杨义先　孙　伟　钮心忻　著

现代密码新理论

科学出版社
www.sciencep.com

现代密码新理论

杨义先　孙　伟　钮心忻　著

科学出版社

2002

内 容 简 介

本书介绍了近年来国内外现代密码学的若干最新理论和实用成果，其中许多成果是作者多年研究的结晶。全书共九章，分别介绍了最新的美国密码标准算法、欧洲密码标准算法、无仲裁认证码、有仲裁认证码、各种常规数字签名方案、群签名方案和多重数字签名方案、代理数字签名方案、有限域上的密码序列设计、Galois 环上的密码序列设计等。全书内容覆盖了现代密码学的三大主要部分：加密算法标准、认证与数字签名、序列密码。

本书可以作为密码学、信息科学、通信与电子系统、信号与信息处理、应用数学等专业的大学生和研究生的教学参考书，也可作为现代密码学、网络安全、信息安全、计算机安全等领域人员的技术培训教材和实用工具书。

图书在版编目(CIP)数据

现代密码新理论/杨义先，孙伟，钮心忻著 .—北京：科学出版社，2002

ISBN 7-03-010631-8

Ⅰ. 现… Ⅱ. ①杨…②孙…③钮… Ⅲ. 密码—理论 Ⅳ. TN918.1

中国版本图书馆 CIP 数据核字（2002）第 049469 号

科学出版社 出版
北京东黄城根北街16号
邮政编码:100717
http://www.sciencep.com
双青印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2002 年 8 月第 一 版 开本：787×1092 1/16
2002 年 8 月第一次印刷 印张：15 1/4
印数：1—3000 字数：347 000
定价：25.00 元
（如有印装质量问题，我社负责调换〈双青〉）

前　言

现代密码学是由飞速发展的信息化社会催生的一门新型学科。1949 年仙农的奠基性论著“保密系统的通信理论（Communication Theory of Secrecy Systems）”的发表，标志着现代密码学的诞生。从此，现代密码学理论研究和工程应用双双进入了疾驰的快车道。分组加密算法标准、公钥密码、身份认证与消息认证、数字签名标准、椭圆曲线密码、量子密码、混沌密码、序列密码等现代密码新理论的成果不断涌现。公钥基础设施、证书认证中心、虚拟专用网、电子现金、网络银行、电子商务安全平台等现代密码应用系统如雨后春笋，一个接一个地用于各种应用系统的网络信息安全保障中。

总之，现代密码学的最大特征就是一个字：快！新的理论分支诞生快，理论水平提高快，理论向应用的转化速度快，“守方”技术进步快、“攻方”手段改进快，安全需求和应用系统的复杂性增长快，应用环境变化快，等等。

如何面对这些众多的“快”？最直接的办法当然就是“以快应快”和“以超前量应快”。这正是本书的目的，本书系统地介绍了近年来现代密码学理论的一些最新进展。

在“以快应快”方面，本书非常及时、系统、全面地介绍了当前国际上最新的加密算法标准，包括美国标准和欧洲标准。这部分内容对那些需要使用标准加密算法的工程师们来说是非常受欢迎的，因为他们可以直接使用这些算法来达到理想的目的。使用了 20 余年的美国数据加密标准算法（DES）已经被更新的先进数据加密标准算法（AES）所替代，但是，到目前为止，还没有书籍对 AES 算法进行详细而全面的介绍。本书及时填补了这个空白，不但用非常形象直观的方式介绍了 AES 算法（原名 Rijndael 算法），而且还对当初进入“决赛圈”的其他 AES 候选算法（RC6 算法、Twofish 算法、MARS 算法、Serpent 算法）进行了系统介绍。由于各方面的原因，美国的加密标准算法在国际上的影响力（特别是在市场上的影响力）基本上是最大的，但是，这并不意味着美国的加密标准算法在技术上是最先进的，因此，本书还介绍了欧洲加密标准算法和其他若干著名的分组加密算法，包括 CS-CIPHER 算法、Hicrocrypt-L1 算法、KHAZAD 算法、IDEA 算法、MISTY1 算法、NIMBUS 算法、SC2000 算法、Camellia 算法、ANUBIS 算法、NOEKEON 算法、Q 算法、GRAND CRU 算法、NUSH 算法、SAFER++算法和 SHACAL 算法等。通过学习众多加密算法，读者不但可以掌握很多实用的新型加密算法，为相关工程应用提供直接的解决方案，而且还可以领悟到分组密码算法设计的精髓，为今后自己设计专用的加密算法打下坚实的基础。虽然以椭圆曲线密码为代表的非对称密码研究也有不少重要的新成果，但本书仅介绍对称加密算法。

在“以超前量应快”方面，本书介绍了在认证码、数字签名方案以及序列密码等方面能够代表国际先进水平的最新成果。这些内容在国内外同类书籍中都是首次出现，其中很多是作者及课题组多年科研成果的结晶。

认证与保密是信息安全的两个重要方面，认证性不能自动提供保密性，而保密性也不能自动提供认证性。认证的目的主要有两个：第一，信源识别（或称为身份认证），

即验证发信人确实不是假的；第二，检验发送信息的完整性（或称为信息认证），也就是说，即使信息确实是经过授权的信源发送者发送的，也要验证在传送过程中是否被篡改、重放或延迟。根据通信双方的互相信任程度，认证可分为无仲裁认证和有仲裁认证两大类。

在无仲裁认证系统中，通信双方是互相信任的，他们团结一致共同抵御敌方的主动攻击，此时，通信系统中只有参与通信的发方和收方及发起攻击的敌方，不需要裁决方。本书在介绍认证系统的数学模型后，重点研究了无仲裁认证码的集合论构造法、几何构造法和纠错编码构造法等多种构造方法。另外，本书还对无仲裁认证码的对策论进行了深入研究。

有仲裁认证系统与现实生活更加靠近，通信双方互不信任，比如：发方发送了一个消息后，否认曾发送过该消息；收方收到消息后，否认曾接收到该消息或宣称接收到了自己伪造的不同于收到消息的另一个消息等。一旦这种情况发生，就需要一个仲裁方来解决问题。有仲裁认证码又可分为单个仲裁人的认证码和多个仲裁人的认证码。本书分析了有仲裁认证码的可能攻击方法，并给出了有仲裁认证码的对策和有仲裁认证码的构造方法。

数字签名是认证的主要手段之一，也是现代密码学的主要研究内容之一。数字签名是日常生活中手写签名的电子对应物，它的主要功能是实现用户对电子形式存放消息的认证。数字签名与传统的签名相比有许多特点。首先，在数字签名中签名同消息是分开的，需要一种方法将签名与消息绑定在一起，而在传统的手写签名中，签名是被签名消息的一部分；其次，在签名验证的方法上，数字签名利用一种公开的方法对签名进行验证，任何人都可以对签名进行验证，而传统手写签名的验证是由经验丰富的消息接收者通过与以前的签名进行比较来确定的；最后，在数字签名中，有效签名的复制同样是有效的签名，而在传统的手写签名中，签名的复制是无效的。因此，在数字签名方案的设计中要预防签名的非法重复使用。数字签名的种类和功能非常多，相应的方案也很多，除了常规的数字签名方案之外，本书还介绍了众多具有代表性的群签名方案、多重数字签名方案、批验证协议和代理数字签名方案。

关于常规的数字签名方案，本书在介绍了其形式化定义和分类后，又介绍了若干基于离散对数、素因子分解和二次剩余问题的常规数字签名方案，比如，一般的 ElGamal 型数字签名方案、N-R 数字签名方案、Miyaji 数字签名方案、HMP 认证加密数字签名方案、H-K 数字签名方案、Shao 数字签名方案、Li 数字签名方案、Harn-K 数字签名方案、He-W 数字签名方案、广义 Shimada 数字签名方案等。还对这些方案的安全性进行了深入分析，指出了其中某些方案的安全漏洞和不足之处。

群签名方案允许组中合法用户以用户组的名义进行签名，具有签名者匿名、只有权威才能辨认签名者等多种特点，有著广泛的实际应用。群签名方案由组、组成员（签名者）、消息接收者（签名验证者）和权威或群中心组成，它有如下特点：（1）只有组中成员才能为消息签名，签名为组签名；（2）消息接收者可以验证组签名的有效性，但不能辨别签名者；（3）一旦发生争论，从消息的组签名权威（或全体组中成员的联合）可以辨别签名者。本书重点研究了 K-P-W 可变群签名方案、L-C 群签名方案和 T-J 群签名方案以及它们的安全性。

在实际生活中，往往有这种需要：多个用户对同一消息进行签名，这类签名的电子对应物就是所谓的多重数字签名。根据签名过程的不同，多重数字签名方案又可分为有序多重数字签名和广播多重数字签名。在有序多重数字签名方案中，由消息发送者规定消息签名的顺序，然后将消息发送到第一个签名者，除了第一个签名者，每一位签名者收到签名消息后，首先验证上一签名者签名的有效性，如果签名有效，继续签名，然后将签名消息发送到下一个签名者；如果签名无效，拒绝对消息签名，终止整个签名。当签名验证者收到签名消息后，验证签名的有效性，如果有效，多重签名有效，否则，多重签名无效。在广播多重签名方案中，消息发送者同时将消息发送给每一位签名者进行签名，然后签名者将签名消息发送给签名收集者，由收集者对签名消息进行整理，再发送给签名验证者验证其签名的有效性。如果有效，多重签名有效，否则，多重签名无效。本书重点研究了 Harn 广播多重数字签名方案和 ElGamal 多重数字签名方案。

为了提高签名验证的效率，可以采用所谓的批验证协议，它特别适用于多组消息签名的情形。每一个批验证协议都包含两个部分：签名收集协议和批验证标准。相应地，每一个批验证协议包含两个过程：签名产生过程和签名验证过程。在签名产生过程中根据签名收集协议一次产生多个消息的签名，在签名验证过程中，签名验证者根据批验证标准一次验证多个签名的有效性。批验证协议具有如下特性：(1) 签名者在签名过程中一次产生多个消息的签名。(2) 多个签名的有效性由签名验证者一次验证完成。(3) 多个有效的签名一定满足批验证协议中的批验证标准。(4) 在批验证协议中有效的多个签名一定是有效的签名。

根据签名产生过程的不同，批验证协议可分为交互式和非交互式两种。如果在签名产生过程中，签名者同签名验证者交互地传递信息，称这种协议为交互式批验证协议；相反，如果在签名产生过程中，签名者同签名验证者不需要交互地传递信息，称这种协议为非交互式批验证协议。本书重点介绍了 N-M-R-V 批验证协议、Harn 交互式和非交互式批验证协议、RSA 批验证协议，以及这些协议的安全性。

在日常生活中，经常会出现委托别人代替自己签名的事情，与此相应的电子对应物便是所谓的代理数字签名。一般说来，代理数字签名方案应该满足以下特性：(1) 基本的不可伪造性。除了原始签名人外，任何人（包括代理签名人）都不能生成原始签名人的普通数字签名。这个性质是任何数字签名体制都应当具备的，它可以保证原始签名人的基本安全。(2) 代理签名的不可伪造性。除了代理签名人外，任何人（包括原始签名人）都不能生成有效的代理签名。特别是如果原始签名人委托了多个代理签名人，那么任何代理签名人都不能伪造其他代理签名人的代理签名。这个性质可以保证代理签名人的基本安全。(3) 代理签名的可区分性。任何一个代理签名都与原始签名人的普通数字签名有明显的区别；不同的代理签名人生成的代理签名之间也有明显的区别。这个性质和性质 (2) 结合起来可以防止签名人之间互相抵赖。(4) 不可抵赖性。任何签名人，不论是原始签名人还是代理签名人，在生成一个数字签名后，不能再对它加以否认。(5) 身份证实性。原始签名人可以根据一个有效的代理签名确定相应代理签名人的身份。利用这个性质，原始签名人可以对代理签名人进行监督，使代理签名人不能在不被发现的情况下滥用他的代理签名权利。(6) 密钥依赖性。代理签名密钥依赖于原始签名人的秘密密钥。(7) 可注销性。如果原始签名人希望代理签名人只在一定时间区间内拥

有生成代理签名的能力，那么必须能够让代理签名人的代理签名密钥在指定的时刻失去作用。代理签名的内容十分丰富，本书重点介绍了基于离散对数问题和基于素因子分解问题的多种代理签名体制和代理多重签名体制，以及多级代理数字签名体制等。

序列密码始终是现代密码研究的重点和难点。序列密码的加密和解密机制虽然非常简单（即将明文（密文）序列与密钥序列进行简单的模 2 相加，便完成了加密（解密）程序），但是，如何生成伪随机性很好的密钥序列却是一个十分困难和关键的问题。仙农已经严格证明了，如果密钥序列是绝对随机的，那么相应的序列密码体制便是绝对安全可靠的。然而，在实际工程中，绝对随机的密钥序列是无法重复生成的，所以如何评价某个给定密钥序列的安全性也是一个必须认真研究的问题。本书将介绍序列密码设计方面的一些最新成果。

有限域理论是序列密码设计的最主要工具。目前，人们已经基于有限域设计出了众多著名的密码序列，但是，关于这些密码序列的某些重要特征（比如，自相关和互相关特性等）仍然不清楚。本书（部分）解决了 d 型序列（TN 序列和二次型序列）、几何序列、广义几何序列的自（互）相关特性问题和线性复杂度计算问题。这些结果都很有理论价值。

由于环的结构不如域完美，因此，在环上设计的某些密码序列更容易抵挡黑客的攻击，因为黑客能够使用的环上数学分析工具十分有限。本书重点介绍了 Galois 环上的三类序列族的设计。

本书是北京邮电大学信息安全中心全体成员集体智慧的结晶。在本书编写过程中，王永传博士、周智博士、李子臣博士、夏光升博士、徐国爱博士、李新博士等为本书提供了丰富的参考文献。特别感谢胡正名教授、李中献博士、冯运波博士、张振涛博士、古利泽硕士、温巧燕教授、罗守山教授、牛少彰教授、卓新建博士。他们同心协力，率领北京邮电大学信息安全中心百余位研究人员在网络信息安全研究方面取得的丰富成果是本书的营养源泉。本书也是国家重点基础研究发展规划项目（编号：G1999035805）、国家杰出青年基金项目（批准号：69425001）、国家自然科学基金项目（批准号：60073049）和高校骨干教师资助计划项目的成果。

由于作者水平有限，书中难免出现各种失误和不当之处，欢迎大家批评指正。

作　者

2001 年 11 月于北京

目　录

第一部分　密码标准

第二部分　认证码与数字签名

第三部分　序列密码设计

第一部分
密码标准

▲ 美国密码标准
▲ 欧洲密码标准

第一章　美国密码标准

1.1　AES(RIJNDAEL)

数据加密标准(DES)作为 20 世纪 70 年代的加密标准,其加密强度越来越不能满足人们的要求。DES 的密钥长度只有 56 比特,随着计算能力的不断提高,利用穷搜索的方法攻击 DES 是完全可能的。特别是在政府或者其他组织的支持下,设计专门的硬件来攻击 DES 已经是轻而易举的事情。在这种情况下,美国国家标准技术局(NIST)在 1997 年开始倡导制定高级加密标准(AES)替代 DES 以满足 21 世纪的信息加密需求。经过几年的招标、筛选,NIST 于 2000 年底最终确定了 AES(RIJNDAEL)。AES 是由比利时密码专家 Joan Daemen 和 Vincent Rijmen 共同设计的。下面我们对 AES 做简单的介绍。

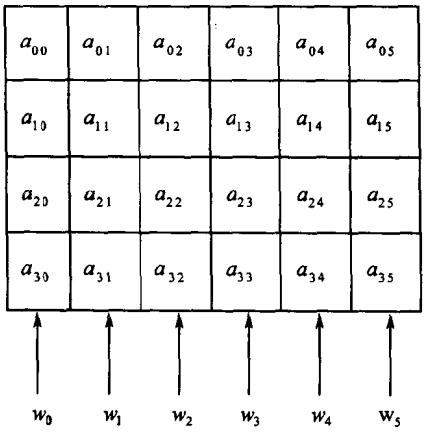

图 1.1　192 比特信息的字表示

RIJNDAEL 的信息块长度和加密密钥长度都是可变的,它们都可以是 128 比特、192 比特和 256 比特。为了方便数据的计算和算法的描述,我们首先把信息块做如下的处理。以 192 比特的信息块为例,假设信息块是 $m_0 m_1 \cdots m_{191}$;写成字节形式就是 $a_{00}a_{01}\cdots a_{05}$ $a_{10}a_{11}\cdots a_{15}\cdots a_{30}a_{31}\cdots a_{35}$,或者写成字的形式就是 $w_0 w_1 \cdots w_5$,如图 1.1 所示。

我们也可以对加密密钥做类似的处理。设 N_b 为信息块经过上述处理后得到的字的个数,N_k 为加密密钥经过上述处理后得到的字的个数。那么根据信息块的长度,$N_b = 4$, 6, 8,根据加密密钥的长度,$N_k = 4, 6, 8$,加密的轮数 N_r 根据表 1.1 由 N_b 和 N_k 控制。

表 1.1 N_r 的取值

N_r / N_b / N_k	4	6	8
4	10	12	14
6	12	12	14
8	14	14	14

整个算法包括加密过程与轮密钥生成两个独立的部分。

1.1.1 加密过程

设信息块是 M，轮密钥分别是 $K_0, K_1, \cdots, K_{N_r-1}$，加密过程如图 1.2 所示。解密过程把加密过程完全反过来即可。

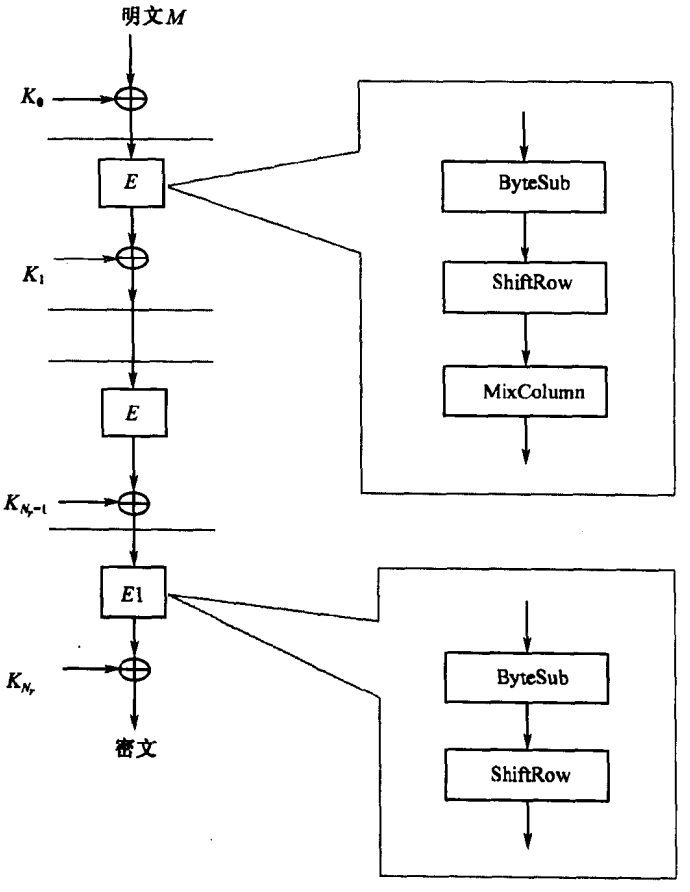

图 1.2 AES 的加密过程

1.ByteSub 函数

把每个 8 比特的字节看成有限域 $GF(2^8)$中的一个元素，那么函数 Bytesub 是作用在每个字节上的非线性变换，它定义为

$$\text{ByteSub}: GF(2^8)\rightarrow GF(2^8)$$

$$x\rightarrow \begin{pmatrix}1&0&0&0&1&1&1&1\\1&1&0&0&0&1&1&1\\1&1&1&0&0&0&1&1\\1&1&1&1&0&0&0&1\\1&1&1&1&1&0&0&0\\0&1&1&1&1&1&0&0\\0&0&1&1&1&1&1&0\\0&0&0&1&1&1&1&1\end{pmatrix}\cdot x^{-1}+\begin{pmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{pmatrix}$$

图 1.3 描述了信息块长度是 192 比特时，函数 ByteSub 的作用情况。

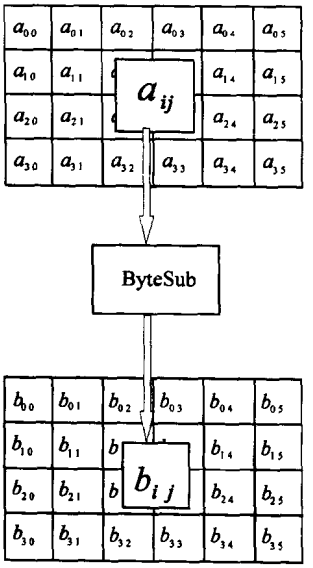

图 1.3　函数 ByteSub

2.ShiftRow 函数

把信息块记为 4 行、N_b 列的矩阵形式，函数 ShiftRow 就是对每行实行不同的左移位，每行的左移位数 C_1, C_2, C_3 分别由 N_b 按照表 1.2 决定。

表 1.2 左移位数的确定

N_b	C_1	C_2	C_3
4	1	2	3
6	1	2	3
8	1	3	4

函数 ShiftRow 的作用可表示成图 1.4。

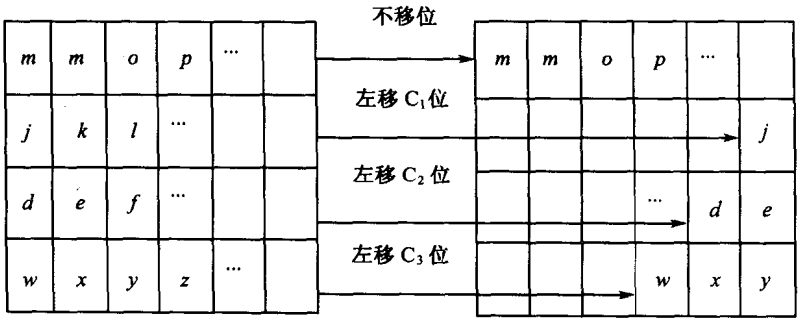

图 1.4 函数 ShiftRow

3. MixColumn 函数

MixColumn 函数是 $GF(2^8)^4$ 上的一个线性变换，变换矩阵 C 定义为

$$C = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$$

其中的运算均在 $GF(2^8)$中进行。图 1.5 描述了信息块长度是 192 比特时，MixColumn函数的作用情况。此处矩阵 C 中的元素 xy 理解为两个 4 比特长的二进制数的串接，比如 02 理解为 0000 0010。

1.1.2 轮密钥的生成

轮密钥的生成过程包括加密密钥的扩张和轮密钥的选取两个部分。

1. 加密密钥的扩张

假设信息块的长度是 N_b 个 32 比特字，由于整个加密过程需要 N_r+1 个轮密钥，每个轮密钥的长度是 N_b 个 32 比特字，所以密钥的扩张过程需要产生 $N_b(N_r+1)$个 32 比特字，记为 $w_0, w_1, \cdots, w_{N_b(N_r+1)-1}$。加密密钥的扩张根据密钥长度 N_k 的不同，有两种不同的扩张方式。假设加密密钥为 $wk_0\, wk_1 \cdots wk_{N_r-1}$，令 $w_0 = wk_0$，$w_1 = wk_1$，$\cdots$，

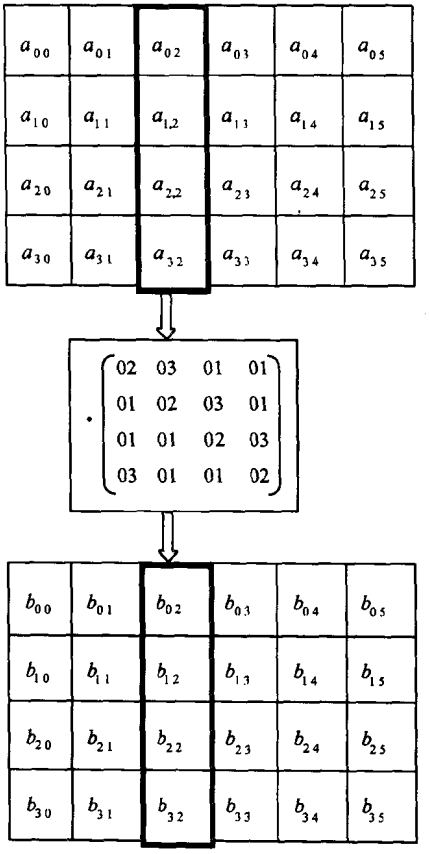

图 1.5　函数 MixColumn

$w_{N_r-1}=wk_{N_r-1}$。

当 $N_r \leqslant 6$ 时，对于 $N_k \leqslant i < N_b(N_r+1)$，如图 1.6 所示。

当 $N_r > 6$ 时，对于 $N_k \leqslant i < N_b(N_r+1)$，如图 1.7 所示。

其中，RotByte 把(a, b, c, d)变为(b, c, d, a)，a, b, c, d 是 8 比特字节；$Rcont[i]=(RC[i],00,00,00)$；$RC[1]=1$，$RC[i]=xRC[i-1]=x^{i-1}$，即 $RC[i]$表示有限域 $GF(2^8)$中值为 x^{i-1}的元素。

2．轮密钥的选取

加密密钥经过扩张产生了 $N_b(N_r+1)$个 32 比特字，把它们均等地分成 N_r+1 块，每块包含 N_b 个 32 比特字，那么第一个轮密钥就是第一个块，第二个轮密钥就是第二个块，依次类推得到所有的轮密钥。

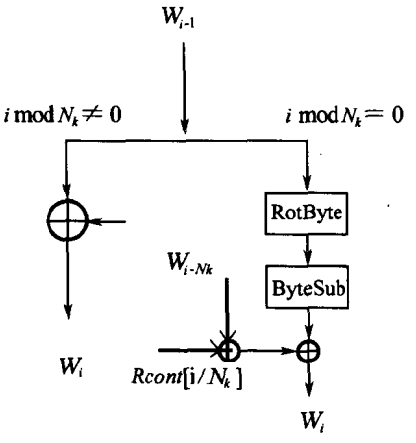

图 1.6 $N_r \leqslant 6$ 时的密钥扩张

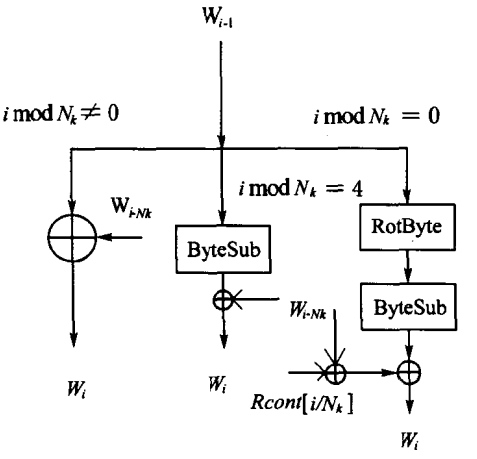

图 1.7 $N_r > 6$ 时的密钥扩张

1.2 MARS

MARS 是美国 IBM 公司的科学家们设计的，信息块长度是 128 比特，密钥是任意长度的。整个算法分成加密过程与子密钥生成两个独立的部分。

1.2.1 加密过程

设信息块为 $d_0 d_1 \cdots d_{127}$，可以写成 4 个 32 比特字 $D[0], D[1], D[2], D[3]$的形式。假设 $K[0], K[1], \cdots, K[39]$是由子密钥生成过程产生的 40 个子密钥，那么 MARS 的加密过程如图 1.8 所示，解密过程是类似的。

整个加密过程涉及到 4 个函数：FM, KFT, KBT, BM。

首先，4 个 32 比特字 $D[0], D[1], D[2], D[3]$分别与 $K[0], K[1], K[2], K[3]$做模 2^{32}加法运算，这里 a 田 b 表示$(a+b) \bmod 2^{32}$，结果作为函数 FM 的输入，函数 FM 的结构如图 1.9 所示。在图 1.9 中，$n \ggg$表示相应的比特串右循环移动 n 位，S_0, S_1 是 2 个 8 比特输入/32 比特输出的 S 盒，它们的定义如下：

$S_0 = \{$ 09d0c479 28c8ffe0 84aa6c39 9dad7287 7dff9be3 d4268361
c96da1d4 7974cc93 85d0582e 2a4b5705 1ca16a62 c3bd279d
0f1f25e5 5160372f c695c1fb 4d7ff1e4 ae5f6bf4 0d72ee46
ff23de8a b1cf8e83 f14902e2 3e981e42 8bf53eb6 7f4bf8ac
83631f83 25970205 76afe784 3a7931d4 4f846450 5c64c3f6
210a5f18 c6986a26 28f4e826 3a60a81c d340a664 7ea820c4
526687c5 7eddd12b 32a11d1d 9c9ef086 80f6e831 ab6f04ad
56fb9b53 8b2e095c b68556ae d2250b0d 294a7721 e21fb253
ae136749 e82aae86 93365104 99404a66 78a784dc b69ba84b