(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 101390332 B
(45)授权公告日 2012.09.05

(21)申请号 200780006379.5

(22)申请日 2007.02.23

(30)优先权数据
11/360,138 2006.02.23 US

(85)PCT申请进入国家阶段日
2008.08.22

(86)PCT申请的申请数据
PCT/US2007/062647 2007.02.23

(87)PCT申请的公布数据
WO2007/101085 EN 2007.09.07

(73)专利权人 德克萨斯仪器股份有限公司
地址 美国德克萨斯州

(72)发明人 M·J·弗利兹

(74)专利代理机构 北京纪凯知识产权代理有限公司 11245
代理人 赵蓉民

(51)Int.Cl.
H04L 9/00(2006.01)
H04L 1/00(2006.01)

(56)对比文件
US 2003/0012406 A1,2003.01.16, 全文.
CN 1516385 A,2004.07.28, 全文.

审查员 李萍

权利要求书 1 页 说明书 6 页 附图 2 页

(54)发明名称

用于带有保留码的同步流密码加密的方法与装置

(57)摘要

一种用于信号加密设备(405)的方法和装置,该信号加密设备被构建为对带有限制码的输入字节(402)的序列执行同步流密码加密。加密设备包括用于由密钥(413)产生伪随机字(431)的序列的密钥流生成器(410),以及用于求和密钥流生成器输出和输入字的加法器(422)。大小基本为可能输入字大小两倍的查找表(416)从求和信号中提供除限制码以外的加密码(408)。信号加密和解密系统被构建为包括用于由密钥(414)产生第二伪随机字的序列(433)的第二密钥流生成器(411),以及从密钥流生成器输出和加密码产生第二求和信号(434)的第二加法器(425)。相应查找表(417)提供从第二求和信号中提供除限制码以外的解密码(403)。

CN 101390332 B

1. 一种对带有限制码的输入字的序列执行同步流密码加密的方法，所述方法包含：

使用密钥流生成器从密钥生成具有重复周期的伪随机字的序列；

将所述输入字和所述伪随机字求和以从中产生求和信号；

将查找表用于所述求和信号以为除所述限制码外的所述输入字产生加密码；以及

在所述重复周期重复之前改变所述密钥。

2. 一种通过执行同步流密码解密通过密钥为带有限制码的加密输入字产生解密码的方法，所述方法包含：

使用密钥流生成器从密钥中生成具有重复周期的伪随机字的序列；

将所述加密输入字和所述伪随机字求和以从中产生求和信号；

将查找表用于所述求和信号以为除所述限制码外的所述加密输入字产生解密字；以及

在所述重复周期重复之前改变所述密钥。

3. 一种通过密钥对带有限制码的输入字执行同步流加密和同步流解密的方法，所述方法包括：

使用密钥流生成器从第一密钥中生成伪随机字；

将所述输入字和所述伪随机字求和以从中产生求和信号；

将第一查找表用于所述求和信号以为除所述限制码外的所述输入字产生加密码；

使用第二密钥流生成器从第二密钥中生成第二伪随机字；

将所述加密码和所述第二伪随机字求和以从中产生第二求和信号；以及

将第二查找表用于所述第二求和信号以为除所述限制码外的所述加密码产生解密码。

4. 一种被构造成接收密钥和带有限制码的输入字的同步流信号加密设备，所述设备包含：

密钥流生成器，其用于从所述密钥中生成伪随机字；

加法器，其连接到所述密钥流生成器的输出和所述输入字，并从中产生求和信号；以及

查找表，其使用所述求和信号来为除所述限制码外的所述输入字产生加密码。

5. 一种被构造成接收密钥和带有限制码的加密输入字的同步流信号解密设备，所述设备包含：

密钥流生成器，其用于从密钥中生成伪随机字；

加法器，其连接到所述密钥流生成器的输出和所述加密输入字，并从中产生求和信号；以及

查找表，其使用所述求和信号来为除限制码外的所述加密输入字产生解密码。

6. 一种同步流信号加密和解密系统，其包含：

第一密钥流生成器，其用于从所接收的第一密钥中生成第一伪随机字；

第一加法器，其连接到所述第一密钥流生成器的输出并接收带有限制码的输入字，并从所述第一伪随机字和所述输入字中产生第一求和信号；

第一查找表，其使用所述第一求和信号来产生除所述限制码外的加密字；

第二密钥流生成器，其用于从第二密钥中生成第二伪随机字；

第二加法器，其连接到所述第二密钥流生成器的输出并接收所述加密字以从中产生第二求和信号；以及

第二查找表，其使用所述第二求和信号来为除限制码外的所述加密字产生解密码，其中所述解密码与所述输入字基本相同。

用于带有保留码的同步流密码加密的方法与装置

技术领域

[0001] 本发明一般涉及数字加密设备，更具体地涉及用于带有保留码的数字数据的同步流密码加密的方法和实现。

背景技术

[0002] 当包含有价值信号内容的信号，特别是带有视频内容的数字信号从信息源通过信道被发送到接收器时，通常需要加密信号以避免被非预期的接收器接收。为可靠地避免不希望的接收，通常每次使用密钥加密输入信号的明文数字中的一个数字，这样在通过信道发送前，连续数字被不同地编码。为连续数字使用不同编码的处理被称为“流密码”，其对于不受欢迎的接收器可能是非常安全的。当使用同样的密钥执行解密，该处理还被进一步描述为被“对称”。因为与编码大块输入数据的其它加密处理相比流密码充分地减少了数字计算量，所以其通常是首选的加密处理。由于对称加密处理为管理密钥的用户带来简便，其也是首选的处理。

[0003] 不变地用一个密钥编码造成编码周期，加密处理在这一编码周期上重复。然而，对于相当复杂的密钥流生成器，如 128 位 AES（高级加密标准，也被称为“Rijndael”，由 Joan Daemen 和 VincentRijmen 创造的广泛使用的块密码）核心，其编码周期重复长度十分长以致该加密充分地不可破解。对于更高的安全级别，在编码周期重复前密钥可以被改变。

[0004] 同步流密码加密涉及对输入字流进行操作的处理，其中一个字接一个字的加密独立于输入数据流来执行。通常依赖同步流密码加密的商业应用是电影院里数字视频图像的放映。标准的数字影院放映系统包括回放服务器，其为同轴链接到数字视频放映机产生数字视频信号，所述放映机如 DLP®放映机。因为由服务器产生的视频数据一般包含比一般可用的 DVD 视频碟片更高的视频分辨率，同轴链接需要强信号加密，并且这种更高的分辨率在另一市场产生高的价值。包含在服务器存储器内的视频数据已经被强加密以避免被复制。同轴链接上公开发送的未加密视频数据可被简单地导入非预期的接收器以便于简单的未加密捕获。

[0005] 图 1 说明了通常用于影院的连接视频源（未显示）和放映机（未显示）的数字信道。分别包含亮度和色度视频数据的输入视频信号 105 和 106 通常具有 10 位的精度，这些输入视频信号在块 108 和块 109 中被加密。来自这些块的数字加密信号通过多路复用器 110 在同轴链接 112 上被多路复用，其中同轴链接 112 把二进制数据传输到解复用器 114。在块 115 和块 116 中解复用信号被解码后，明文亮度和色度信号在输出引线 117 和 118 被再现。

[0006] 用于商业影院的服务器和放映机之间的标准同轴链接是 1.45Gb/s 的 HD-SDI（高清晰度串行数字接口）链接。HD-SDI 链接是带有 1024 种可能数据码的十位链接。对于代表视频信号的 10 位的字，有 8 个码被限制于通常使用的视频规格 SMPTE-292(SMPTE 电影与电视工程师学会)，这样可以为其它视频设备提供同步功能和其它控制功能。在 SMPTE-292 规格中的 8 位限制码是十位信号中 1024 种可能码中的最前 4 个和最后 4 个 10 位二进制码，

即码为 0000，...，0003 和 1020，...，1023（这里用 10 进制计数法表示）。对于功能信道，这八位限制码可不被加密，而不禁止放映机的操作。因此，在这类系统中不允许调制器 / 解调器生成或操作这些限制码。

[0007] 图 2 显示了通常用于视频信号的现有技术中的数字信号加密处理。通过用服务器内的伪随机密钥流调制明文输入来完成加密，并且通过放映机内同样的伪随机密钥流解调前面得到的密文来完成解密。使用查找表（“LUT“）并以计数器模式运行的 AES 核作为密钥流生成器可以实现强而有效的加密和解密引擎。为加密和解密使用大致相同处理的加密 / 解密安排被称为“互补”。

[0008] 在图 2 中，来自视频源的信号 202，通常包含 10 位视频字的明文数据流被提供给加密块 205。使用输入给加密块 205 的密钥 213，密钥流生成器 210 在引线 231 上产生 10 位字的伪随机流。使用查找表 216 执行编码，查找表 216 包含 10 位输入字和来自密钥流生成器 210 的 10 位伪随机字的可能的组合。由查找表产生并在引线 208 上传输的合成的 10 位密文数据流被输入解密块 206。在解密块 206 中，密钥流生成器 211 使用密钥 214 在引线 232 上产生 10 位字的伪随机流。使用查找表 217 执行解码，查找表 217 同样包含 10 位输入字和来自密钥流生成器 211 的 10 位字的可能组合。明文输出数据被提供给引线 203。这种加密 / 解密安排可被构造成对称且互补的。

[0009] 图 2 中说明的安排可用于产生不包括 8 个限制字的密文，并可以宽范围的编码映射图操作。通过适当地定义查找表映射数据可以实现几乎任何其它编码方案。然而，这个方案的显著缺点是查找表需要使用大量存储器，这导致使用如现有 FPGA（现场可编程门阵列）实现是不切实际的。对于通常用于影院应用的 10 位数据输入 /10 位加密系统，需要大概百万个条目的查找表。

[0010] 图 3 说明了现有技术中可用于产生除八个限制字外的密文的第二种调制 / 解调安排。在图 3 中，明文 10 位数据流 302 被输入到加密块 305。通过把密钥 313 输入到密钥流生成器 310 执行加密，在引线 331 上产生 10 位字的伪随机流。明文输入 302 被连接到加法器 321，加法器 321 从输入数据中减去数字 4。来自加法器 321 的输出和密钥流生成器 310 的输出被连接到加法器 322，产生 11 位求和输出并提供给块 316。块 316 在其输入执行模 -1016 操作，其输出被连接到加法器 323，加法器 323 把输入数据上加上数字 4 以在引线 308 产生 10 位密文输出，其在通信信道如同轴链接上被传输。在如求和操作中遇到的模操作中，从求和结果中减去模指数改变了超过模指数的求和结果，进而消除了需要额外的位来表示求和结果的可能性。

[0011] 在通信信道远端的接收时，块 306 内执行的解密处理使用提供给密钥流生成器 311 的密钥 314，密钥流生成器 311 产生由 332 表示的 10 位字的伪随机流。三个加法器，即 324、325 和 326 也被用于解密处理，从数据流减去 4 数字然后加上数字 4 以产生 10 位明文输出 303。块 317 执行进一步的模 -1016 操作。

[0012] 图 3 说明的处理被用于电影院以为需要排除 8 个受限制的二进制码的放映安排提供视频数据保护。这种方案不需要用于查找表的存储器，但需要 6 到 8 个十位加法器（可能包括用于 2 个模功能的 2 个加法器）。这一方案在选择加密映射的情况下被最大地限制，并在必须为每个输入数据字执行需要六到八个独立额外操作的数据处理量的方面效率低。需要支持如 1.45Gb/s 高清视频信号的算术操作的大量数目导致对高性能数字电路元件的

需要，这增加了管芯面积和集成电路成本。

[0013] 在本技术中，调制 / 解调对的使用，特别是用于同步流密码加密的带有或不带有限制字的基于相加或模相加的调制 / 解调对是众所周知的。然而，现有技术处理中安排的限制和保持高级别的数据安全需要大的查找表或用于每个输入字加密 / 解密的大规模数字计算，所述安排不包括来自数据流的限制字的编码。数据映射选择中的不灵活也妨碍现有技术方案。因此，需要一种装置和方法，这种装置和方法执行不被这些限制阻碍的，特别是用于通信高数据率信号系统的高安全的加密和解密。

发明内容

[0014] 本发明的实施作为为带有限制码的输入字序列执行同步流密码加密的信号加密设备而达到技术优势。信号加密设备接收密钥和输入字流 (a stream of input word)。信号加密设备包括从密钥产生伪随机字流的密钥流生成器，以及将密钥流生成器连接到输入字的加法器，由加法器产生求和信号流。使用求和信号流的查找表为除限制码外的输入字产生加密码。

[0015] 依照另一个优选实施例，信号解密设备接收密钥和带有限制码的经过加密的字流。信号解密设备包括用于从密钥产生伪随机字流的密钥生成器，以及连接到密钥生成器和经过加密的字流的加法器，由加法器产生求和信号流。查找表使用求和信号流为输入字产生除限制码外的解密码。

[0016] 在另一个优选实施例中，信号加密和解密系统为输入字序列执行同步流密码加密和解密。系统接收密钥和带有限制码的输入字流。该系统包括用于从密钥中产生伪随机字流的密钥流生成器，以及连接到密钥流生成器和输入字的加法器，由加法器产生求和信号流。查找表使用求和信号流为除限制码外的输入字产生加密码。该系统还包括用于从密钥产生第二伪随机字流的第二密钥流生成器，以及连接到密钥流生成器和和加密字流的第二加法器，由第二加法器产生第二求和信号流。第二查找表使用第二求和信号流为除限制码外的输入字产生解密码。

[0017] 本发明的另一个实施例是为带有限制码的输入字序列执行同步流密码加密的方法。该方法包括接收密钥和输入字流。所述方法还包括使用密钥流生成器从密钥中产生伪随机字流，以及从密钥流生成器的输出和输入字流产生求和信号。该方法还包括使用由求和信号存取的查找表来为除限制码外的输入字流产生加密码。

[0018] 在另一个优选实施例中，该方法包括为带有限制码的加密字序列执行同步流密码解密。该方法包括接收密钥和加密字流。所述方法还包括使用密钥流生成器从密钥中产生伪随机字流，以及从密钥流生成器的输出和加密字流产生求和信号。该方法还包括使用由求和信号流存取的查找表来为除限制码外的加密字流产生解密码。

[0019] 本发明解决了不需要大量内存或大量数字处理编码带有限制码的字的输入序列的问题。

[0020] 本发明的实施例方便地提供了信号加密设备和信号解密设备以及可以使用最小存储器加密带有限制码的输入字而使用最小数字计算来执行加密和解密处理的方法。

附图说明

[0021] 为了更加完整地了解本发明及其优势，现在在下文给出结合附图的描述作为参考，其中附图有：

[0022] 图 1 说明了现有技术中显示 10 位视频亮度和色度视频信号的加密和解密的示例性框图；

[0023] 图 2 说明了现有技术中显示加密和解密带有限制码的 10 位输入信号的框图，所述加密和解密使用的查找表的大小足以包含输入数据和密钥流数据的组合；

[0024] 图 3 说明了现有技术中显示加密和解密带有限制码的 10 位输入信号的框图，所述加密和解密使用六个加法器和两个模操作；

[0025] 图 4 说明了显示加密和解密带有限制码的 10 位输入信号的本发明实施例的框图，所述加密和解密使用两个加法器和查找表，并且每个表带有两倍于每个可能输入字的条目；和

[0026] 图 5 说明了显示用于加密和解密带有限制码的 10 位输入字变址转换的本发明实施例的循环表。

具体实施方式

[0027] 下文详细讨论本优选实施例的制造和使用。然而应该意识到本发明提供的许多可用的发明概念可以在广泛的具体设备场境下实施。具体讨论的实施例仅是对制造和使用本发明的具体方式的说明，而不是对本发明范围的限制。

[0028] 本发明实施例将关于具体场境中的优选实施例来讨论，即用于编码数字数据流的装置和方法，其中数字数据流包含在解码和编码流中的保留数据码。实施例包含可对称或互补地执行信号加密和解密的处理。

[0029] 图 4 说明了本发明的加密和解密处理以及方法的示例性实施例，其可以执行除限制码外的加密和解密，所述限制码如根据 SMPTE-292 规格操作的在 HD-DSI 链接中的八个限制码。代表视频信号且通常不一定为 10 位字的输入明文数据流 402 被连接到加密块 405。加密块 405 包括接收密钥 413 并产生伪随机比特流 431 的密钥流生成器 410，10 位字用作编码输入数据。这一伪随机比特流和明文输入数据在加法器 422 中被一个字接一个字地相加以在线路 432 上产生 11 位结果。通过使用查找表 416，10 位字的密文流产生并连接到信道 408。在本实例中的查找表 416 包含 2048-16 = 2032 个条目，每个条目为 10 位，这将在下文被细节地描述。信道 408 可以如视频规范 SMPTE-292 所描述的一位接一位地传输数据。用于八个限制码的输入数据没有被加密。

[0030] 包含在查找表 416 中的映射被安排，这样加密处理没有生成限制码。查找表映射是互补的，这样加法器 422 产生的调制结果可以被第二加法器 425 解调。用于加密和解密处理的查找表映射基本是相同的。同样的密钥可用于两个处理，并可随时间改变以增强安全性。

[0031] 解密块 406 按同样的方式操作。解密块 406 包括密钥流生成器 411，其接收密钥 414，并产生伪随机比特流 432，用于解码密文数据的 10 位字在线路 408 上提供。优选密钥 413 和 414 是同样的密钥，即系统可以是对称的。在加法器 425 中比特流 433 和明文输入数据被一个字接一个字地相加以产生如信号 434 表示的 11 位结果。使用查找表 41710 位字的明文流产生并连接到输出 403。查找表 417 包含 2048-16 = 2032 个条目，每个条目为 10

位，所述查找表优选基本与查找表 416 相同，即该处理可是互补的。解密处理可以被想象成“反转”用于加密的表。

[0032] 可以通过下述等式建立本发明实施例的示例性查找表，Y = [((A-X)-4) 求模 (1016)]+4 其中词条 A 是任意常数，X 是查找表的输入，而 Y 是查找表的输出。如具体实施例，可以选择 A 的值为 917。对于使用 A = 917 的实例，下列查找表被产生为表示 11 为字的 2032 个输入条目，其输入和数出如下表指出：

输入	输出
0	917
1	916
2	915
…	…
912	5
913	4
914	1019
915	1019
…	…
1928	5
1929	4
1930	1019
1931	1018
…	…
2046	903
2047	902

[0033] 通过适当地建立上表中指明的输出，没有产生所述八个限制码。此外，应该注意到如这个加密处理所预期的，多于一个输入可产生同样的输出。

[0034] 还可参照图 5 进一步描述本发明实施例中的加密 / 解密处理。图 5 所说明的是一个环 501，其表示包含 10 位输入字的加标签条目的循环表，这一循环表带有将被加密的 1016 个可能值，但不包括在 SMPTE-292 规定中的八个限制码。表中的单元被加标签为 4，

5,...,1018,1019。因此,表包含 1016 个条目,没有八个限制字的位置。在图 5 说明的实施例中,通过从输入字逆时针选择变址“D”个条目的表条目执行明文输入字的编码以产生密文字。然后通过从密文字顺时针选择变址为“D”个条目的表条目执行密文字的解码。在图 5 说明的实例中,在加密期间,表条目号码 5 被逆时针变址 412 以产生表条目 417。在解密的反向处理期间,表条目号码 417 被顺时针变址 D = 412 以产生表条目 5。可通过在减法模式下操作“加法器”来执行这种反操作。表条目变址 D 是伪随机数,其可以从输入密钥导出,所述输入密钥可随时间变化以为输入数据流的加密提供高级别的安全性。因此,必须在每个输入字执行的数字运算仅在循环表内变址,这可以通过最小数字计算执行并能够容易地修改为以高数据率的流操作,例如加密 1.45Gb/s 的数据链接。计算伪随机变址 D 来选择加密或解密字需要的更庞大计算可以在大致较低的速率下执行,而基本不会损害加密的安全性。

[0035] 本处理优于现有技术的改进是不需要用于加密或解密的大量表。此外,也因此避免了用于输入字的大量数字计算的需要。而另一个改进是通过简单重定义 LUT 映射增加了支持信道编码方案和需要保留码的灵活性。

[0036] 虽然已经细节地描述了本发明的实施例及其优势,应该注意到可以对其进行多种改变、代替和变更而不背离本发明权利要求定义的精神和范围。例如,本领域技术人员容易理解如本文描述的形成能提供带保留码的数据流的信号加密和解密的过程和系统的方法和技术的使用可以变化,而仍处于本发明的宽范围内。本领域技术人员还将理解到在上文描述的处理中,如果需要作适应性调节,如 RGB 和灰度视频表示的多种视频信号表示可以被替换为亮度色度视频信号表示,并仍处于本发明的范围之内。在包括其它视频系统的其它应用中,在本发明的宽范围内,10 位字的大小可以被改变。作为另一个例子,所述方法和装置也可以用于除视频数据外的其它数据。此外,本申请的范围不旨在限制于说明书中描述的处理、机械、制造,问题、手段、方法以及步骤的组合的具体实施例中。本领于技术人员容易从本发明公开的内容意识到,可以依照本发明实现目前存在的或不久后将被开发的,与本文描述的相应实施例执行基本相同的功能或达到基本相同结果的处理、机械、制造,问题、手段、方法以及步骤的组合。因此,所附权利要求旨在将这些处理、机械、制造,问题、手段、方法以及步骤的组合包括在本发明范围之内。

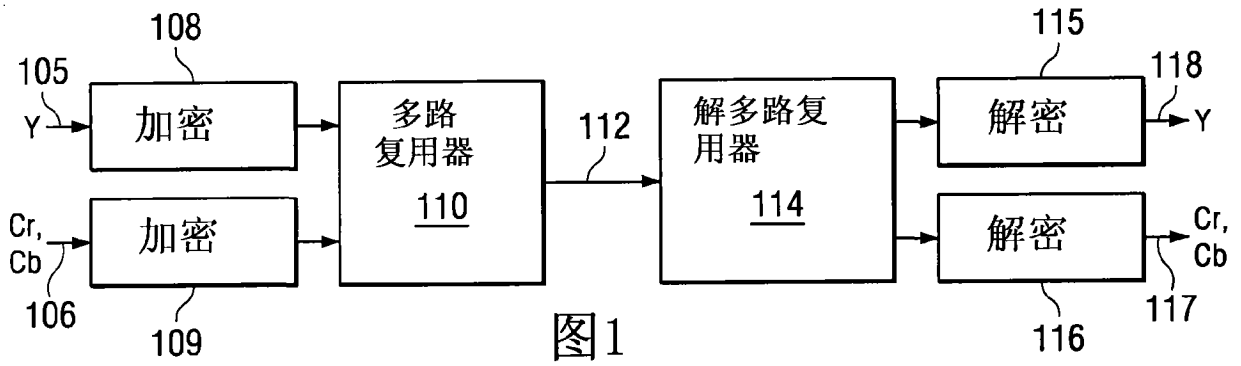

图1

（现有技术）

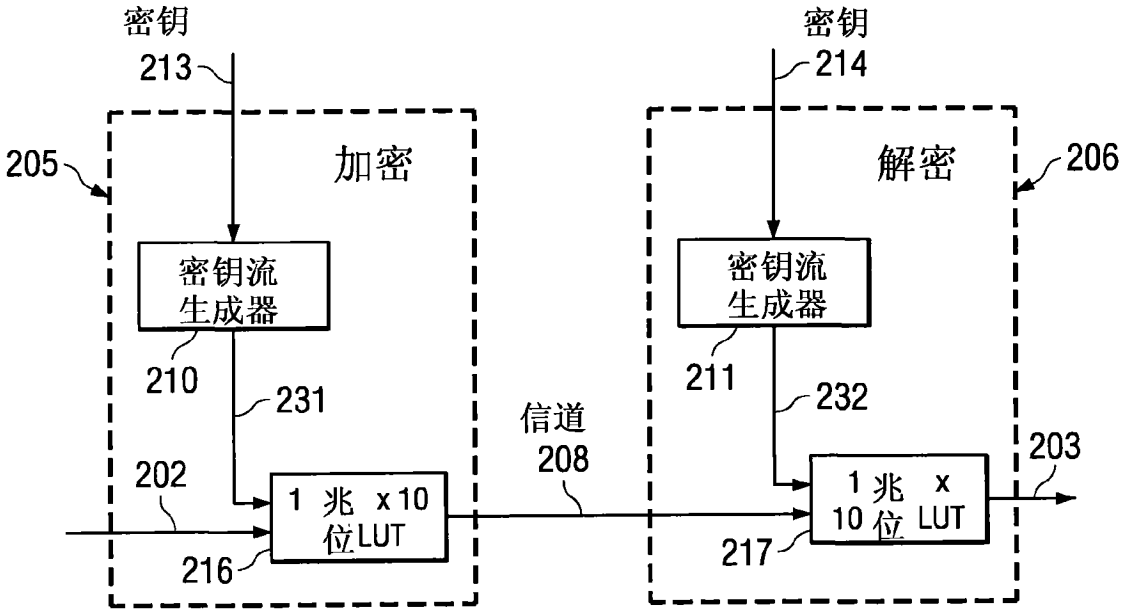

图2

（现有技术）

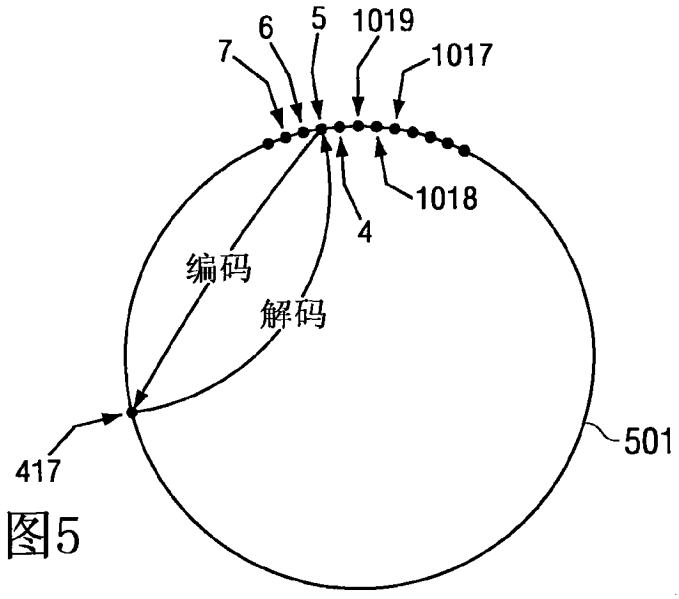

图5

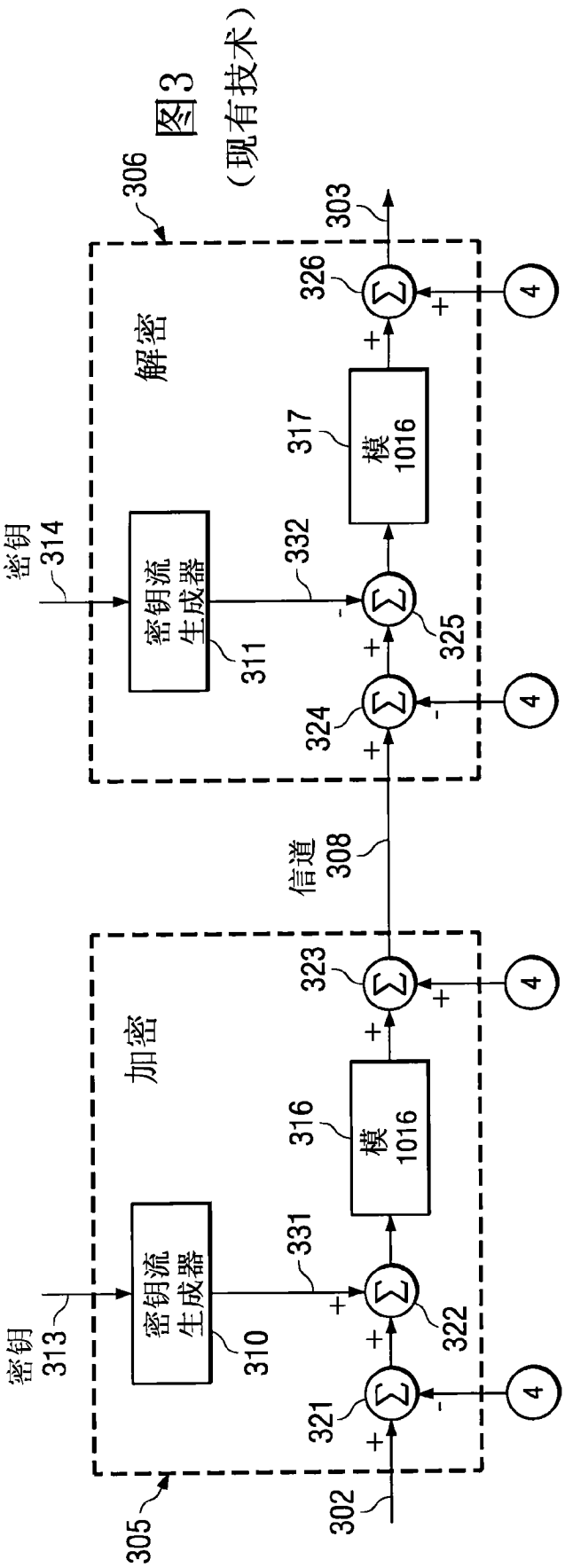
图3
（现有技术）
306
解密
密钥
314
密钥流
生成器
311
317
模
1016
332
303
326
325
324
信道
308
加密
密钥
313
密钥流
生成器
310
316
模
1016
331
323
322
321
302
305
4

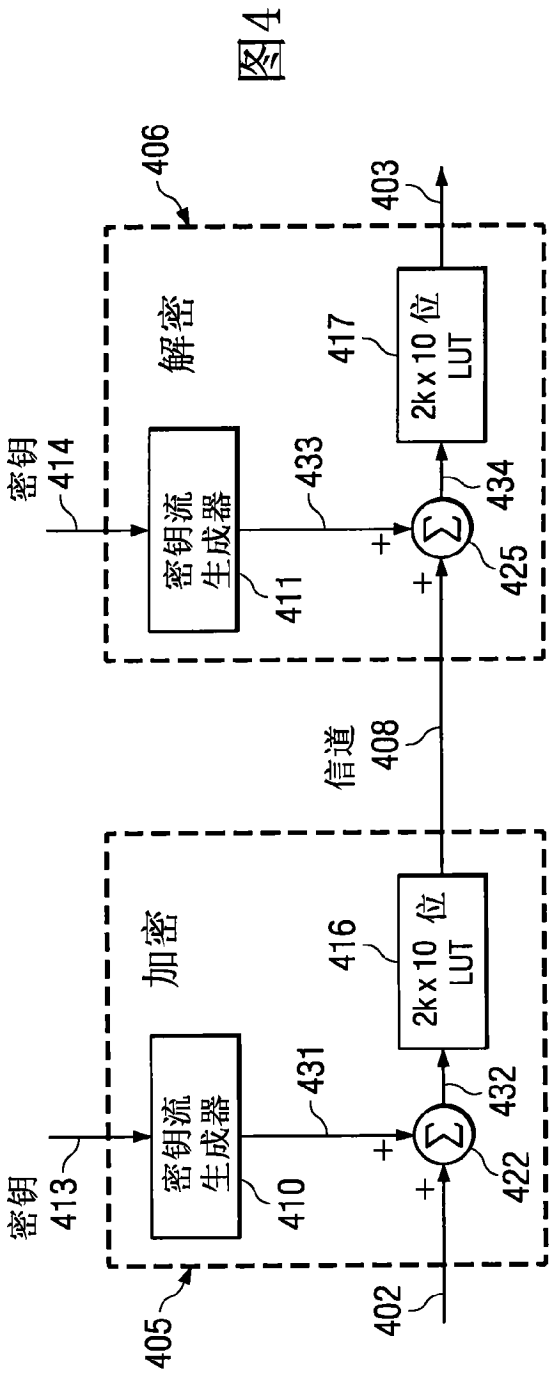
图4
406
解密
密钥
414
密钥流
生成器
411
417
2k x 10 位
LUT
433
403
434
425
信道
408
加密
密钥
413
密钥流
生成器
410
416
2k x 10 位
LUT
431
432
422
405
402