 2608 和内容类型 2602 的组(步骤 S2920),则在读出的有无链接 2608 表示是链接中的情况下(步骤 S2920:是),从组块间链接值保持部 216 读出与读出的内容类型 2602 关联地存储着的链接值并输出到链接值选择部 226。

[0435] 链接值选择部 226 由于已从运算判断部 2521 接收初期值选择信号,因此从初始值选择部 2525 选择所输入的链接值,并输出到运算部 222(步骤 S2925)。

[0436] 在步骤 S2920 中,在读出的有无链接 2608 不表示是链接中的情况下(步骤 S2920:否),读出初始值保持部 224 保持的初始值并输出到链接值选择部 226。

[0437] 链接值选择部 226 由于已从运算判断部 2521 接收初期值选择信号,因此,若从初始值选择部 2525 输入初始值,则将所输入的初始值作为运算部 222 使用的链接值,并输出到运算部 222(步骤 S2930)。

[0438] 步骤 S2925 或步骤 S2930 的处理结束后的步骤 S2935 ~ 步骤 S2965 的处理,与实施方式 1 的内容解密处理装置 2000 的动作中的、步骤 S835 ~ 步骤 S865 的处理相同,故省略说明。

[0439] 另外,步骤 S2935 对应于步骤 S835,步骤 S2940 对应于步骤 S840,步骤 S2945 对应于步骤 S845,步骤 S2950 对应于步骤 S850,步骤 S2955 对应于步骤 S855,步骤 S2965 对应于步骤 S865。

[0440] 在步骤 S2965 中,从第 2 处理部 2502 开始待机起,在规定期间、例如 1ms 的期间,通

过 CPUA111 或 CPUB112 向输入缓冲器 201 写入了后续的组块的情况下（步骤 S2970：是），再次开始步骤 S1202 的处理。

[0441] 在规定期间、例如 1ms 的期间，没有通过 CPUA111 或 CPUB112 向输入缓冲器 201 写入后续的组块的情况下（步骤 S2970：否），判断为内容数据 302 中不存在后续的组块，第 2 处理部 2502 结束内容解密处理，内容解密处理装置 6000 结束内容解密处理。

[0442] （补充）

[0443] 以上，作为本发明的内容解密处理装置的一个实施方式，说明了以下内容解密处理装置：即使解密对象的数据流的数据结构为，在属于第 1 种密码帧（例如加密后的视频帧）的由进行链接的密码块列构成的密码组块间、存在属于第 2 种密码帧（例如加密后的音频帧）由进行链接的密码块列构成的密码组块的数据结构，也能够正确地对数据流进行解密，但也可以进行如下变形，本发明当然不限于上述实施方式所示的内容解密处理装置。

[0444] （1）在实施方式 1 中，CPU 模块 110 由 CPUA111 和 CPUB112 这 2 个 CPU 构成，但 CPU 的数量也可以是 1 个，也可以是 3 个以上，也可以是具有双 CPU 核功能的 1 个处理器，也可以是具有四 CPU 核功能的 1 个处理器。

[0445] （2）在实施方式 1 中，ROM121 为 ROM，但也可以含有可读写的非易失性存储器。

[0446] （3）在实施方式 1 中，密码引擎 150 为 DSP，但不一定必须是 DSP，也可以是例如通过 CPUA111 或 CPUB112 执行软件而实现的结构，也可以是通过 CPUA111、CPUB112 以外的 CPU 执行软件而实现的结构，也可以是通过 ASIC、FPGA 等来实现的结构。

[0447] 同样地，在实施方式 1 中，AV 解码器 160 为 DSP，但不一定必须是 DSP，也可以是例如通过 CPUA111 或 CPUB112 执行软件而实现的结构，也可以是通过 CPUA111、CPUB112 以外的 CPU 执行软件而实现的结构，也可以是通过 ASIC、FPGA 等来实现的结构。

[0448] （4）在实施方式 1 中，周边设备模块 130 由硬盘装置 131、硬盘装置接口 141、读取写入装置 132、读取写入装置接口 142、输出装置 133、输出装置接口 143、输入装置 134、输入装置接口 144、通信装置 135 构成，但至少具备输出装置 133、输出装置接口 143、输入装置 134、输入装置接口 144 即可，可以不用具备上述所有组成部分。

[0449] （5）在实施方式 1 中，AV 解码器 160 具有 MPEG2 解码功能、MPEG4 解码功能和 MPEG4-AVC 解码功能，但也可以具有对以这些编码方式编码后的数据以外的数据进行解码的功能。

[0450] （6）在实施方式 1 中，输出装置 133 由 LCD(Liquid Crystal Display) 与扬声器构成，但也可以代替 LCD 而采用 PDP(Plasma Display Panel, 等离子显示面板)、有机 EL(Electro-Luminescence, 电致发光) 显示器、布朗管（ブラウン管）等。

[0451] （7）在实施方式 1 中，再生机 1000 为个人计算机，但只要具有对内容进行解密的功能即可，例如可以是通用计算机、电视接收机、DVD 再生机、DVD 刻录再生机、BD 再生机、BD 刻录再生机、PDA(Personal Digital Assistance, 个人数字助理) 或便携通信终端等。

[0452] （8）在实施方式 1 中，输入装置 134 由接受用户的操作的键盘与鼠标构成，但只要具有接受用户对再生机 1000 的操作命令的功能即可，例如可以是接收用户操作的输入按键、接收来自用户操作的遥控器的信号的接收装置等。

[0453] （9）在实施方式 1 中，解密对象的内容为将加密后的视频 ES、加密后的音频 1ES 与加密后的音频 2ES 复用的内容，但只要为至少 2 个以上互不相同的 ES 复用的内容，则可以

是除此之外的 ES 复用的内容。

[0454] 例如,认为可以是将视频 1ES、视频 2ES、视频 3ES 与音频 ES 复用的内容等。

[0455] 此外,通过将所拍摄的影像以 MPEG4-AVC 方式编码、对由编码而得的许多视频帧的每个以密码块链接方式加密从而得到加密后的视频 ES,但也可以采用例如 MPEG2、MPEG4、Motion JPEG (Joint Photographic Experts Group) 等的、除 MPEG4-AVC 方式以外的方式进行编码。

[0456] 并且,通过将所拍摄的声音以 MPEG4-AVC 方式编码、对由编码而得的许多音频帧的每个以密码块链接方式加密从而得到加密后的音频 1ES 与音频 2ES,但也可以采用例如 MPEG2、MPEG4 等的、除 MPEG4-AVC 方式以外的方式进行编码。

[0457] (10) 在实施方式 1 中,组块头的每个构成要素的位长和出现顺序是固定的,但只要具有表示位长的信息,则位长可以不固定,并且只要具有表示顺序的信息,则顺序也可以不固定。

[0458] (11) 在实施方式 1 中,由 3 个密码块构成组块数据,但也可以由 3 个以外的数量的密码块构成。

[0459] (12) 在实施方式 1 中,密码块采用 AES 密码方式在 CTR 模式下进行密码链接化,但也可以采用 CBC (Cipher Block Chaining, 密码块链接) 模式等 CRT 模式以外的模式而加密,例如,也可以采用 DES (Data Encryption Standard, 数据加密标准) 密码方式等 AES 密码方式以外的密码方式而加密。

[0460] 此外,密码块的位长为 128 比特,链接值的位长为 128 比特,密钥的位长为 128 比特,但它们的位长可以根据密码块的密码方式而为 128 比特以外的位长。

[0461] 例如,密码块的密码方式是 DES 密码方式的情况下,密码块的位长成为 56 比特,链接值的位长成为 56 比特,密钥的位长成为 56 比特。

[0462] (13) 在实施方式 1 中,运算部 222 采用具有 AES 密码电路 701 的结构,但根据密码块的加密方式,也可以采用例如 DES 密码等 AES 密码以外的密码方式的密码电路。

[0463] (14) 在实施方式 1 中,增量器 703 从所输入的链接值中对下位 32 比特的部分增加 1 来计算下一个链接值,但也可以例如对下位 64 比特的部分增加 1 来计算下一个链接值,从而对下位 32 比特以外的部分增加 1,例如也可以增加 2 或 -1 等 1 以外的数。

[0464] (15) 在实施方式 1 中,虽然利用附图说明了解密对象的内容的格式,但解密对象的内容的文件形式也可以是不违反所说明的格式的形式,例如 ASF (Advanced Streaming Format, 高级流格式)、MP4 文件形式、QuickTime 文件形式。

[0465] (16) 在实施方式 1 中,举出了按每个内容类型而准备在密码中使用的密钥的例子,但也可以例如准备 1 个基本密钥,按每个内容类型实施特定处理,从而生成各内容类型用的密钥。

[0466] (17) 在实施方式 1 中,CPU 模块 110 由 2 个 CPU 构成,存储器模块由 ROM 和 RAM 构成,密码引擎 150 由 DSP 构成,AV 解码器 160 由 DSP 构成,但也可以采用除此以外的结构,例如,将 CPU 模块 110、存储器模块 120、周边设备模块 130、密码引擎 150、AV 解码器 160、以及总线 140 的一部分以 1 个集成电路来实现。

[0467] 图 30 是表示再生机 1000 的模块结构的模块图,表示了再生机 1000 中,将 CPU 模块 110、存储器模块 120、周边设备模块 130、密码引擎 150、AV 解码器 160、以及总线 140 的

一部分以 1 个集成电路 10 来实现的情况。

[0468] (18) 在实施方式 4 中,解密对象的内容为密钥信息 2205 包含在组块头 2200 中的数据格式,但密钥信息 2205 不包含在构成组块头 2200 的密码块中也可以。

[0469] 在采用这样的数据格式的内容的情况下,构成为,组块信息取得部 2210 从组块数据的密码块取得密钥信息,密钥生成部 2101 从组块信息取得部 2210 取得密码信息。

[0470] 密钥生成部 2101 在密钥信息被加密的情况下,对加密后的密钥信息进行解密后制作密钥。

[0471] 同样地,在实施方式 4 中,解密对象的内容为初始值信息 2206 包含在组块头 2200 中的数据格式,但初始值信息 2206 不包含在构成组块头 2200 的密码块中也可以。

[0472] 在采用这样的数据格式的内容的情况下,构成为,组块信息取得部 2210 从组块数据的密码块取得初始值信息,密钥生成部 2101 从组块信息取得部 2210 取得初始值信息。

[0473] 密钥生成部 2101 在初始值信息被加密的情况下,对加密后的初始值信息进行解密后制作密钥。

[0474] (19) 在实施方式 4 中,密钥信息 2205 是用于生成密钥的信息,初始值信息 2206 是用于生成初始值的信息,但密钥信息 2205 可以是密钥本身,初始值信息 2206 可以是初始值本身。

[0475] (20) 在实施方式 4 中,密钥信息 2205 既可以对属于各加密后的 ES 的所有帧通用,也可以按组块单位而互不相同,此外,在密钥信息 2205 包含于构成组块数据 2200 的密码块的情况下,在 1 个组块内存在多个密钥信息 2205,同一组块内的密码块采用互不相同的密钥信息 2205 也可以。

[0476] 同样地,在实施方式 4 中,初始值信息 2206 既可以对属于各加密后的 ES 的所有帧通用,也可以按组块单位而互不相同,此外,在初始值信息 2206 包含于构成组块数据 2200 的密码块的情况下,在 1 个组块内存在多个密钥信息 2205,同一组块内的密码块采用互不相同的密钥信息 2205 也可以。

[0477] (21) 在实施方式 5 中,第 1 处理部 2501 由 CPUA111 控制,第 2 处理部 2502 由 CPUB112 控制,但也可以采用除此以外的结构,例如,第 1 处理部 2501 可以由 CPUA111 和 CPUB112 控制,第 2 处理部 2502 可以由 CPUA111 和 CPUB112 控制。

[0478] 进一步地,CPU 模块 110 由 3 个以上 CPU 构成的情况下,第 1 处理部 2501 可以由 3 个以上 CPU 控制,第 2 处理部 2502 可以由 3 个以上 CPU 控制。

[0479] 此外,也可以构成为,在 CPU 模块中存在具有隐藏所处理的信息的功能的安全 (secure)CPU,由第 2 处理部 2502 控制该安全 CPU,从而使第三者不知道密钥蓄积部 214 存储的密钥和初始值。

[0480] (22) 在实施方式 5 中,说明了在第 1 处理部 2501 结束了组块数据蓄积处理后、第 2 处理部 2502 开始内容解密处理的例子,但即使第 1 处理部 2501 的组块数据蓄积处理未到达最后而结束,在密码信息蓄积部 2530 中已存储有一部分组块的信息的状态下第 2 处理部 2502 也可以开始内容解密处理。

[0481] (23) 在实施方式 1 中,外部记录介质 137 采用 DVD、DVD-R、DVD-RAM、BD、BD-R、BD-RE 等,但只要是可读取的记录介质即可,例如可以是 CD (Compact Disc)、CD-R、SD 卡等。

[0482] 此外,读取写入装置 132 能够向 DVD、DVD-R、BD、BD-R、BD-RE 等写入并读取数据,

但只要是能进行数据的读写的记录介质即可,例如可以构成为,能够向 CD、CD-R、SD 卡等写入并读取数据。

[0483] (24) 在实施方式 1 中,外部记录介质 136 是光通信线路、电话通信线路、广播波等,但只要它们的形态是能够传输数字信号的形态即可,例如可以是有线的形态、无线的形态、或红外线的形态。

[0484] 工业上的可利用性

[0485] 本发明能够广泛应用于对加密后的数字数据进行解密的解密处理装置。

[0486] 符号说明

[0487] 150 密码引擎

[0488] 201 输入缓冲器

[0489] 202 输出缓冲器

[0490] 210 组块信息取得部

[0491] 211 密码尺寸计算部

[0492] 212 密钥设定部

[0493] 213 链接判断部

[0494] 214 密钥蓄积部

[0495] 216 组块间链接值保持部

[0496] 221 运算判断部

[0497] 222 运算部

[0498] 223 密钥保持部

[0499] 224 初始值保持部

[0500] 225 初始值选择部

[0501] 226 链接值选择部

[0502] 227 组块内链接值保持部

[0503] 228 链接值记录部

[0504] 229 输出选择部

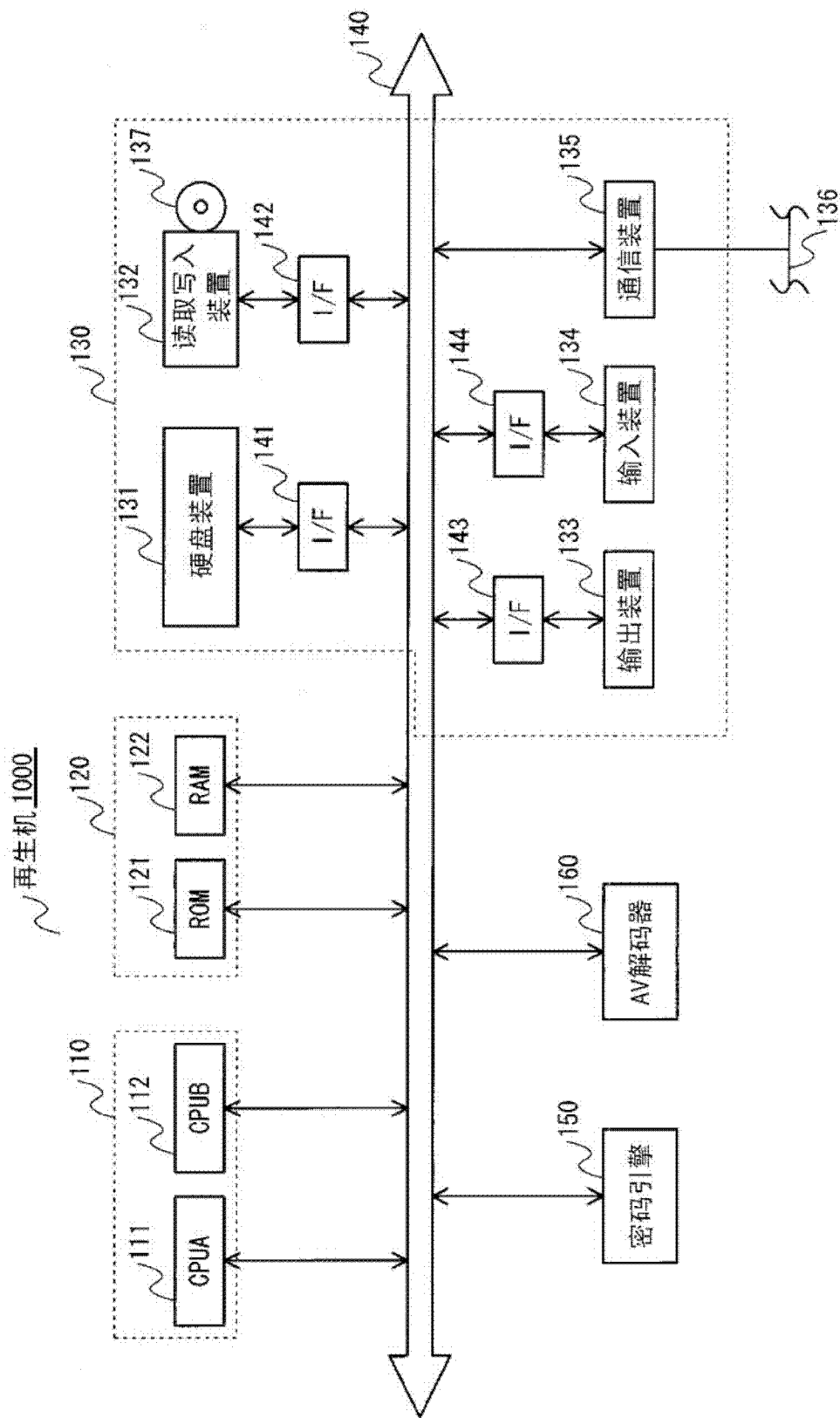


图 1

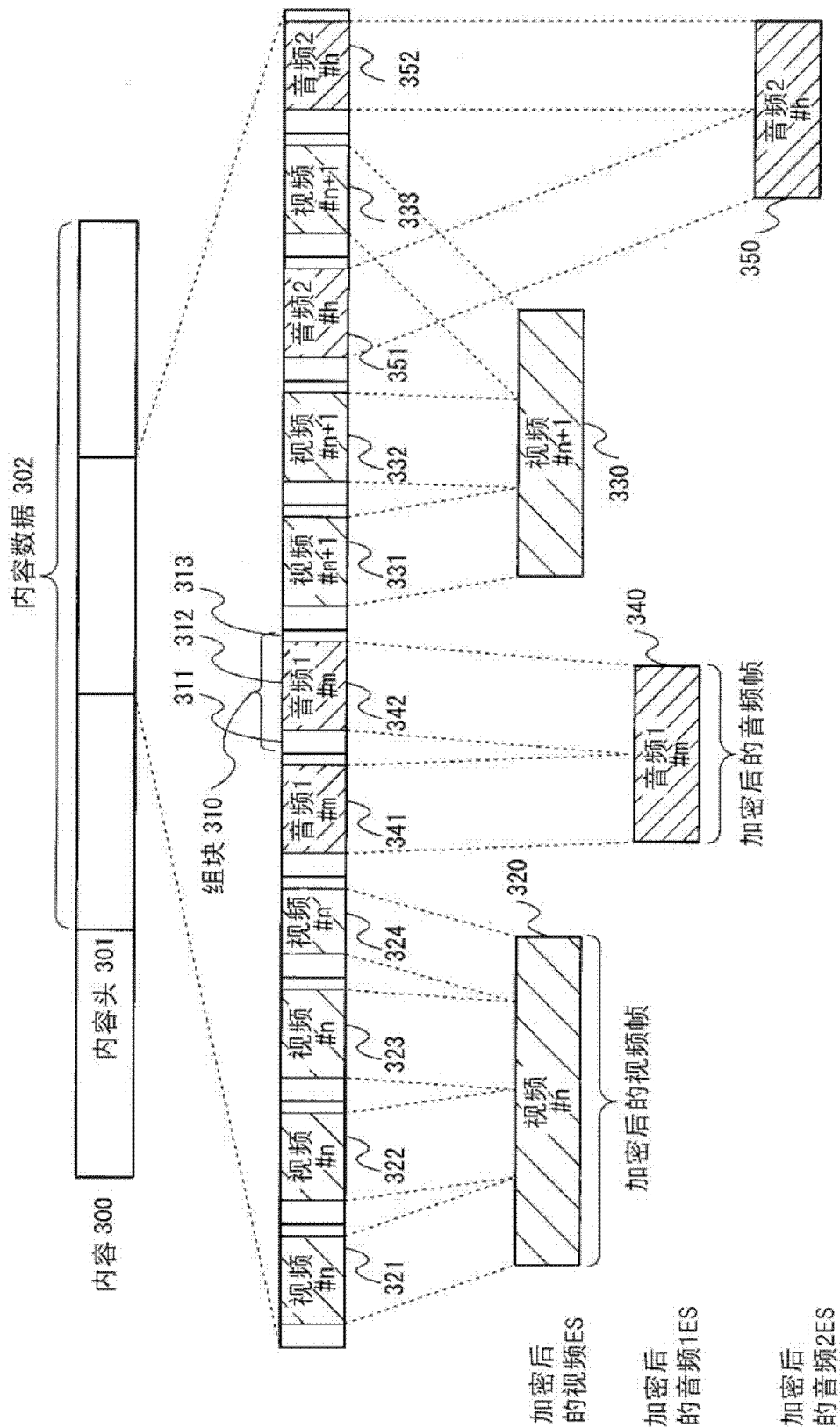


图 2

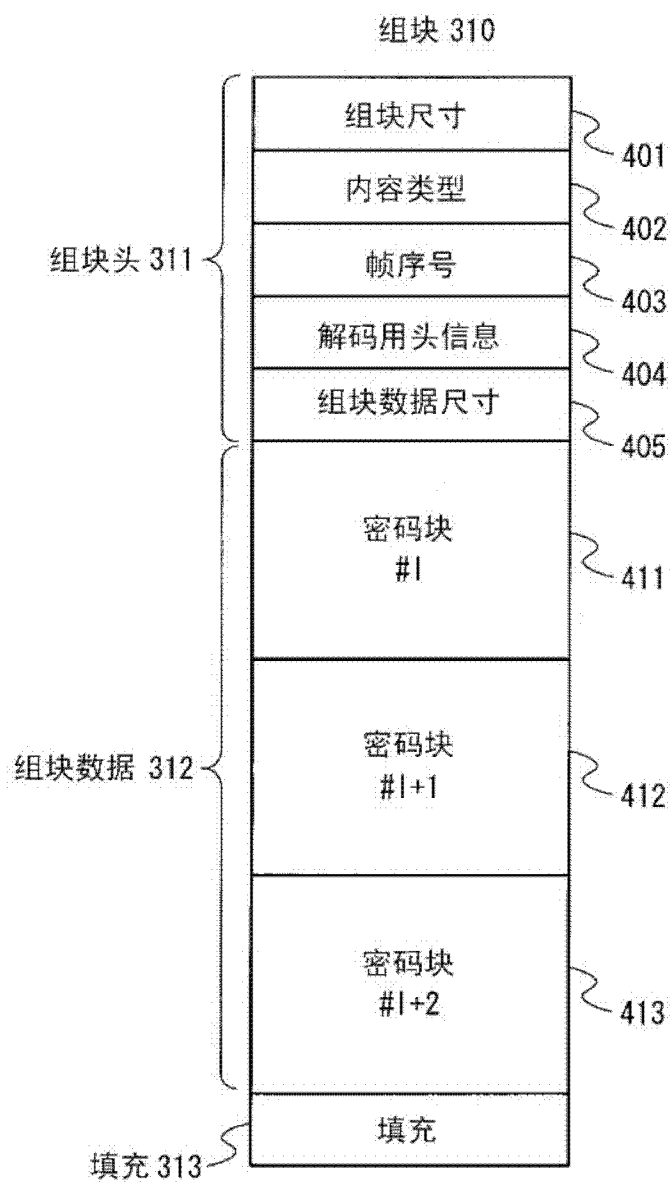


图 3

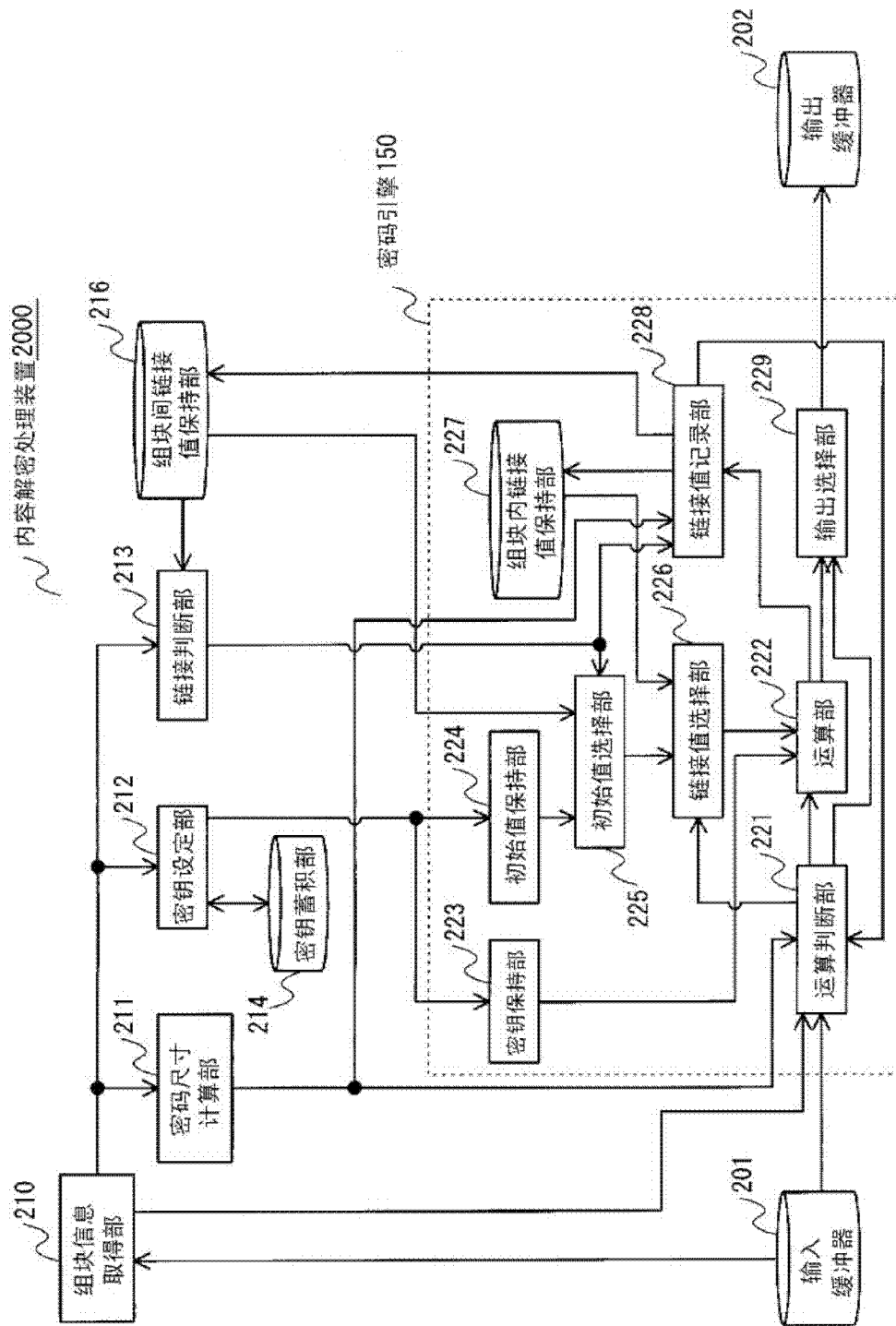


图 4

402	502	503
内容类型	密钥	初始值
视频	0xAAAAFFFF	0x88880000
音频1	0x01234567	0xFEDCBA98
音频2	0x89ABCDEF	0x76543210

图 5

402	602	603
内容类型	帧序号	链接值
视频	0x00000002	0x88880006
音频1	0x00000001	0xFEDCBA9B
音频2	0x00000001	0x76543213

图 6

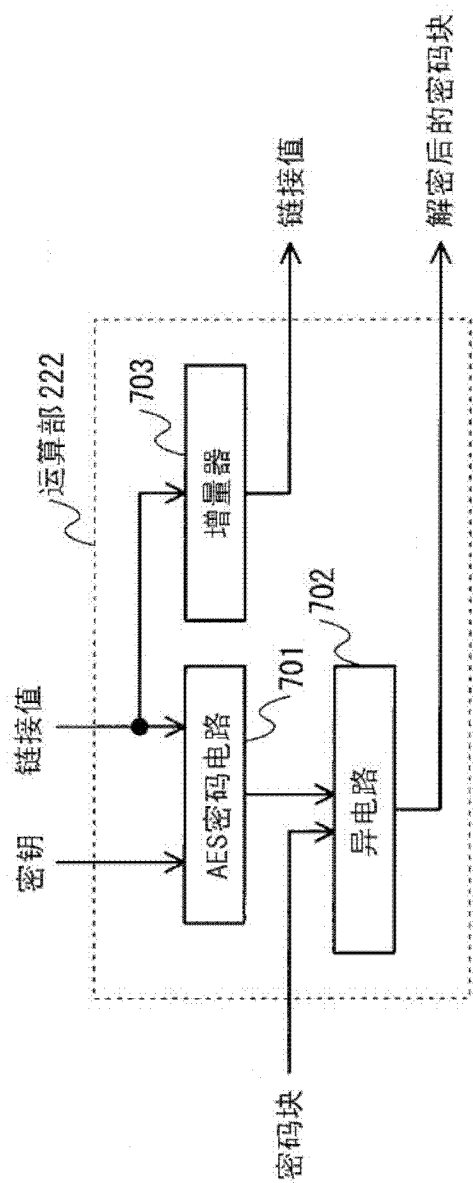


图 7

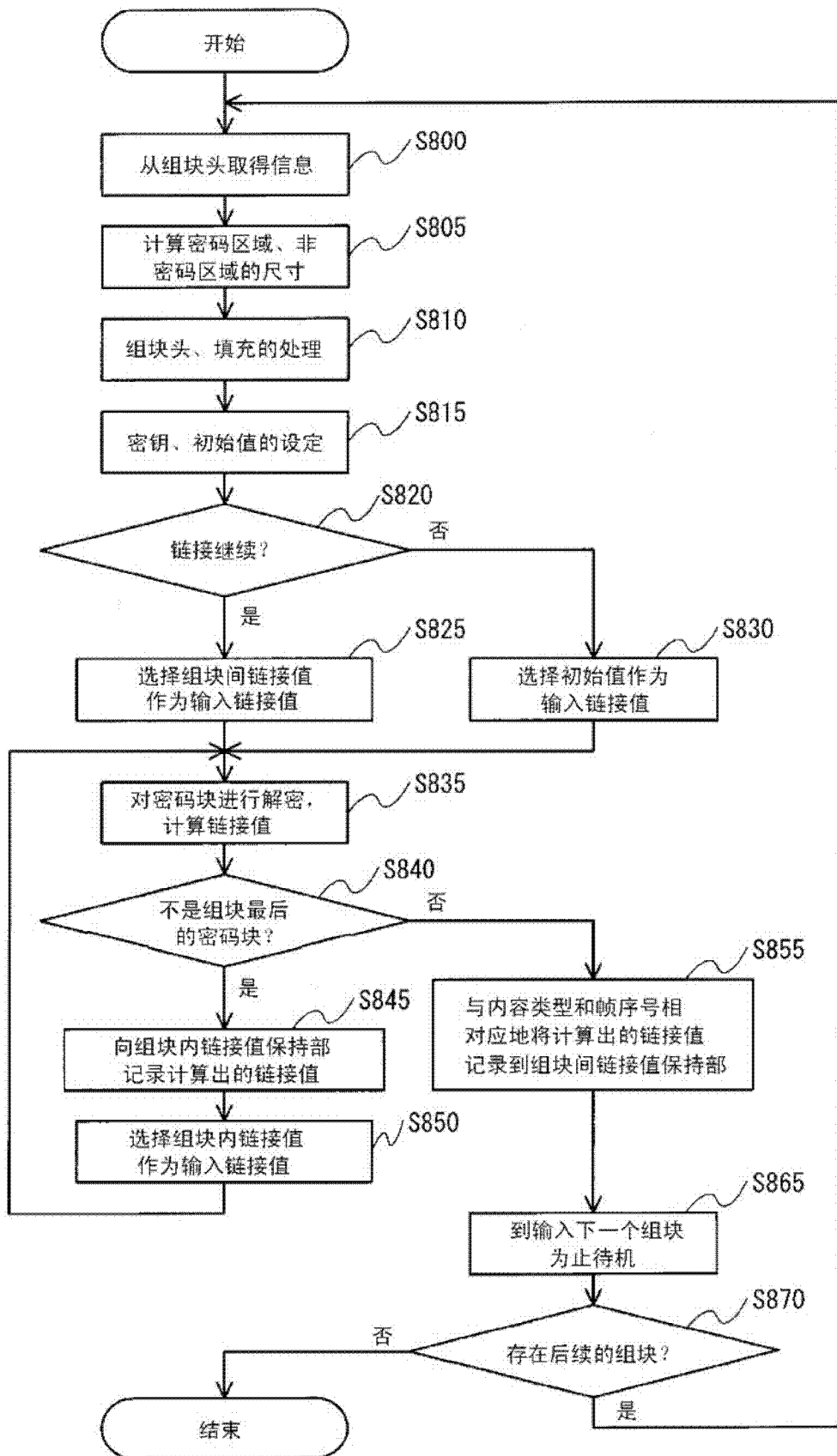


图 8

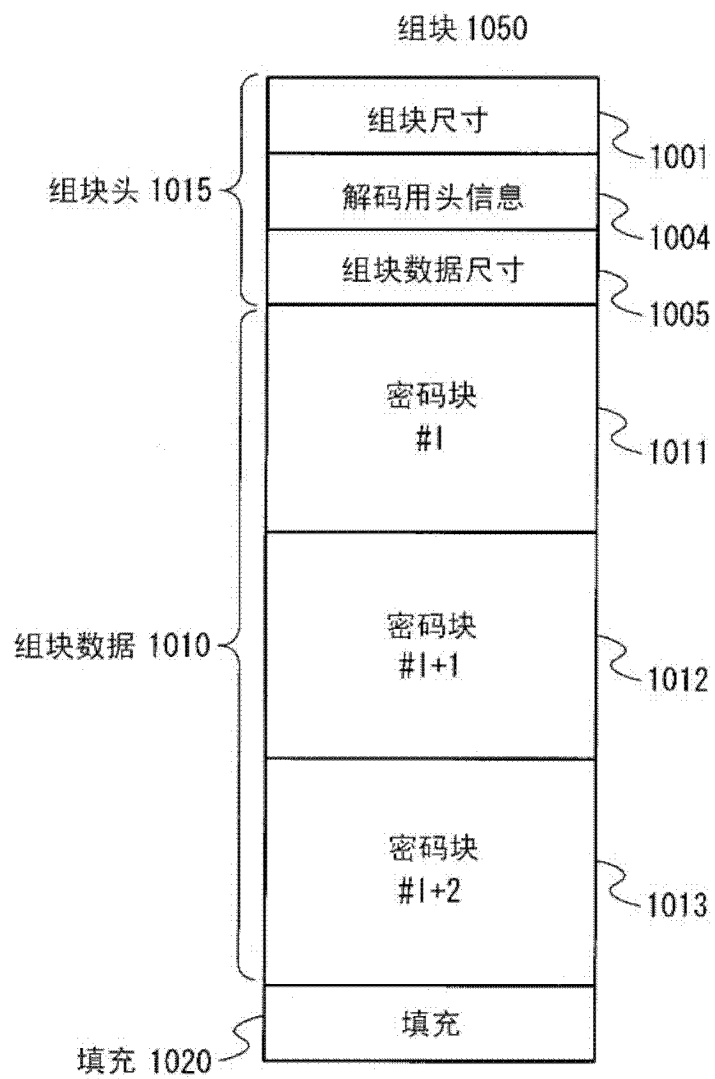


图 9

1101 开始地址	1102 内容类型	1103 帧序号
address_0	视频	0x00000000
address_1	视频	0x00000001
address_2	视频	0x00000002
address_3	音频1	0x00000000
...	...	...

图 10

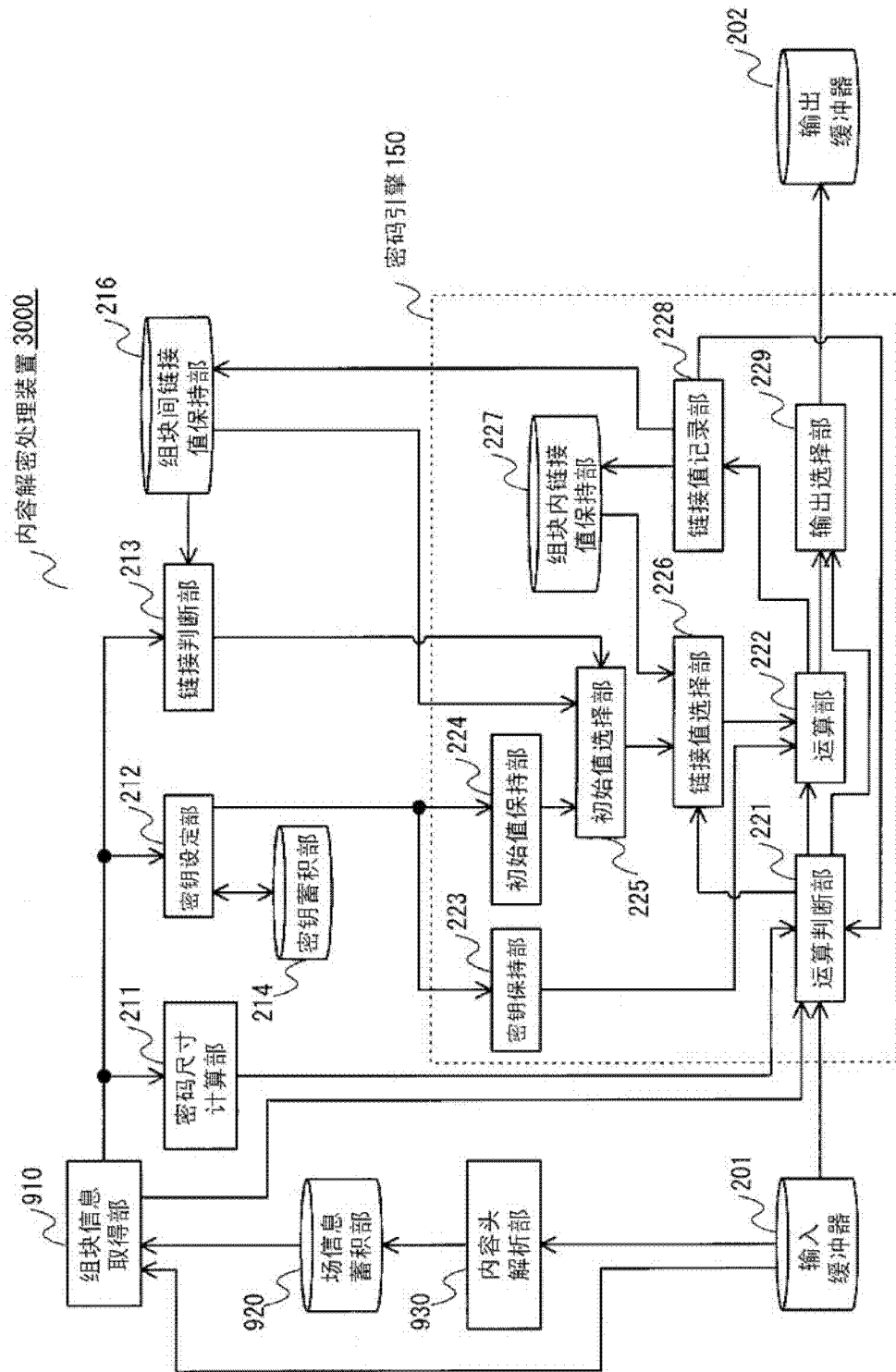


图 11

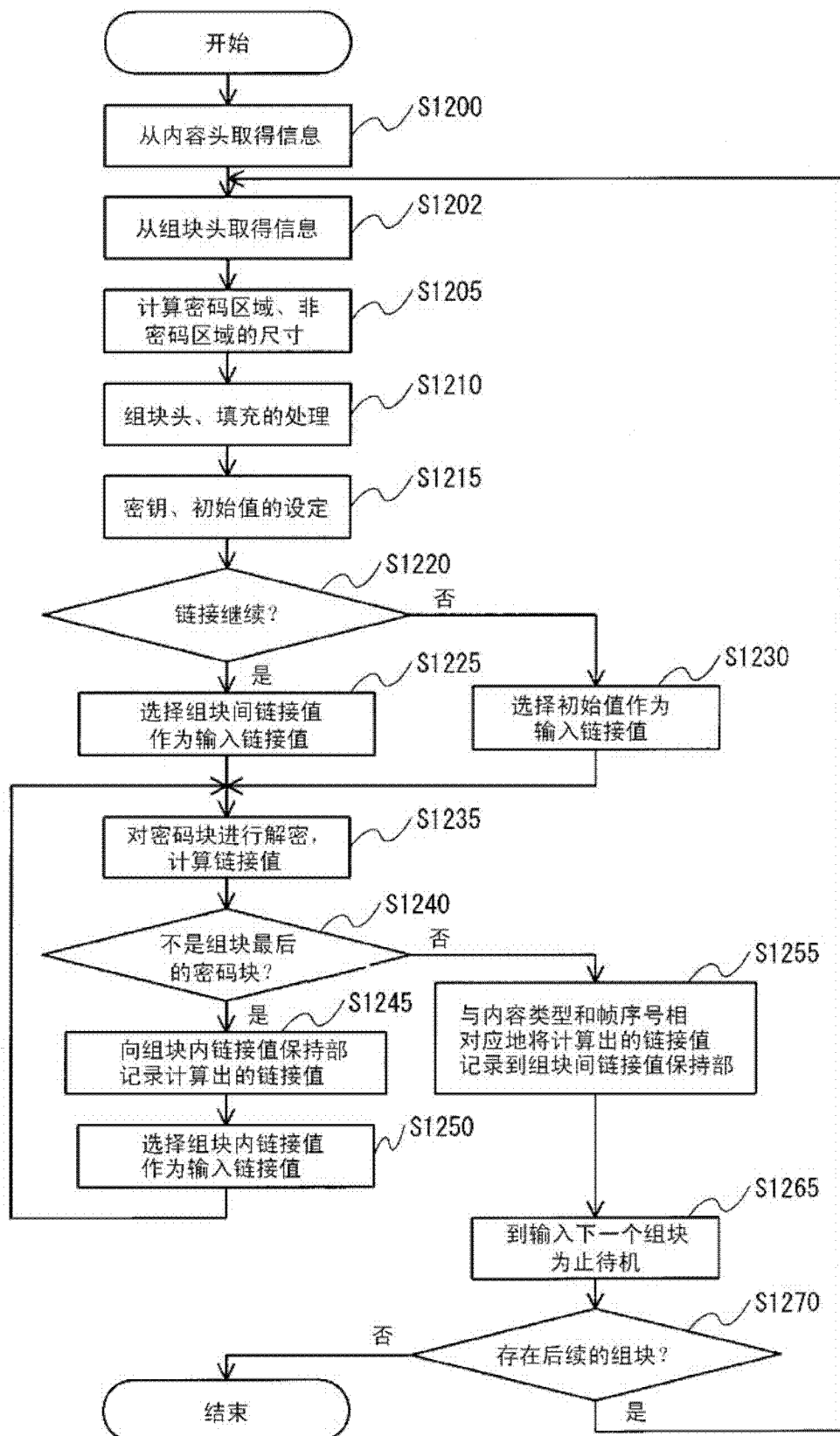


图 12

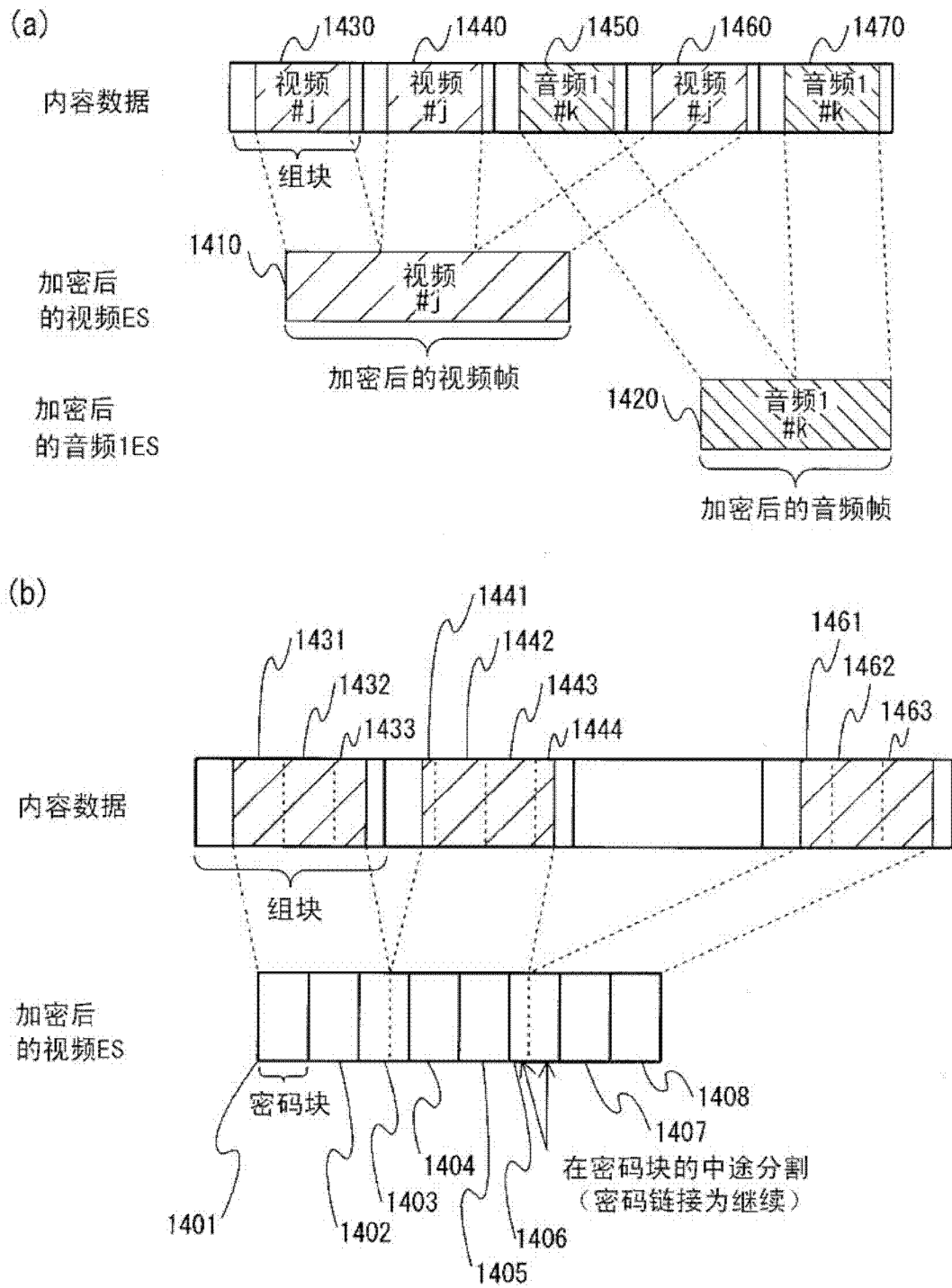


图 13

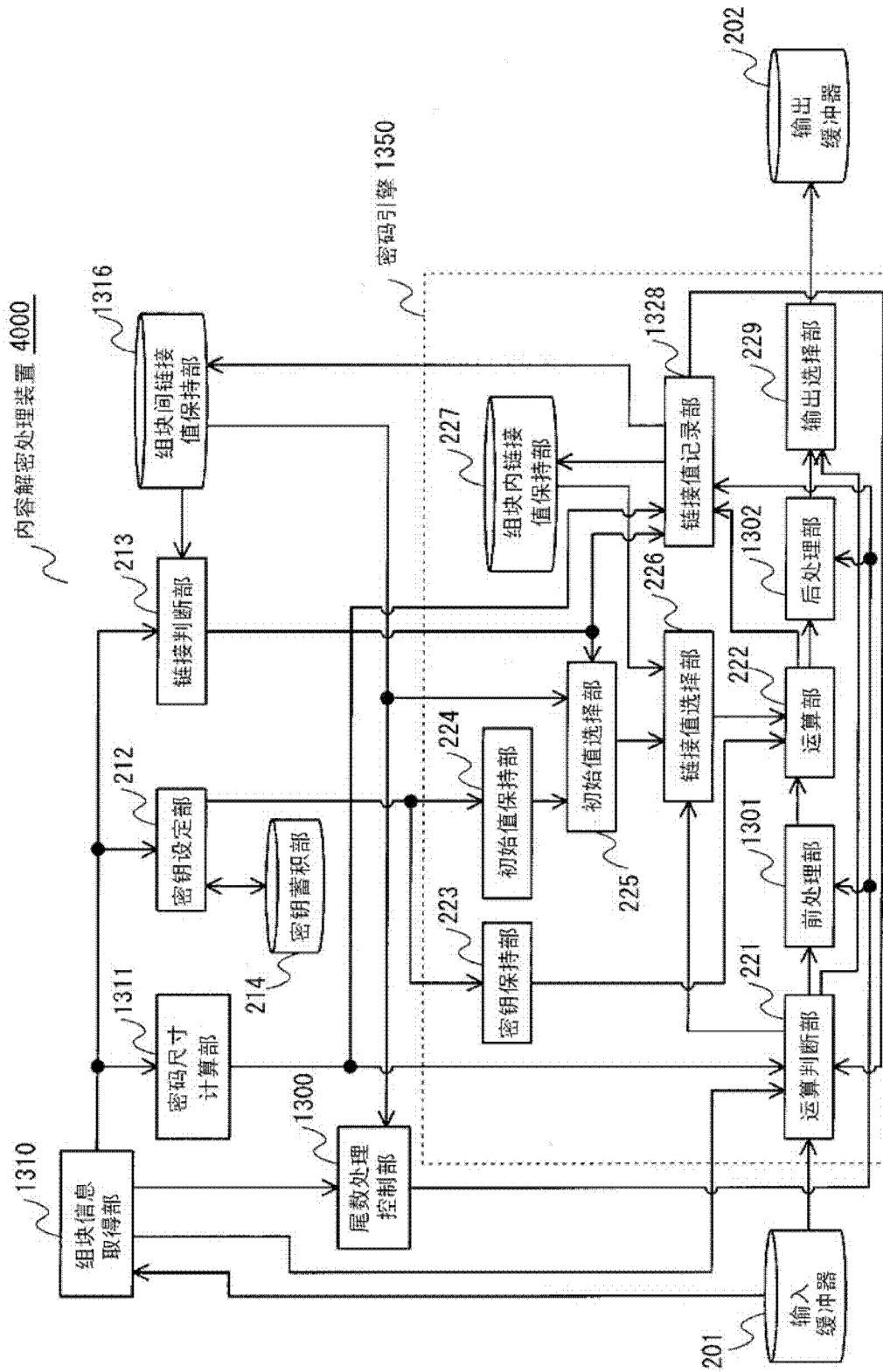


图 14

内容类型	帧序号	链接值	尾数数据尺寸
视频	0x00000100	0x01234567	0x1F
音频1	0x00000050	0x11223344	0x80
音频2	0x00000055	0x88881111	0x42

图 15

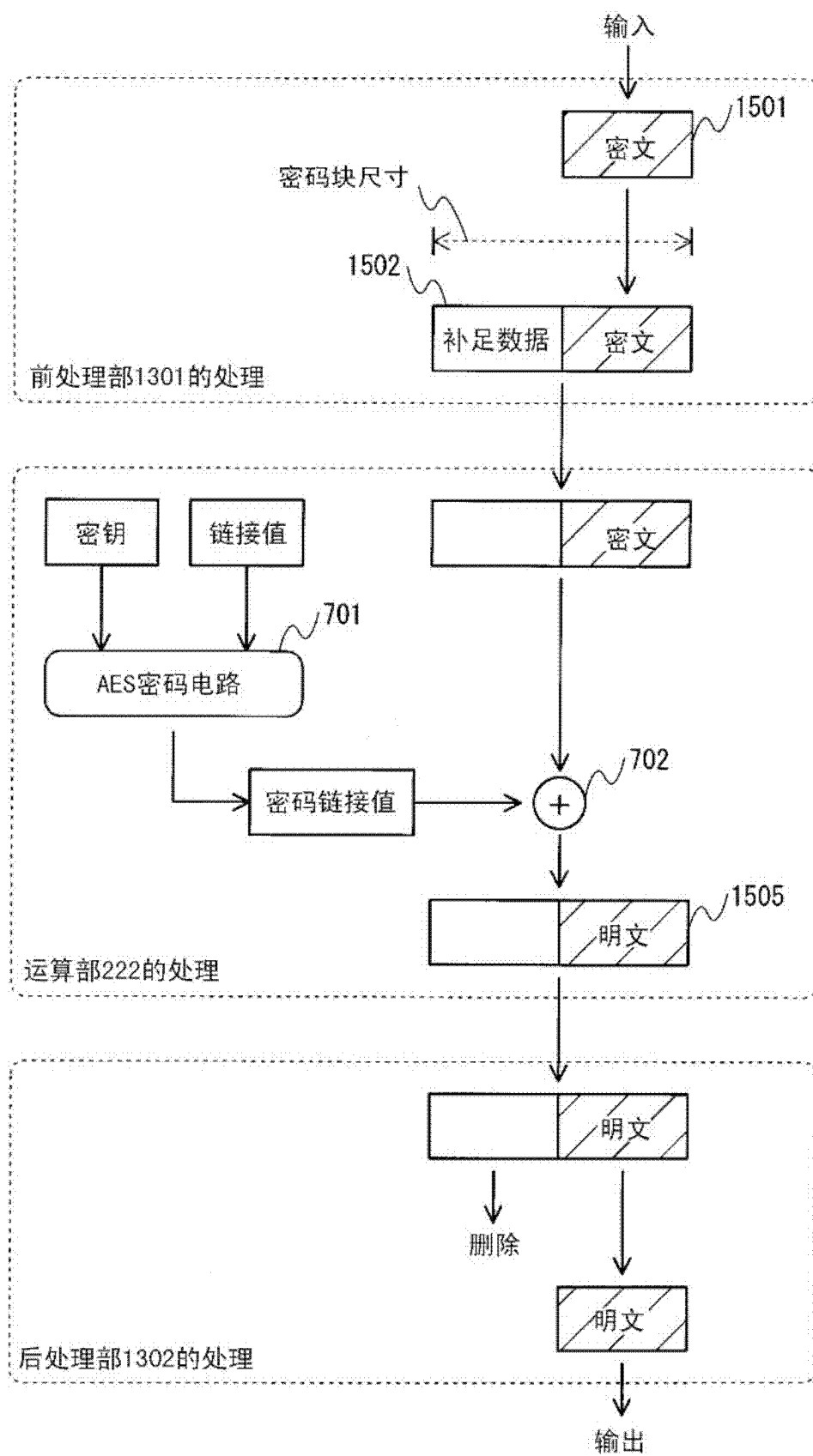


图 16

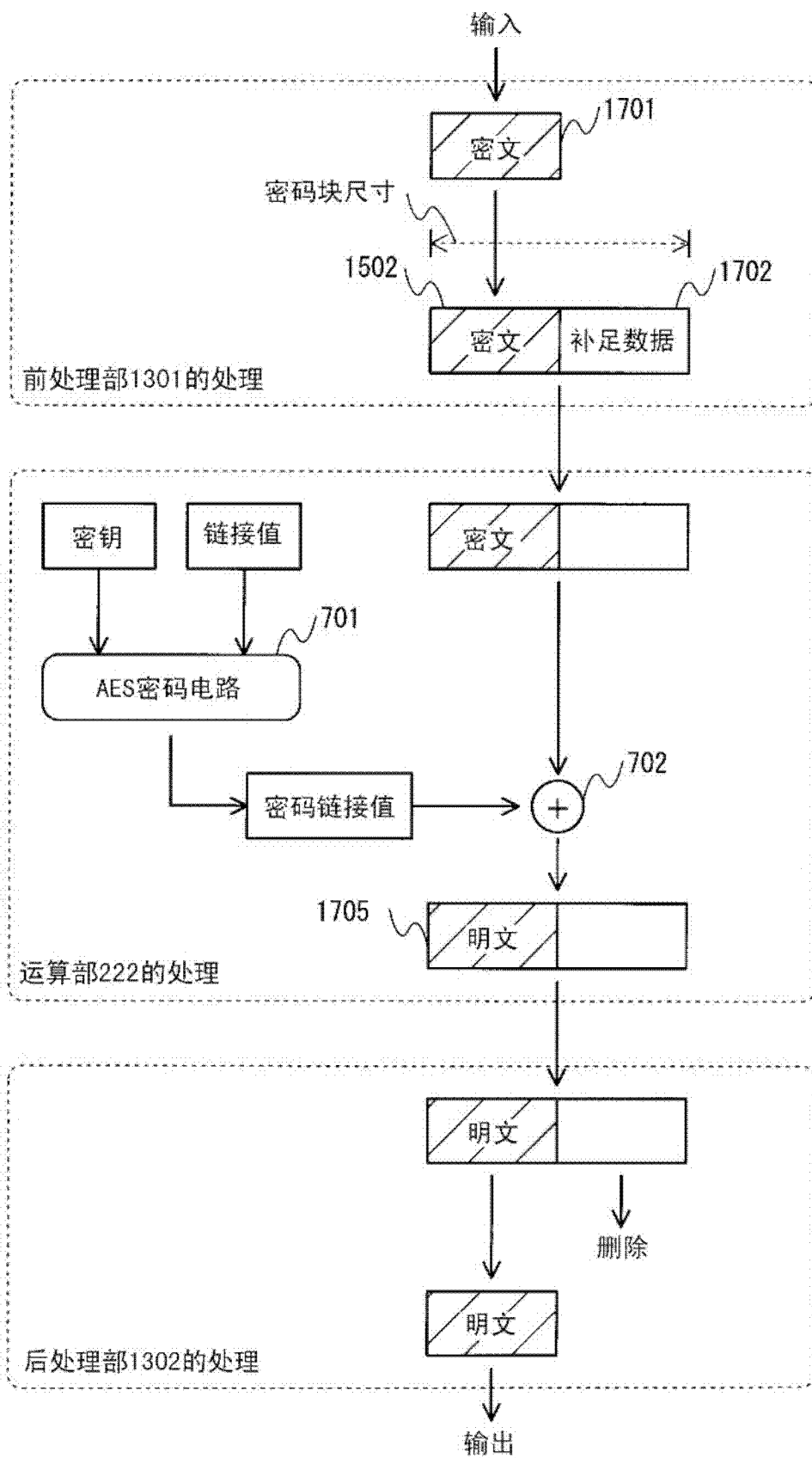


图 17

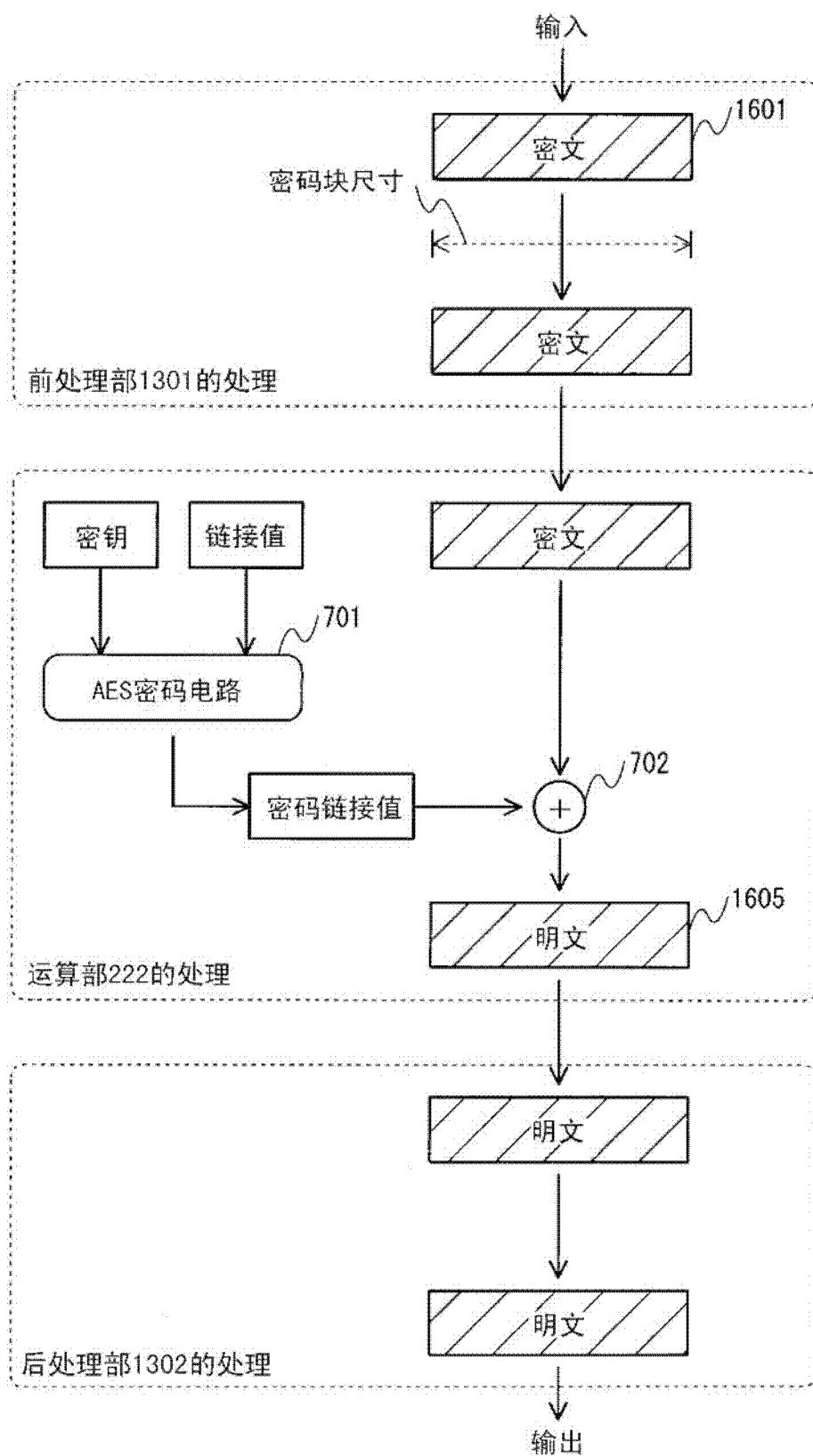


图 18

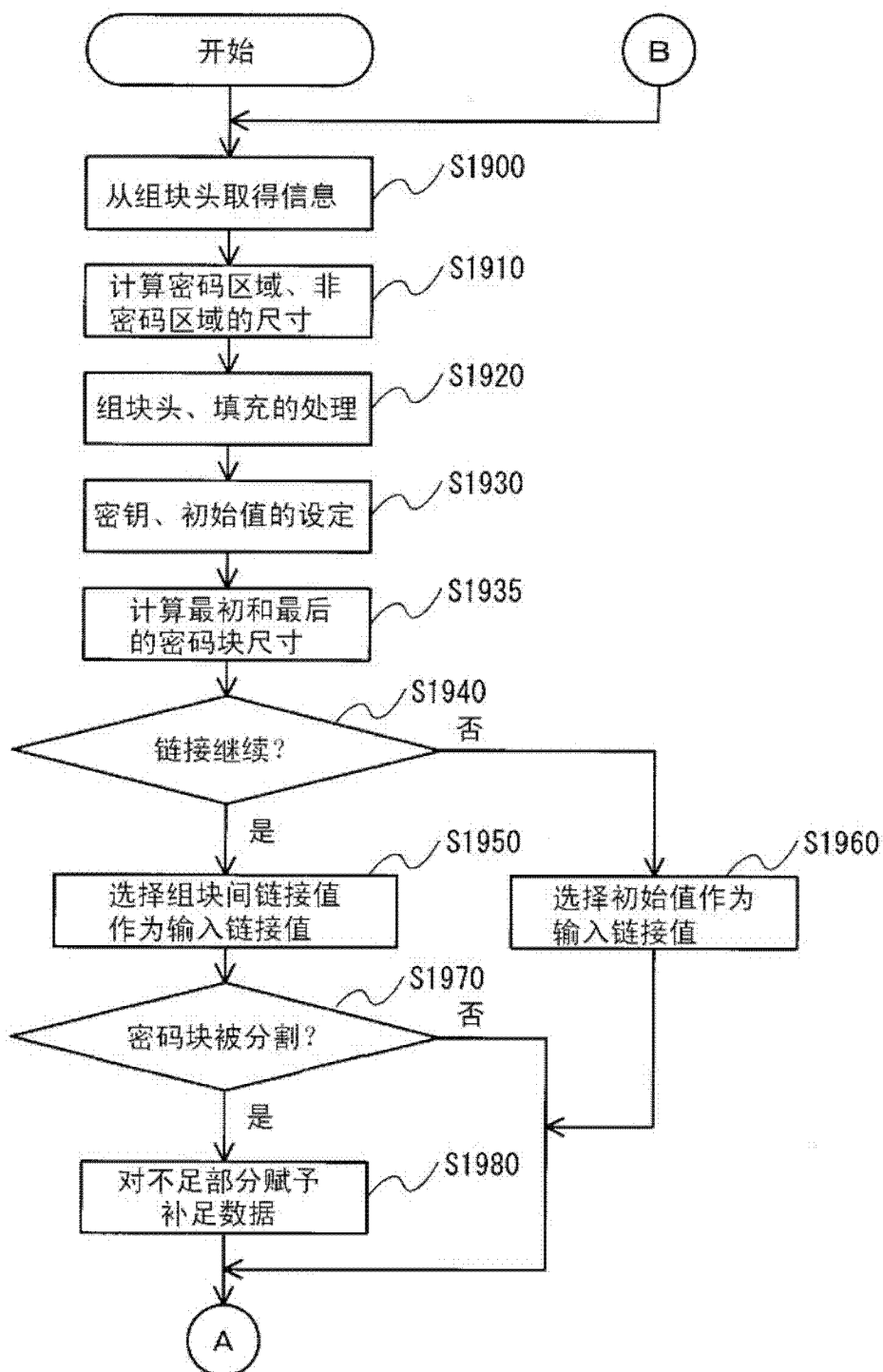


图 19

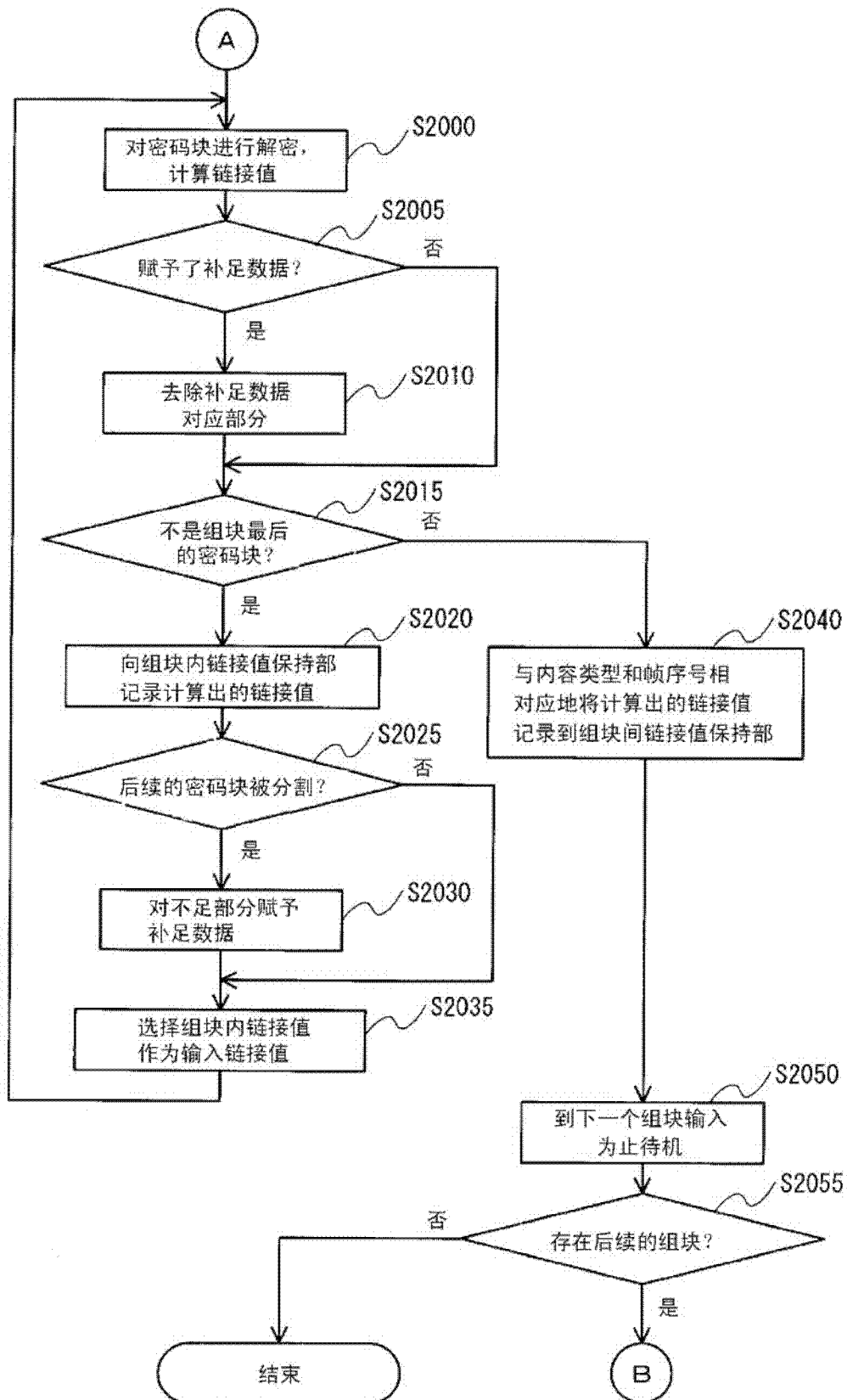


图 20

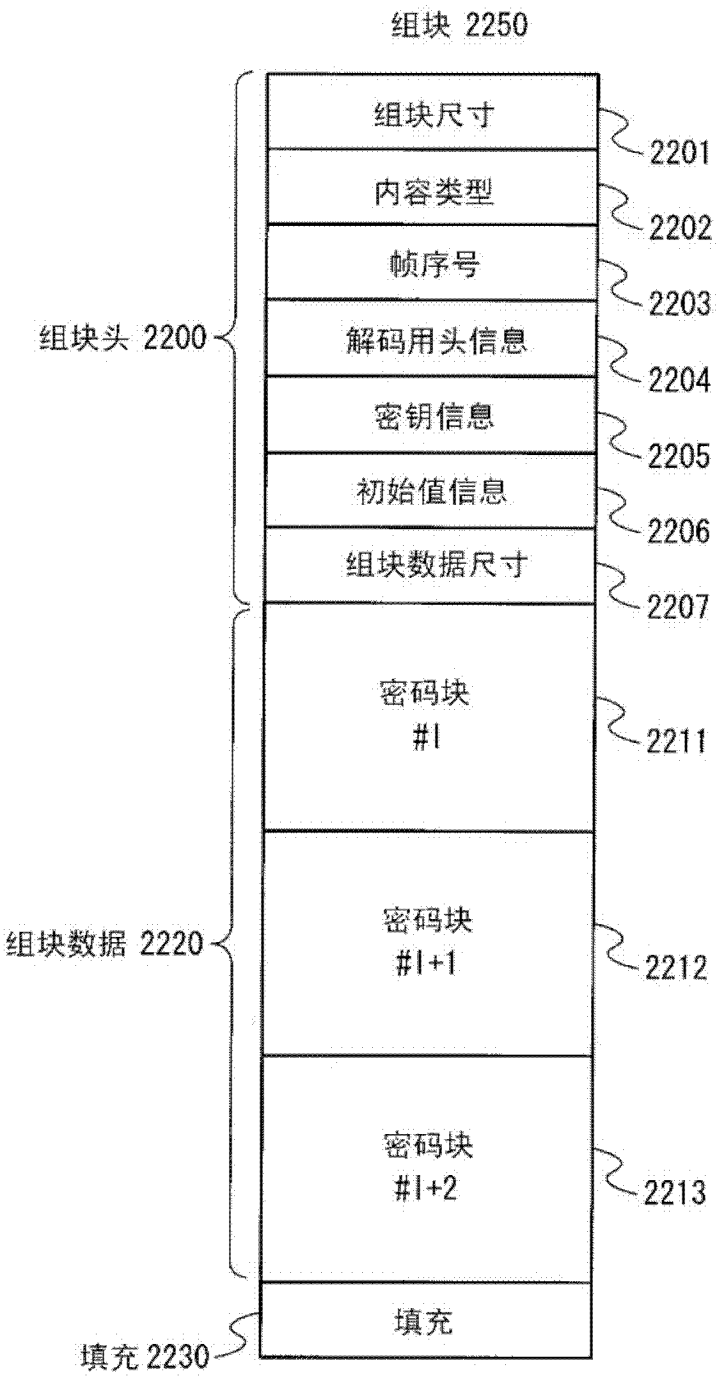


图 21

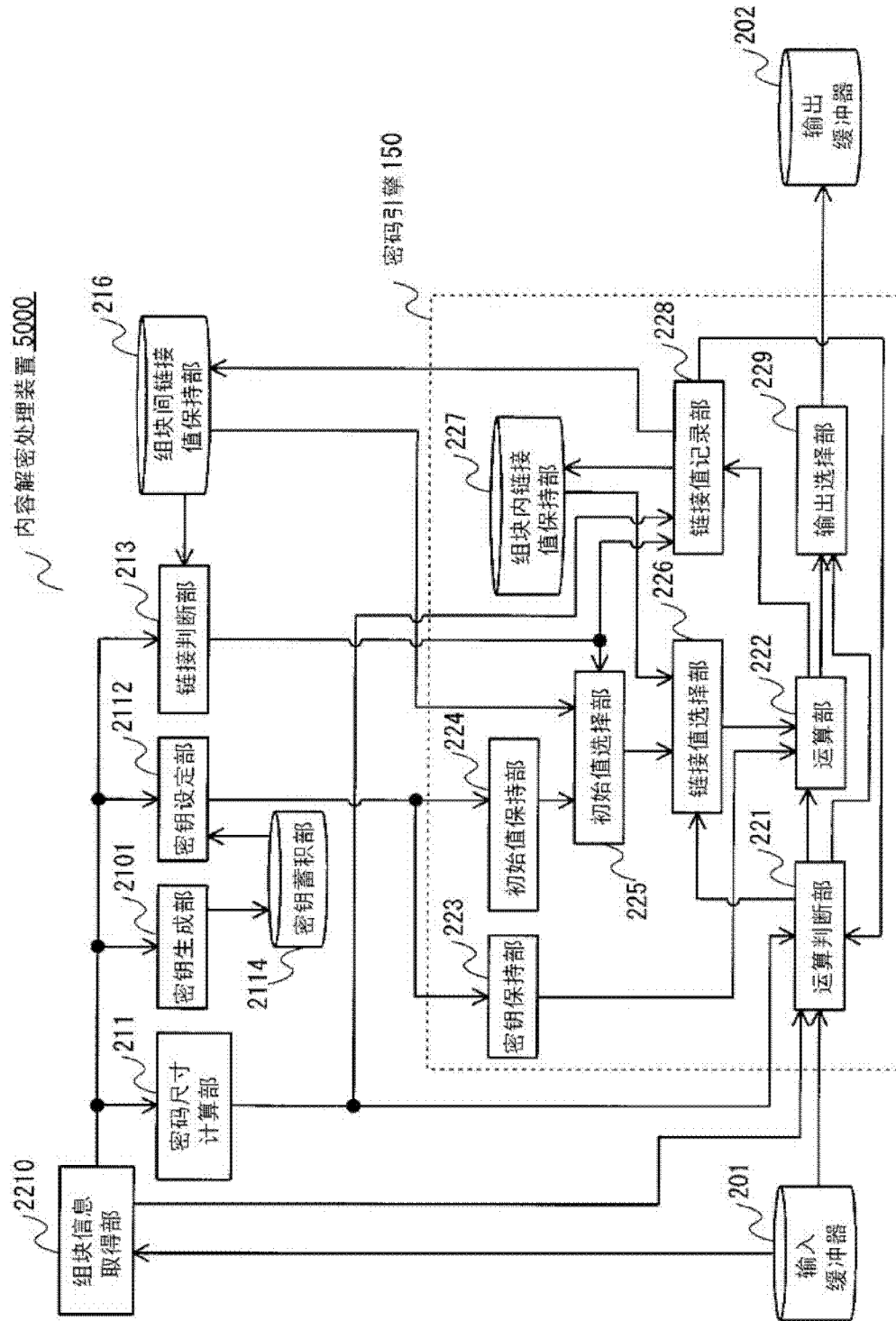


图 22

2300	2301	2302	2303
内容类型	帧序号	密钥	初始值
视频	0x00000000	0xAAAAFFFF	0x88880000
音频1	0x00000000	0x01234567	0xFEDCBA98
音频2	0x00000000	0x89ABCDEF	0x76543210
视频	0x00000001	0x02468024	0x23467890
音频1	0x00000001	0x43219876	0xBCDABC00
音频2	0x00000001	0xFFAB9912	0xABCFFF00
视频	0x00000002	0xECA86420	0x02468ACE
...	...	...	...
...	...	...	...
...	...	...	...

图 23

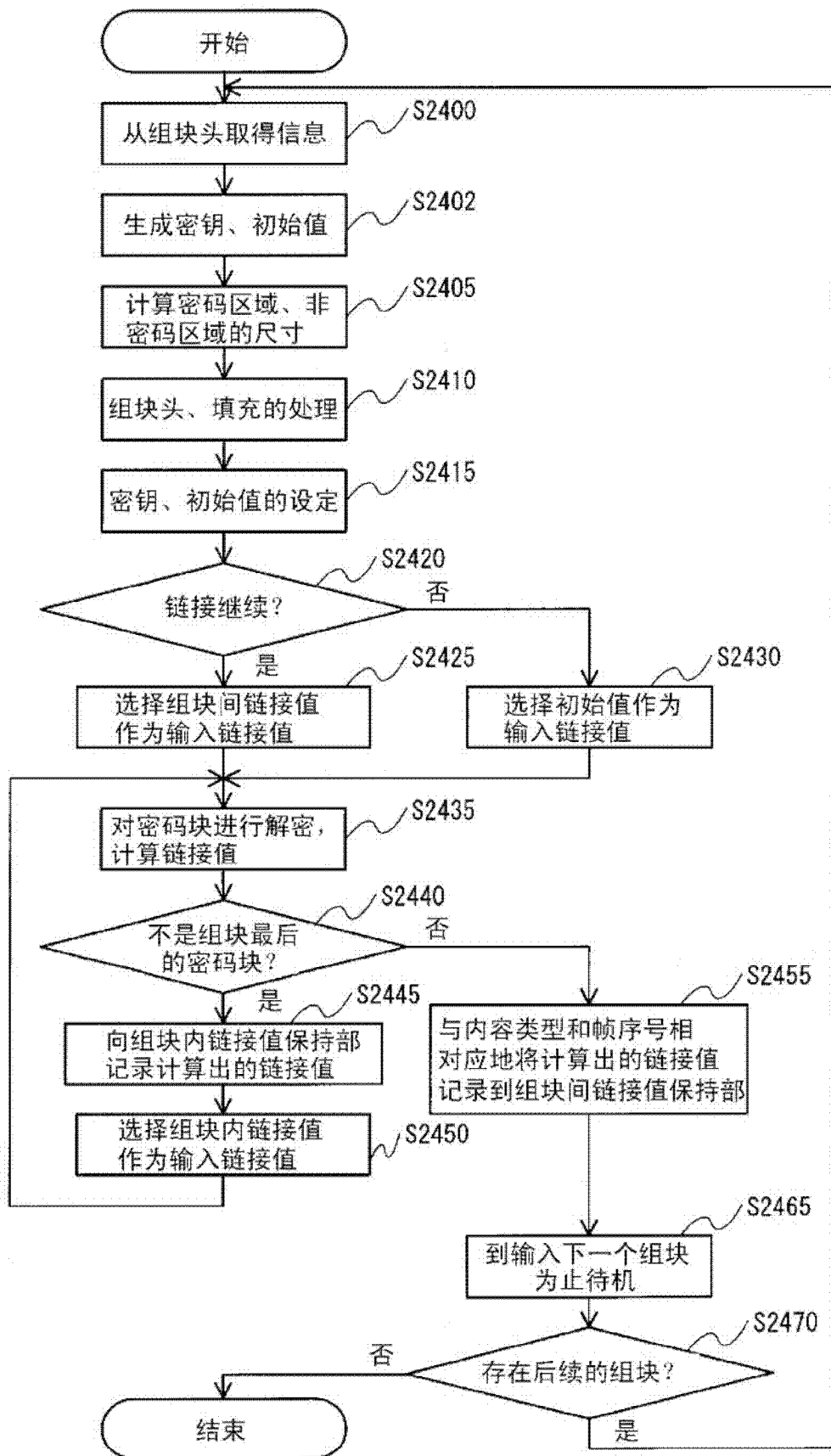


图 24

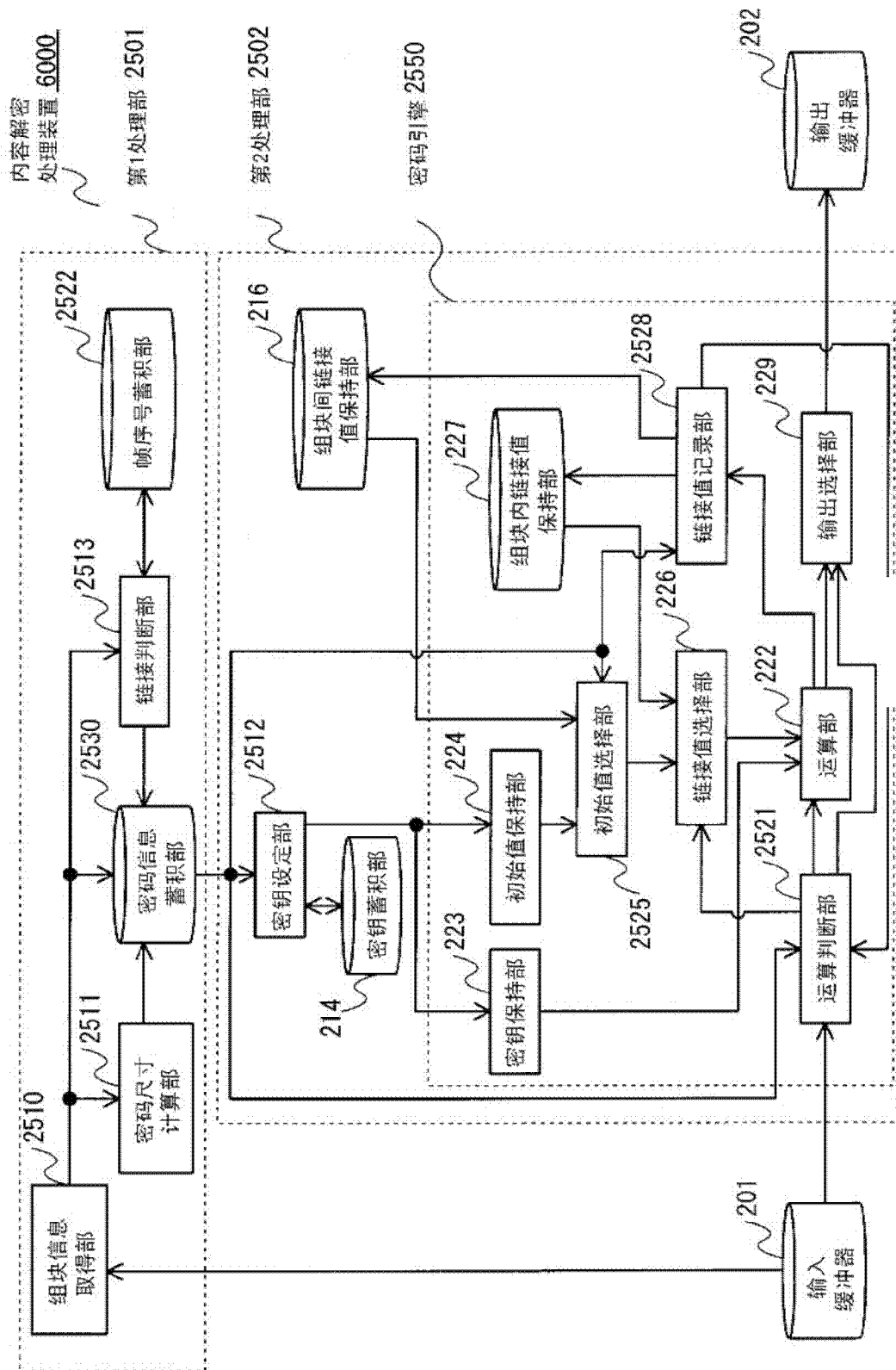


图 25



内容类型	帧序号
视频	0x00000002
音频1	0x00000001
音频2	0x00000001

图 26

2601	2602	2603	2604	2605	2606	2607	2608
开始地址	内容类型	帧序号	组块数据 开始地址	密码块数	填充开始地址	组块结束地址	有无链接
address_0	视频	0x00000000	size_0	0x03	address_a0	address_b0	X
address_1	视频	0x00000000	size_1	0x03	address_a1	address_b1	O
address_2	视频	0x00000000	size_2	0x03	address_a2	address_b2	O
address_3	音频1	0x00000000	size_3	0x03	address_a3	address_b3	X
...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...

图 27

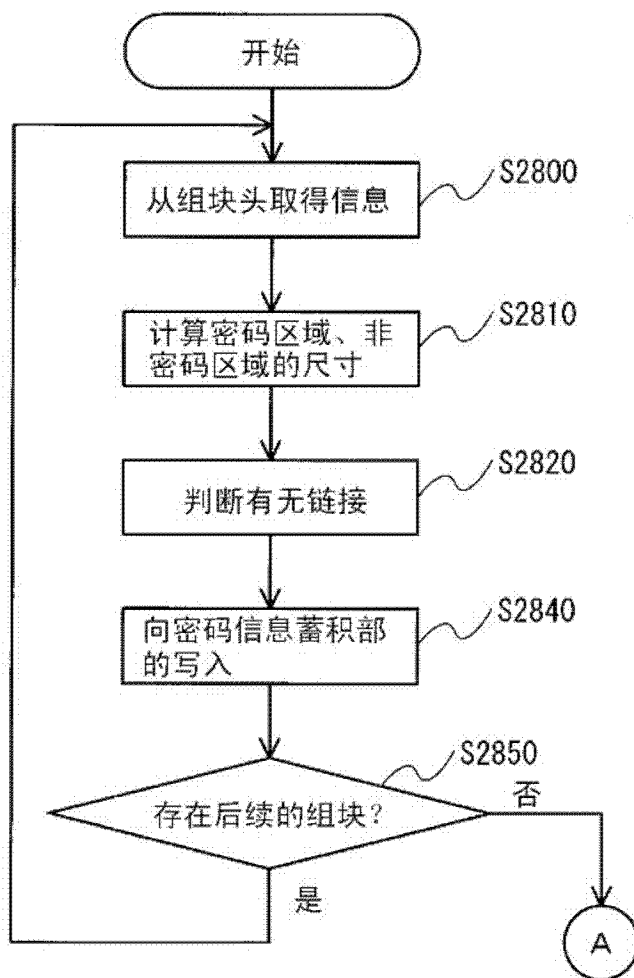


图 28

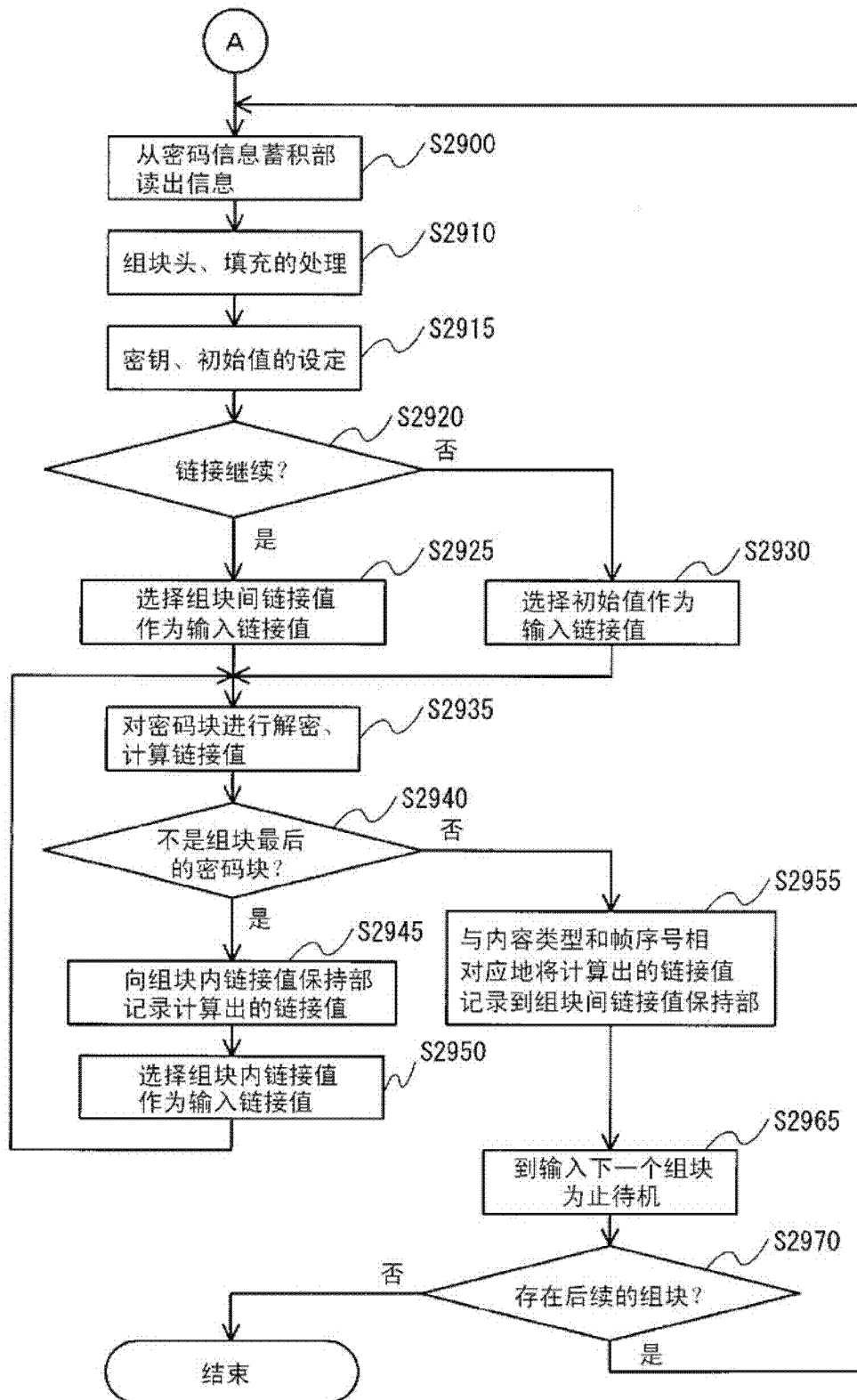


图 29

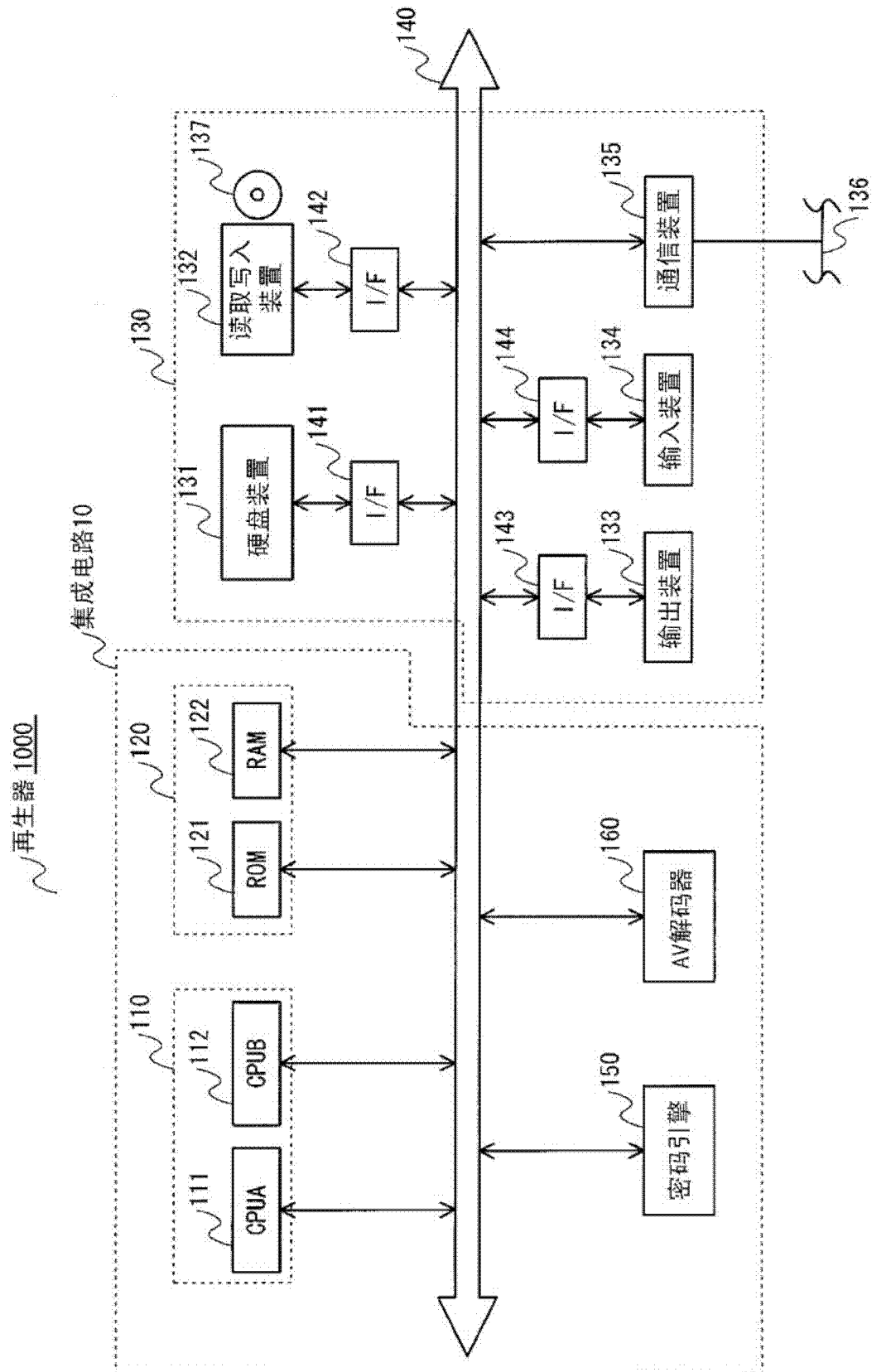


图 30