[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04K 1/00

[12] 发明专利说明书

[21] ZL 专利号 96110239.X

[45] 授权公告日 2004 年 5 月 19 日

[11] 授权公告号 CN 1150713C

[22] 申请日 1996.6.28 [21] 申请号 96110239.X

[30] 优先权

[32] 1995. 7. 3 [33] FR [31] 9508004

[71] 专利权人 汤姆森多媒体公司

地址 法国库伯瓦

[72] 发明人 马里奥·德维托 雅克·斯特恩
路易斯·格雷戈里
让 一伯纳德·费希尔

审查员 行朝霞

[74] 专利代理机构 北京市柳沈律师事务所

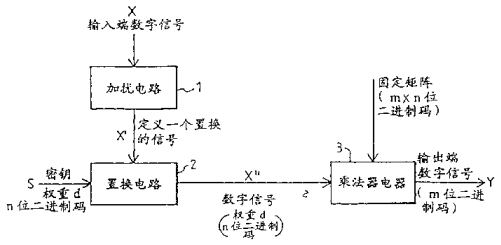
代理人 马 莹

权利要求书 2 页 说明书 8 页 附图 4 页

[54] 发明名称 保密通信系统中的数字信号处理方法

[57] 摘要

本发明涉及一种处理 k 维数字信号的方法，使得输出的第二数字信号(y，y1)不能从输入数字信号(x，x1)推断出，该方法将数字信号(x，x1)传送到一个实现单向函数的设备，并包括：1. 将输入端的数字信号(x，x1)传递给第一电路 C(1，2，4)，该电路对所述信号进行修改，给出作为输出的具有应用到实现单向函数的设备所必须特性的 n 维第三数字信号(x″，x′1)；2. 将来自第一电路 C(1，2，4)的第三信号(x″，x′1)传递给实现所述单向函数的第二电路(3；5)，该第二电路(3；5)给出所述第二数字信号(y，y1)作为输出。 本发明特别应用于保密通信系统。



ISSN1008-4274

1. 一种在保密通信系统中处理第一 k 维数字信号的方法，使得从输入端的所述第一数字信号(x, x1)不能推断出输出端的第二数字信号(y, y1)，所述方法将所述第一数字信号(x, x1)传递给一个实现单向函数的设备，其特征在于，该处理包括如下步骤:

将所述输入端的第一数字信号(x, x1)传递给一第一电路 C(1, 2, 4)，该电路 C(1, 2, 4)对该第一数字信号进行修改，并输出一 n 维第三数字信号(x", x'1)，该第三数字信号(x", x'1)具有应用到实现单向函数的设备的特性;

将来自所述第一电路 C(1, 2, 4)的所述第三信号(x", x'1)传递给实现所述单向函数的第二电路(3; 5)，该第二电路(3; 5)给出所述第二数字信号(y, y1)作为输出。

2. 根据权利要求 1 所述的方法，其特征在于所述电路 C 包括接收作为输入的所述输入信号(x)的一个加扰电路(1)，以及包括接收来自所述加扰电路的信号(x')且给出能够为实现所述单向函数的所述电路所接收的一个数字信号(x")作为输出的一个格式化电路(2)。

3. 根据权利要求 2 所述的方法，其特征在于所述格式化电路(2)由一个置换电路构成，如此定义的置换被应用于一个 n 维以及汉明权重为 d 的数字信号。

4. 根据权利要求 2 所述的方法，其特征在于所述格式化电路由一个按词典编辑方式排序的电路所构成。

5. 根据权利要求 1 所述的方法，其特征在于所述电路 C 包括一个以输入端的所述数字信号(x1)为根源的伪随机生成器(4)，所述生成器给出具有 n 维以及一个高概率的汉明权重 d 的一个数字信号(x'1)作为输出。

6. 根据权利要求 1 至 5 中任一项所述的方法，其特征在于所述电路 C 由一个被称为密钥的数字信号(s)所控制。

7. 根据权利要求 6 所述的方法，其特征在于所述密钥是一个具有 n 维且汉明权重为 d 的二进制信号。

8. 根据权利要求 1 所述的方法，其特征在于通过将一个二进制形式的第三数字信号(x", x'1)同一个二进制矩阵 M 相乘而得到所述单向函数。

9. 根据权利要求 8 所述的方法，其特征在于所述矩阵 M 是 m × n 维的，

n 表示所述矩阵的列数。

10. 根据权利要求 8 或 9 所述的方法，其特征在于所述二进制矩阵 M 是随机生成的。

11. 根据权利要求 10 所述的方法，其特征在于由一个伪随机电路来生成所述矩阵 M 的系数 a_{ij}。

12. 根据权利要求 8 或 9 所述的方法，其特征在于规定所述汉明权重 d 和所述矩阵 M(m, n)的维数的所述参数 d、n、m 在 Gilbert-Warshamov 界限下被选择，即：$m = n \times H_2(d/n)$

这里 $H_2(x)$是熵函数：

$H_2(x) = -x \times \log_2(x)-(1-x) \times \log_2(1-x)$。

13. 根据权利要求 12 所述的方法，其特征在于所述矩阵的维数是 n 和 $m = n/2$，还在于汉明权重 d 等于 $0.11 \times n$。

14. 根据权利要求 4 所述的方法，其特征在于来自所述伪随机生成电路的所述信号被传递给 N 个实现单向函数的电路，使得在输出端得到 N 个具有 m 位长度的信号。

15. 根据权利要求 1 所述的方法，其特征在于所述的方法被用来在进入控制系统中生成一个控制字。

16. 根据权利要求 15 所述的方法，其特征在于，在收费电视系统的情况下，在发送器级别和接收器或多个接收器级别上采用相同的单向函数来生成所述控制字或多个控制字。

17. 根据权利要求 1 所述的方法，其特征在于所述方法被用于计算一个具有共同密钥的密码错误检测码。

18. 根据权利要求 1 所述的方法，其特征在于所述方法被用于建立一个伪随机生成器。

保密通信系统中的数字信号处理方法

技术领域

本发明涉及这样一种对 k 维的数字信号的处理方法，使得不能从输入端的数字信号推断出输出端的数字信号。

背景技术

这种方法在保密通信系统中特别有用。一般来说，这些系统是需要使用控制字或特征字(signature)的有条件进入系统(Coditional-access system)。使用这种保密信息交换的系统非常多。具体的可以列举收费电视系统、可处理长期委托书(standing orders)的银行类系统、或任何其它导致机密信息交换的同类系统。

在像收费电视系统中所实现的有条件进入系统中，一般都采用 n 个二进制位的数字信号来形成一控制字，从而可以特别地控制所传递信息的加扰和解扰(Scrambling and unscrambling)这个控制字必须频繁地更换，而且一般是从发送站传输到接收系统或终端。

只有被授权的人才能得到该控制字。因此，控制字在传输到接收器的过程中被加密。接收器是像智能卡(Smart card)一类的保密系统。该接收器或许可以同一个非保密的解扰系统配合并将解密后的控制字提供给这个非保密的解扰系统。为了进行这种事务，采用了一种密钥密码系统，其中发送器和接收器共用一被称为共同密钥的共同数字信号。因此，发送器加密该控制字，然后接收器以相对称的操作将其解密。

为了进行此类操作，有很多的处理方法为本领域的技术人员所知，因而可以特别地提及 DES 系统，即“数字加密标准”系统。

这种处理有这样的缺点，即，为了将信息加密然后解密，需要采用一种可逆的函数。然而，有些须解决的事务不需要采用一固定的和有意义的数字信号来进行加密和解密，而常常是对发送人和接收人来说能够共用一个保密的随机数字信号就足够了。于是采用一单向的函数就够了，就是说

如果所述函数未被完全知道，则它不允许找到该数字信号的像。具体地说，可以采用一种基于密钥的随机函数(hash function)，其操作原理为已知但是没有有效的密钥却是不能被利用的。

因此，如图 1 所示的有关单向函数的应用中，含有一个用 A 表示的随机数字信号生成电路的发送器 E 随机地取出一个被称为控制字选择因子的随机数字信号 m。于是在单向函数 f 的作用下，其映象就是由发送器 E 和接收器 R 所共用的保密的随机数字信号，今后就称之为控制字。发送器将控制字选择因子 m 传送给接收器，且发送器和接收器都在单向函数 f 下用相同的密钥来计算出其像，从而得到相同的控制字 m。在保密性方面仅有的制约就是如果不知道一定的秘密即共用的密钥，就不可能从控制字选择因子 m 计算出控制字 m，而该共用密钥是处在两个保密的范围(发送器和接收器)之内。

目前的技术水平是采用密码通信安全可靠的可逆函数，如 DES，或是采用密码通信能力差的函数。后者仅有的防护办法就是复杂的计算和结构的秘密，这相当于说密钥就是函数本身而且限制其使用的是它的通用性。

发明内容

本发明的目的就是提出一种数字信号的处理方法，该方法具体地阐述了这个问题，只要函数是公开的而只有一个有限字长的钥匙是保密的，一个密钥的泄露并不危及采用不同密钥的相同型式的系统。

本发明还有一目的就是提出一种处理方法，该方法可用于保密型的所有数字信号传输系统。

因此，本发明的主题就是保密通信系统中 K 维数字信号的处理方法，使得不能从输入端的数字信号推断出输出端的数字信号，也就是将数字信号传递给一个实现单向函数的设备，该方法的特征在于处理包括如下步骤:

1. 将所述输入端的第一数字信号传递给第一电路，该电路对该信号进行修改，给出作为输出的 n 维第三数字信号，该第三数字信号具有应用到实现单向函数的设备所必须的特性;

2. 将来自该第一电路的所述第三信号传递给实现所述单向函数的第二电路，该第二电路给出所述第二数字信号作为输出。

根据一个实施例，通过将一个 m×n 维矩阵 M 乘以数字信号(X")来实现单向函数，矩阵 M 的系数 a_{ij} 一劳永逸地被随机地只选取一次。这种函数在例如法国专利申请 No.92 15915 中有描述，申请人是 Jacques Stern。

尤其是为了限制存贮器的存贮量，矩阵系数 a_{ij} 最好由一个伪随机函数来生成。

根据该实施例，加扰电路的选择要显示出良好的扩散质量。也就是说在输入端很弱小的信号变化会在输出端造成一个很大的信号差别。加扰函数最好由密钥来控制。

同样地，格式化电路的目的就是将输入端的信号转换为 n 维二进制码的、权重近似为 d 的一个数据项，其中 d 是由 Gilbert-Warshamov 界限(bound)所确定：$m = n.H_2(d/n)$，这里 $H_2(x)$是熵函数(entropy function)

$H_2(x)=-x \log_2(x)-(1-x)\log_2(1-x)$。

根据一优选实施例，m=n/2；输入到单向函数的数字信号的权重必须大约为 0.11 × n。

在本发明的范围内，加扰和格式化函数可以依照下面三个处理中的一个来实现，即：

- 一个已知类型的加扰电路和一个格式化电路，其输入定义了长度为 n 和权重为 d 的二进制字的一种置换(permutation)，

- 或者是，一个已知类型的加扰电路和一个格式化电路，其输入单向地定义了一个长度为 n 且权重为 d 的二进制字，

- 或者是，一个单一的加扰和置换电路，其输入和密钥定义了一个有偏的伪随机生成器；以至于输出长度为 n 的字具有或以很高概率出现在 d 或其附近的权重。

本发明的主题还有就是在进入控制系统中、具体说是收费电视系统中采用上面所述的方法来产生一控制字以便在发送器的级别上和接收器或多个接收器的级别上用相同的单向函数来产生该控制字或多个控制字。

附图说明

通过参照附图并对各个实施例的详细描述会展现出本发明的其它特性和优点，其中：

图 1 已经作了描述，它是用图来表示采用一个单向函数在发送器和接收器之间传递数字信息;

图 2 表示一设备，它使得可以在输出端得到不能从输入端数字信号推断出的一个数字信号;

图 3 表示另一设备，它使得可以在输出端得到不能从输入端数字信号推断出的一个数字信号;

图 4 表示又一个设备，它使得可以在输出端得到不能从输入端数字信号推断出的一个数字信号;

图 5 表示一个设备，它使得以输入端的一个数字信号出发可以在输出端得到不能从输入端数字信号推断出的多个数字信号;

图 6 和图 7 表示采用上述的设备之一来进行密码的检验;

图 8 表示采用图 2、3 和 4 中的设备来构造随机生成器。

具体实施方式

根据本发明所述的方法和设备是基于校正子解码(Syndrome decoding)(SD)的问题。该问题在申请人名叫 Jacques stern 的法国专利申请 No.92 15915 中作了描述。它可按如下所述的那样来解释：考虑一个二进制矩阵 M 和一个二进制矢量 y，需要找一个具有相对高或相对低的权重的二进制矢量 x，使得 Mx=y。权重不用说是表示在相关矢量中二进制码的 1 的个数。如果恰如其分地选取了 m × n 维矩阵 M 和矢量 x 的汉明权重(Hamming weight)，则上面所提出的问题用现有已知的计算手段实际上是很难解决的。已证明了利用现有的计算手段，当输入端的数字信号 x 有一个低的汉明权重 d 时，该问题是很困难的。一般来说，规定汉明权重和矩阵 M 维数的参数 d, n, m 基本上在 Gilbert-Warshamov 界限下被选择，该界限给出了随机码(n、m)的最小权重 d 的理论上限定值，即:

$$m = n.H_2(d/n)$$

这里，$H_2(x)$是熵函数 $H_2(x) = -x.\log_2(x)-(1-x).\log_2(1-x)$。

图 2 所示的一种设备可以实现第一种处理数字信号的方法，使得从输入端的数字信号不能推出输出端的数字信号。

在该设备中，输入端的数字信号 x 被传递给为本领域的技术人员所共知的加扰电路 1。该数字信号是一种由 k 维的二进制字组成的信号。在输出

端得到一个定义了一种置换并被传递到置换电路 2 的数字信号(x')。

该电路有二个输入端：一个接收置换的定义，另一个接收被施以该置换的二进制字；在输出端得到被置换的字。该电路在第一输入端接收信号(x')，在第二输入端接收一个密钥 s。在所述的实施例中，该密钥 s 由具有先前所定义的权重 d 的 n 位二进制数字信号组成。因此，在置换电路 2 的输出端就得到一个含有 n 位且有权重 d 的随机数字信号(x")。

该信号(x")被传递到一个乘法器电路 3 以进行输入端的 n 位二进制字同维数为 m × n 位的一个固定的二进制矩阵的矩阵相乘。在输出端得到一个 m 位的数字信号(y)。

在上面所述的方案中，输入端的数字信号(x)被用来置换密钥 s。出于保密原因，在输入端的数字信号首先被加扰，其结果被用来定义一个 n 位二进制码范围内的置换。该加扰可以是相对简单的，因为只要二进制码被很好地散开就足够了，也就是说，输入信号的一位二进制码的值能影响输出信号的多位二进制码的值。这里对本领域的技术人员可以有很多种可能的办法。例如采用对应表(Correspondence tables)或伪随机生成器。

在 n 位二进制码范围内定义一个置换可以通过定义每一位二进制码的象(image)或是通过采用置换生成器来进行，该置换生成器是本领域的技术人员所共知的那种，例如在 SIAM. J of Computing 17(2) April 1988，上面 M.luby 和 C.Rackoff 写的文章“怎样从伪随机函数建立伪随机置换”中所描述的那样，这种生成器需要较少的输入数据。通过采用 n 位的钥匙，其中前面少数几位二进制码是 1，而其它各位都为 0，可以避免需要存贮整个密钥。在此情况下，该钥匙不再是秘密的，且该方案的全部“保密”是在输入端的数字信号的加扰中，这种加扰对保密要求来说是够好了。

m × n 维二进制码矩阵包括，一劳永逸地随机选取一次的系数 a_{ij}。该矩阵被存在一个存贮器中。为了避免存贮整个矩阵 M，有可能以一个已知的方式利用伪随机函数来生成每一个系数 a_{ij}。

具有 M 维二进制码的输出端信号 y 在所有的进入控制系统中都可被用作控制字。在收费电视系统的情况下，在发送器级别和接收器或多个接收器级别上可以同样好地产生输出端的信号 y。

现在参照图 3 将描述另一个 k 维数字信号的处理方法以及采用该方法的设备，使得不能从输入端的数字信号推断出输出端的数字信号。在图 3

所示的情况下，输入端的数字信号 x 被送到本领域技术人员所共知的一个加扰电路。该数字信号是由 k 维二进制字构成的信号。在输出端得到一数字信号 x'，该信号按照词典编辑方式对所有权重为 d 和长度为 n 的可能的字进行排序并单向地给出一个字的索引。

将信号 x'格式化成一个权重为 d 和长度为 n 的字的最好方法就是采用本领域技术人员所共知的按照词典编辑的方式排序。于是，可以用最少位数的二进制码来定义一个权重为 d 和长度为 n 的字，该最少位数即是在 n 中取 d 的组合数的以 2 为底的对数。k 就会有该值。

下面就是按词典编辑方式排序的算法。

输入:

V: 索引值

n: 字的长度

d: 字的权重

输出:

长度为 n 权重为 d 的二进制码序列

1. C = 在 n 中取 d 的组合数

2. 如果 n > 0

a) C' = C(n-d)/n

b) 如果 V ≤ C'

则输出二进制码 0

C = C'

c) 如果不是

则输出二进制码 1

i = i-C'

C = C.d/n

d) n = n - 1

现在参照图 4 来描述另一个 k 维数字信号的处理方法以及采用该方法的设备，使得不能从输入端的数字信号推断出输出端的数字信号。在图 4 所示的情况下，在输入端，k 位二进制码的数字信号 x1，同时还有作为密钥的数字信号 s，被传递给一个伪随机生成器 4。

伪随机生成器是这样选取的，使得在输出端 n 维的数字信号有一固定

的具有高概率的汉明权重(Hamming Weight)d，而 n 取决于实现单向函数的电路。这样，在伪随机生成器的输出端就得到一个长度为 n 个二进制码以及权重约为 d 的随机数字信号 x'1。接下来，信号(x'_1)被传递到一乘法器电路 5，并在该电路中同具有 m×n 维二进制码的一个固定矩阵的系数相乘以便在输出端给出具有 M 位二进制码长度的数字信号 Y1。该固定矩阵同参照图 2 所描述的一样。

采用质量良好的伪随机生成器来得到随机信号，给我们的应用提供了一个足够的扩散。因此，如果钥匙继续是秘密的，即使知道了输入端的数字信号，该加扰还是足够好，仍能提供好的保密措施。

然而，为定义数字信号的二进制设置(settings)而采用伪随机生成器会造成一个问题。实际上，有些设置不只产生一次。在用于存贮信号的二进制设置的存贮器胜任的情况下，有可能简单地删掉该冗余值并且取出另一个设置，但是如果不可能存贮它们，具体地说当是在智能卡中进行计算时，那么随机信号的权重比所取得的设置数要小，这是必须要考虑的。为了得到所需的平均值，需要取出比权重更多的信息项。当输入到单向函数的字的权重不需要精确为 d、而也许是一个很接近 d 的值时，那么只要计算出非冗余值的统计分布，这个方法就能成立。这样，如果要求平均得到 56 个非冗余设置，则应意识到必须取 59 个设置，所取的 25％准确地来自 56、66％来自 55 到 57 之间、98％来自 53 到 59 之间。

现在来描述该系统的另一个实施例，该实施例可能实现一种处理数字信号的方法使得从输入端的数字信号不能推断出输出端的数字信号，其中从输入端的一个数字信号出发能在输出端得到符合所述准则的若干个数字信号。

如图 5 所示，输入端的数字信号 x_2 与密钥 5 同时被传递到一个伪随机生成器 6。如果输入端的信号是用来产生长度为 n 位二进制码和权重约为 di 的输出端信号 $x'_{2.1}$、$x'_{2.2}$、……$x'_{2.i}$……$x'_{2.N}$ 的一个长度为 k 位二进制码的数字信号，则可能产生 N×n 个二进制码，由此提供给 N 个矩阵乘数 M_1、M_2、M_3、……M_N 以便得到输出端的 N 个数字信号 Y_{21}、Y_{22}、……Y_{2N}，每个都具有 m 位二进制码的长度。用在乘法器 $M_1, M_2, M_3, \ldots\ldots M_N$ 级别上的矩阵同参照图 2 到图 4 所描述的矩阵具有一样的特性。根据一个优选模式产生这样一些信号需要采用一个可靠的允许生成大约 N×n 个二进制码的

伪随机生成器。上述的这些设备可以有大量的应用。这样，如图 6 和图 7 所示，上述这些设备可用来计算具有共用密钥的密码错误检测码。这意味着发送器和接收器共用一个密钥，且用该密钥计算并检验错误检测码。如图 6 所示，一个信息 M 被分为多个包含 k 位二进制码的并以 B_i 标记的块，i 从 1 变化到 n。我们定义 C_0 为一个具有 k 个二进制码长度的固定的数字信号，C_0 可能全部都是零，且错误检测码被定义为 C_n，这里 C_i 的获得如图 6 所示。在此情况下，同图 2 到图 4 的所有电路相对应的设备表示为 7。该电路是如此来定义的，使得 k=m(输入端的信号二进制位数和输出端信号的二进制位数相同)。在输入端，该电路接收从一个加法器 8 来的一个 k 位二进制数字信号 x_3，而加法器在一个输入端接收块 B_i 之一且在另一个输入端接收 k 位二进制数字信号 C_{i-1}，C_{i-1} 实际上是从电路 7 在前一个步骤所得到的信号，这样就给出了信号 C_i。

如果 k 大于 m，有另外一个办法来将一个信息的 k-m 个二进制码同一个输出字连结起来。在此情况下，作为一个二进制字的信息 M，被分为 k-m 个二进制码的许多块，B'_1、B'_2、……B'_n。如图 7 所示，B'_i 同有 m 个二进制码大小的一个信号 C_{i-1} 一起被输入到一个连结电路(Concatenation Circuit)9，从连结电路出来的二进制字 X'_3 被传到上面已定义的电路 7 以得到了字 C_i。

此外，当输入端的信号的二进制位数比输出端的小时，图 2、3 和 4 所述的电路还可以被用作一个伪随机二进制生成器。例如，如图 8 所示，如果输入信号由 k 个二进制码的二进制字组成，这里 K＜m，则采用下面的方案：计算输入端的象、以前面的 m-k 个二进制码为输出端的随机序列以及用相继的 k 个二进制码来产生一个新的输入字。这在图 8 中表示出来，一个输入字 10 被传送到电路 7。来自电路 7 的 m 位输出字被分为二个部分，起始的 m-k 位被传到输出端，形成伪随机生成器的输出，剩余部分被反馈回来，正如前面所看到的。在所代表的实施例中，k = m-k = 128 位二进制码。显然 k 可以和 m-k 不一样。

在这样一种采用伪随机生成器的情况下，可以省去加扰系统。

很显然，对于本领域技术人员来说，上述的系统可以很多方式应用于对保密系统进行密码加密的领域中，例如，用于收费电视、银行系统、保密进入系统等等。

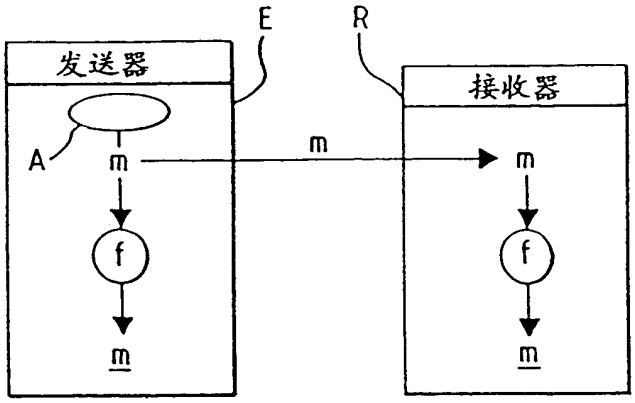


图 1

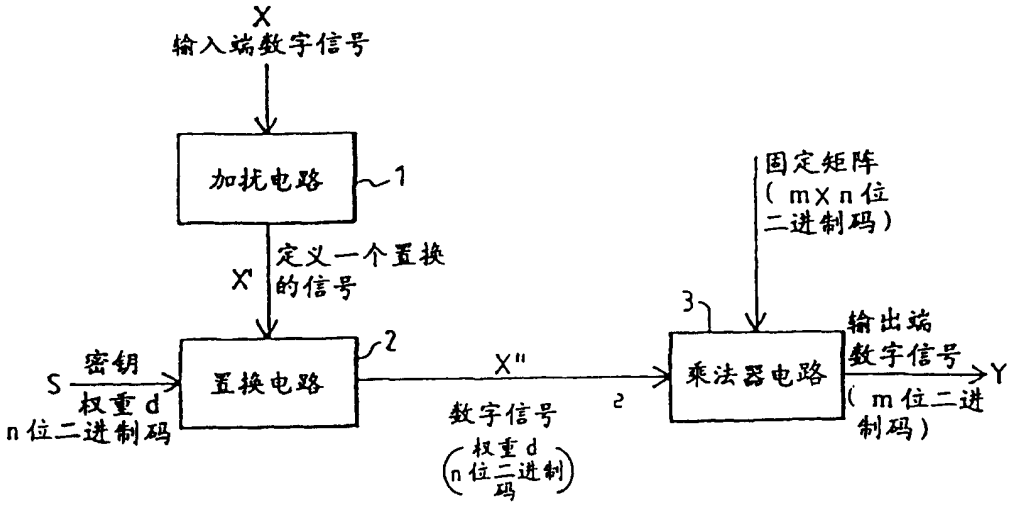

X
输入端数字信号
加扰电路
1
X'
定义一个置换的信号
密钥
S
权重 d
n 位二进制码
置换电路
2
X"
数字信号
(权重 d n 位二进制码)
固定矩阵
(m X n 位二进制码)
3
乘法器电路
输出端数字信号
Y
(m 位二进制码)

图 2

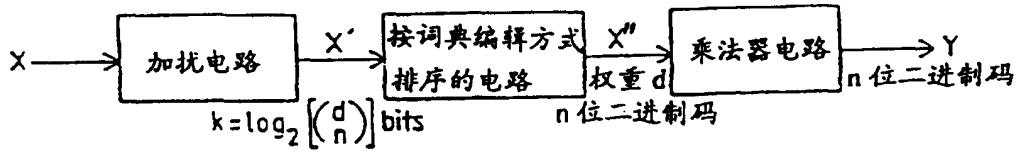

X
加扰电路
X'
按词典编辑方式排序的电路
X"
权重 d
n 位二进制码
乘法器电路
Y
n 位二进制码
k = log2 [(d n)] bits

图 3

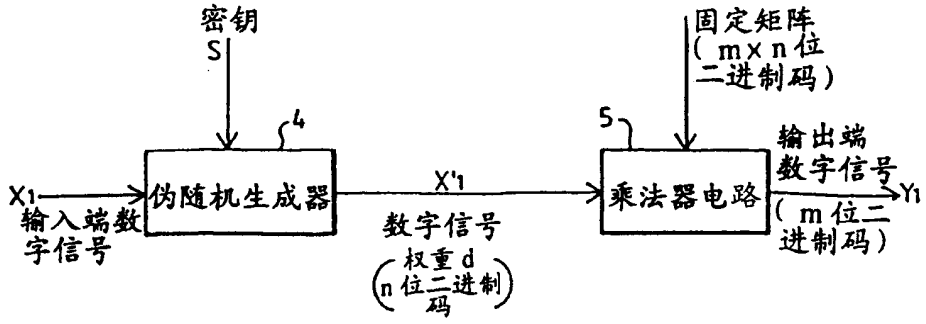

密钥
S
4
固定矩阵
(m×n位
二进制码)
5
输出端
数字信号
X1
输入端数
字信号
伪随机生成器
X'1
数字信号
(权重d
n位二进制
码)
乘法器电路
Y1
(m位二
进制码)

图 4

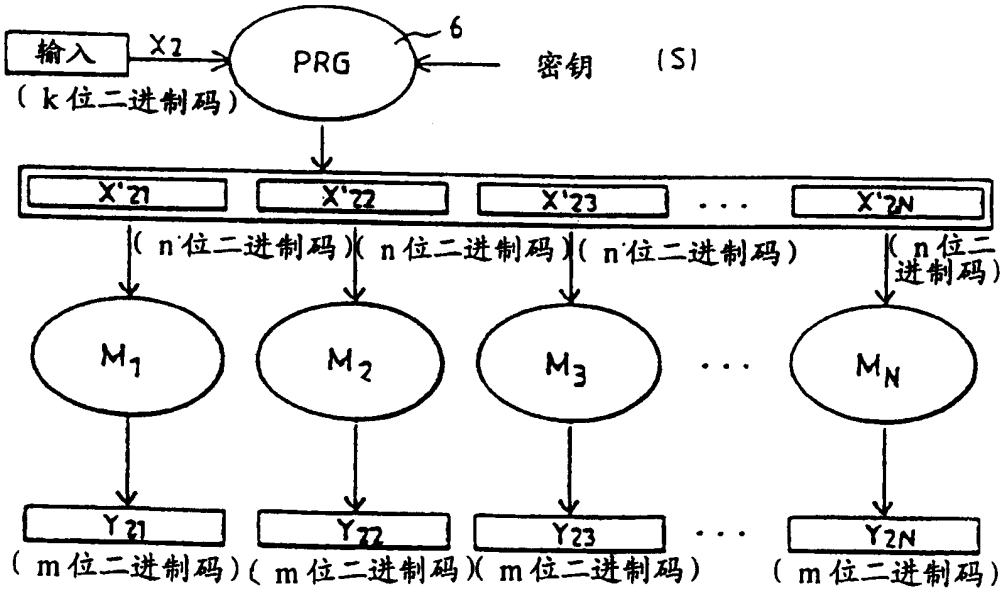

输入
X2
PRG
6
密钥 (S)
(k位二进制码)
X'21
X'22
X'23
X'2N
(n位二进制码)
(n位二进制码)
(n位二进制码)
(n位二
进制码)
M1
M2
M3
MN
Y21
Y22
Y23
Y2N
(m位二进制码)
(m位二进制码)
(m位二进制码)
(m位二进制码)

图 5

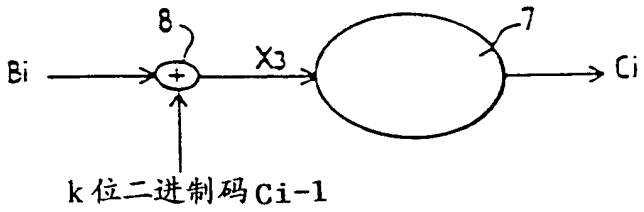


图 6

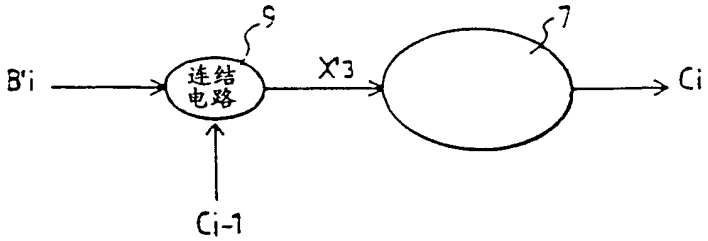


图 7

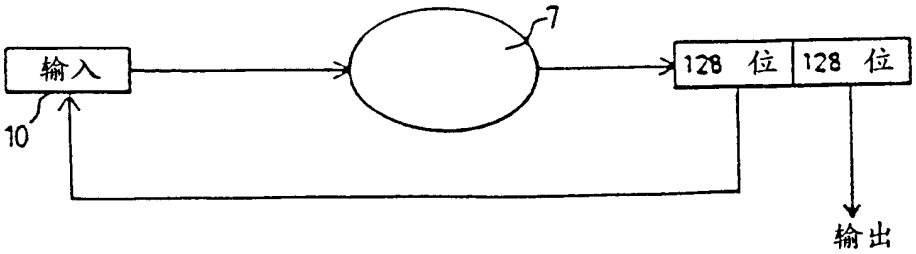


图 8