

[12] 发明专利说明书

[21] ZL 专利号 94191886.6

[45]授权公告日 2000年7月5日

[11]授权公告号 CN 1054245C

[22]申请日 1994.3.16 [24] 颁证日 2000.4.21

[21]申请号 94191886.6

「30」优先权

[32]1993.5.5 [33]EP [31]93107314.2

[32]1993.5.13 [33]US [31]08/061,205

[86]国際申請 PCT/US94/02960 1994.3.16

[87]國際公布 WO94/26045 英 1994.11.10

[85]进入国家险段日期 1995.10.24

[73]专利权人 刘尊全

地址 美国加利福尼亚

[72]发明人 刘慕金

[56]參考文獻

EP0095923A2

USS 010 573 1991 4 23

W07940418 1979-7-12

宋本昇 郭凤麟

[74]专利代理机构 中国国际贸易促进委员会专利商标事

务所

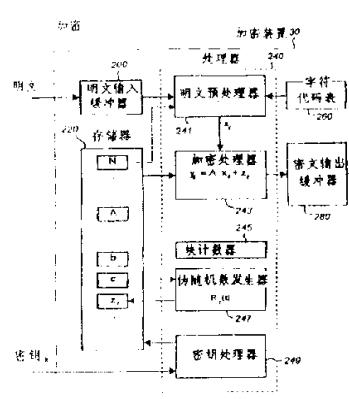
代理人 于 静

权利要求书 4 页 说明书 22 页 附图页数 7 页

[54]发明名称 数据加密的装置和方法

[57] 摘要

本发明提供一种数据加密的方法和装置,使用户将明文加密成密文和将密文解密成明文,包括:提供一个加密参数组来控制加密、和一个解密参数组来控制解密;提供一个密钥,在用户之间共享;从所述的密钥导出所述的加密参数组的用户可选择的部分;响应所述的加密参数组,产生一个映射集中的一个映射,把明文映射成密文;从所述的密钥导出所述的解密参数组的用户可选择部分;和响应所述的解密参数组,产生与所述映射相关的一个逆映射,把密文逆映射成明文。



权 利 要 求 书

1. 一种密码系统（30, 50），使用户把明文加密成密文和将密文解密恢复成明文，其特征在于，包括：

一个加密参数组（ N, A, Z_t, b, c ）和一个解密参数组（ N, A^{-1}, A, Z_t, b, c ），分别控制加密和解密；

一个密钥（K），在用户之间共用；

用于从所述的密钥推导出所述的加密参数组的用户可选择的部分的密钥处理器（249）；

一个产生映射的加密处理器（243），响应所述的加密参数组，产生一个映射集之中的一个映射，把明文映射成密文，该映射集的大小取决于所述的加密参数组；

用于从所述的密钥导出所述的解密参数组的用户可选择部分的密钥处理器（349）；和

一个产生逆映射的解密处理器（343），响应所述的解密参数组，产生与该映射相关的一个逆映射，把密文逆映射成明文。

2. 根据权利要求1所述的密码系统，其特征在于，还包括：

一个明文预处理器（241），响应一个块大小的参数，根据所述的块大小参数将明文逐块地分成相应大小的明文块或明文向量；其中：

所述的映射把明文向量映射为相应的密文向量；和

所述的用户可选择的加密参数组包括所述的块大小参数。

3. 根据权利要求2所述的密码系统，其特征在于：

所述的用户可选择的加密参数组包括一个映射矩阵（A）；

所述的映射是这样的：每个密文向量是一个向量和，该向量和包括一个第一向量和分量，该第一向量和分量是由该映射矩阵和相应的明文向量的乘积形成的；

所述的解密参数组包括与所述的映射矩阵相关的一个逆映射矩阵；和

所述的逆映射是这样的：每个明文向量是所述的逆映射矩阵与一个合成向量的乘积，该合成向量是由相应的密文向量减去除

了其第一向量和分量之外的向量和所产生的。

4. 根据权利要求3所述的密码系统，其特征在于，还包括：

生成一个伪随机数发生器（247），每个块有一个伪随机向量；其中：

所述的向量和包括一个第二向量和分量，该第二向量和分量是由所述的伪随机向量组中的一个伪随机向量形成的。

5. 根据权利要求4所述的密码系统，其特征在于：

所述的用户可选择的加密参数组和解密参数组的每组都包括用于产生所述的伪随机向量的参数。

6. 根据权利要求1所述的密码系统，其特征在于，还包含：

所述的密钥处理器（249），用于从具有预定长度的输入产生所述的密钥。

7. 一种密码方法，使用户将明文加密成密文和将密文解密成明文，其特征在于，该方法包括以下步骤：

提供一个加密参数组（ N, A, Z_t, b, c ）来控制加密、和一个解密参数组（ N, A^{-1}, A, Z_t, b, c ）来控制解密；

提供一个密钥（K），在用户之间共享；

从所述的密钥导出所述的加密参数组的用户可选择的部分；

响应所述的加密参数组，产生一个映射集之中的一个映射（A），把明文映射成密文，所述的映射集的大小取决于所述的加密参数组；

从所述的密钥导出所述的解密参数组的用户可选择部分；和

响应所述的解密参数组，产生与所述映射相关的一个逆映射（ A^{-1} ），把密文逆映射成明文。

8. 根据权利要求7所述的密码方法，其特征在于，还包括以下步骤：

响应一个块大小参数，把明文逐块地分成明文块或明文向量，每块的大小是根据所述的块大小参数确定的；其中：

所述的映射将明文向量映射成相应的密文向量；和

所述的用户可选择的加密参数组包括所述的块大小参数。

9. 根据权利要求7所述的密码方法，其特征在于，还包括以下步骤：

根据一个具有预定长度的输入，产生所述的密钥。

10. 根据权利要求8所述的密码方法，其特征在于，其中：

所述的用户可选择的加密参数组包括一个映射矩阵；

所述的映射是这样的：每个密文向量是一个向量和，该向量和包括一个第一向量和分量，该第一向量和分量是由该映射矩阵和相应的明文向量的乘积形成的；

所述的解密参数组包括一个与该映射矩阵相关的逆映射矩阵；和

所述的逆映射是这样的：每个明文向量是该逆映射矩阵与一个合成向量的乘积，该合成向量是由相应的密文向量减去除了第一向量和分量之外的向量和而产生的。

11. 根据权利要求10所述的密码方法，其特征在于，还包括以下步骤：

产生一个伪随机向量组，每块有一个伪随机向量；其中：

所述的向量和包括一个第二向量和分量，该第二向量和分量是由所述的伪随机向量组的一个伪随机向量形成的。

12. 根据权利要求11所述的密码方法，其特征在于：

所述的用户可选择的加密和解密参数组都包括用于产生所述的伪随机向量组的参数。

13. 根据权利要求8所述的密码方法，其特征在于，还包括以下步骤：

从每个明文向量中选择明文单元的子集作为基础明文单元；

从每个密文向量中选择相应的密文单元的子集作为基础密文单元；

产生所述的映射，其中每个密文单元都是一个和值，所述的和值包括一个第一和分量和一个第二和分量，因此：

对于所述基础密文单元而言，

每个第一和分量都是线性地依赖于与所述的相应基础明文单元，所述的线性依赖关系是由用户可选择的基本系数确定的；并且

每个第二和分量都是逐块变化的伪随机数；和

对于不在该子集中的每个密文单元而言，

每个第一和分量都是基础明文单元的子集的线性组合，该线性组合是由一个用户可选择的组合系数组确定的；

每个第二和分量都是相应的明文单元的非线性函数，该非线性函数是由用户确定的；

产生所述的逆映射，其中：

每个基础明文单元都是反线性地依赖于合成值，该合成值是相应的密文单元减去除了该和的第一和分量之外所得到的和值；
和

每个不在该子集中的明文单元都是在一个合成值上运算的所述非线性函数的反函数，所述的合成值是由相应的密文单元减去除了第一和分量以外所得到的合值而形成的。

说 明 书

数据加密的装置和方法

本发明是属于密码学领域，特别是关于用密钥控制进行数据加密与解密的装置和方法。

在现代的电子时代中，通过在公共电信信道上交换的数据处理日常的商务、公务及私人事务与日俱增。敏感的数据常常是储存在不安全的存储器中。通过电信信道交换的数据或存在不安全存储器中的数据易被其他人未经许可的存取，因而就不能确保其机密性。

数据加密就是防止数据在存储器中或在公共电信信道上传输时被非授权存取的一种方法。加密是把明文转换为不可理解的密文的一种计算形式。解密是把无法理解的密文恢复为明文的加密的逆计算。

在实践中，数据首先由加密者把明文加密成密文后才用于公共信道传输或储存起来。收到或检索这些数据时，解密者需把密文解密成明文，以便获得原来的数据。

在密钥加密方案中，用密钥把有关加密者如何进行加密的信息传送到被授权的解密者那里，以便解密者能构成一个逆运算，进行有效的解密。另一方面，如果不是不可能的话，其它非授权解密者无此密钥是十分困难破译密文的。

常规的密钥加密系统中，建立一种计算的步骤序列或算法来加密解密。密钥加密系统通常都是设计成算法是公知的。唯独需要保

密的是密钥，而该密钥只能是发送者和被授权接受者之间共享。

典型的密钥提供一个用户选择的值，这值和明文一起作为算法的输入进行加密和解密。通常，这种算法通过某种模运算将密钥值加到明文上来改变明文。

在实际上，密钥通过保密信道由发送者秘密地传送给授权接收者。这样，授权接收者采用公知算法，借助密钥有效地把密文解密。另一方面，其它不知道密钥或没有任何其它密码破译方式的人就不得不在该密钥长度中一个个的找出可能的密钥，看看是否能可懂的解密。当密钥长度很长时，认为加密系统有很高的加密强度，而且其解密计算是不可行的。

如果在合理的时间内，利用合理的资源实际上不能实现，这个计算任务是不可行的计算。如在可能的最快的计算机上计算 100 年可认为是不合理的。类似地，使用 100 万亿美元专门制造的计算机可认为是不合理的。

密钥系统的一个例子是“一次密钥体制”“one-time pad”或 Vernam 方案，首先把明文编码为二进制比特串并且用模 2 加法加到密钥上，把明文转换成密文。密钥是和明文一样长的一串随机比特，而且只能用一次。该方案被证明非常安全，但是不希望的是需要密钥的每个位对应明文的每个位。要求密钥的位和要传递的信息一样长，而不能再次使用，使得从现代数据事务处理的角度看这种方案是不实用的。

有人已试图采用伪随机生成器产生大量的密钥随机位。伪随机生成器通常是用一个反馈移位寄存器来实现的。所产生的伪随机序列完全取决于移位寄存器中的初始值。初始值可以用作密钥，因此

可以使少量的密钥位产生一长串“随机”位。然而，采用伪随机生成器的一次插入密钥体制加密系统对已知明文的攻击很敏感，也就是在知道了一部分密文及其相应的明文时是很敏感的。

其它的方法也考虑采用较短密钥串的密钥加密系统。在这些方法中较显著的是“数据加密标准”(DES)，由美国国家标准局于1977年元月在联邦信息处理标准(FIPS)出版物第46号上公布。自那以后，DES就被确定为一个标准的公开加密方法。根据DES，加密和解密是按块进行的，每个块为64位长。基本的算法包括一系列预定排列的十六次迭代，加入密钥和在每个64位块的每个分块中的预定置换运算。56位密钥通过移位寄存器循环生成十六个迭代值。

在过去十年中DES被正式作为标准采用，但普遍认为现时应该有一种新的更好的标准来取代。一个原因是：56位密钥太短。它仅能产生大约 10^{17} 个可能密钥的密钥间隔。从现代高速和多处理器计算机来看，在此密钥长度的密钥间隔的穷举在计算上是有可能的（即尝试每个可能的密钥，看是否能得到解密的方法）。另一个缺点是基本设计原理，例如各种不同排列的选择、置换和所需的迭代次数都没有清楚的说明。对有关该系统中设有“陷阱”(trapdoor)的可能性一直都存争论。因此，如果用户不能容易地和精确地鉴定该系统的实际安全性，它就不能是一个真正的公开加密系统。此外，用户没有系统的方法修正算法或变换以使系统更安全或增加加密强度。不管怎样，要增加加密强度，计算机的开销就要呈指数增加。这是因为DES，和其它短密钥方法一样，基于增加计算量原理获得加密。相同的短密钥在不同条件下多次使用以把长的多的明文加密。

另一种方法是RSA(Rivest, Shamir 和 Adleman)公共密钥系

统。它基于计算复杂性(*computationally complex*)的原理获得加密强度。用户选择两个非常大的素数,最好每个上百位的数字,产生一对不同的加密与解密的密钥。加密是用密钥在模算法下控制取幂完成的。密钥可做成对任何要对信息加密的用户是公共的,但它不能导出解密的密钥。这样,加密的信息只能由有解密密钥的用户读出。不希望的特性是系统的安全取决于使用很难得到的两个非常大的素数。并且,如果找出一种很快的方法分解这两个大的素数的乘积,系统就很容易被攻破。

为此,仍需要有一种改进的数据加密系统。

本发明总的是为数据加密和解密提供改进的方法和装置,而不会有前述方法的缺点。

本发明的一个目的是为加密和解密提供一种方法和装置,其基本原理是清楚易懂并是可公开的,又不损害它的安全性。为此,本发明提供了一个真正的能够作为标准的公共加密系统。

本发明的另一个目的是为数据加密和解密提供一种极其安全的方法和装置。

本发明的再一个目的是为数据加密和解密提供一种用户可以选择加密强度的方法和装置。

本发明的又一个目的是为数据加密和解密提供一种容易实现和计算开销小的方法和装置。

这些和其它的目的是通过产生一个用户可以选择的映射实现的,该映射是从一个巨大映射集选出来的。该映射作用于分成块的明文。明文块的大小 N 是用户可选择的,每个明文块都等效于一个 N 维的明文向量 x 。该映射是由一组用户可选择的映射参数所指定

的，该映射把明文向量 x 映射为 N 维的密文向量 y 。相应的逆映射也存在，用于把密文向量 y 反向映射为明文向量 x 。映射集中映射的基本原理和形式是可以公开的而不会影响该方法和装置的安全性。该映射的特征是：映射集的大小是块的大小和每个映射参数范围的指数函数。

根据本发明一个方面，提供一种密码系统，使用户把明文加密成密文和将密文解密恢复成明文，其特征在于，包括：一个加密参数组 (N, A, Z_t, b, c) 和一个解密参数组 (N, A^{-1}, A, Z_t, b, c)，分别控制加密和解密；一个密钥，在用户之间共用；用于从所述的密钥推导出所述的加密参数组的用户可选择的部分的密钥处理器；一个产生映射的加密处理器，响应所述的加密参数组，产生一个映射集之中的一个映射，把明文映射成密文，该映射集的大小取决于所述的加密参数组；用于从所述的密钥导出所述的解密参数组的用户可选择部分的密钥处理器；和一个产生逆映射的解密处理器，响应所述的解密参数组，产生与该映射相关的一个逆映射，把密文逆映射成明文。

根据本发明另一个方面，提供一种密码方法，使用户将明文加密成密文和将密文解密成明文，其特征在于，该方法包括以下步骤：提供一个加密参数组 (N, A, Z_t, b, c) 来控制加密、和一个解密参数组 (N, A^{-1}, A, Z_t, b, c) 来控制解密；提供一个密钥，在用户之间共享；从所述的密钥导出所述的加密参数组的用户可选择的部分；响应所述的加密参数组，产生一个映射集之中的一个映射，把明文映射成密文，所述的映射集的大小取决于所述的加密参数组；从所述的密钥导出所述的解密参数组的用户可选择部分；和响应所述的解密参数组，产生与所述映射相关的一个逆映射，把密文逆映射成明文。

根据本发明的一个方面，块的大小和每个映射参数的范围也是保密的，只能通过密钥在用户之间秘密使用。这样，不知道密钥的人用通常破译密码的方法在映射集中尝试每个映射从而找出明文是不可行的。这是因为他们面临着在不确定大小的映射集中采用在计算上是不可行的穷举法任务。

根据本发明的另一方面，块的大小 N 和每映射参数的范围无需保密。一旦选择一个足够大的值产生具有被认为是非常大的预定大小的映射集，块大小 N 和参数范围作为标准并公开。要破译密码的其他人在这个非常大的映射集中仍然面临在计算上不可行的穷举法的任务。

在优选的实施例中，映射的形式为

$$y_t = A \cdot x_t + z_t$$

而相应的逆映射为

$$x_t = A^{-1} [y_t - z_t]$$

这里，

x_t 和 y_t 分别与第 t 块相应的 N 维明文和密文向量；

A 和 A^{-1} 分别是 $N \times N$ 映射和相应的逆映射矩阵；而

Z_t 是对应于第 t 块的 N 维第二个分向量。

A 和 Z_t 构成映射参数，它们是密钥的一部分。实质上， $N \times N$ 映

射矩阵 确定了该映射的空间。如果每个矩阵单元都可以在 L 范围内变化，那么映射集具有通过排列所有的矩阵单元得出的大小，即 $L^{N \times N}$ 。这是一个指数函数，而且即使 N 和 L 的值不是很大，其映射集也会变得非常之大。例如，如果 $N=3, L=100$ ，整个映射集就有 10^{18} 个映射。

在优选的实施例中，加入第二个分向量 Z_2 组成每个密文向量以进一步增强本方法的安全性。特别是对已知明文的攻击(attack)及对较小块的统计攻击这一潜在薄弱环节特别有效。在一种实现中，第二分向量是伪随机向量，它随块的不同而变化。在另一种实现中，第二分向量是非线性函数或非线性函数和伪随机向量的混合。

目前的实现方法没有常规方法(加入一串伪随机数对一明文串加密)相同的弱点。这是因为该映射发生在 N 维空间中，每个伪随机数一般不像常规情况那样直接加到单个的明文字符上以便把明文字符转换为密文字符，而是加到明文字符的线性组合上。别人来分析这种方法的伪随机数的问题在数学上称为非确定的多项式(*NP*)问题。

本发明的一个重要方面是提供了映射结构，一般地其大小而且特别是具体映射的特性是用户可以用密钥随意选择的。没有密钥，其他人面临在一个不确定的映射集中用穷举法找出计算上不可行的任务。

本发明的另一个重要方面是计算机开销只随块大小的平方增加，而加密强度呈指数增加。这样，在计算机开销很小的情况下得到很高的加密强度。相反，一般的加密系统计算机开销随加密强度的增加呈指数增长。这是 *NP* 的另一种表现形式。

本发明的其它目的、特点和优点都会从后面的优选实施例的描述中更好的理解，本发明的描述应结合附图。

图 1 示意地示出了应用于本发明的一个一般的密钥加密系统；

图 2A 示出常规加密系统的计算开销与加密强度的关系曲线；

图 2B 示出本发明的计算开销和加密强度的关系曲线；

图 3 示出本发明的加密强度随映射参数的指数函数增加，映射参数诸如块的大小 N 和每个映射矩阵单元的范围 L ；

图 4 示出根据本发明的优选实施例的加密装置的功能方框图；

图 5 示出根据本发明的优选实施例的解密装置的功能方框图；

图 6A 示出块大小 $N=9$ 时的基本明文向量单元的各种排列或可能的选择；和

图 6B 示出从一个块中选择一些单元的实际排列配置，块单元是按 3×3 图安排的。

图 1 概要示出应用于本发明的一个一般的密钥加密系统。用加密装置或过程 30 把明文 x_{10} 加密成密文 y_{20} 。加密者以用户可选择的密钥 k_{10} 控制加密过程 30。密钥 k 是与解密者秘密地共用的，解密者又用它控制解密装置或过程 50，将接收到的密文 y 解密为明文 x 。

本发明的一个重要方面是提供了映射结构以生成映射集。用户一般可用 密钥选择映射集的大小和特别是指定的映射特性。没有密钥，其他人面临在不确定的映射集中采用穷举的计算上是不可行的任务。

映射将明文映射或加密为密文。每个映射都可由一组映射参数来确定，这组参数实质上是用户可选择的，因为它是由密钥 k 导出

的。

本发明将每个明文流分成一块一块的明文向量。块的大小也是用户通过密钥可选择的。如果块的大小为 N , 那么该映射把一个 N 维明文向量映射为对应的 N 维密文向量。

映射的特征是映射集的大小取决于块的大小和每个映射参数的范围。用户可以通过调整这些参数选择所需要的加密强度等级。如果每个映射参数有一个范围 L , 那么, 如后面所述, 映射集的大小为 $L^{N \times N}$ 。这样, 密钥的空间就随 N 呈指数增加。例如, 如果 $L=100, N=3$, 那么 $(k) \approx 10^{18}$, 这比 DES 大十倍。如 N 扩大到 9, 则 $(k) \approx 10^{162}$ 。这就意味着攻击者即使知道 N 的大小, 在采用穷举的办法时需要尝试 10^{162} 个密钥。在优选的实施例中, N 和 L 也是保密的, 攻击者面对的是一个不确定的大密钥空间。

本发明的另一个重要方面是加密强度可增加到非常高等级而不需要相应高的计算开销。相反, 传统的加密系统的计算开销随加密强度的增加呈指数增长。这是 NP 的另一种表现形式。

图 2A 示出传统加密系统的计算开销与加密强度之间的曲线关系。图 2B 示出本发明的计算开销与加密强度的曲线关系。两图比较可以看出, 传统加密系统的计算开销呈指数增长, 而本发明的计算开销呈对数增长。这是因为本发明的计算开销随块大小的平方增长, 而加密强度却呈指数增长。

图 3 示出本发明的加密强度随映射参数(如块的大小 N , 每个映射矩阵单元的范围 L) 的指数函数增长。图中还表明了 L 两个值之间的关系。 $L=2$ 对应的情况是每个映射矩阵单元可以如从“0”和“1”两个数值中取一个。 $L=100$ 对应的情况是每个映射矩阵单元可

以从 100 个可能值的范围内变化，例如从 0 到 99 或者负 49 到 50。可以看出，本发明在计算开销增加很小的情况下可获得极高的加密强度。

加密和解密的方法：

本发明的优选方法包括以下步骤：

步骤 1. 选择块的大小 N

每个明文块都对应一个 N 维的明文向量。每个 N 维明文向量都可加密成 N 维的密文向量。因此，

$$\text{明文 } \mathbf{x} = \mathbf{x}_i = [x_1, x_2, \dots, x_N]$$

$$\text{密文 } \mathbf{y} = \mathbf{y}_i = [y_1, y_2, \dots, y_N]$$

$$i = 1, 2, \dots, N$$

初始的明文通常是字符流的形式。通过预先定义的字符代码表可把字符表达方式转换为数字表达方式。 x_i 和 y_i 都是以数字表达方式编码的。

一般来说， x_1, x_2, \dots, x_n 没有必要与进来的明文字符流中单元的相同序列对应。映射前的初始块排列可用于混淆块单元的原始顺序。初始块排列可规定为加密信息的一部分，通过密钥从一个用户传输到另一个用户。这样，另一个用户可执行相反的步骤，在密文已解密成明文后把明文重新排列成原来的顺序。

步骤 2. 由用户选定的一组映射参数： A, Z_t, \dots 生成第 t 块的映射

$$\mathbf{y}_t = A \mathbf{x}_t + \mathbf{z}_t \quad (2)$$

这里，

t 代表第 t 个块或向量的标记，

A 一般说来是一个可逆的 $N \times N$ 映射矩阵

$$\Lambda = \alpha_{ij} = \begin{bmatrix} & & & \\ | & a_{11} & a_{12} & \dots & a_{1N} | \\ | & a_{21} & a_{22} & \dots & a_{2N} | \\ | & . & . & . & . | \\ | & . & . & . & . | \\ | & a_{N1} & a_{N2} & \dots & a_{NN} | \\ \vdots & & & & \end{bmatrix} \quad (3)$$

$i, j = 1, 2, \dots, N$

$$\text{for } z_t = (z_i)_t = [z_1, z_2, \dots, z_N]_t \quad (4)$$

是第二个向量分量，它可根据具体实施例呈现不同的形式。在一个实施例中，它是随块的不同而变化的一个随机向量，这将在后面更加详细地叙述。例如：

$$(z_i)_t = b_i R(t, c_i) \quad (5)$$

这里

$R(t, C_i)$ 是 t 的伪随机函数，

b_i 是一个常数向量，例如，

$$b = [b_1, b_2, \dots, b_N],$$

C_i 是 R 的初始值。

在另一种实施例中， $(Z_i)_t$ 也可能是 x_i 的非线性函数。

步骤 3. 用户之间秘密地共用一个密钥，把加密信息从一个用户传递到另一个用户用于解密。例如：

$$\begin{aligned} k &= [\text{块大小}; \text{映射参数, 随机函数的详细描述}; \text{初始块排列}, \dots] \\ &= [N; A; z_t, \dots; \dots] \end{aligned} \quad (6)$$

通常为分别控制加密和解密，密钥 k 可推导出一组加密或解密参数。密钥间隔 $\{k\}$ 包括了所有可能的密钥集，这些密钥是由在其范围内每个密钥参数所有可能的值生成的。例如，如果每个映射矩阵单元具有以可能值的范围，如

$$\begin{aligned} \{L\} &= \{0, 1, 2, \dots, L-1\} \\ a_{ij} &\in \{L\} \end{aligned}$$

那么，给定 N ，一个密钥空间中存在的可能密钥集由下式给出：

$$\{k\} \approx L^{N \times N} \quad (7)$$

步骤 4. 由方程(2)生成第 t 块的逆映射

$$x_t = A^{-1}(y_t - z_t) \quad (8)$$

逆映射参数 A^{-1} , z_t, \dots 是从方程(6)中的密钥导出的。特别是逆映射矩阵是由对映射矩阵 A 求逆得到的。

映射或逆映射最好用整数量来实现以避免舍位问题。因此，所有的映射参数和明文表示式都是用整数给出的并且计算是精确的。在密文已解密成明文后，用解密时使用的同一字符代码可把数字表示的明文解码回原来用字符表示的明文。

在优选的实施例中，第二向量分量 z_t 不为零。加入该分量构成每个密文向量以便进一步增强安全性，特别是防止已知明文(*known*

—plaintext)攻击和在块较小时统计攻击的潜在弱点。

在一个实施例中,第二向量分量是逐块变化的一个伪随机向量。对第 t 块,由方程(2),通过下式给出每个密文向量单元:

$$y_1 = a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n + b_1 R(t, c_1)$$

$$y_2 = a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n + b_2 R(t, c_2)$$

$$y_N = a_{N1}x_1 + a_{N2}x_2 + \dots + a_{Nn}x_n + b_N R(t, c_N) \quad (9)$$

密钥具有参数 $k = [N; a_{ij}; b_i; c_i; \dots]$ (10)

解密由方程(8)给出,并且明文由下式恢复

$$x_t = A^{-1}(y_t - z_t)$$

在另一个优选实施例中,采用一种快速计算把密文转换成明文而无需对 $N \times N$ 映射矩阵 A 求逆。在此情况下,第二个分量(z_i)最好是非线性函数或伪随机函数。如前面所述的,密文向量单元通常由方程(2)给出:

$$y_i = a_{ij}x_j + z_i \quad (11)$$

$$i, j = 1, 2, \dots, N$$

这种方法需要从每个明文向量中选出基础明文向量单元的随机子集

$$x_s \in \{x_i\} \quad s = s_1, s_2, \dots, s_M$$

$$\text{因此 } \{x_i\} = \{x_s\} \cup \{x_r\} \quad x = x_1, x_2, \dots, x_{N-M}$$

$$1 < M \leq N$$

把密文映射定义为 x_s 's 的函数：

$$y_i = a_{is}x_s + z_i \quad (12)$$

具有如下特性

(a) 当 $i=s$ 时

$$y_s = a_{ss}x_s + z_s \quad (13)$$

且 z_s 是如方程(5)中的随机值

$$z_s = b_s R(t, c_s)$$

(b) 当 $i=r$ 时

$$y_r = a_{rs}x_s + z_r \quad (14)$$

这里

$$z_r = b_r G(x_s) \quad (15)$$

且 $G(x_s)$ 是一个非线性函数，例如，

$$G(x_s) = x_s^3 \quad (16)$$

由方程(13)得出

$$x_s = [y_s - b_s R(t, c_s)] / a_{ss}$$

由方程(14)和(15)得出

$$x_s = G^{-1}(z_r / b_r)$$

$$\begin{aligned} &= G^{-1}[(y_r - a_{rs}x_s) / b_r] \\ &= G^{-1}[y_r - ((y_s - b_s R(t, c_s)) a_{rs} / a_{ss}) / b_r] \end{aligned}$$

例如： $N=9$

$s=1, 5, 8$

那么 $i = 1, 2, \dots, 9$
 $x = 2, 3, 4, 6, 7, 9$

而密钥是： $k = [N=9; s_1=1, s_2=5, s_3=8; a_{11}, a_{55}, a_{88}; a_{21}, a_{25}, a_{28}, a_{31}, a_{35}, a_{38}, \dots, a_{98}; b_1, b_2, \dots, b_9; c_1, c_5, c_8; \dots] \quad (17)$

为了加密第 t 块，由方程(13)得出

$$\begin{aligned} y_1 &= a_{11}x_1 + b_1R(t, c_1) \\ y_5 &= a_{55}x_5 + b_5R(t, c_5) \\ y_8 &= a_{88}x_8 + b_8R(t, c_8) \end{aligned}$$

由方程(14)得出

$$\begin{aligned} y_2 &= a_{21}x_1 + a_{25}x_5 + a_{28}x_8 + b_2G(x_2) \\ y_3 &= a_{31}x_1 + a_{35}x_5 + a_{38}x_8 + b_3G(x_3) \\ y_4 &= a_{41}x_1 + a_{45}x_5 + a_{48}x_8 + b_4G(x_4) \\ y_6 &= a_{61}x_1 + a_{65}x_5 + a_{68}x_8 + b_6G(x_6) \\ y_7 &= a_{71}x_1 + a_{75}x_5 + a_{78}x_8 + b_7G(x_7) \\ y_9 &= a_{91}x_1 + a_{95}x_5 + a_{98}x_8 + b_9G(x_9) \end{aligned}$$

为了解密第 t 块，由方程(13)，基础明文向量单元可很容易由下式得出：

$$x_1 = [y_1 - b_1 R(t, c_1)] / a_{11}$$

$$x_5 = [y_5 - b_5 R(t, c_5)] / a_{55}$$

$$x_9 = [y_9 - b_9 R(t, c_9)] / a_{99}$$

由方程(14)和(15),非基础明文向量单元是

$$x_2 = G^{-1}[(y_2 - (a_{21}x_1 + a_{25}x_5 + a_{29}x_9)) / b_2]$$

$$x_3 = G^{-1}[(y_3 - (a_{31}x_1 + a_{35}x_5 + a_{39}x_9)) / b_3]$$

$$x_4 = G^{-1}[(y_4 - (a_{41}x_1 + a_{45}x_5 + a_{49}x_9)) / b_4]$$

$$x_6 = G^{-1}[(y_6 - (a_{61}x_1 + a_{65}x_5 + a_{69}x_9)) / b_6]$$

$$x_7 = G^{-1}[(y_7 - (a_{71}x_1 + a_{75}x_5 + a_{79}x_9)) / b_7]$$

$$x_8 = G^{-1}[(y_8 - (a_{81}x_1 + a_{85}x_5 + a_{89}x_9)) / b_8]$$

由方程(16)得出 $G^{-1}, G^{-1}[]$ 是 [] 的立方根。这样可迅速恢复明文 (x_1, x_2, \dots, x_9) 而不需对一个 $N \times N$ 矩阵求逆。

加密和解密装置:

图 4 是根据本发明的一个优选实施例的加密装置的功能方框图。加密装置 30 实质上包含了一个明文输入缓冲器 200, 用于接收输入的明文, 一个存储器 220, 处理器 240, 字符代码表 260 和密文输出缓冲器 280。

存储器 220 除了别的之外用于存储控制参数以控制加密过程。这种控制参数的例子是 N, A, z_i, \dots 。如上所述, N 是块的大小, A 是 $N \times N$ 映射矩阵, z_i 是构成密文向量 y_i 的第二个分向量的向量。也可以有控制 z_i 的其它参数, 如 $z_i = z_i(b, c)$, 这里 b 是 N 维恒定向量而 c

是输入伪随机数发生器的初始值向量。

处理器 240 包括几种功能，由图中的功能框表示，如明文预处理器 241，加密处理器 243，块计数器 245，伪随机数发生器 247，以及密钥处理器 249。

在操作中，密钥 k 首先被密钥处理器处理，获得诸如 N, A, z_i (b, c) 的控制参数，然后这些参数储存在存储器 220 中。密钥处理器最好对储存的密钥有效的规则集检查输入的密钥是否有效。如果发现输入的密钥无效，装置应传达出信息告诉用户出了什么问题。在一种实现的方式中，密钥 k 包含了一连串的控制参数，密钥处理器 249 把这些参数分析出来后储存在存储器 220 中。在另一个实施例中，密钥 k 包含简化的输入集，它与需求的控制参数集比较。处理器 249 也作为密钥生成器，它将简化了的输入集扩展为完整的控制参数集，最后储存在存储器 220 中。例如，如果要求密钥间隔为 2^{256} ，那么密钥为 256 比特长并且可由预定的密钥映射来映射为完整的控制参数集。一旦控制参数在适当位置，即可由处理器 240 处理。

以字符流的形式输入到加密装置 30 的输入明文经明文输入缓冲器 200 缓冲后，由明文预处理器 241 处理。

明文预处理器 241 按照从存储器 220 取出的块大小参数，把输入的明文字符流大小 N 的块逐块分析。在一种实现方式中，明文预处理器也根据存储器 220 中的参数进行初始的块排列。字符代码表 260 用于将每个字符转换为数值以使得每个块等效于明文向量 x 。字符代码表可选择地设置在加密装置 30 的外面。

块计数器 245 跟踪所处理的块。因此，第 t 个块产生明文向量 x_t 。



然后把明文向量 x_i 输入到加密处理器 243，计算出对应的密文向量 y_i 。密文向量 y_i 是通过将 $N \times N$ 矩阵 A 作用于 x_i ，再给它加上第二个分向量 z_i 。矩阵 A 和第二个分向量可从存储器 220 中得到。

在优选的实施例中，第二个分量是逐块变化的随机分量。伪随机数发生器 $R_c(c)247$ 对每个块提供一个伪随机向量序列。每个序列都取决于初始值向量 c 。对第 t 个块， z_t 假定该序列中的第 t 个伪随机向量。

这样密文向量由加密处理器 243 计算出来，然后通过密文输出缓冲器 280 从加密装置 30 输出。

图 5 是根据本发明在一个具体实施例的解密装置的功能方框图。解密装置 50 在结构上和加密装置 30 相似，实质上是执行加密装置 30 的相反操作。它包含一个密文输入缓冲器 300，用于接收输入的密文，一个存储器 320，一个处理器 340，一个字符代码表 360 以及明文输出缓冲器 380。

存储器 320 除了别的之外用于储存控制参数以控制解密。这些控制参数的例子有 N , $A, z_i(b, c), \dots$ ，这些参数同加密的控制参数一样，并且也是可从输入的密钥中导出的。但在解密装置中，映射矩阵 A 不直接用于计算，而是用于导出的逆映射矩阵 A^{-1} 。

处理器 340 包括几种功能，由图中以功能框表示，如密文预处理器 341、解密处理器 343、块计数器 345、伪随机数发生器 347 以及密钥处理器 349。这些功能框同加密装置 30 中的是对应的。

另外，处理器 340 也包括一个逆处理器 344，逆处理器 344 可由给定的映射矩阵 A 计算逆映射矩阵 A^{-1} 。

在操作中，同加密装置相似，密钥 k 首先由密钥处理器 349 处

理。推导出控制参数如 $N, A, z_i(b, c), \dots$, 然后存入存储器 320。一旦控制参数在适当位置, 它们可由处理器 340 存取。

输入到解密装置 50 以变换的数字串流的形式的密文经密文输入缓冲器 300 缓冲后, 由密文预处理器 341 处理。

密文预处理器 341 根据从存储器取出的块大小参数把输入的密文流大小为 N 的块逐块分析。这样, 每个块都等效于密文向量 y 。

块计数器 345 跟踪所处理的块。因此, 第 t 个块产生密文向量 y_t 。

然后把密文向量 y_t 输入到解密处理器 343, 计算出对应的明文向量 x_t 。明文向量 x_t 是先从 y_t 减去第二个分向量 z_t , 再将 $N \times N$ 逆映射矩阵 A^{-1} 作用于所得向量而得到的。逆映射矩阵 A^{-1} 和第二个分量可以从存储器 320 中获得。第二个分量同加密装置 30 中的向量是相同的。

在优选的实施例中, 第二个分量是逐块变化的随机分量。伪随机数发生器 $R_i(c)347$ 同加密装置 30 中的一样, 它提供相同的伪随机向量序列, 该序列用于在加密装置 30 中将每个块随机化。

初始明文进行初始的块排列后, 解密处理器 343 将响应存储器 320 中的参数也执行相反的块排列。

一旦明文向量 x_t 被解密, 就被类似加密装置中所用的字符代码表 360 解码。字符代码表可选择地设置在解密装置 50 以外。把明文向量中被编码数值解码为它们原来的字符状态。

这样, 恢复成初始明文后, 通过密文输出缓冲器 380 从解密装置 50 中输出。

图 4 和图 5 分别表示了加密和解密装置的优选硬件实施例, 它

们是图 1 所示的加密系统的一部分。本发明也考虑了采用在软件控制下用于实现加密装置 30 和解密装置 50 实现的各种功能的计算机。例如，处理器 240 和 340 可以用普通计算机的微处理器。存储器 220, 320 和缓冲器 200, 300 可用计算机的各种类型存储器。软件可放在计算机的一个存储器中，根据上述方法控制加密和解密。

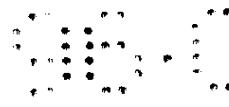
随机图像方案一映射参数的系统选择

如上所述，本发明要求用户从映射集中选择一种映射。它是利用密钥表示的，并可从该密钥导出一组映射参数。该映射集实质上是通过 $N \times N$ 映射矩阵单元在指定范围内排列起来生成的。如上面指出的，即使 N 和 L 为中等值，映射集的大小实际上变得非常之大。

在优选的实施例中，用一种系统的方法把映射分成不同的组，以易于区别和辨认它们。这样，用户能够有系统地从分类的映射中作出选择。如果密钥需要常常更改，或者如果一组密钥需要指定给一组人，用这种方法是特别方便的。

这种方案是通过把块或明文单元排列起来建立映射分类的。这同在前面快速计算实现中所述的从明文向量中选择基础明文向量单元的子集是类似的。用户随机选取基础明文向量单元的子集。在最简单的实施例中，把剩下的未选取的明文向量单元置零。这样，仅从被选取的基础明文向量单元的线性组合得出每个密文向量单元。换言之，密文向量实质上被映射成由选取的基础明文向量单元隔开的子间隔。

一般来说，当每个单元取两个值中的一个时，就有 2^N 种方法来排列 N 个单元。由二项式定理， 2^N 个选择可以分组为 N 个单元中的 M 个基本向量单元的所有可能排列的和



$$\sum_0^M C(N, M) = \sum \frac{N!}{M! (N-M)!} = 2^N$$

图 6A 列出了块的大小 $N=9$ 时的各种排列或基础明文向量单元的可能选择。因此共有 $2^9=512$ 种排列。

图 6B 是在 3×3 的图像中从一块中选择多个单元的实际排列的结构图, 每个块中的单元是按照从左到右, 从上至下的顺序安排的。该结构是按 M 的递增顺序安排的, 并有从#1 到#511 的结构号(#0 结构未出现, 它相应于无基础向量单元被选择的不重要的情况)。例如, 参照图 6B, 用户可选取结构#54, 它规定基础明文向量为 $x=[x_1, 0, x_3, 0, x_5, 0, 0, 0, 0]$ 。如果用户知道密钥周期地被更改, 他们能很容易地利用本方案选出结构的预定序列, 提供相应的密钥序列。

而在另一个实施例中, 生成系统的映射参数的方案可由前面提到的初始块排列实现。一般来说, 明文向量单元 x_1, x_2, \dots, x_N 不必对应于明文字符流中单元进入的顺序相同。例如, x_1 可对应字符流的一个块中第 7 个字符, 而 x_2 可对应第 1 个字符。在 N 时隙上填入 N 个单元就有 N 的阶乘种($N!$)方法。用户可随意选择初始块的排列方式或将其说明编入密钥中。根据一个预定的顺序, 将块单元排列成各种不同的结构(或图象), 再根据另一种预定的顺序将其读出, 就生成了不同的顺序。例如, 对块大小为 $N=9$, 一个图象为 3×3 的矩阵。块单元 $[x_1, x_2, \dots, x_9]$ 能够以从左到右, 从上至下顺序分配到矩阵中。通过从下至上, 从左到右读出矩阵单元可得到一种不同的排列 $[x_7, x_4, x_1, x_8, x_5, x_2, x_9, x_6, x_3]$ 。一般来说, 通过所用的图像、单元的设置方式和从图象中读出单元的方式的变化可以获得不同的排

列。

虽然上面已经叙述本发明各个方面的实施例是优选实施方式，但本领域的技术人员懂得可以有各种修改。因此，本发明由所附的权利要求书的整个范围保护。

说 明 书 附 图

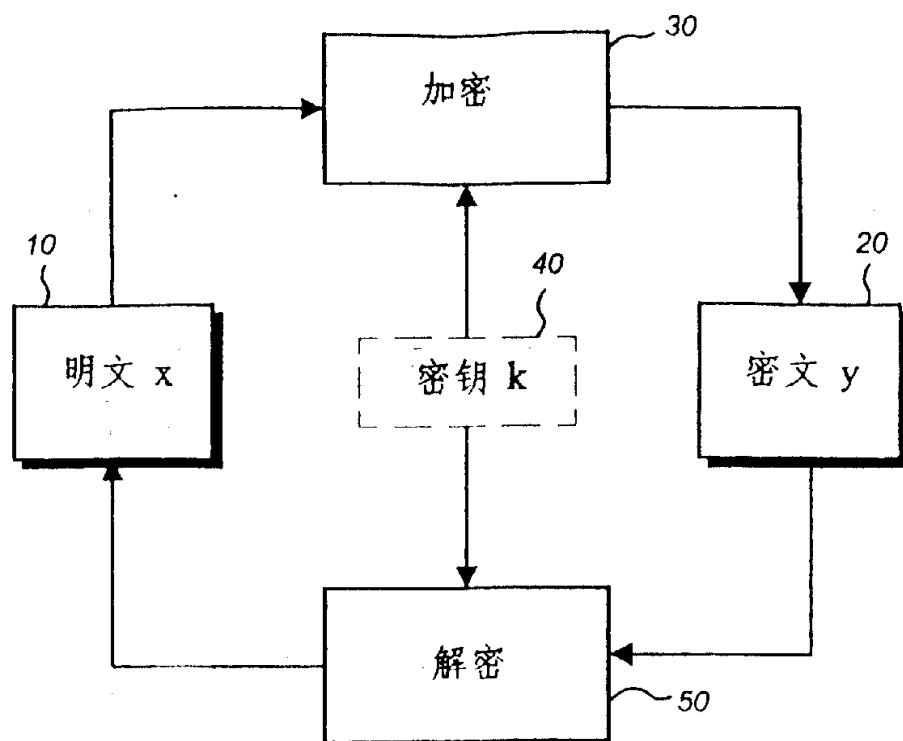


图1

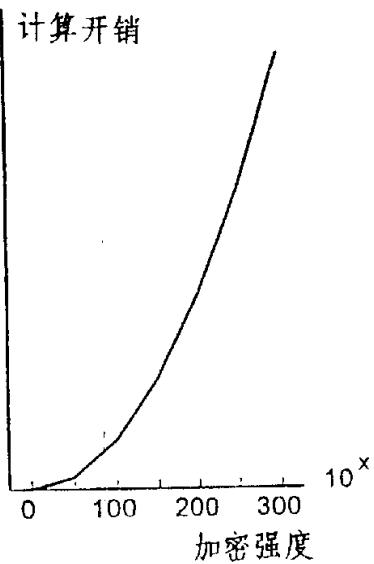


图. 2A

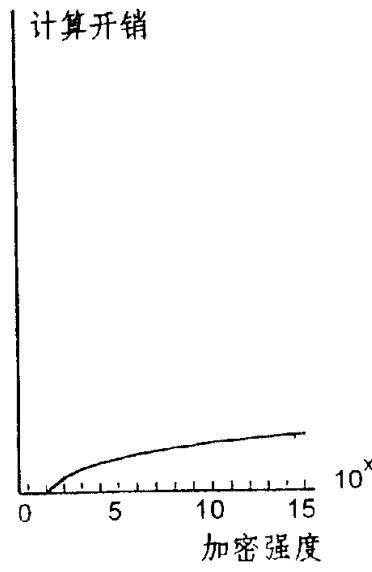


图. 2B

现有技术

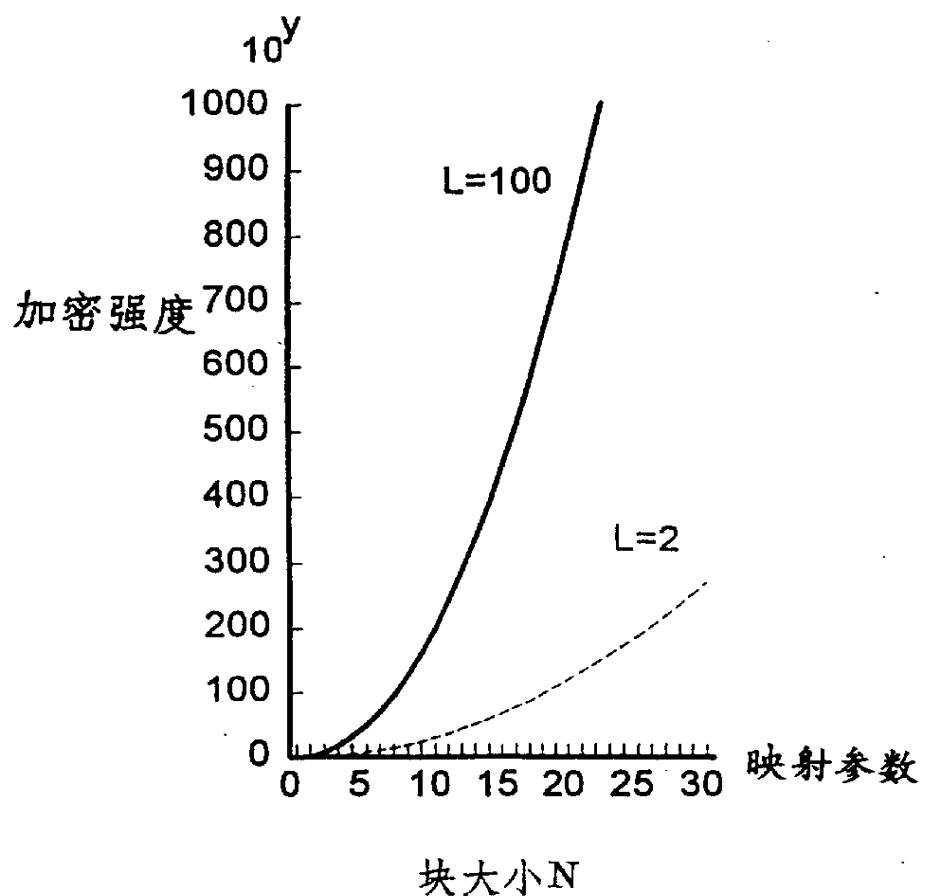


图3

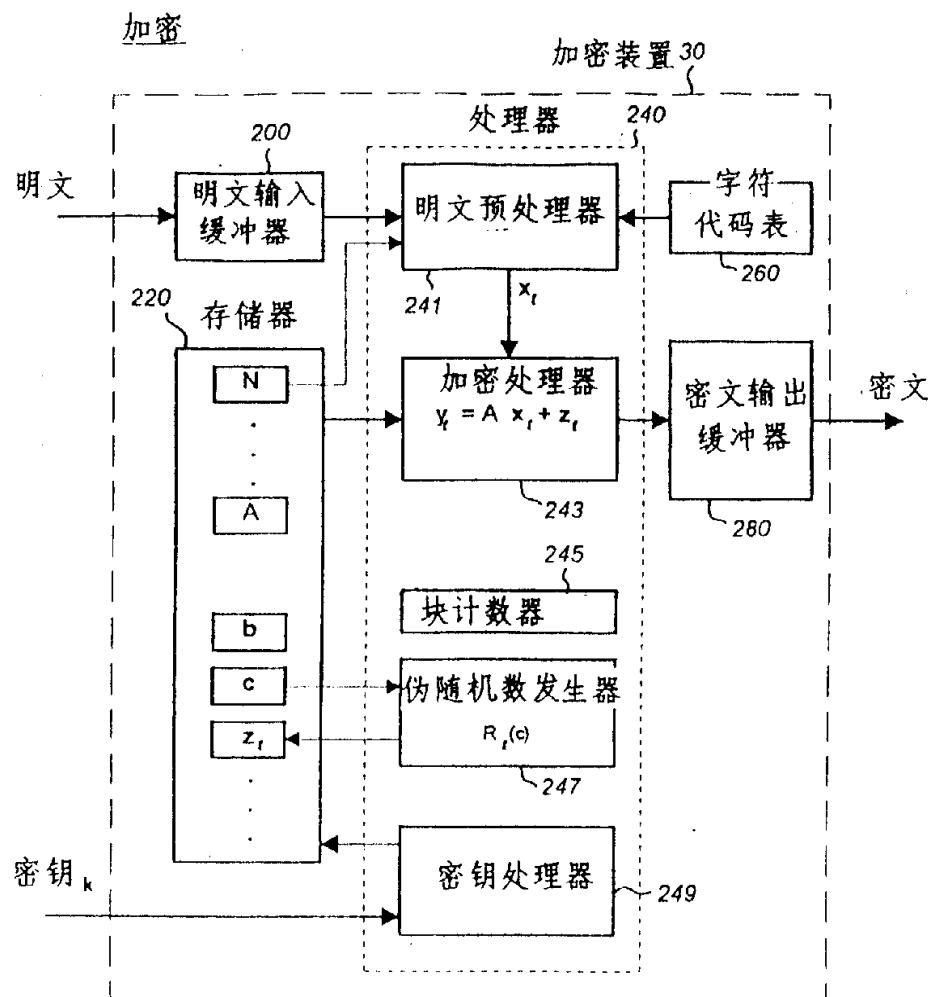


图 4

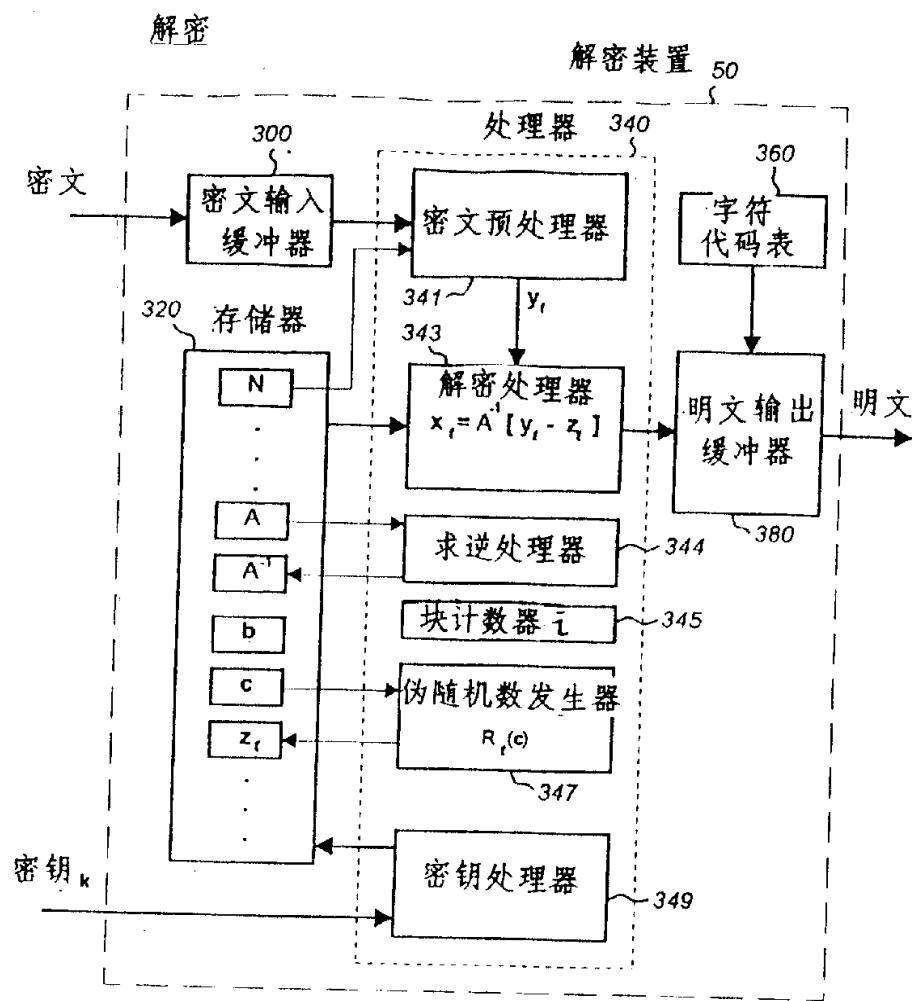


图 5

N = 9, M = 0 - 9 $2^9 = 512$		
二项式系数 C(N,M)	每组的可能选择	结构号 (参照图 6 B)
C(9,0)	1	# 0 未出现
C(9,1)	9	1-9
C(9,2)	36	10-45
C(9,3)	84	46-129
C(9,4)	126	130-255 (未示出)
C(9,5)	126	256-381 (未示出)
C(9,6)	84	382-465 (未示出)
C(9,7)	36	466-501 (未示出)
C(9,8)	9	502-510
C(9,9)	1	511

图 6A

No 1	No 2	No 3	No 4	No 5	No 6	No 7	No 8
..	.,	..*	..*	..*	..*	..*	..*
..*	..*	..*	..*	..*	..*	..*	..*
..*	..*	..*	..*	..*	..*	..*	..*
No 9	No 10	No 11	No 12	No 13	No 14	No 15	No 16
...*	**,	*,*	*,	*,	*,	*,	*,
..*	..*	..*	..*	..*	..*	..*	..*
..*	..*	..*	..*	..*	..*	..*	..*
No 17	No 18	No 19	No 20	No 21	No 22	No 23	No 24
*..	,**	,*	,*	,*	,*	,*	,*
..*	..*	..*	..*	..*	..*	..*	..*
..*	..*	..*	..*	..*	..*	..*	..*
No 25	No 26	No 27	No 28	No 29	No 30	No 31	No 32
,*	,*	,*	,*	,*	,*	,*	,*
..	,	,*	,*	,*	,*	,*	,*
..*	..*	..*	..*	..*	..*	..*	..*
No 33	No 34	No 35	No 36	No 37	No 38	No 39	No 40
..*	..*	..*	..*	..*	..*	..*	..*
..	,	,*	,**	,*	,*	,*	,*
..	,	,*	..*	,*	,*	,*	,*
No 41	No 42	No 43	No 44	No 45	No 46	No 47	No 48
..*	..*	..*	..*	..*	..*	..*	..*
,*	,*	,*	,*	,*	,*	,*	,*
,*	,*	,*	,*	,*	,*	,*	,*
No 49	No 50	No 51	No 52	No 53	No 54	No 55	No 56
**,	**,	**,	**,	**,	**,	**,	**,
..*	..*	..*	..*	..*	..*	..*	..*
..*	..*	..*	..*	..*	..*	..*	..*
No 57	No 496
,
..*
No 497	No 498	No 499	No 500	No 501	No 502	No 503	No 504
***	***	***	***	***	***	***	***
***	***	***	***	***	***	***	***
***	***	***	***	***	***	***	***
No 505	No 506	No 507	No 508	No 509	No 510	No 511	
***	***	***	***	***	***	***	
***	***	***	***	***	***	***	
***	***	***	***	***	***	***	

图 6B