(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110785960 B
(45)授权公告日 2023.06.20

(21)申请号 201780092255.7

(22)申请日 2017.06.27

(65)同一申请的已公布的文献号
申请公布号 CN 110785960 A

(43)申请公布日 2020.02.11

(85)PCT国际申请进入国家阶段日
2019.12.18

(86)PCT国际申请的申请数据
PCT/JP2017/023646 2017.06.27

(87)PCT国际申请的公布数据
WO2019/003321 JA 2019.01.03

(73)专利权人 三菱电机株式会社
地址 日本东京都

(72)发明人 反町亨

(74)专利代理机构 北京三友知识产权代理有限公司 11127
专利代理师 马建军 邓毅

(51)Int.Cl.
H04L 9/06(2006.01)
G09C 1/00(2006.01)
H04B 1/707(2011.01)

(56)对比文件
US 2017033833 A1,2017.02.02
US 6463150 B1,2002.10.08
CN 103621007 A,2014.03.05
JP 2002118497 A,2002.04.19
JP 2016103799 A,2016.06.02
WO 2012146550 A1,2012.11.01
Huang Chunguang ect..Permutation of Image Encryption System Based on Block Cipher and Stream Cipher Encryption Algorithm.《2015 Third International Conference on Robot, Vision and Signal Processing (RVSP)》.2016,全文.
郑世慧;张国艳;杨义先;李忠献;.基于混沌的带密钥散列函数安全分析.通信学报.2011,(第05期),全文.
吴林煌;杨秀芝;.DVB通用加扰算法研究与硬件实现.中国有线电视.2008,(第12期),全文.

审查员 刘慧敏

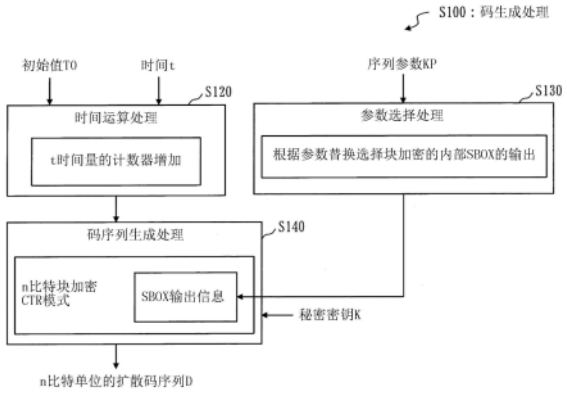
权利要求书2页 说明书10页 附图13页

(54)发明名称

码生成装置、码生成方法和计算机能读取的存储介质

(57)摘要

码生成装置(100)使用输出多个块作为扩散码序列(D)的块加密处理生成多个扩散码序列。参数选择部(130)取得与多个扩散码序列的各扩散码序列(D)唯一对应的序列参数(KP)。秘密密钥取得部(150)取得秘密密钥(K)。码序列生成部(140)在通过使用序列参数(KP)和秘密密钥(K)的块加密处理生成多个扩散码序列的各扩散码序列(D)时,使用序列参数(KP)对从处理要素输出的输出数据进行变更。



CN 110785960 B

1.一种码生成装置,该码生成装置使用输出多个块作为扩散码序列的块加密处理生成多个扩散码序列,所述块加密处理具有被输入输入数据且输出输出数据的处理要素,其中,所述码生成装置具有:

参数选择部,其选择与所述多个扩散码序列的各扩散码序列唯一对应的序列参数;

秘密密钥取得部,其取得秘密密钥;以及

码序列生成部,其使用所述序列参数和所述秘密密钥执行所述块加密处理,由此生成所述多个扩散码序列的各扩散码序列,所述码序列生成部在生成各扩散码序列时,使用所述序列参数对从所述处理要素输出的所述输出数据进行变更,

其中,

作为所述处理要素,所述块加密处理具有根据置换表以比特为单位对所述输入数据进行置换的置换处理,以及

所述码序列生成部被配置为仅使用一种块加密处理生成所述多个扩散码序列,

所述块加密处理保持可证明的安全性,

所述码序列生成部被配置为利用所述序列参数的至少一部分对置换处理的输出数据进行掩蔽,由此变更输出数据,

所述码序列生成部被配置为以计数器模式执行所述块加密处理,由此生成所述多个扩散码序列的各扩散码序列,

所述码生成装置具有时间运算部,该时间运算部被配置为对在计数器模式中使用的计数器值进行向上计数,按照每个阈值时间将所述计数器值输出到所述码序列生成部,以及

所述码序列生成部根据所述计数器值、所述秘密密钥和所述序列参数生成所述多个扩散码序列中的各扩散码序列。

2.根据权利要求1所述的码生成装置,其中,

所述参数选择部选择多个序列参数,所述多个序列参数分别与多个扩散码序列的各扩散码序列唯一对应,

所述码生成装置具有多个码序列生成部,通过所述参数选择部将所述多个序列参数的各序列参数输出到所述多个码序列生成部的各码序列生成部,由此生成所述多个扩散码序列。

3.一种码生成装置的码生成方法,该码生成装置使用输出多个块作为扩散码序列的块加密处理生成多个扩散码序列,所述块加密处理具有被输入输入数据且输出输出数据的处理要素,其中,

参数选择部选择与所述多个扩散码序列的各扩散码序列唯一对应的序列参数,

秘密密钥取得部取得秘密密钥,

码序列生成部使用所述序列参数和所述秘密密钥执行所述块加密处理,由此生成所述多个扩散码序列的各扩散码序列,

码序列生成部在生成各扩散码序列时,使用所述序列参数对从所述处理要素输出的所述输出数据进行变更,

其中,

作为所述处理要素,所述块加密处理具有根据置换表以比特为单位对所述输入数据进行置换的置换处理,

所述码序列生成部仅使用一种块加密处理生成所述多个扩散码序列，

所述块加密处理保持可证明的安全性，以及

所述码序列生成方法还包括由所述码序列生成部掩蔽作为所述序列参数的至少一部分的置换处理的输出数据，由此变更输出数据，

所述码序列生成部以计数器模式执行所述块加密处理，由此生成所述多个扩散码序列的各扩散码序列，

所述码生成方法包括：

利用时间运算部对在计数器模式中使用的计数器值进行向上计数，按照每个阈值时间将所述计数器值输出到所述码序列生成部，

所述码序列生成部根据所述计数器值、所述秘密密钥和所述序列参数生成所述多个扩散码序列中的各扩散码序列。

4.一种存储有码生成装置的码生成程序的计算机能读取的存储介质，该码生成装置使用输出多个块作为扩散码序列的块加密处理生成多个扩散码序列，所述块加密处理具有被输入输入数据且输出输出数据的处理要素，其中，所述码生成程序使作为计算机的码生成装置执行以下处理：

参数选择处理，选择与所述多个扩散码序列的各扩散码序列唯一对应的序列参数；

秘密密钥取得处理，取得秘密密钥；以及

码序列生成处理，使用所述序列参数和所述秘密密钥执行所述块加密处理，由此生成所述多个扩散码序列的各扩散码序列，所述码序列生成处理在生成各扩散码序列时，使用所述序列参数对从所述处理要素输出的所述输出数据进行变更，

其中，

作为所述处理要素，所述块加密处理具有根据置换表以比特为单位对所述输入数据进行置换的置换处理，

所述码序列生成处理仅使用一种块加密处理生成所述多个扩散码序列，

所述块加密处理保持可证明的安全性，以及

所述码序列生成处理包括输出数据的掩蔽过程，所述掩蔽过程是所述序列参数的至少一部分的替换处理，由此对所述输出数据进行变更，

所述码序列处理以计数器模式执行所述块加密处理，由此生成所述多个扩散码序列的各扩散码序列，

所述码生成程序使所述码生成装置进一步执行：

时间计算处理，对在计数器模式中使用的计数器值进行计数，按照每个阈值时间将所述计数器值输出到所述码序列生成部，

所述码序列处理根据所述计数器值、所述秘密密钥和所述序列参数生成所述多个扩散码序列中的各扩散码序列。

码生成装置、码生成方法和计算机能读取的存储介质

技术领域

[0001] 本发明涉及生成隐匿性较高的多个扩散码序列的码生成装置、码生成方法和计算机能读取的存储介质。

背景技术

[0002] 近年来，已提供利用卫星通信或无线通信的各种服务。在这些服务中，为了实现通信的连续性和隐匿性而使用谱扩散方式。谱扩散方式存在直扩方式和跳频方式。在直扩方式中，在比发送数据本身宽的频率中扩散能量进行数据通信。在跳频方式中，按照一定的规则高速切换频率，在发送接收机之间进行通信。

[0003] 在直扩方式中，使用扩散码序列，将希望传输的信号扩展到宽带。由此，直扩方式具有希望传输的信号看起来像噪音这样的特性。该特性使希望传输的信号不容易被拦截，提高抗干扰性。由此，直扩方式不容易引起针对窄带信号的干扰。这样，直扩方式中的扩散码序列不会产生与其他信号之间的较高的干扰，在实现可靠且安全的传输方面是重要的。

[0004] 在一般被利用的直扩方式中，使用周期性较短的扩散码序列，由此，通信的连续性提高。但是，通过在一定期间内观测周期性较短的扩散码序列，被估计出的可能性较高，隐匿性较低。但是，为了提高来自干扰电波的耐性，需要提高隐匿性。因此，使用延长扩散码序列的周期这样的方法。或者，使用采用利用第三者无法预测的秘密信息的扩散码序列这样的方法。在专利文献1中，作为提高扩散码序列的隐匿性的技术，公开有使用混沌序列的方法。

[0005] 在专利文献1中公开有应用于卫星导航系统和CDMA(Code Division Multiple Access)通信系统的混沌扩散码的生成方法。在专利文献1中公开有：基于混沌序列的扩散码具有自相关特性和互相关特性，隐匿性提高。基于混沌序列的扩散码的隐匿性示出具有伪随机性的随机性。但是，基于混沌序列的扩散码的隐匿性未示出使用加密技术的情况下示出的严格的安全性。此外，为了使用基于混沌序列的扩散码进行隐匿性较高的谱扩散通信，需要实现混沌序列的同步建立。但是，在专利文献1中未示出同步建立用的有效方式。

[0006] 此外，在专利文献2～专利文献7中的现有技术中，公开有使用混沌序列实现隐匿性的提高的方式。但是，在专利文献2～专利文献7中的现有技术中未示出混沌序列的同步建立用的有效方式。

[0007] 作为混沌序列的同步建立用的有效方式，可考虑利用n比特块加密算法的CTR(Counter：计数器)模式的方式。

[0008] 现有技术文献

[0009] 专利文献

[0010] 专利文献1：日本特表2010-511336号公报

[0011] 专利文献2：日本特开平9-186630号公报

[0012] 专利文献3：日本特开平11-266179号公报

[0013] 专利文献4：日本特开2000-252751号公报

[0014] 专利文献5:日本特开2001-292129号公报

[0015] 专利文献6:日本特开2002-290274号公报

[0016] 专利文献7:日本特开2007-96815号公报

发明内容

[0017] 发明要解决的课题

[0018] 以往,提出了使用混沌序列或较长寄存器尺寸的反馈移位寄存器的码生成方式。在利用现有的码生成方式的通信系统中,提高扩散码序列的隐匿性,或者增大扩散码序列的周期。由此,无法搜索码全体,难以实现同步建立。因此,提出了使用实际数据发送用的扩散码序列和同步捕捉用的导频序列的通信系统。

[0019] 但是,在该通信系统中,对1个通信频带进行二分割来发送信号,因此,通信效率降低。此外,在使用导频序列的情况下,在通信系统的接收侧,需要用于导出经过一定时间后的扩散码序列的专用运算功能和导出时间。

[0020] 在对多个卫星之间进行中继的通信系统中,对通信进行中继的中继卫星需要根据通信对方的卫星数量和地面的控制站数量,同时生成多个扩散码序列。在现有的隐匿性较高的码生成方式中,需要按照每个扩散码序列而不同的混沌序列、较长寄存器尺寸的反馈移位寄存器或非线性转换函数,按照每个扩散码序列需要生成装置。由此,存在搭载于卫星时的安装规模受到较大制约这样的课题。

[0021] 在本发明中,其目的在于,提供通过对块加密算法的结构的一部分进行变更而生成隐匿性较高的多个扩散码序列的码生成装置。

[0022] 用于解决课题的手段

[0023] 本发明的码生成装置使用输出多个块作为扩散码序列的块加密处理生成多个扩散码序列,所述块加密处理具有被输入输入数据且输出输出数据的处理要素,其中,所述码生成装置具有:参数选择部,其选择与所述多个扩散码序列的各扩散码序列唯一对应的序列参数;秘密密钥取得部,其取得秘密密钥;以及码序列生成部,其使用所述序列参数和所述秘密密钥执行所述块加密处理,由此生成所述多个扩散码序列的各扩散码序列,所述码序列生成部在生成各扩散码序列时,使用所述序列参数对从所述处理要素输出的所述输出数据进行变更。

[0024] 发明效果

[0025] 本发明的码生成装置使用输出多个块作为扩散码序列的块加密处理生成多个扩散码序列。参数选择部选择与多个扩散码序列的各扩散码序列唯一对应的序列参数。秘密密钥取得部取得秘密密钥。码序列生成部使用序列参数和秘密密钥执行块加密处理,由此生成多个扩散码序列的各扩散码序列。码序列生成部在生成各扩散码序列时,使用序列参数对从处理要素输出的输出数据进行变更。这样,根据本发明的码生成装置,使用与扩散码序列唯一对应的序列参数对块加密处理的处理要素的一部分进行变更,由此能够生成多个扩散码序列。由此,根据本发明的码生成装置,发挥能够生成隐匿性较高的多个扩散码序列这样的效果。

附图说明

[0026] 图1是实施方式1的码生成装置100的结构图。

[0027] 图2是示出实施方式1的码生成装置100的码生成处理S100的流程图。

[0028] 图3是示出用于与实施方式1的码生成装置100进行比较的比较例的扩散码生成方式的图。

[0029] 图4是实施方式1的在码序列生成部140中使用MISTY(注册商标)的情况下的具体的结构图。

[0030] 图5是示出实施方式1的在码序列生成部140中使用MISTY(注册商标)的情况下的SBOX的输出结构例1-1的图。

[0031] 图6是示出实施方式1的在码序列生成部140中使用MISTY(注册商标)的情况下的SBOX的输出结构例1-2的图。

[0032] 图7是示出实施方式1的在码序列生成部140中使用MISTY(注册商标)的情况下的SBOX的输出结构例2的图。

[0033] 图8是示出实施方式1的在码序列生成部140中采用图7的输出结构例2的情况下的S7函数的输出结构例2-1的图。

[0034] 图9是示出实施方式1的在码序列生成部140中采用图7的输出结构例2的情况下的S9函数的输出结构例2-2的图。

[0035] 图10是实施方式1的变形例的码生成装置100的结构图。

[0036] 图11是实施方式2的码生成装置100a的结构图。

[0037] 图12是示出实施方式2的码生成装置100a的码生成处理S100a的流程图。

[0038] 图13是示出实施方式2的码生成装置100a的效果的例子的图。

具体实施方式

[0039] 下面,使用附图对本发明的实施方式进行说明。另外,在各图中,对相同或相当的部分标注相同的标号。在实施方式的说明中,针对相同或相当的部分,适当省略或简化说明。

[0040] 实施方式1

[0041] ***结构的说明***

[0042] 使用图1对本实施方式的码生成装置100的结构进行说明。

[0043] 本实施方式的码生成装置100实现能够生成隐匿性较高的多个扩散码序列的扩散码方式。码生成装置100使用输出多个块作为扩散码序列的块加密处理生成多个扩散码序列。块加密处理具有多个处理要素。下面,将块加密处理也称作块加密算法。此外,将块加密处理的处理要素也称作块加密算法的内部结构要素。

[0044] 码生成装置100是计算机。码生成装置100具有处理器910,并且具有存储器921、辅助存储装置922、输入接口930和输出接口940这样的其他硬件。处理器910经由信号线而与其他硬件连接,对这些其他硬件进行控制。

[0045] 作为功能要素,码生成装置100具有初始值取得部110、时间运算部120、参数选择部130、码序列生成部140、秘密密钥取得部150和码序列输出部160。初始值取得部110、时间运算部120、参数选择部130、码序列生成部140、秘密密钥取得部150和码序列输出部160的

功能通过软件实现。

[0046] 处理器910是执行码生成程序的装置。码生成程序是实现初始值取得部110、时间运算部120、参数选择部130、码序列生成部140、秘密密钥取得部150和码序列输出部160的功能的程序。

[0047] 处理器910是进行运算处理的IC(Integrated Circuit:集成电路)。处理器910的具体例是CPU(Central Processing Unit:中样中央处理单元)、DSP(Digital Signal Processor:数字信号处理器)、GPU(Graphics Processing Unit:图形处理单元)。

[0048] 存储器921在暂时存储数据的存储装置。存储器921的具体例是SRAM(Static Random Access Memory:静态随机存取存储器)、DRAM(Dynamic Random Access Memory:动态随机存取存储器)。

[0049] 辅助存储装置922是保管数据的存储装置。辅助存储装置922的具体例是HDD(Hard Disk Drive:硬盘驱动器)。此外,辅助存储装置922也可以是SD(注册商标)(Secure Digital:安全数字)存储卡、CF(CompactFlash:闪存)、NAND闪存、软盘、光盘、高密度盘、蓝光(注册商标)盘、DVD(Digital Versatile Disk:数字多功能盘)这样的移动存储介质。

[0050] 输入接口930是与鼠标、键盘、触摸面板这样的输入装置连接的端口。具体而言,输入接口930是USB(Universal Serial Bus:通用串行总线)端子。另外,输入接口930也可以是与LAN(Local Area Network:局域网)连接的端口。

[0051] 输出接口940是连接有显示器这样的显示设备的缆线的端口。具体而言,输出接口940是USB端子或HDMI(注册商标)(High Definition Multimedia Interface:高清晰度多媒体接口)端子。具体而言,显示器是LCD(Liquid Crystal Display:液晶显示器)。

[0052] 码生成程序被读入到处理器910,由处理器910来执行。在存储器921中,不仅存储有码生成程序,还存储有OS(Operating System:操作系统)。处理器910一边执行OS,一边执行码生成程序。码生成程序和OS也可以存储在辅助存储装置922中。辅助存储装置922中存储的码生成程序和OS被载入到存储器921,由处理器910来执行。另外,码生成程序的一部分或全部也可以嵌入OS中。

[0053] 码生成装置100也可以具有代替处理器910的多个处理器。这些多个处理器分担执行码生成程序。与处理器910同样,各个处理器是执行码生成程序的装置。

[0054] 码生成程序利用、处理或输出的数据、信息、信号值和变量值存储在存储器921、辅助存储装置922或处理器910内的寄存器或高速缓冲存储器中。

[0055] 码生成程序是使计算机执行将初始值取得部110、时间运算部120、参数选择部130、码序列生成部140、秘密密钥取得部150和码序列输出部160的各部的“部”改写成“处理”、“步骤”或“工序”后的各处理、各步骤或各工序的程序。此外,码生成方法是作为计算机的码生成装置100执行码生成程序而进行的方法。

[0056] 码生成程序可以记录在计算机能读取的存储介质中来提供,也可以作为程序产品来提供。

[0057] ***动作的说明***

[0058] 接着,对本实施方式的码生成装置100的各部的动作进行说明。

[0059] 图2是示出本实施方式的码生成装置100的码生成处理S100的图。

[0060] 使用图1和图2对本实施方式的码生成装置100的码生成处理S100进行说明。

[0061] 码生成处理S100具有时间运算部120进行的时间运算处理S120、参数选择部130进行的参数选择处理S130以及码序列生成部140进行的码序列生成处理S140。

[0062] 初始值取得部110经由输入接口930取得初始值T0。初始值取得部110将取得的初始值T0输出到时间运算部120。初始值T0是在块加密处理的CTR模式中使用的计数器值的初始值。

[0063] <时间运算处理S120>

[0064] 时间运算部120对在CTR模式中使用的计数器值进行向上计数，按照每个阈值时间t将计数器值Ct输出到码序列生成部140。时间运算部120从初始值取得部110接受初始值T0。此外，时间运算部120取得生成扩散码的间隔即阈值时间t。时间运算部120运算t时间后的初始值T0作为计数器值Ct，将计数器值Ct输出到码序列生成部140。然后，时间运算部120对计数器值进行向上计数，按照每个t时间将计数器值Ct输出到码序列生成部140。时间运算部120也称作t时间后初始值运算部。

[0065] 图3是示出比较例的扩散码生成方式的图。如图3所示，比较例的扩散码生成方式具有生成t时间后的初始值的专用运算功能。此外，比较例的扩散码生成方式具有用于取得同步的同步捕捉功能。此外，比较例的码生成方式具有多个码序列生成部，这多个码序列生成部具有按照要生成的每个扩散码序列而不同的算法。

[0066] 在时间运算处理S120中，时间运算部120导出t时间后的计数器值Ct。具体而言，时间运算部120实施t时间量的计数器增加，由此导出t时间后的计数器值Ct。由此，不需要如图3那样使用专用运算功能。此外，如果准确的时间推移这样地同步，则能够根据以时间的推移量向上计数出的计数器值导出扩散码序列。由此，也不需要使用用于捕捉同步的同步捕捉功能。

[0067] <参数选择处理S130>

[0068] 在参数选择处理S130中，参数选择部130选择与多个扩散码序列的各扩散码序列唯一对应的序列参数KP。具体而言，参数选择部130经由输入接口930取得序列参数KP。参数选择部130根据序列参数KP选择或生成算法结构要素131。算法结构要素131用于生成与序列参数KP对应的扩散码序列。参数选择部130将算法结构要素131输出到码序列生成部140。

[0069] 算法结构要素131是根据与扩散码序列唯一对应的序列参数KP求出的信息。具体而言，算法结构要素131用于对从在码序列生成处理S140中使用的块加密算法的处理要素输出的输出数据进行变更。这里，作为处理要素，块加密算法具有根据置换表以比特为单位对输入的输入数据进行置换的置换处理。置换处理的具体例是SBOX。

[0070] 参数选择部130根据输入的序列参数KP选择或生成输出参数Op。输出参数Op用于对从SBOX输出的输出数据的多个比特进行变更。然后，参数选择部130将输出参数Op作为算法结构要素131输出到码序列生成部140。

[0071] 另外，如果块加密算法保持可证明的安全性，则在根据序列参数KP对从SBOX输出的输出数据进行了变更的情况下，差分解读法的差分特性概率或线性解读法的线性特性概率的安全性也不会降低。这里，作为保持可证明的安全性的块加密算法的具体例，可举出MISTY(注册商标)。通过在块加密算法中采用MYSTY，能够对SBOX的输出数据进行变更而不会降低差分解读法的差分特性概率或线性解读法的线性特性概率的安全性。

[0072] 秘密密钥取得部150经由输入接口930取得秘密密钥K。秘密密钥取得部150将取得

的秘密密钥K输出到码序列生成部140。

[0073] <码序列生成处理S140>

[0074] 在码序列生成处理S140中，码序列生成部140通过使用序列参数KP和秘密密钥K的块加密算法，生成多个扩散码序列的各扩散码序列。码序列生成部140在生成扩散码序列时，使用序列参数KP对从处理要素输出的输出数据进行变更。

[0075] 具体而言，码序列生成部140从时间运算部120接受t时间后的计数器值Ct，从秘密密钥取得部150接受秘密密钥K。此外，码序列生成部140从参数选择部130接受序列参数KP作为算法结构要素131。码序列生成部140根据t时间后的计数器值Ct、秘密密钥K和序列参数KP生成扩散码序列。码序列生成部140将生成的扩散码序列输出到码序列输出部160。此外，码序列生成部140生成以CTR模式执行块加密算法而输出的块作为扩散码序列。

[0076] 具体而言，码序列生成部140利用n比特块加密算法的CTR模式生成n比特单位的扩散码序列。

[0077] 在CTR模式的块加密方式中，对块加密算法的计数器(以下记作CTR)输入初始值，对秘密密钥输入秘密信息。然后，CTR模式的块加密方式生成n比特的随机数据串。然后，在CTR模式的块加密方式中，CTR增加1比特，CTR被输入到块加密算法。然后，CTR模式的块加密方式生成下一个不同的n比特的随机数据串。在n比特块加密的情况下，能够生成2^n次的增加量的n比特随机数据。因此，能够利用n比特$\times 2^n$次的随机数据作为扩散码序列。在一般的块加密算法中，当前利用块尺寸为64比特的MISTY(注册商标)和KASUMI或块尺寸为128比特的AES和Camellia(注册商标)。在采用这些块加密算法的CTR模式的码序列生成处理S140中，码序列生成部140能够生成具有64比特$\times 2^{64}=2^{70}$的周期的隐匿性较高的扩散码序列。或者，码序列生成部140能够生成具有128比特$\times 2^{128}=2^{135}$的周期的隐匿性较高的扩散码序列。

[0078] 这样，在本实施方式的码序列生成处理S140中，码序列生成部140根据序列参数KP使处理要素的输出变化，由此，仅使用1种块加密算法就能够生成多个扩散码序列。

[0079] 码序列输出部160从码序列生成部140接受扩散码序列。码序列输出部160经由输出接口940输出扩散码序列。扩散码序列用于在通信系统中实施谱扩散的直扩方式。

[0080] 接着，对本实施方式的码序列生成处理S140的具体例进行说明。

[0081] 图4是示出在本实施方式的码序列生成处理S140中使用MISTY(注册商标)的情况下的具体的结构的图。

[0082] 如图4所示，在MISTY(注册商标)中，FI函数的处理要素SBOX由具有7比特的输入和7比特的输出的S7函数以及具有9比特的输入和9比特的输出的S9函数构成。码序列生成部140针对该S7函数和S9函数的输出数据的合计16比特，使用16比特的序列参数KP进行运算，对输出数据的结构进行变更。

[0083] 图5是示出在本实施方式的码序列生成处理S140中使用MISTY(注册商标)的情况下的SBOX的输出结构例1-1的图。

[0084] 在图5的SBOX的输出结构例1-1中，码序列生成部140利用序列参数KP的至少一部分对置换处理即SBOX的输出数据进行掩蔽，由此对SBOX的输出数据进行变更。具体而言，码序列生成部140使用序列参数KP的16比特中的7比特的信息作为掩蔽信息。由序列参数KP的16比特中的7比特构成的掩蔽信息能够生成1～127这127种。在图5中，示出MISTY(注册商

标)的S7函数的掩蔽信息为27即16进制表现0x1b的情况。此外,码序列生成部140使用序列参数KP的16比特中的9比特的信息作为掩蔽信息。使用序列参数KP的16比特中的9比特的信息的掩蔽信息能够生成1～511这511种。在图5中,示出MISTY(注册商标)的S9函数的掩蔽信息为451即16进制表现0x1c3的情况。

[0085] 另外,作为掩蔽信息的比特的组合还能够取0,但是,从加密学的安全性的观点来看,不应该使用0本身,因此,从序列参数KP中排除0。

[0086] 在参数选择处理S130中,参数选择部130将输入的序列参数KP分割成7比特和9比特的信息,输出通过分割而得到的7比特的信息和9比特的信息作为输出参数Op。即,这些掩蔽信息是根据序列参数KP选择或生成的输出参数Op的例子。

[0087] 另外,在使用这些掩蔽信息对MISTY(注册商标)进行处理的情况下,也可得到与不使用这些掩蔽信息对MISTY(注册商标)进行处理的情况大致相同的处理性能和安装性能。

[0088] 图6是示出本实施方式的在码序列生成部140中使用MISTY(注册商标)的情况下的SBOX的输出结构例1-2的图。

[0089] 图6的S7函数表是以表形式表现MISTY(注册商标)的S7函数的置换表。在码生成功能通过硬件安装来实现的情况下,以图6所示的AND-XOR表现来表现S7函数。该情况下,y0～y6这7比特成为S7函数的输出数据。在图6的SBOX的输出结构例1-2中,将y0～y6这7比特的各式的最后的整数项的0或1的表现置换成序列参数KP的16比特中的7比特的信息。

[0090] 在图6中仅记载有S7函数的情况,但是,S9函数也与S7函数同样,通过y0～y8这9比特的AND-XOR表现来表示。该情况下,y0～y8这9比特是S9函数的输出数据。在输出结构例1-2中,将y0～y8这9比特的各式的最后的整数项的0或1的表现置换成序列参数KP的16比特中的9比特的信息。

[0091] 图7是示出本实施方式的在码序列生成部140中使用MISTY(注册商标)的情况下的SBOX的输出结构例2的图。

[0092] 在图7的SBOX的输出结构例2中,码序列生成部140以比特为单位更换从SBOX输出的输出数据和序列参数KP的至少一部分,由此对输出数据进行变更。码序列生成部140将S7函数的输出数据7比特输入到7选1选择器,以比特为单位更换S7函数的输出数据。码序列生成部140在以比特为单位更换S7函数的输出数据时,使用序列参数KP对更换进行控制。该情况下,S7函数的输出数据可以是7!(>2的12次方)种组合。

[0093] 同样,码序列生成部140将S9函数的输出数据9比特输入到9选1选择器,以比特为单位更换S9函数的输出数据。码序列生成部140在以比特为单位更换S9函数的输出数据时,使用序列参数KP对更换进行控制。该情况下,S9函数的输出数据可以是9!(>2的18次方)种组合。

[0094] 接着,对图7的SBOX的输出结构例2的具体的安装结构进行说明。

[0095] 图8是示出图7的S7函数的输出结构例2中的具体的安装结构2-1的图。

[0096] 图8的安装结构2-1具有2选1选择器,该2选1选择器选择是否对S7函数的输出数据的上位第1比特和第2比特分别进行反转。根据序列参数KP的16比特中的最上位比特的KP1的值对该2选1选择器的选择进行控制。具体而言,如果KP1为0,则比特不反转。如果KP1为1,则比特反转。同样地,图8的安装结构2-1具有2选1选择器,该2选1选择器选择是否对S7函数的输出数据的上位第3比特和第4比特分别进行反转。根据序列参数KP的16比特中的上位第

2比特的KP2的值对该2选1选择器的选择进行控制。具体而言，如果KP2为0，则比特不反转。如果KP2为1，则比特反转。如图8所示，安装结构2-1具有多个选择器，使用KP1～KP6的各个值对各选择器进行控制。使用序列参数KP的16比特中的上位7比特对从最后的选择器输出的输出数据进行掩蔽，输入到比特反转电路。如果KP7为0，则比特反转电路输出比特而不反转，如果KP7为1，则比特反转电路对全部比特进行反转。在图8中，示出序列参数KP的16比特为0x8523(16进制表现)的情况的具体例。

[0097] 图9是示出图7的S9函数的输出结构例2中的具体的安装结构2-2的图。

[0098] 图9的安装结构2-2具有2选1选择器，该2选1选择器选择是否对S9函数的输出数据的上位第1比特和第2比特分别进行反转。根据序列参数KP的16比特中的下位9比特中的最上位比特的KP8的值对该2选1选择器的选择进行控制。下位9比特中的最上位比特是序列参数KP的16比特中的上位第8比特的比特。具体而言，如果KP8为0，则比特不反转。如果KP8为1，则比特反转。同样地，图9的安装结构2-2具有2选1选择器，该2选1选择器选择是否对S9函数的输出数据的上位第3比特和第4比特分别进行反转。根据序列参数KP的16比特中的上位第9比特的KP9的值对该2选1选择器的选择进行控制。具体而言，如果KP9为0，则比特不反转。如果KP9为1，则比特反转。如图9所示，安装结构2-2具有多个选择器，使用KP8～KP15的各个值对各选择器进行控制。使用序列参数KP的16比特中的下位9比特对从最后的选择器输出的输出数据进行掩蔽，输入到比特反转电路。如果KP16为0，则比特反转电路输出比特而不反转，如果KP16为1，则比特反转电路对全部比特进行反转。在图9中，示出序列参数KP的16比特为0x8523(16进制表现)的情况的具体例。

[0099] 图8的安装结构2-1的输出数据的组合数与输出结构例1的情况大致相同，是2的16次方。此外，通过图8的安装结构2-1实现的处理性能和安装性能比输出结构例1差。但是，在图8的安装结构2-1中，输出数据的比特位置被更换，因此，与输出结构例1相比，能够期待扩散码序列的估计困难性的提高。

[0100] ***其他结构***

[0101] <变形例1>

[0102] 另外，如图4所示，MISTY(注册商标)在FI函数中具有2个S9函数。因此，在图5的输出结构例1-1和图6的输出结构例1-2中，也可以使序列参数KP的比特数从16比特增加到25比特，对第1个S9函数和第2个S9函数的输出数据的输出选择方法进行变更。该情况下，能够利用1个码生成装置生成大约2的25次方种隐匿性较高的不同的扩散码序列。

[0103] <变形例2>

[0104] 图5的SBOX的输出结构例1-1示出码序列生成部140使用由参数选择部130分割后的序列参数KP在S7函数和S9函数的输出中进行掩蔽的结果。即，参数选择部130将分割后的序列参数KP直接交给码序列生成部140。但是，参数选择部130也可以生成作为在S7函数和S9函数的输出中进行掩蔽的结果而得到的新的SBOX信息，将生成的SBOX信息交给码序列生成部140。

[0105] <变形例3>

[0106] 在本实施方式中，码生成装置100的功能通过软件实现，但是，作为变形例，码生成装置100的功能也可以通过硬件实现。

[0107] 图10是示出本实施方式的变形例的码生成装置100的结构的图。

[0108] 码生成装置100具有电子电路909、辅助存储装置922、输入接口930和输出接口940。

[0109] 电子电路909是实现初始值取得部110、时间运算部120、参数选择部130、码序列生成部140、秘密密钥取得部150和码序列输出部160的功能的专用电子电路。

[0110] 具体而言，电子电路909是单一电路、复合电路、程序化的处理器、并行程序化的处理器、逻辑IC、GA、ASIC或FPGA。GA是Gate Array的简称。ASIC是Application Specific Integrated Circuit的简称。FPGA是Field-Programmable Gate Array的简称。

[0111] 码生成装置100的结构要素的功能可以通过1个电子电路实现，也可以分散到多个电子电路来实现。

[0112] 作为另一个变形例，也可以是，码生成装置100的结构要素的一部分功能通过电子电路实现，其余功能通过软件实现。

[0113] 处理器和电子电路分别被称作处理线路。即，在码生成装置100中，初始值取得部110、时间运算部120、参数选择部130、码序列生成部140、秘密密钥取得部150和码序列输出部160的功能通过处理线路实现。

[0114] 在码生成装置100中，也可以将初始值取得部110、时间运算部120、参数选择部130、码序列生成部140、秘密密钥取得部150和码序列输出部160的“部”改写成“工序”。此外，也可以将码生成处理、时间运算处理、参数选择处理和码序列生成处理的“处理”改写成“程序”、“程序产品”或“记录有程序的计算机能读取的存储介质”。

[0115] ***本实施方式的效果的说明***

[0116] 根据本实施方式的码生成装置100，采用保持可证明的安全性的块加密处理的CTR模式，因此，不会降低扩散码序列的安全性。此外，根据本实施方式的码生成装置100，通过对块加密处理的结构的一部分进行变更，能够生成全部不同的多个扩散码序列。由此，本实施方式的码生成装置100能够使生成扩散码序列的电路的数量比所需要的扩散码序列数少。由此，根据本实施方式的码生成装置100，能够抑制电路规模的增大，并且生成隐匿性较高的多个扩散码序列。进而，根据本实施方式的码生成装置100，在要求隐匿性较高的扩散码序列的通信系统中，能够确保通信系统整体的安全性。

[0117] 此外，根据本实施方式的码生成装置100，仅根据序列参数对块加密算法的SBOX的输出数据进行变更，就能够生成多个扩散码序列。由此，本实施方式的码生成装置100具有1种块加密算法即可。特别地，将本实施方式的码生成装置100应用于安装规模的制约较大的卫星搭载设备是有效的。

[0118] 实施方式2

[0119] 在本实施方式中，对与实施方式1不同之处进行说明。另外，对与实施方式1相同的结构标注相同的标号，有时省略其说明。

[0120] 图11是示出本实施方式的码生成装置100a的结构的图。此外，图12是示出本实施方式的码生成处理S100a的图。

[0121] 使用图11和图12对本实施方式的码生成装置100a的结构和动作进行说明。

[0122] 在参数选择处理S130a中，参数选择部130取得多个序列参数1～m。多个序列参数1～m的各序列参数唯一识别多个扩散码序列的各扩散码序列。

[0123] 秘密密钥取得部150取得多个秘密密钥K1～Km。

[0124] 码序列生成部140具有执行多个码序列生成处理S401～S40m的多个码序列生成部401～40m。参数选择部130将多个序列参数1～m的各序列参数输出到多个码序列生成部401～40m的各码序列生成部。此外，秘密密钥取得部150将多个秘密密钥K1～Km的各秘密密钥输出到多个码序列生成部401～40m的各码序列生成部。

[0125] 在码序列生成处理S140a中，多个码序列生成部401～40m分别生成扩散码序列。这样，码生成装置100a生成m种隐匿性较高的扩散码序列D1～Dm。

[0126] 使用图13对本实施方式的码生成装置100a的具体效果进行说明。

[0127] 如图13所示，假设多个环绕卫星经由1个数据中继卫星而与多个地面站进行通信的情况。设数据中继卫星在X种通信路径中分别利用隐匿性较高的相互不同的扩散码序列。此外，设同时进行的中继和下行链路中使用的路径也是Y个。此时，在图3的比较例的扩散码生成方式中，需要与通信路径对应的X个扩散生成电路。而且，比较例的扩散码生成方式从X个扩散生成电路中选择同时进行的中继和下行链路中使用的Y个扩散生成电路，生成Y个扩散码序列。

[0128] 另一方面，在本实施方式的码生成处理S100a中，如果同时进行的中继和下行链路中使用的路径为Y个，则安装Y个扩散生成电路即可。而且，在码生成处理S100a中，通过对扩散生成电路分别输入X种序列参数，能够应对同时进行中继和下行链路的情况。一般而言，同时进行的中继和下行链路中使用的路径的数量远远小于通信路径的组合数。因此，将本实施方式的码生成装置100a应用于安装规模的制约较大的卫星搭载设备特别有效。

[0129] 在实施方式1、2中，设码生成装置的各部为独立的功能块来进行说明。但是，码生成装置的结构也可以不是上述实施方式这种结构。码生成装置的功能块能够实现在上述实施方式中说明的功能即可，可以是任意结构。

[0130] 也可以组合实施实施方式1、2中的多个部分。或者，也可以实施这些实施方式中的一个部分。除此之外，还可以任意组合实施这些实施方式的整体或一部分。

[0131] 另外，上述实施方式是本质上优选的例示，并不意图限制本发明的范围、本发明的应用物的范围和本发明的用途的范围。上述实施方式能够根据需要进行各种变更。

[0132] 标号说明

[0133] 100、100a：码生成装置；110：初始值取得部；120：时间运算部；130：参数选择部；131：算法结构要素；140：码序列生成部；150：秘密密钥取得部；160：码序列输出部；909：电子电路；910：处理器；921：存储器；922：辅助存储装置；930：输入接口；940：输出接口。

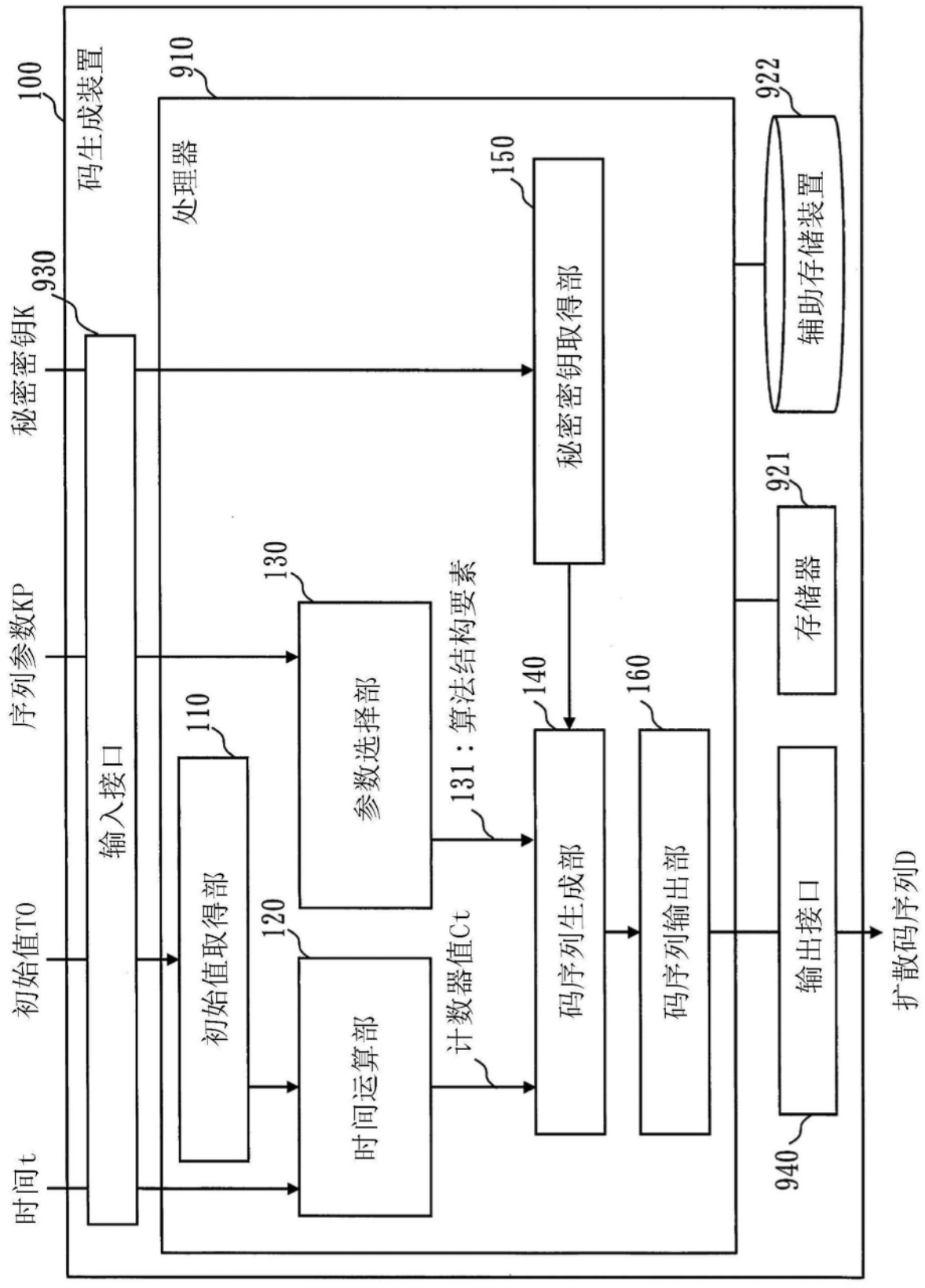

100
码生成装置
910
处理器
922
辅助存储装置
930
秘密密钥K
150
秘密密钥取得部
序列参数KP
130
参数选择部
921
存储器
110
初始值取得部
131：算法结构要素
140
160
初始值T0
120
时间运算部
计数器值Ct
码序列生成部
码序列输出部
时间t
输入接口
940
输出接口
扩散码序列D

图1

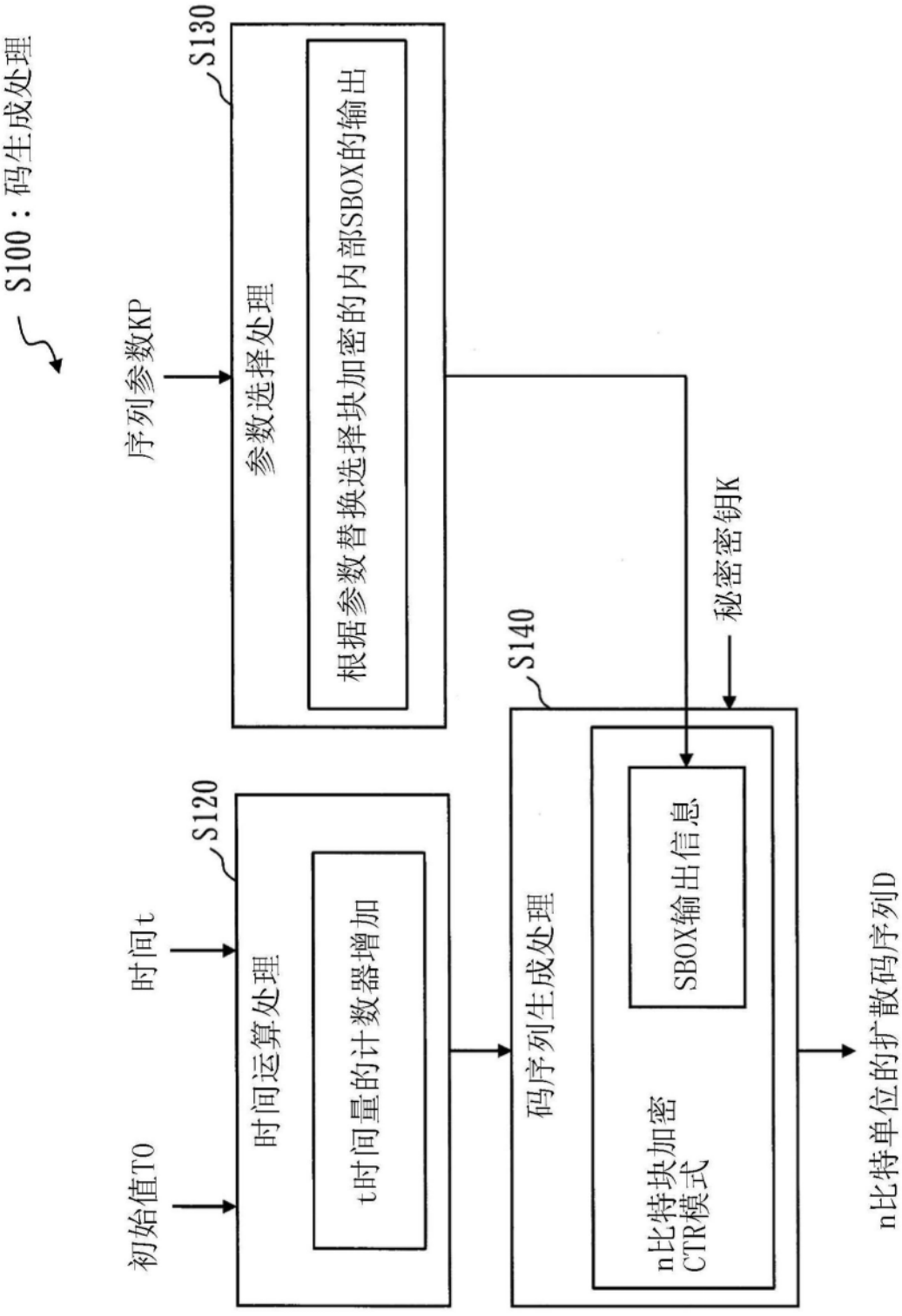

S100：码生成处理
S130
参数选择处理
根据参数替换选择块加密的内部SBOX的输出
序列参数KP
秘密密钥K
S140
码序列生成处理
SBOX输出信息
n比特块加密
CTR模式
S120
时间运算处理
t时间量的计数器增加
时间t
初始值T0
n比特单位的扩散码序列D

图2

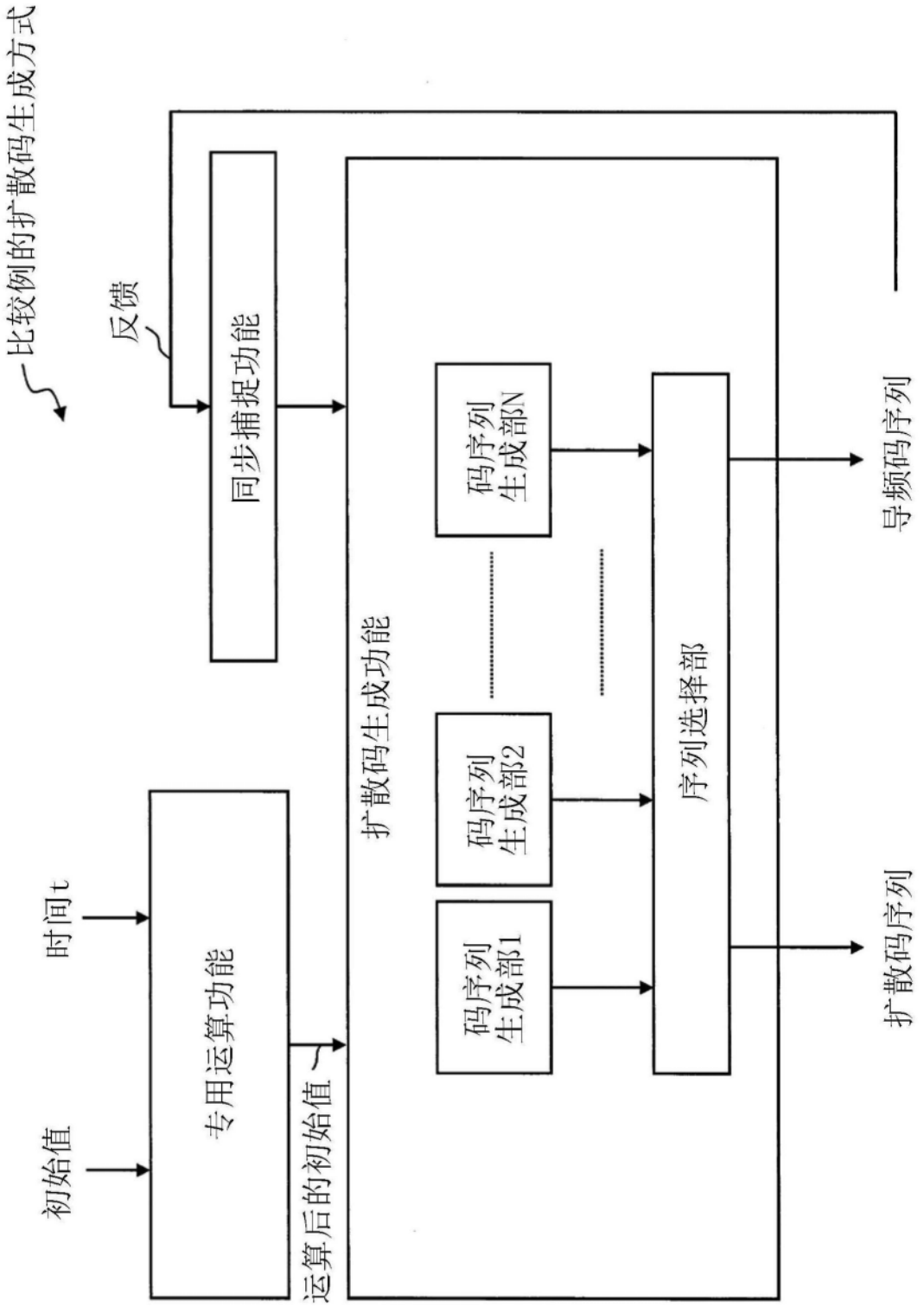

比较例的扩散码生成方式
反馈
同步捕捉功能
扩散码生成功能
码序列
生成部N
码序列
生成部2
码序列
生成部1
序列选择部
导频码序列
扩散码序列
时间t
初始值
专用运算功能
运算后的初始值

图3

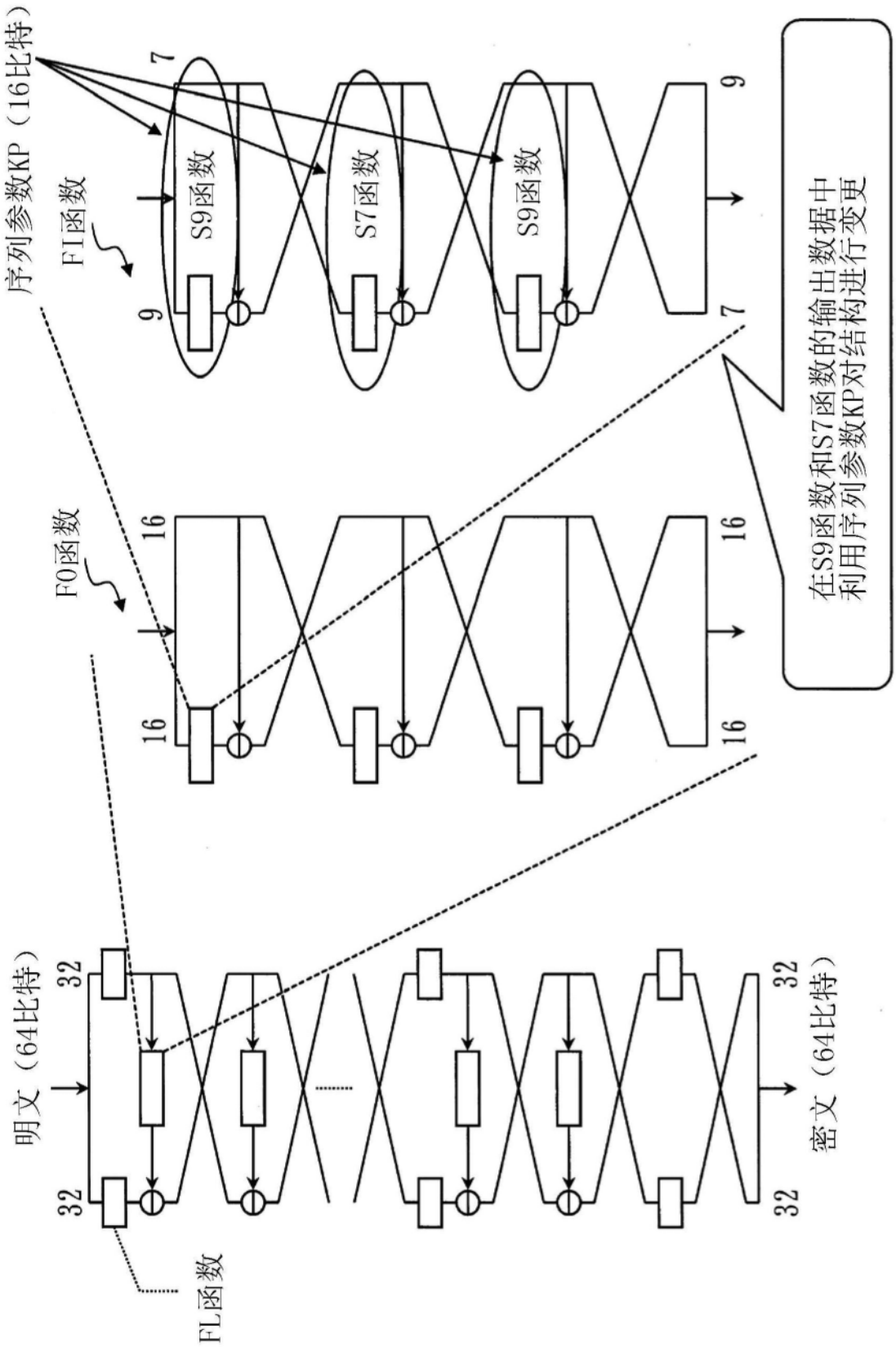

序列参数KP（16比特）
FI函数
S9函数
S7函数
S9函数
7
9
9
7
F0函数
16
16
16
16
在S9函数和S7函数的输出数据中
利用序列参数KP对结构进行变更
明文（64比特）
32
32
FL函数
32
32
密文（64比特）

图4

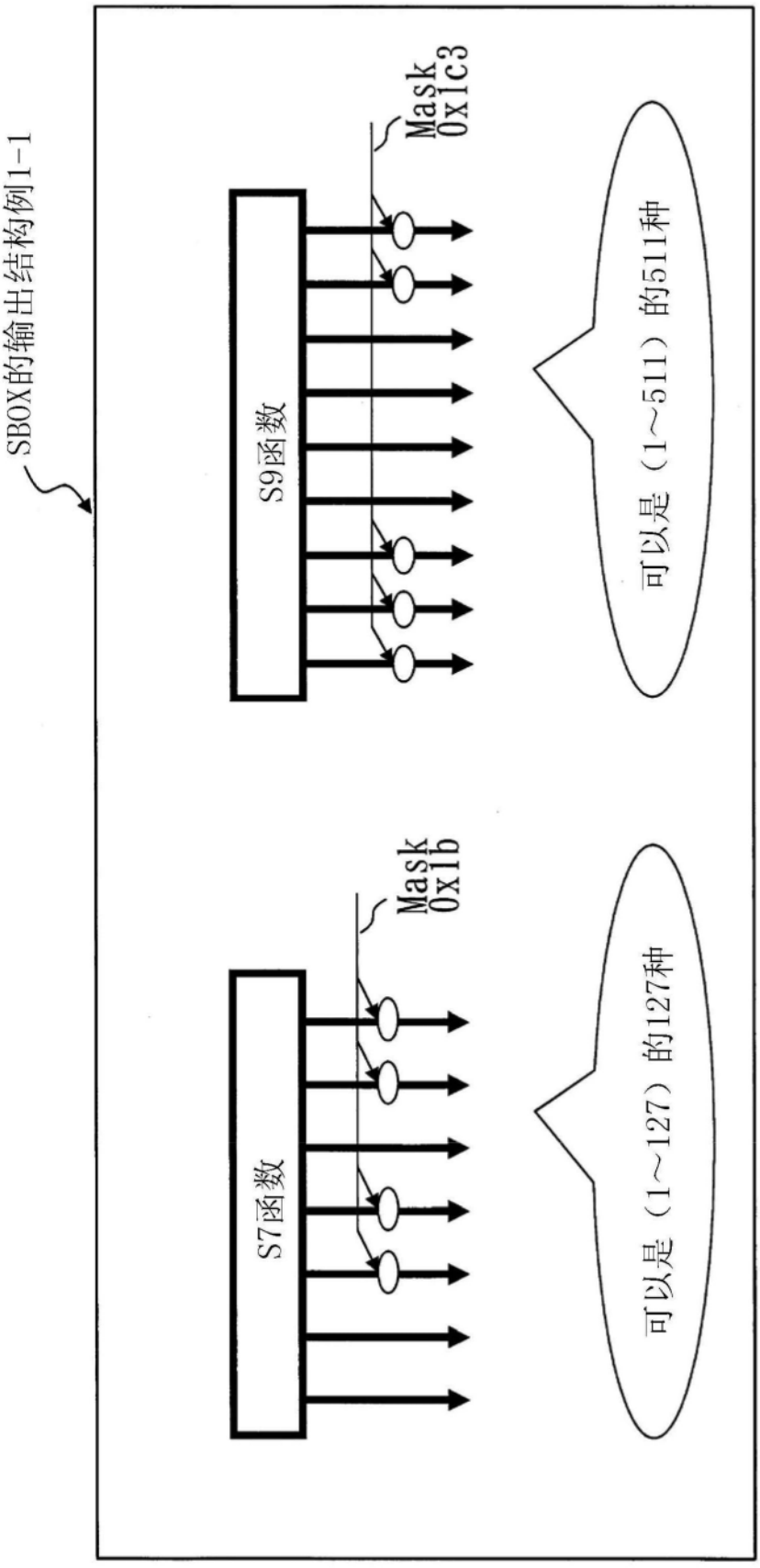

SBOX的输出结构例1-1
S9函数
Mask
0x1c3
可以是（1～511）的511种
S7函数
Mask
0x1b
可以是（1～127）的127种

图5

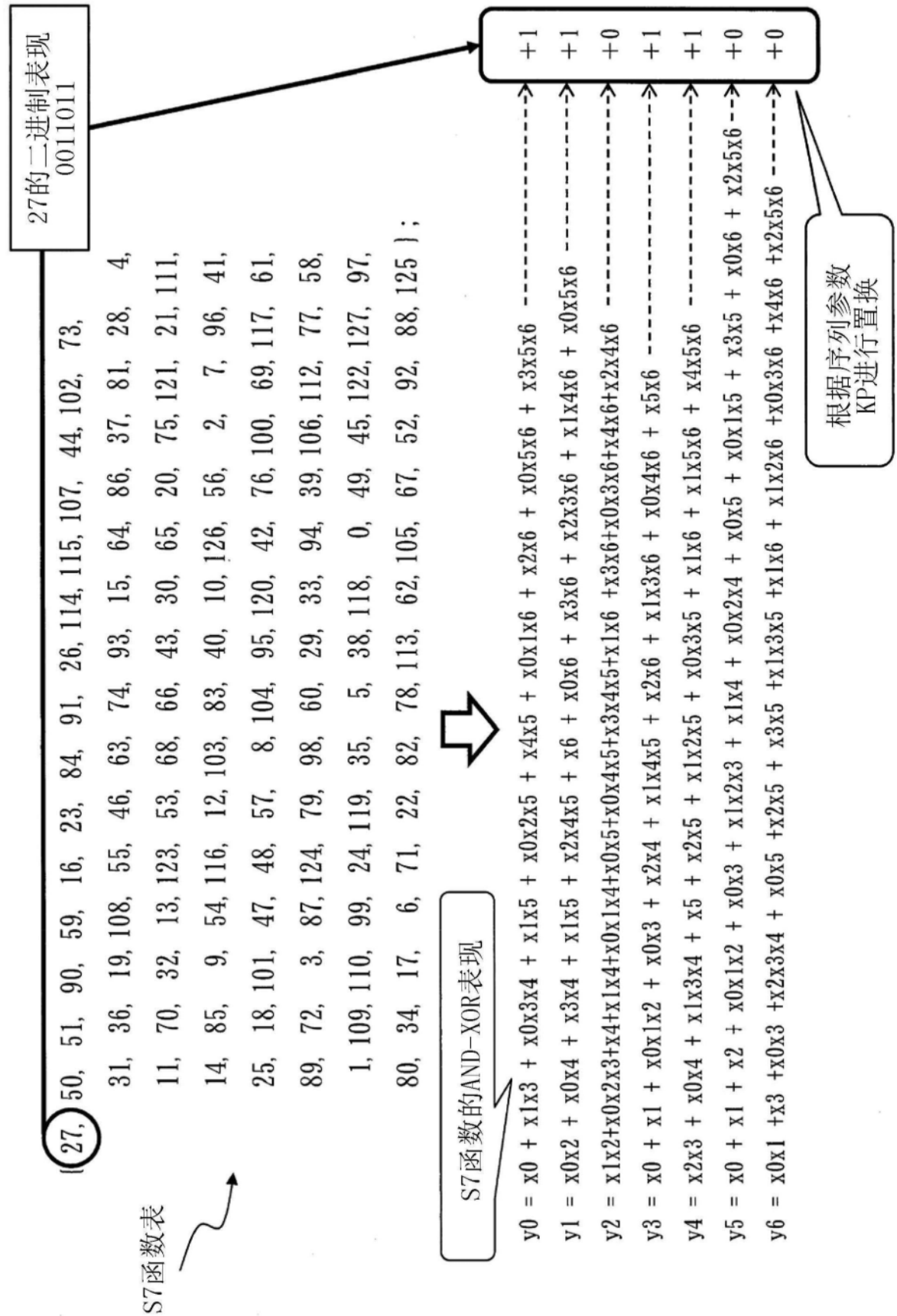

27的二进制表现
0011011
S7函数表
{27, 50, 51, 90, 59, 16, 23, 84, 91, 26, 114, 115, 107, 44, 102, 73,
31, 36, 19, 108, 55, 46, 63, 74, 93, 15, 64, 86, 37, 81, 28, 4,
11, 70, 32, 13, 123, 53, 68, 66, 43, 30, 65, 20, 75, 121, 21, 111,
14, 85, 9, 54, 116, 12, 103, 83, 40, 10, 126, 56, 2, 7, 96, 41,
25, 18, 101, 47, 48, 57, 8, 104, 95, 120, 42, 76, 100, 69, 117, 61,
89, 72, 3, 87, 124, 79, 98, 60, 29, 33, 94, 39, 106, 112, 77, 58,
1, 109, 110, 99, 24, 119, 35, 5, 38, 118, 0, 49, 45, 122, 127, 97,
80, 34, 17, 6, 71, 22, 82, 78, 113, 62, 105, 67, 52, 92, 88, 125 };
S7函数的AND-XOR表现
y0 = x0 + x1x3 + x0x3x4 + x1x5 + x0x2x5 + x4x5 + x0x1x6 + x2x6 + x0x5x6 + x3x5x6 ----------> +1
y1 = x0x2 + x0x4 + x3x4 + x1x5 + x2x4x5 + x6 + x0x6 + x3x6 + x2x3x6 + x1x4x6 + x0x5x6 ----------> +1
y2 = x1x2+x0x2x3+x4+x1x4+x0x1x4+x0x5+x0x4x5+x3x4x5+x1x6 +x3x6+x0x3x6+x4x6+x2x4x6 ----------> +0
y3 = x0 + x1 + x0x1x2 + x0x3 + x2x4 + x1x4x5 + x2x6 + x1x3x6 + x0x4x6 + x5x6 ----------> +1
y4 = x2x3 + x0x4 + x1x3x4 + x5 + x2x5 + x1x2x5 + x0x3x5 + x1x6 + x1x5x6 + x4x5x6 ----------> +1
y5 = x0 + x1 + x2 + x0x1x2 + x0x3 + x1x2x3 + x1x4 + x0x2x4 + x0x5 + x0x1x5 + x3x5 + x0x6 + x2x5x6 --> +0
y6 = x0x1 +x3 +x0x3 +x2x3x4 + x0x5 +x2x5 + x3x5 +x1x3x5 +x1x6 + x1x2x6 +x0x3x6 +x4x6 +x2x5x6 ----> +0
根据序列参数
KP进行置换

图6

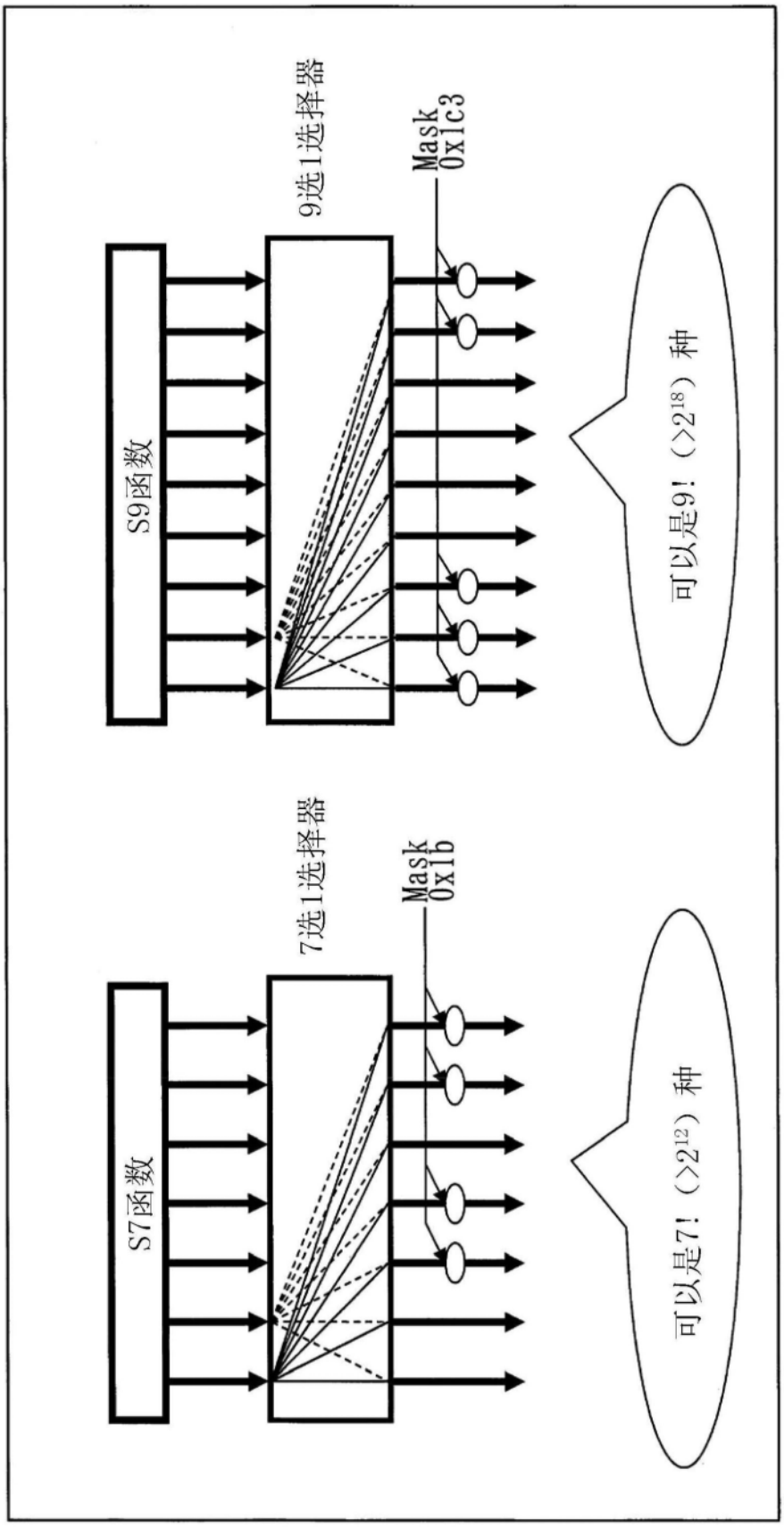

S9函数
9选1选择器
Mask
0x1c3
可以是9!（>2^18）种
S7函数
7选1选择器
Mask
0x1b
可以是7!（>2^12）种

图7

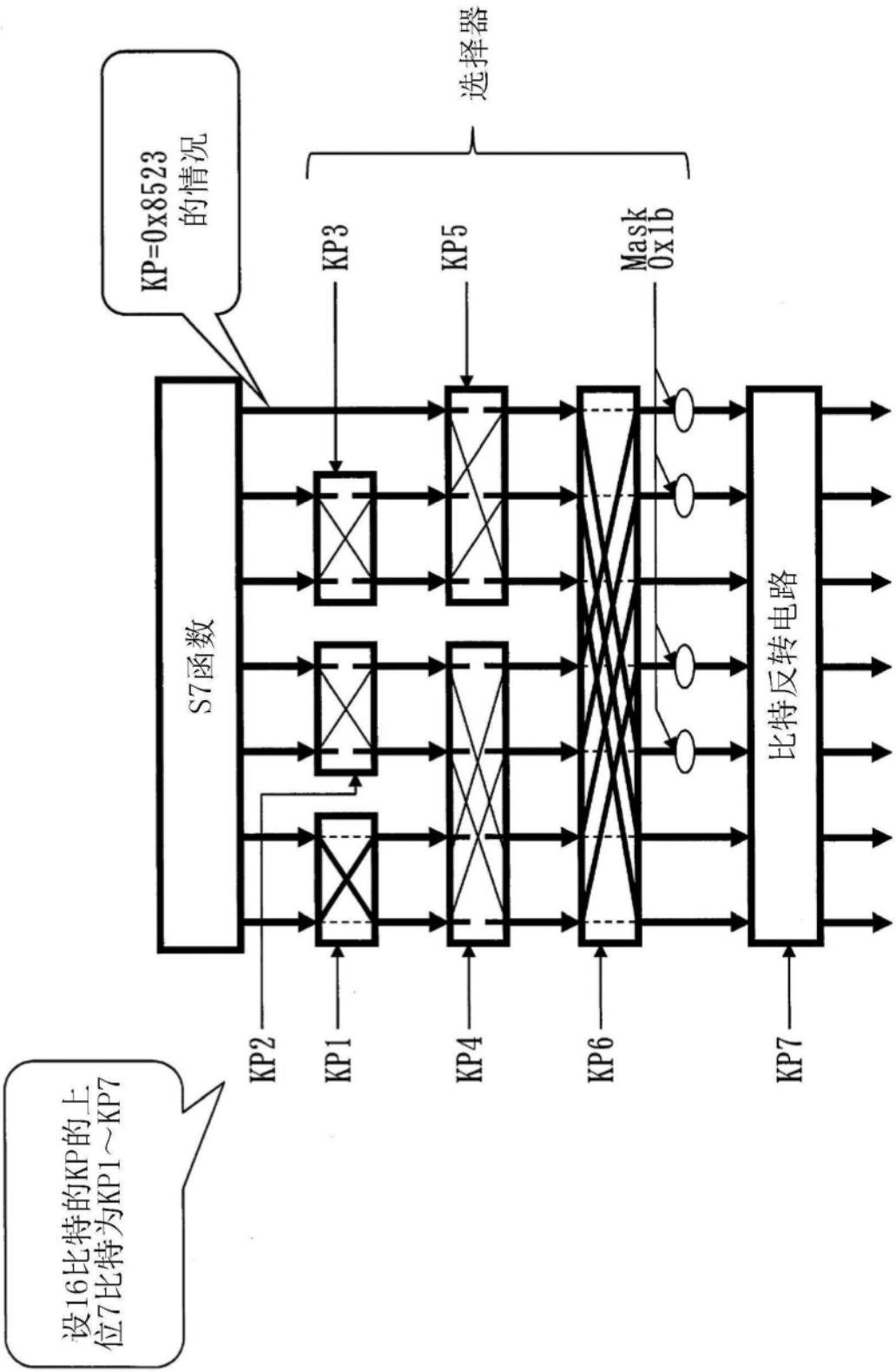

选择器
KP=0x8523
的情况
KP3
KP5
Mask
0x1b
S7函数
比特反转电路
KP2
KP1
KP4
KP6
KP7
设16比特的KP的上
位7比特为KP1～KP7

图8

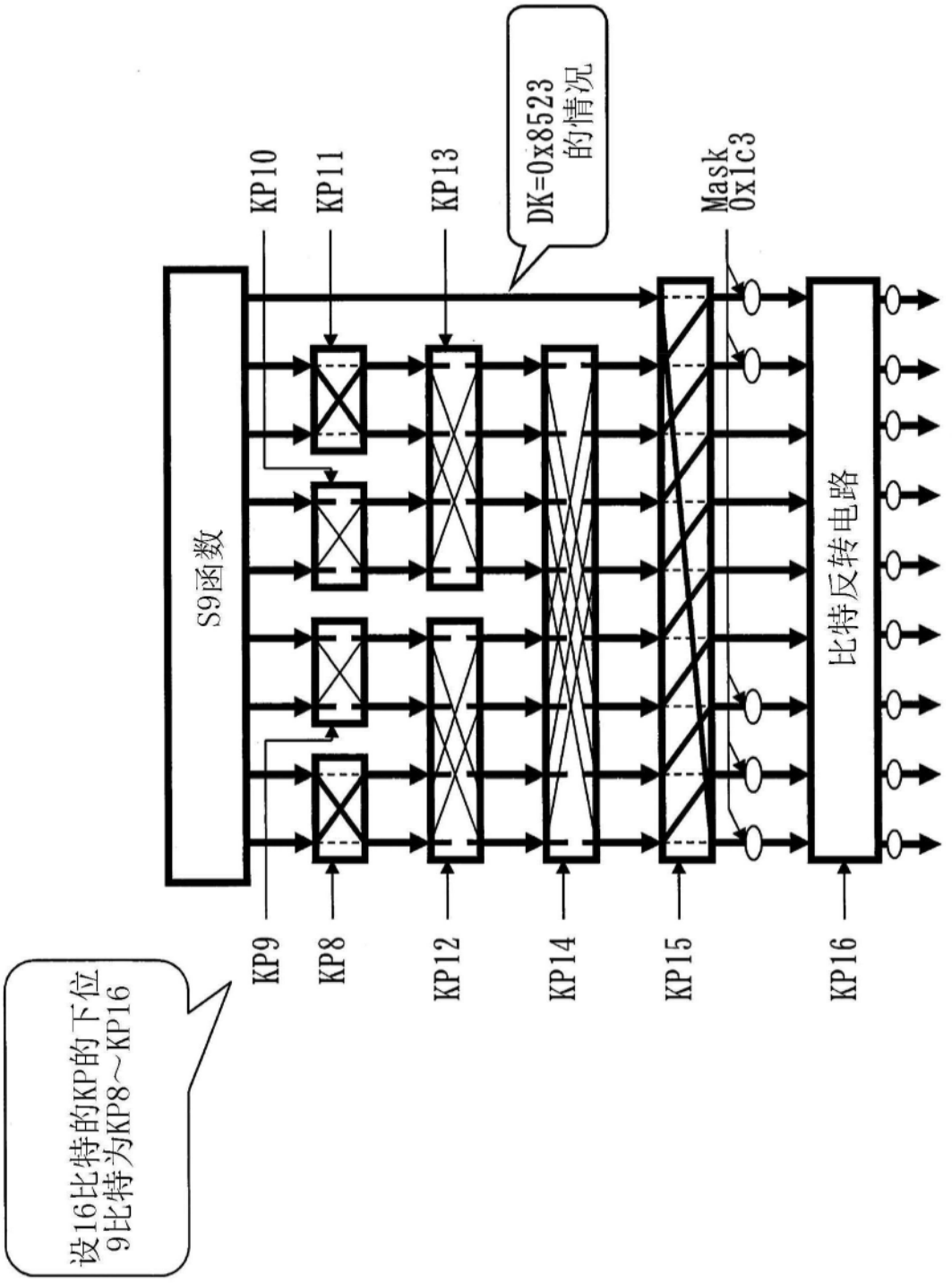

KP10
KP11
KP13
DK=0x8523
的情况
Mask
0x1c3
S9函数
比特反转电路
KP9
KP8
KP12
KP14
KP15
KP16
设16比特的KP的下位
9比特为KP8～KP16

图9

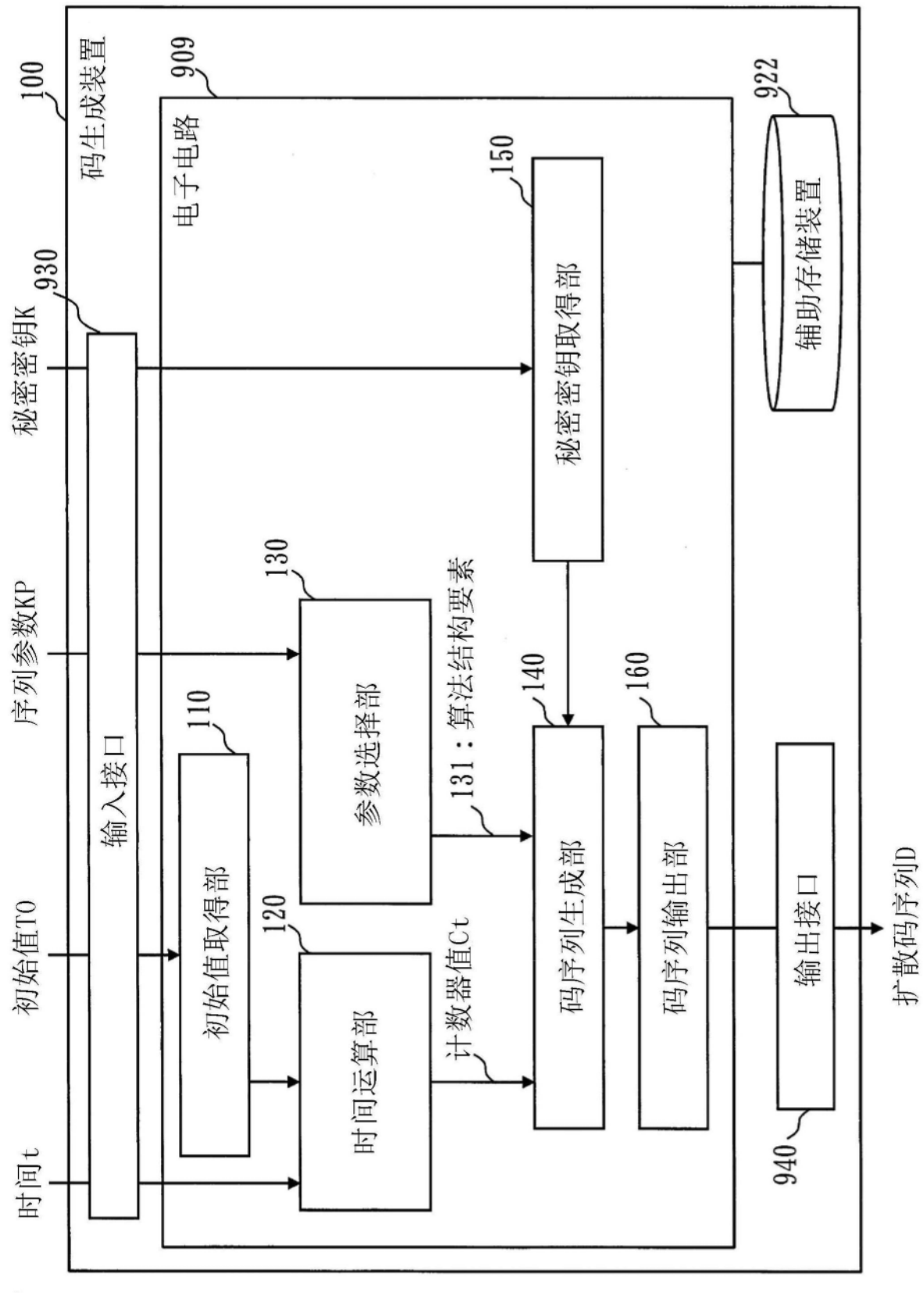

100
码生成装置
909
电子电路
922
辅助存储装置
930
秘密密钥K
150
秘密密钥取得部
序列参数KP
130
参数选择部
131：算法结构要素
初始值取得部
110
初始值T0
120
时间运算部
计数器值Ct
140
码序列生成部
160
码序列输出部
时间t
输入接口
940
输出接口
扩散码序列D

图10

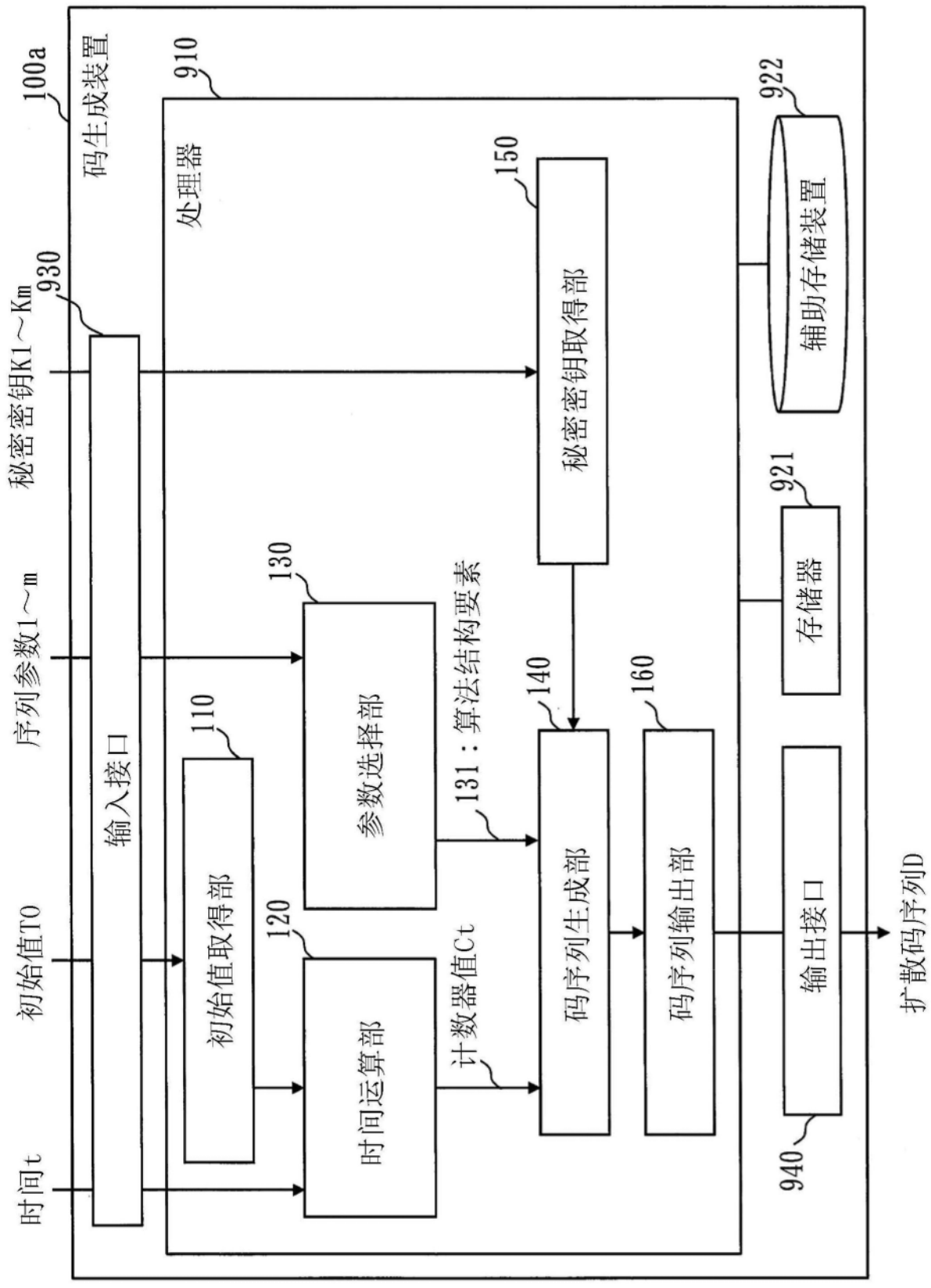

100a
码生成装置
910
处理器
922
辅助存储装置
930
秘密密钥K1～Km
150
秘密密钥取得部
序列参数1～m
130
参数选择部
921
存储器
输入接口
110
初始值取得部
131：算法结构要素
140
160
初始值T0
120
时间运算部
计数器值Ct
码序列生成部
码序列输出部
时间t
940
输出接口
扩散码序列D

图11

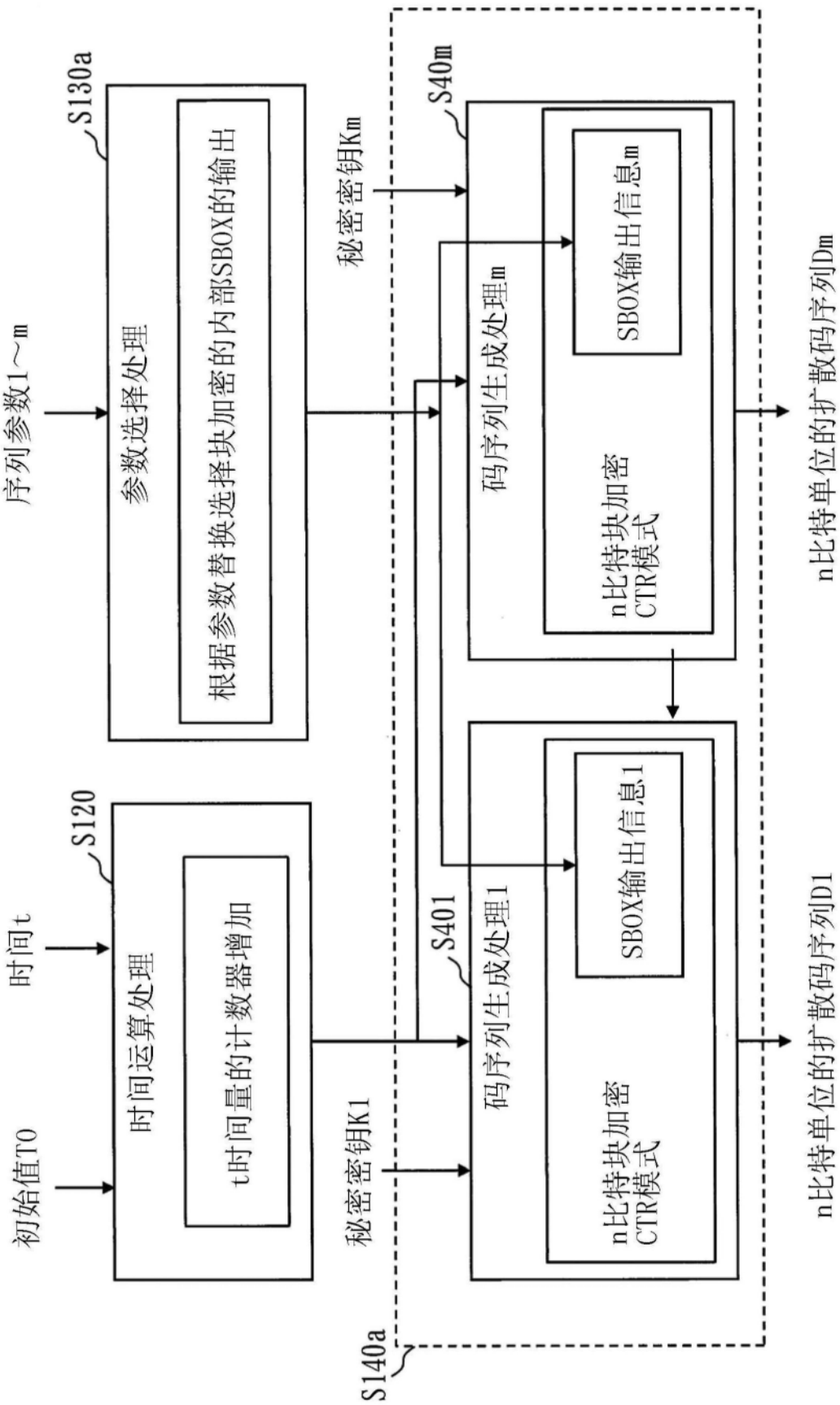

S130a
参数选择处理
根据参数替换选择块加密的内部SBOX的输出
序列参数1～m
秘密密钥Km
S40m
码序列生成处理m
SBOX输出信息m
n比特块加密
CTR模式
n比特单位的扩散码序列Dm
S120
时间运算处理
t时间量的计数器增加
时间t
初始值T0
秘密密钥K1
S401
码序列生成处理1
SBOX输出信息1
n比特块加密
CTR模式
n比特单位的扩散码序列D1
S140a

图12

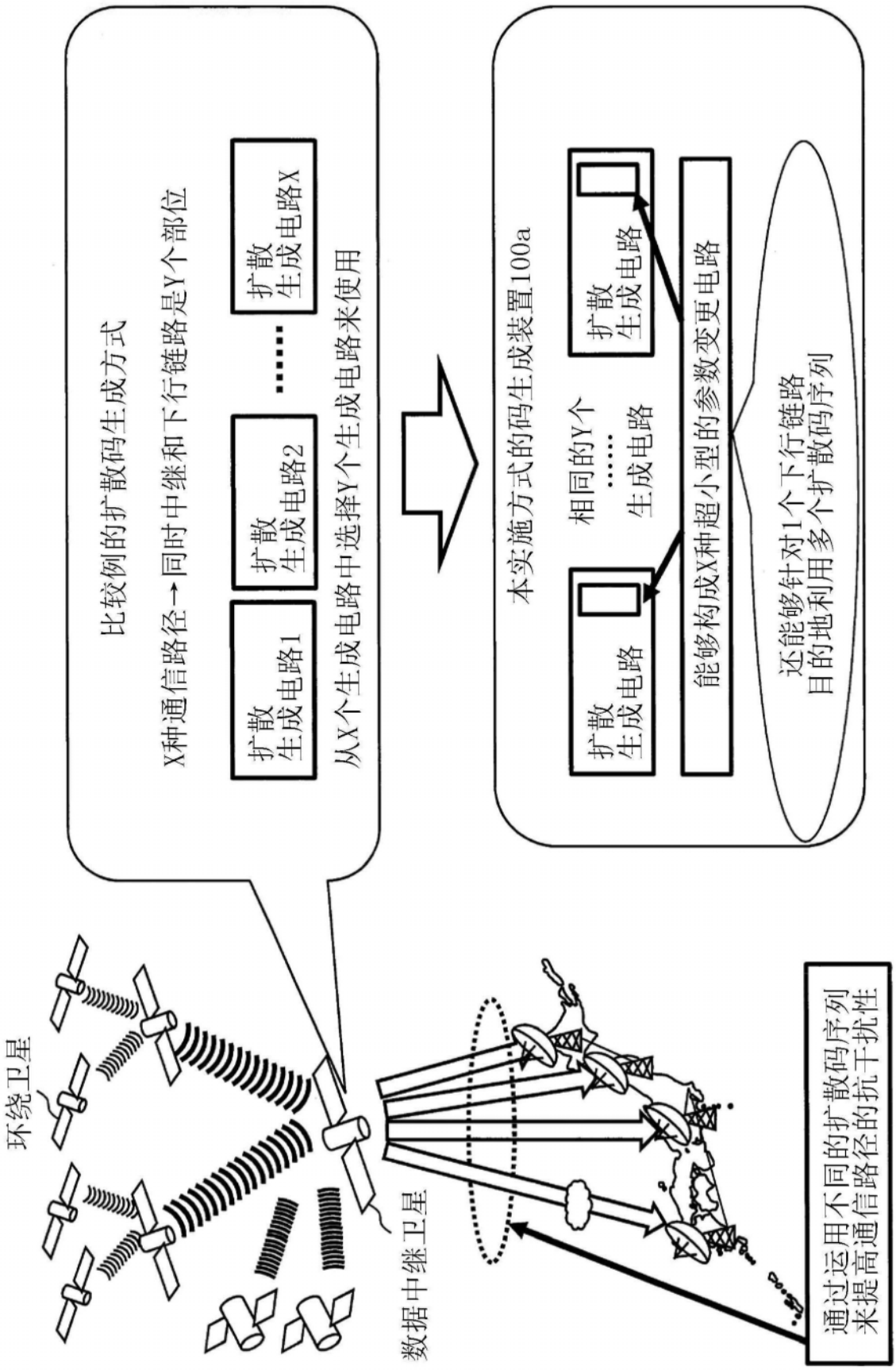

比较例的扩散码生成方式
X种通信路径→同时中继和下行链路是Y个部位
扩散生成电路1
扩散生成电路2
……
扩散生成电路X
从X个生成电路中选择Y个生成电路来使用
本实施方式的码生成装置100a
扩散生成电路
相同的Y个
……
生成电路
扩散生成电路
能够构成X种超小型的参数变更电路
还能够针对1个下行链路
目的地利用多个扩散码序列
环绕卫星
数据中继卫星
通过运用不同的扩散码序列
来提高通信路径的抗干扰性

图13