电子科技大学

UNIVERSITY OF ELECTRONIC SCIENCE AND TECHNOLOGY OF CHINA

博士学位论文

DOCTORAL DISSERTATION

论文题目 分组密码算法设计与评估应用研究

学科专业 信息安全

指导教师 [redacted]

作者姓名 [redacted]

学 号 [redacted]

分类号　　密级　公　开

UDC[注1]

学　位　论　文

分组密码算法设计与评估应用研究

（题名和副题名）

罗　岚

（作者姓名）

指导教师姓名　魏正耀　院士　秦志光　教授

电子科技大学　　成都

（职务、职称、学位、单位名称及地址）

申请专业学位级别　博士　专业名称　信息安全

论文提交日期　2008.9　论文答辩日期　2009.5.23

学位授予单位和日期　电子科技大学

答辩委员会主席

评阅人

年　月　日

注 1：注明《国际十进分类法 UDC》的类号。

The Application Research of Design and Evaluation on Block Cipher

Major: Information Assurance

Advisor: Professor Wei ZhengYao Professor Qin ZhiGuang

Author: Luo Lan

独 创 性 声 明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作及取得的研究成果。据我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得电子科技大学或其它教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

签名：罗　岚　　日期：**2008** 年 **9** 月 **1** 日

关于论文使用授权的说明

本学位论文作者完全了解电子科技大学有关保留、使用学位论文的规定，有权保留并向国家有关部门或机构送交论文的复印件和磁盘，允许论文被查阅和借阅。本人授权电子科技大学可以将学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。

（保密的学位论文在解密后应遵守此规定）

签名：罗 岚　导师签名：魏正耀，秦志光

日期：**2008** 年 **9** 月 **22** 日

摘　要

分组密码算法是信息安全研究方向密码学的一个分枝，本文是对分组密码算法在各种公开通信模式下的应用研究。把分组密码算法的一些特征运用到互联网通信、无线网络通信及目前计算机通信中几个前沿模式：可信计算、量子通信。分组密码算法应具备保密背景下的安全要求，还有工程实现方面各个利益集团的标准。基于 IP 的三网合一标准水落石出，分组密码算法的地位以及客观应用要求显而易见。由于通信、网络标准是由国际几个大的机构统一制定，因此，对分组密码算法的设计提出了更高的要求，以满足信息与网络安全中实现数据加密、数字签名、认证及密钥管理的需要。

美国新一代加密标准 AES 的公开征集活动，对分组密码算法设计与分析产生了推动。欧洲、日本、韩国等地区、国家也先后开展了分组加密算法标准的征集工作。欧洲加密标准（New Europe Schemes for Signature Integrity and Encryption, NESSIE）的征集与美国相比，起步虽晚，但充分发挥了综合优势，并有后来居上的趋势。欧洲加密标准覆盖面广，对加密、签名、认证等方面都有所考虑，同时激发了这一领域公开讨论与研究的热情。本论文立足 IP 标准的背景，在对国际领先分组密码算法的解读与分析基础上，对分组密码算法的设计、评估应用研究做如下的探讨和创新。主要内容为：

1、研究了现行公开使用的分组密码算法标准，提出分组密码算法设计框架在安全前提下，简洁设计更适合于网络化的使用环境；在密码强度与运算速度的取舍中需要具有冗余度，以应对网络中的各种不同类型故障。

2、提出了分组密码算法相关协议的设计与评估是基于密钥的。特别，从可信计算角度分析了协议的安全性以及存在的漏洞，使用层次划分的方法进行安全协议设计并且给出安全强度证明。对密钥提出唯速度与硬件标准设计方案。对密钥与密码结合方式进行研究，提出相应的硬件实现策略。

3、提出了以信息安全协同作为背景，对各个层次所使用的分组密码算法进行不同强度级别的设计与使用。在基于 IP 的三网合一标准下，使分组密码算法的作用尽量得到发挥。对分组密码算法的运算模式和可证安全性进行了简单创新研究。

4、对分组密码算法模块设计、评估做出量化，运算并证明最低安全标准值。给出相应设计与分析方案；对线性模块提出基于运算速度及基于安全强度的设计

思路，列举几个创新性设计方案。分组密码算法在可信计算平台中的数据安全通信与认证的一种设计以及在无线传感网络用户接入、RFID 与量子密钥分发等多种新型通信模式下的使用。

关键词：分组密码算法设计与评估，密码协议，三网合一与现代通信，可证安全

ABSTRACT

The block cipher algorithm is a research direction of cryptography in information assurance. This Doctoral Dissertation is the application in every kind of communication. According to the character of block cipher the suitable application has been studied in Internet environment, in wireless networks, as well as the new computer communication including trusted computing and quantum communication. It has applied in wireless networks and international network. The block cipher algorithm design need satisfied both assurance and performance. When the international standards based on IP have been defined, the block cipher design becomes more important than ever before. Due to the application environment owns itself international standard, block ciphers must satisfy with those big corporations' stricter needs. It can be used in data encrypt, digital signature, authentication and key management etc.

Advanced Encryption Standard of America call for algorithm published. This plan promoted both design and analysis of block cipher around the world. Europe, Japan amd South Korea have thrown money to call for encryption algorithm. Though NESSIE is later than America, European spent more money and include more broadly field of encryption algorithm such as encryption, signature, authentication. This thesis states the block cipher algorithm's design and analysis. It also discussed the IP standard of block cipher. In this thesis contributions are given regarding theses various topics:

1、The thesis regard that simple design of block ciphers and protocol is the main trend in the field and it must be based on network after studying AES, Camellia，Anubis etc. If consider more complexity usage, the extension choice between security and speed should be more widely. This design principle can deal with different problem in network.

2、The protocols of block cipher face to key exchange of symmetric cipher as well as both the design and evaluation must take this way either. The security and vulnerability of a protocol are analyzed based on the trusted computing. This thesis suggested that the protocol design should be distinguished and proof its security according to different network layer. The key design should change only satisfied the

speed standard from satisfied with both software and hardware. The connected module between algorithm and key also has been analysed in this thesis. The delay hardware design was proposed and discussed.

3、According to TCP/IP, different layer uses different style block cipher. The block cipher make as more as possible contribution to information assurance through this way. The operation modes of block cipher have been discussed and their provable security were analysed.

4、The block cipher module design and evaluation have been calculated into every kind of number and the basically numerical value was given. The thesis design kinds of innovating proposals of block cipher's difference part. A design of data security algorithm to trusted network connect was proposed in this thesis. Furthermore, kinds of block cipher's application in such as wireless network, RFID and quantum key distribution were deeply researched in this thesis.

KEYWORDS: Design and Evaluation on Block Cipher, Cryptographic Protocol, Modern Communication and Convergence 3-Net via IP, Provable Secure

目　　录

第一章　绪　论

1.1 研究动机及意义

网络技术的发展和普及使得网络安全、信息安全、数据通信保密成为必须研究的课题。随着密码技术广泛应用于金融、商业等民间信息安全保护，密码从军事、政治和外交通信应用的神秘色彩中解放出来。虽然密码学用于保护军事和外交可追溯到几千年前，但是直到 1949 年香侬在《贝尔系统技术杂志》上发表了“保密系统的通信理论”[1]一文，它才真正成为一门系统的科学。二十世纪七十年代，国际密码学界发生了革命性的两大事件。一是 Diffie 和 Hellman 发表了“密码学的新方向”[2]一文，提出了一种崭新的密码体制——公钥密码体制，改变了长期以来单钥密码体制的局面；另一件是美国国家标准局（National Bureau of Standards , NSB）公开征集标准密码算法，并于 1977 年正式公布使用美国数据加密标准（Data Encryption Standard, DES）[3]。这两个事标志着现代密码学的诞生。事实说明了：密码算法可以公开，密码的安全性可以依赖于密钥保密。近 30 年来，现代密码学无论在理论上还是在应用上都得到了巨大的发展。

密码学主要由密码编码学和密码分析学两个分支组成。密码编码学是使消息保密的技术和科学，它的主要任务是寻求生成高强度密码的有效算法，满足对消息进行加密或认证的要求。密码分析学是分析密数据的技术和科学，它的主要任务是分析密码或进行相关分析，实现获取机密信息或进行诈骗破坏活动。这两个分枝是相互对立、相互依赖的关系。正是由于两者之间的对立促进了密码学的快速发展。在现存的密码技术中，由于分组密码具有速度快、易于标准化、便于实现等特点，通常是信息与网络安全中实现数据加密、数字签名、认证及密钥管理的核心算法，在计算机通信和信息系统安全领域有着广泛的应用。分组密码算法（Block Cipher, BC）主要应用在网络上，可以非常方便地通过多种运算模式实现数据加密及信息认证等功能。较其它密码形式具备几个优势：

1、易于标准化。在各种网络数据通信中，信息遵循相关协议，尤其是在三网合一后的基于 IP 的标准，使分组密码算法的使用前景更加广阔。

2、使用分组密码算法容易实现同步。一个组的传输错误不会影响到其它组，丢失一个密数据组也不会影响随后的加/解密。

对分组密码算法的研究一直受到国际密码界的高度重视。由于相对的公开性，这一分枝的评估与设计其实是对各个国家密码学水平、计算能力上的一种展示和竞争。随着通信方式标准化的进程，分组密码算法的设计从硬件和软件的角度也做了相应的调整；其评估手段与方式也从最初民间自发性的分析演变成设计时的一系列标准化的分析。

1.2 研究现状

1.2.1 国际研究现状

分组密码算法的诞生和发展有着广泛的实用背景和重要的理论价值。60 年代后期，美国 IBM 公司即开始研制分组密码算法，并研究出几种复杂度较高的密码体制。1973 年 5 月 5 日，美国国家标准局，即现在的国家标准与技术研究所（National Institute of Standards and Technology, NIST），在 Federal Register 上发布了公开征集标准密码算法的请求，并确定了一系列的设计准则：

1、算法必须提供较高的安全性。

2、算法必须完全确定并且易于理解。

3、算法的安全性必须依赖于密钥而不依赖于算法。

4、算法必须对所有的用户都有效。

5、算法必须适合于各种应用。

6、用以实现算法的电子器件必须很经济。

7、算法必须能够有效使用。

8、算法必须能够验证。

9、算法必须能够出口。

1977 年 1 月 NBS 选用该公司研制的分组密码算法作为 DES 标准，并公开密码算法——这就是最早的通用分组密码算法。DES 的公布反映了民间密码使用环境对密码技术的新要求，使密码的编码思想产生了根本的改变：从过去依赖于密码算法保密走向依赖于密钥保密。这种密码设计思想的改变对密码编码产生了革命性的影响。尽管密码学界对 DES 算法的安全性提出了种种质疑，但在其公布后的二十多年中还是得到了普遍的应用。DES 的推出，密码学界对分组密码算法表示出了极大的兴趣，因此促进了分组密码算法算法设计与分析的发展。DES 推出后，又先后推出了几十种分组密码算法体制，比较著名的有 FEAL、REDOC、LOKI、

IDEA、GOST、Blowfish、SAFER、RC5 等。

随着科技水平的发展，DES 变得越来越不安全[4]：尽管采用了三重 DES 作为临时方案，但并不能满足人们的安全需要。为此，美国国家标准技术局于 1997 年 4 月 15 日开始在全球范围内公开征集新一代加密标准（Advanced Encryption Standard, AES），专门成立了 AES 工作组，目的是确定一个公开的、全球免费使用的分组密码算法，用于保护下一代敏感信息。1997 年 9 月 21 日 NIST 在 Federal Register 上公布了征集 AES 的公告：要求比三重 DES 快而且至少和三重 DES 一样安全；分组长度为 128 比特，密钥长度为 128、192 和 256 比特。1998 年 8 月 20 日 NIST 召开第一次 AES 候选会议，并公布了 15 个候选算法；1999 年 3 月 22 日举行第二次 AES 候选会议；1999 年 4 月 15 日公布了从 15 个算法中选出的 5 个算法：MARS、RC6、Twofish、Serpent、Rijndael；2000 年 10 月 2 日选定 Rijndael 为 AES 的唯一候选算法；2001 年 2 月 28 日，NIST 公布了 FIPS 草案供公众讨论；2001 年 11 月 26 日 NIST 发布正式标准文本 FIP197，确立 Rijndael 为 AES 标准算法，2002 年 3 月 26 日 FIP197 正式生效。

对于分组密码算法的标准化，运算模式是伴随算法进展的一部分。1980 年，NIST 公布了 4 种 DES 的运算模式[5]：ECB、CBC、CFB、OFB。在文件 FIPS113 中公布了 DES 的认证模式 CBC—MAC。在文件 FIPS46—3 中，公布了 Triple—DES 的 7 种运算模式，它们同时被包含进 ISO 的相关文件中[1][6][7][8]。对于 AES，2001 年秋季在文件 800-38A 中公布了 AES 用于保密性的 5 种运算模式：ECB、CBC、CFB、OFB 和 CTR。只有 CTR 是唯一选定的新的保密运算模式。

美国新一代加密标准的公开征集活动，对分组密码算法设计与分析产生了新的推动。欧洲、日本、韩国等地区、国家也先后开展了加密标准的征集工作。欧洲加密标准的征集与美国相比，起步虽晚，但是有后来居上的趋势。这个标准覆盖面广，对加密、签名、认证等方面都有所考虑。

1.2.2 国内研究现状

中国对分组密码算法的研究主要集中在信息安全国家重点实验室、西安电子科技大学、信息产业部下属的部分院所、电子科技集团下属公司等。对使用的分组密码算法由于涉及国家安全，并非盲目地接受国外产品。但有长期分组密码算法研究的机构都没有参与国际上公开的标准征集活动。

在国家 863 计划、自然科学基金资助下，有一些设计方面的专利、方案，大

都是在国际现行标准下的一些改动。对分组密码算法的评估方法多集中在线性分析、差分分析[9]、代数分析上，对如 SLIDE 分析等方法研究也有所进展。中国密码学家在追踪国际前沿技术同时，取得了实际应用中的累累硕果，也为分组密码算法的研究者参与国际竞争提供了机会。无线网络上使用的分组密码算法 SMS4 已经公布，标志着中国在信息安全领域也逐渐由算法保密向部分算法公开转变。随着下一代计算机互联网时代的来临，对分组密码的保密强度、运算速度、工程实现提出了更高的要求。从分组密码诞生以来，其密码学基础一直是混乱与扩散原理。由于数学发展的不确定因素，对分组密码整体结构和关键部分的分析、测试与比较必须伴随分组密码的发展而进行。本文在研究过程中加入部分自主知识产权，力争使分组密码理论的创新与密码技术的优化在中国得到更广泛的重视，缩小与国际先进水平的差距。对先进密码理论的应用也是算法设计与分析中重要的一个方面，应用研究也是这个领域比较薄弱的一个环节，密码编码理论和密码分析理论近来已经有相当的进展。

1.2.3 对称密码体制及流密码简介

以密钥的角度，密码体制可分为对称密码体制和公开密钥体制。以下按照这种分类方法进行描述。

设 M 为明消息空间或消息空间，C 为密数据空间，K 为密钥空间；设 E_k 为由明消息变为密数据的密码函数，D_k 为由密数据变为明消息的解密函数，其中 E_k 为 D_k 的逆函数。

定义 1-1：设一个密码体制是一系列的加密、解密函数串，分别设为：

$$\{E_k：k\in K\}和\{D_k：k\in K\}$$

如果满足下列等式：

$$M=D_k（E_k（m））\qquad 其中，\ m\in M, k\in K$$

即加密密钥与解密密钥相同，则称为对称密码算法体制。

通常，对称密码算法可分为流密码（Stream Cipher，SC）和分组密码（Block Cipher，BC）。分组密码算法与流密码算法可以在设计时作为相互的参考部件使用。如果在运算速度要求的满足的前提下，使用分组密码算法作为流密码的非线性部分是简单而且安全的途径。同样，使用流密码算法中的一些非线性函数作为分组密码算法圈结构中的 S 盒部分也是可行的。称上述密码算法模式为交叉渗透设计，这两类算法的关系不做进一步讨论。

流密码是对称密码体制中的一种，起源于 20 世纪 20 年代的 Vernam 体制。随着数学理论和微电子技术的发展，伪随机序列的产生、存储、及分配都有了完善的基础。因此流密码得到广泛的研究与应用，尤其是在各个国家的核心机构。在流密码体制中，如果密钥流经过 d 个符号之后重复，则称该流密码是周期的，否则称之为非周期的。密钥流元素 k_j 的产生由第 j 时刻流密码的内部状态 s_j 和实际密钥 k 所决定，记为 $k_j=f(k, s_j)$。加密变换 E_{kj} 与解密变换 D_{kj} 都是时变的，其时变性由加密器或解密器中的记忆文件来保证。加密器中存储器的状态 s 随时间变化而变化，这种变化可用状态转移函数 f_s 表示。如果 f_s 与输入的明消息无关，则密钥流 $k_j=f(k, s_j)$与明消息无关，j=1，2，…，从而 j 时刻输出的密数据 $c_j=E_{kj}(m_j)$与 j 时刻之前的明消息也无关，称此种流密码为同步流密码。在同步流密码中，只要发送端和接收端有相同的实际密钥和内部状态，就能产生相同的密钥流，此时发送端和接收端的密钥生成器是同步的。一旦不同步，解密工作立即失败。如果状态转移函数 f_s 与输入的明消息符号有关，称为自同步流密码。目前应用较广泛的流密码是同步流密码。

一个同步流密码是否具有很高的密码强度主要取决于密钥流生成器的设计。为了设计安全的密钥流生成器，必须使用复杂的线性变换和非线性变换，这就给理论分析工作带来了很大困难。密钥流生成器的目的是由一个短的随机密钥(也称实际密钥或种子密钥)k 生成一个长的密钥流，用这个长的密钥流对明消息加密或对密数据解密，从而一个短的密钥可用来加密更长的明消息或解密更长的密数据。对一个密钥流生成器的实际安全要求是它的不可测性，即要求生成的密钥流具有随机性，使密码分析者不可能从截获的 i 比特子段生成大于 i 比特的密码。

构造密钥流生成器是流密码核心的内容，目前有各种各样的构造方法，这些方法可划分为四大类方法：信息论方法、系统论方法、复杂度理论方法和随机化方法。根据已知的构造方法设计出来的大多数密钥流生成器已被证明是不安全的，仅有少数还没有被证明是不安全的。即使现在还没有被证明是不安全的，迟早会被证明是不安全的：因为现在被认为是安全的密码，都是基于国际上某个数学难题没有解决，即破密码系统的难度等价于解决国际上某个公开数学问题的难度。一旦这个数学问题被解决，与之同难度的密码系统就不安全了。下面介绍由两个移位寄存器组成的收缩密钥流生成器，该构造方法属于系统论方法。

大多数实际使用的流密码都围绕线性移位寄存器（Linear Feedback Shift，LFSR）设计。使用门电路非常容易构造，但是，LFSR 使用软件实现效率很低。相比较而言，汇编语言比 C 语言实现速度快。

流密码算法不象分组密码那样有公开的国际标准，各国都在研究和应用，但是很少有公开的完整算法。欧洲正在征集的流密码标准算法展示了目前设计的趋势——非线性移位反馈技术与标准化工作。由于各个国家的流密码的设计技术与分析技术都掌握在核心部门，几乎不具备公开讨论的环境。如果前沿的卫星通信技术或各个国家用于特殊目的的通信手段能公开讨论，那么相应的流密码算法才可能有确定目的的征集与悬赏式的分析讨论。以下是在部分公开通信环境下所使用的流密码算法：

1、A5 算法

A5 是欧洲数字蜂窝移动电话系统中使用的流密码加密算法（如图 1-1），用于从用户手机到基站的连接加密，由法国人设计。3 个 LFSR 组成，移位寄存器的长度分别为 19、22 和 23，但抽头位较少，3 个 LFSR 在时钟控制下步进，三者的输出进行异或产生输出位。

可以看出，A5 的基本思路是有优势的，它的效率很高，能通过所有已知的统计测试，弱点是 LFSR 的简单设计导致无法抵抗分析。

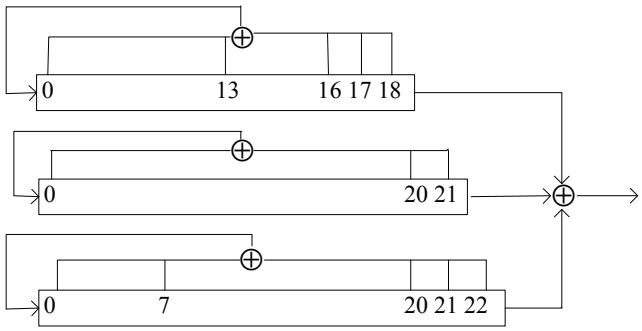


图 1-1 A5 加密算法

2、E0 算法

提到 E0 加密算法（如图 1-2），必须提及蓝牙无线通信系统。因为 *E*0 是由蓝牙的安全角度出发而设计的一种流密码算法。E0 流密码算法是用于无线通信的一种加密手段，其中线性移位寄存器的反馈多项式分别如下：

$$F(X)=X^{25}+X^{20}+X^{12}+X^{8}+1 \quad (1\text{-}1)$$

$$F(X)=X^{31}+X^{24}+X^{16}+X^{12}+1 \quad (1\text{-}2)$$

$$F(X)=X^{33}+X^{28}+X^{24}+X^{4}+1 \quad (1\text{-}3)$$

$$F(X)=X^{39}+X^{36}+X^{28}+X^{4}+1 \quad (1\text{-}4)$$

两个求逆 S 盒进行 2BIT 的变换，T_1，T_2 是两个线性变换：

$Z_T = X_T^1 \oplus X_T^1 \oplus X_T^2 \oplus X_T^3 \oplus X_T^4 \oplus C_T^0$　　（1-5）

$S_{T+!} = (S_{T+!}^0, S_{T+!}^1) = \lfloor (y_t + C_t)/2 \rfloor$　　（1-6）

$Y_T = X_T^1 + X_T^1 + X_T^2 + X_T^3 + X_T^4$　　（1-7）

$C_{T+!} = (C_{T+!}^0, C_{T+!}^1) = (S_{T+!}^0, S_{T+!}^1) \oplus T_1(C_T) \oplus T_2(C_{T-1})$　　（1-8）

$Y_T \in \{0, 1, 2, 3, 4\}$，$S_T \in \{0, 1, 2, 3\}$　　（1-9）

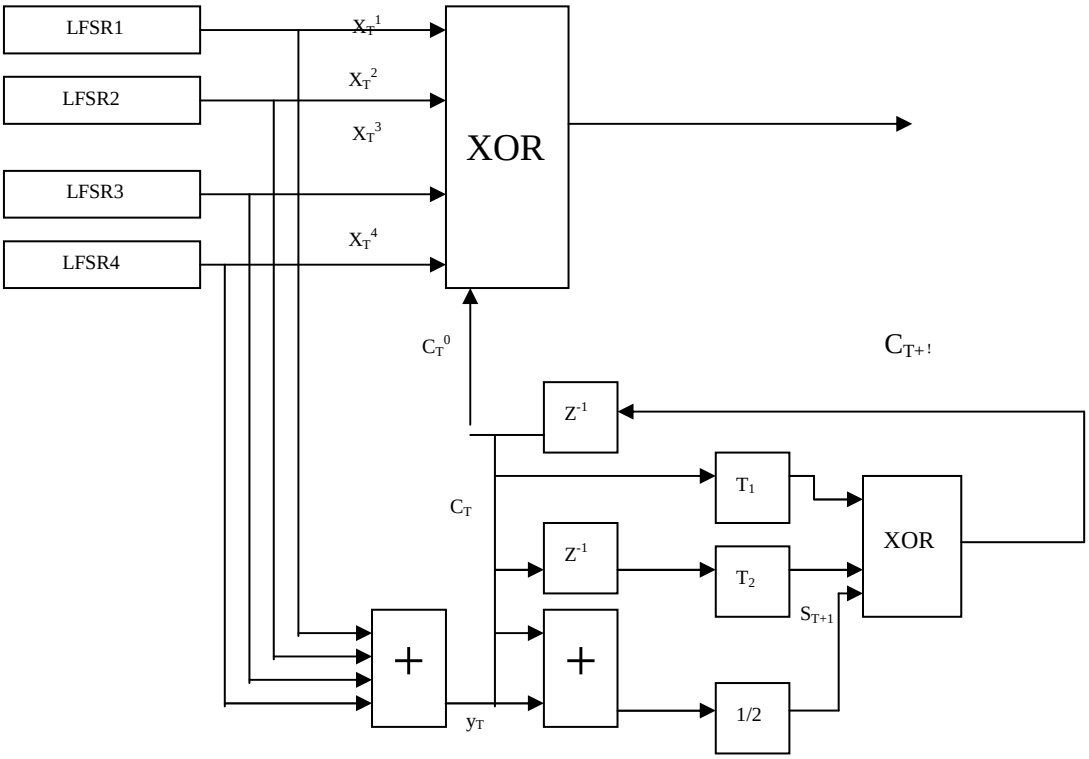


图 1-2 E0 加密算法

3、RC4 算法

RC4 算法是由 Ron Rivest 1987 年为 RSA 数据安全公司设计的可变密钥长度的流密码,广泛用于商业密码产品中。1994 年 9 月其源代码在 Cypherpunks 邮件列表中公开，迅速广为流传。RC4 可以简单的描述为：非线性部分为一个八进八出的 S-box，是 0 到 255 的置换，并且该置换是一个可变长度的密钥函数。RSA 数据安全公司宣称该算法对差分和线性分析是免疫的，几乎没有小循环，并且有很高的非线性。其具体加密步骤如下：

两个初值为 0 的记数器，产生一个随机字节。

$I = (I+1) \bmod 256$

$J = (J+1) \bmod 256$

交换 S_i 和 S_j

$$t=（S_i+S_j）\bmod 256$$

$$K=S_t$$

字节 K 与明消息异或产生密数据，同样 K 与密数据异或产生明消息。加密速度是 DES 的 10 倍。S-box 的初始化也非常简单。进行线性填充：

S_0=0，S_1=1，…，S_{255}=255。

使用密钥填充另一个 256 字节的数组，不断重复直到填充到整个数组，K_0，K_1，…，K_{255}。将指针 j 初始化为 0，从 I=0 到 255 做 $j=（j+S_i+K_i）\bmod 256$，交换 S_i 和 S_j。RC4 的密钥扩展、加密伪代码如图 1-3、1-4。其中 swap 为交换函数。

```
for i = 0 to 255 do
    S[i] = i
     j = 0
for i = 0 to 255 do
    j = (j + S[i] + k[i ]) (mod 256)
    swap (S[i], S[j])
```

图 1-3 RC4 密钥扩展代码

```
i = j = 0

for each message byte Mi

      i = (i + 1) (mod 256)
      j = (j + S[i]) (mod 256)
      swap(S[i], S[j])
t = (S[i] + S[j]) (mod 256)

Ci = Mi XOR S[t]
```

图 1-4 RC4 加密算法

4、流密码的迭代模型及可证安全性

定义 1-2：一个函数 $f:\{0,1\}^n \to \{0,1\}^n$, 定义 $f^{(i)}(x)$ 为 f 函数迭代 i 次后的结果。则：

$f^{(i)}(x) \triangleright f(f^{(i-1)}(x)), f^{(0)}(x) \triangleright x$。假设 G 是一个算法，$\{0,1\}^n$，$y=f^{(i)}(x)$，设函数的‘0’、‘1’比特概率定义为：$P(0)$, 偏差为 $Adv_f^{p(0)}$。把随机预言机制定义为理想的 1/2 模式，则 f 的随机预言偏差为：

$$Adv_f^{p(0)} = P(0) - \frac{1}{2} \quad (1\text{-}10)$$

一个流密码算法的非线性部分一定存在线性偏差，如果偏差边界不够紧。则可以进行线性逼近，在某种范围内可以使得算法在一定差错率中得到相对还原。使用一个线性函数 g 逼近后，在定义域范围内，非线性部分与线性偏差的距离定义为：

$$D_f^g(x) = \{x \mid f(x) - g(x)\} \quad (1\text{-}11)$$

如果迭代 i 次后，与理想随机预言机制偏差边界为：$D^{(i)}{}_f^g(x) = \prod_i (D_f^g(x) - \frac{1}{2})$。

显然，边界值 $D^{(i)}{}_f^g(x)$ 和 $Adv_f^{p(0)}$ 呈几何级数阶迅速下降，小的线性偏差会使流密码结构抗击多种分析的能力增强。

一个同步流密码是否具有足够的密码强度主要取决于密钥流生成器的设计。由于必须在生成器中使用线性变换，而线性模块无论从电磁泄露、序列特征都被分析透彻。因此，设计流密码体制的重点倾向于非线性模块。对基本数学理论产生的非线性函数的公开讨论并不多见。事实上，由于国际上对分析能力的评判没有结论，从设计进行流密码体制的可证安全性工作是必要环节。从 NESSIE 算法征集中流密码算法的空缺可以看到：对流密码算法的分析能力远超过设计者的想象。对流密码算法设计进行可证安全性的工作是对运算不可能的证明，一个密码系统的安全性还与密钥、通信协议等有很强的联系。

1.2.4 分组密码算法相关使用情况及存在的主要问题

1.2.4.1 分组密码算法在互联网环境下的使用情况

在互联网上，分组密码算法在各个结构层次有广泛的使用。以下按照 TCP/IP 协议中的五层结构来简单介绍分组密码算法的使用情况：

对于 TCP/IP 协议的物理层，主要是网络硬件基础设施，除了有量子加密的设想之外，目前还没有关于安全措施的方案；只是可信计算中提及安全硬件，但处于讨论阶段，各方都按各自的理解进行局域网络的安全构建。链路层的安全措施一般采取面向数据的对称密码的硬件加密，分组密码算法也是其中的一种选择，这一层次的加密主要是有特殊安全需求的专网用户使用。链路层密码算法产品根据各个国家的法律有一部分在市场上供应，但是使用的算法一般都有自主知识产

权。事实上，TCP/IP 的底层安全设施、协议并没有在互联网上公开、大范围的使用。网络层的安全方法使用最广的是网络安全协议（IP Security , IPSEC），虚拟安全网络（Virtual Private Network，VPN）是基于互联网络的常用安全方案。VPN 是利用现存的网络结构、通过不信任的第三方进行 IP 层安全通信的手段。IPSEC 可以在各种路由、服务器、各种终端固定用户及防火墙之上运行，其中主要包括三个主要协议：认证头协议（Authentication Header，AH），提供基于传输包的安全认证服务；有效载荷安全封装协议（Encapsulating Security Payload，ESP），提供加密服务；互联密钥交换协议（Internet Key Exchange，IKE），进行密钥等参数的连接协商。IPSEC 协议的优势在于充分考虑到了下一代互联网的兼容问题，包括 IPV4、IPV6 两种版本。分组密码算法在 IPSEC 协议中是指定的数据加密标准，包括 3DES、AES，许多产品还根据安全的考虑提供包括 NESSIE 最终获胜的分组密码算法作为加密选择。局域网络的安全保障是由 X.25 协议实施的。应用层上的分组密码算法使用得更加频繁：随着 MD5 与 Hash 函数出现安全疑虑，基于分组密码算法的 CBC 模式逐渐在多种场合如口令认证、身份验证上逐渐加大使用力度。微软是率先把 AES 商业化的公司，推出的压缩工具包的身份认证口令都采用了 AES 加密算法。IDEA[10]分组密码算法在 PGP 邮件加密中使用。

总之，在网络的链路层、IP 层、应用层分组密码算法都有使用。可以预见，随着使用层面逐渐扩大，如果要达到安全的目的，与算法相关的协议等需要更完善的考虑。

1.2.4.2 分组密码算法在无线网络环境下的使用情况

随着无线网络在全球逐步被广泛纳入移动办公范畴，信息安全问题成为非常薄弱、受关注的一环。无论是使用防火墙或是入侵检测，无线网络都存在明显的漏洞。分组密码算法由于其在互联网各个层次上使用的基础，已为许多国际标准组织采纳作为数据安全、身份认证的手段。国际标准组织 ISO 的 *802.XX* 系列协议就是专门针对无线网络而制定的。为了保证无线网络的安全，包括数字证书、密钥协商和传输数据加解密三个部分。*802* 系列协议在短时间进行了高频率的升级，对数据安全的部分已经在 AES 基础上进行运算。

1999 年 6 月，用于三代移动通信的密码算法首次提出，经过几次修改升级，2001 年 7 月制定了最新的标准[11]。加密算法并没有特别要求是分组密码算法，但是必须可以保证数据的安全性与完整性。算法最终还是使用了参考 KASUMI 分组密码算法[12]的 f8、f9 加密算法[13]。

中国的宽带无线 IP 标准工作也一直与相关国际标准组织保持交流和沟通，相应的 64 位、128 位或 256 位加密标准，无线网络存在一定的安全缺陷。随着三网合一基于 IP 的网络标准出台，无线网络安全应该与互联网络安全纳入同一标准，这也是加入标准工作的一个渠道。

1.2.5 分组密码算法相关标准简介

2004 年 7 月，NIST 宣布撤回对 DES 分组密码算法的标准，这影响到了 NIST FIPS 46-3 和 NIST FIPS 81 协议。但是 NIST 推出 NIST SP 800-67 支持 3DES 协议，并且推广 AES 的使用。ISO/IEC 18033-3 中包括 6 个分组密码：三个 64 位的算法，3DES、MISTY1、CAST-128，三个 128 位算法，AES、Camellia、SEED。其中关于 3DES 的标准可参考[14][15]和[16]，同时，3DES 也在 ISO/IEC 18033-3[17]中标准化。AES 是 NIST Pub-197[18][19]中已经正式公布的加密算法，同时 AES 也是 NESSIE 中 128 比特标准推荐的算法。AES 被各种标准广泛采用的原因在于它在软件和硬件上的灵活使用，特别是 SMART CARDS 的设计。关于 AES 的评论可以参考[20]和[21]。

1.3 论文主要工作

本论文的理论和应用研究工作是在国家自然科学基金 60673075、国家 863 计划 2006AA01Z428 及四川省青年创新基金 05GG006-003-503 等项目的资助下完成的。在项目完成过程中，作者遵循国际惯例在算法公开的前提下，对分组密码算法的评估与设计、分组密码算法相关协议进行了应用研究。本文以信息安全为基础，以信息论中扩散和混乱的原则为理论依据，通过对国际上高标准的分组密码算法的分析，提出一定的创新观点。研究工作可以概括为如下几点：

1、研究了现行公开使用的分组密码算法标准，提出分组密码算法设计框架在安全前提下，简洁构架更适合于网络化的使用环境；密码强度与运算速度的取舍中需要具有冗余度，以应对网络中的各种不同类型故障。

2、提出了分组密码算法相关协议的设计与评估应该是基于密钥的。特别，从可信计算角度分析了协议的安全性以及存在的漏洞，使用层次划分的方法进行安全协议设计并且给出安全强度证明。对密钥提出唯速度与硬件标准设计方案。对密钥与密码结合方式进行研究，提出相应的硬件实现策略。通过针对硬件的远程时间分析，说明分组密码算法在硬件实现时需要考虑防范措施，作出相应建议。

提出分组密码算法带 Bit 延迟、基于高次迭代的安全设计思路与理由。

3、提出了以信息安全协同为背景，对各个层次所使用的分组密码算法进行不同强度级别的设计与使用。在基于 IP 的三网合一标准下，使分组密码算法的作用发挥到尽可能大的限度。

4、对分组密码算法非线性模块设计、评估做出量化，运算并证明最低安全标准值。给出几个设计与分析方案；对线性模块提出基于运算速度及基于安全强度的设计思路，列举针对分组密码算法部分模块的创新性设计方案。

1.4 论文章节安排

分组密码算法在美国、欧洲及部分亚洲发达国家采取公开征集的方式，提交的方案可以通过多种公开途径进行评估与分析。可以看到有些算法确实存在一定的弱点，而且算法的总体框架基本处于对经典的 Feistel、SP 加密结构细节修改上。本论文希望能从分组密码的基础理论研究、评估与分析研究、实际应用研究的角度进行创新性的探讨，对该方向的现有成果通过总结，解决实际中存在的问题。介于上述出发点，本文安排如下：

第二章是对分组密码算法结构与相关协议的基础研究，是本文论述的理论体系基础。包括：分组密码算法运用到的基本数学原理、两种作为标准的框架结构——Feistel 和 SP 简介、几个在 AES 及 NESSIE 鳞选中获胜的加密算法介绍、与分组密码算法相关的协议研究，本章是全文的基础。

第三章对分组密码算法设计与评估的研究。首先对算法分析做了研究，这是设计与评估中必须面临的检测，也是推动设计发展的原动力；随后对分组密码算法的各个模块展开研究：线性模块设计与评估、非线性模块研究与评估、密钥设计与结合方式研究、算法运算模式研究，分组密码算法在可证安全性领域的初步研究，本章是全文的核心及创新部分。

第四章叙述了分组密码算法使用的协议环境，对安全协议的分析方法和可能存在的漏洞进行分析后，提出在网络环境中基于分组密码算法的几个协议设计模型。特别针对可信计算平台，强调了分组密码算法应该发挥的重要作用。对 RFID、电子商务与电子政务平台中使用的分组密码算法提出安全建议。对目前量子通信提出使用分组密码算法加强安全的建议。

第五章是全文总结，提出在本文的基础上分组密码算法公开研究方向。

1.5 小结

随着三网合一基于 IP 的标准制定，密码算法在设计、评估及使用上都在进行相应的调整。分组密码算法是容易与标准接口的一类密码，通过长期网络化的使用与公开征集，使得分组密码算法成为公众最为熟悉的一类数据安全手段。发达国家在这一领域控制着使用权。中国信息安全一贯采取的措施是基于密码算法保密的前提的，但是随着国家实力的提高，参与国际竞争是必然的趋势，这需要对分组密码算法有相当的设计与评估基础。本文在对已有成果的研究上，指出分组密码算法的设计与评估的重要性，希望引起国家对信息安全中公开部分的重视与投入。下一章是一些基础理论的介绍，而研究重点在第三章中论述，使用情况与安全保障问题在第四章进行讨论。

第二章　分组密码算法典型结构研究

2.1 数学原理

2.1.1 基本定义

分组密码的一般定义可以描述为：对密钥集合 K 中一个给定的密钥 $k \in K$，一个加密变换函数 E_K ，设明消息分组长度为 n 比特，则：E_K 可以看作是 Z_2^N 上的一一对应或置换。

如果 P、$C \in Z_2^N$ 分别表示明消息和密数据，则加密变换为：

$$C = E_K（P）$$

解密变换为：

$$P = E_K^{-1}（C）$$

分组密码算法加、解密模型如图 2-1：

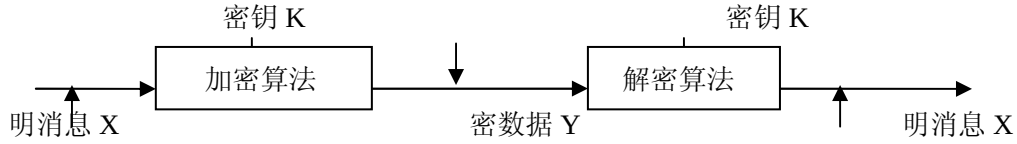


图 2-1 分组密码的数学模型

把分组密码算法看作使 S_2^n 的一个子集，是单表代替密码，只不过代替表必须足够大且能抗各种形式的分析。算法集合表示为：$\{ E_k \mid k \in K \} \subseteq S_2^n$ ，其中，K 是密钥集合，k 表示密钥。

也可以把分组密码算法看作一个映射 E：$Z_2^N \times K \rightarrow Z_2^N$，对明消息 $P \in Z_2^N$ 和密钥 $k \in K$，密数据 $C = E（P，k）$ 是一个多输出布尔函数。

一个 N *bits* 对称密钥分组密码算法函数 e：$\{0，1\}^N \times \{0，1\}^L \rightarrow \{0，1\}^N$,其中密钥 $k \in \{0，1\}^L$，加密函数 $e（p，k）$ 记为：$e_k（p）$ 是 $\{0，1\}^N$ 到 $\{0，1\}^N$ 上的可逆映射，逆映射是解密函数，记为：$d_k（c）= d（p，k）$ 其中 c 为 $e_k（p）$。

分组密码算法的分组与密钥大小体现了计算机发展的水平，目前标准的分组与密钥大小至少为 128 比特。

2.1.2 预备知识

1、有限域 GF（2^8）上相关定义

以下以 AES 为例，进行符号说明。有限域中元素[22][23]按照如下惯例表达，在有限域 GF（2^8）上，定义数的表达、加法、乘法：

字节 b 由 8 bits 组成，记为 $b_7\,b_6\,b_5\,b_4\,b_3\,b_2\,b_1\,b_0$ 作为如下{*0*、*1*}多项式的系数：

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b_0x^0$$

例如：一个 16 进制的数‘58’（二进制为 01011000）代表如下多项式：

$$x^6 + x^4 + x^3$$

2、加法定义

有限域 GF（2^8）上多项式加法是对应系数位上数字进行异或（0+0=0、0+1=1、1+0=1、1+1=0），例如：‘58’+‘82’=‘DA’，或用多项式表示如下：

$$（x^6 + x^4 + x^3）+（x^7 + x）= x^7 + x^6 + x^4 + x^3 + x$$

用二进制表示可以写成：“01011000”+“10000010”=“11011010”。显然，加法可以看作二进制异或在八维向量空间上的表出。这样关于加法构成一个交换群：满足结合率，加法单位元为‘00’，每一个元素有加法逆元，在 GF（2^8）上加法与减法相同。

3、乘法定义

通常，一个算法中会有一个 GF（2^8）上的非褪化不可约多项式作为乘法的模多项式（非褪化指多项式的最高项指数为 8，不可约指一个多项式只能被 1 和自身整除）。以下把多项 $m（x）= x^8 + x^4 + x^3 + x + 1$（或 16 进制的‘11B’）为例，‘58’·‘82’=‘59’或：

$$（x^6 + x^4 + x^3）（x^7 + x）= x^{13} + x^{11} + x^{10} + x^7 + x^5 + x^4$$

$$x^{13} + x^{11} + x^{10} + x^7 + x^5 + x^4（mod\ x^8 + x^4 + x^3 + x + 1）$$

$$= \quad x^6 + x^4 + x^3 + 1$$

显然，乘法的结果多项式次数小于 8，而且乘法不能向加法一样用字节表出。乘法满足结合率，有单位元‘01’，有逆元，逆元可以通过以下方法求出：

设次数低于 8 的多项式 $b（x）$ 满足（$b（x）$，$m（x）$）=1，根据欧几里德多项式：

$$b（x）a（x）+ m（x）c（x）=1$$

则：

$$b（x）a（x）=1（mod\ m（x））$$

即：　　$b^{-1}(x) = a(x)(mod\ m(x))$

并且满足乘法对加法的分配率：

$$a(x)(b(x)+c(x))$$
$$= a(x)b(x)+a(x)c(x)$$

上述运算对 GF（2^8）上的 256 个值构成有限域。

4、关于 x 的幂乘定义

如果定义 $b(x)$ 与多项式 x 的乘法为：

$$b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x^1$$

则 $x \cdot b(x)$ 为上式模 $m(x)$ 的表达式，如果 $b_7=0$，表达式唯一，如果 $b_7=1$，还需要减去 $m(x)$。显然，该运算相当于字节左移一位后对位加‘*1B*’，运算定义为：$b = xtime(a)$。对目前硬件设备是 32 位的机器而言，*xtime* 进行的是 4 次运算。高阶运算可以用反复多次的 *xtime* 运算进行实现，例如：‘57’·‘13’=‘FE’

$$‘57’\cdot‘02’ = xtime(57) = ‘AE’$$
$$‘57’\cdot‘04’ = xtime(AE) = ‘47’$$
$$‘57’\cdot‘08’ = xtime(47) = ‘8E’$$
$$‘57’\cdot‘10’ = xtime(8E) = ‘07’$$
$$‘57’\cdot‘13’ = ‘57’\cdot(‘01’ \oplus ‘02’ \oplus ‘10’)$$
$$= ‘57’ \oplus ‘AE’ \oplus ‘01’ = ‘FE’$$

5、有限域 GF（2^8）上系数多项式

多项式可由有限域 GF（2^8）上系数定义，这样，4 字节的向量可以代表次数低于 4 的多项式系数。多项式的加法直接定义为对应项系数相加，即对位异或。乘法如下定义：

设 $a(X) = a_3x^3 + a_2x^2 + a_1x^1 + a_0x^0$ ，$b(X) = b_3x^3 + b_2x^2 + b_1x^1 + b_0x^0$ 则

$a(X)b(X) = c(X) = c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x^1 + c_0$ ，*其中*：

$$c_0 = a_0b_0$$
$$c_1 = a_1b_0 + a_0b_1$$
$$c_2 = a_2b_0 + a_1b_1 + a_0b_2$$
$$c_3 = a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3$$
$$c_4 = a_3b_1 + a_2b_2 + a_1b_3$$
$$c_5 = a_3b_2 + a_2b_3$$
$$c_6 = a_3b_3$$

问题是，$c(X)$ 已经超出 4 字节所表出的范围，因此定义 4 阶多项式进行模

运算来降低次数。如果选择 $x^4 + 1$ 作为模多项式，则：$x^j \bmod x^4 + 1 = x^{j \bmod 4}$。

定义模乘法为：$a（X）\odot b（X）= d（X）= d_3x^3 + d_2x^2 + d_1x^1 + d_0$ ，其中：

$$d_0 = a_0b_0 \oplus a_3b_1 \oplus a_2b_2 \oplus a_1b_3$$
$$d_1 = a_1b_0 \oplus a_0b_1 \oplus a_3b_2 \oplus a_2b_3$$
$$d_2 = a_2b_0 \oplus a_1b_1 \oplus a_0b_2 \oplus a_3b_3$$
$$d_3 = a_3b_0 \oplus a_2b_1 \oplus a_1b_2 \oplus a_0b_3$$

运算可以写作矩阵的形式：

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} \quad （2\text{-}1）$$

事实上，作为模多项式，$x^4 + 1$ 是可约的，但运算非常简单。

6、多项式的 x 幂乘

定义有限域 GF（2^8）上多项式的 x 幂乘 $x \odot b（X）$为：

$$b_3x^4 + b_2x^3 + b_1x^2 + b_0x^1$$

模 $x^4 + 1$ 为：$b_2x^3 + b_1x^2 + b_0x^1 + b_3$ 。用矩阵表出只要取（2-1）中 a_1=‘01’，a_j=‘00’，当 j≠1 时。C（X）= x ⊙ b（X）可以表出成：

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 00 & 00 & 00 & 01 \\ 01 & 00 & 00 & 00 \\ 00 & 01 & 00 & 00 \\ 00 & 00 & 01 & 00 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} \quad （2\text{-}2）$$

因此，关于 x 或 x 幂次方的乘积可以看作向量字节的圈移位。

2.2 分组密码算法整体结构

因为分组密码算法在数学上等价于一个置换类：$\{ E_k \mid k \in K \} \subseteq S_2^n$ ，K 是密钥集合，k 表示密钥。

分组密码算法遵循 Shannon 的混乱与扩散原则。

混乱使明消息、密钥和密数据三者关系足够复杂，以此来掩盖它们之间的关系——保证不可能用明消息和密数据的解析式来表达密钥参数。

扩散使得明消息或密钥的任何一位数字变化都会导致密数据的变化。

混乱与扩散的尺度因密码算法的不同而有所变化，现代密码学中，混乱效果

通过利用非线性变换实现，扩散效果通过数字分位的位置变换或线性变换实现。用数学度量，线性偏差和非线性次数可以看作混乱的度量，差分概率和非线性扩散可以看作扩散的度量。

一个安全的分组密码算法要满足密钥求解困难，采用迭代的方式。多次迭代的基本结构为：$E_K = P_1（k）P_2（k）…P_r（k）$。

E_K 等于 r 个由密钥参量 k 决定的简单置换 P_i 的乘积，称 r 为加密轮函数，P_i 称为轮变换或基础置换。一般的，P_1、P_2、…P_r 的差异仅是密钥的选择方式不同。

双重加密结构：设有一个分组加密算法 e_k ，则令 $e（x）= e_{k2}（e_{k1}（x）)$ 且 $k1$、$k2$ 相互独立，是一个分组密码算法双重加密模式。三重加密结构：设有一个分组加密算法 e_k ，则令 $e（P）= e_{k3}^{(3)}（e_{k2}^{(2)}\ e_{k1}^{(1)}（P）)$ 称为三重加密算法，这里，$e^{(i)}$ 表示 $e_k（X）$ 或 $d_k（X）$，称 $e（P）= e_{k3}^{(3)}（d_{k2}^{(2)}\ e_{k1}^{(1)}（P）)$ 为 *EDE*—三重加密，如果 $k1 = k3$ 则称为双密钥三重加密。

2.2.1 Feistel 结构

Feistel 结构属于局部无逆结构，由 Horst Feistel 在设计 Lucifer 分组密码时发明。数据加密标准 DES 使用了这种结构而为全球广为接纳，这种类型也称为 DES 型分组密码算法，如 E2、RC5、GOST、Camellia 等都采取了这种结构。

输出密数据为（R_r ，L_r），其中，F 是非线性函数，一般称为轮函数。Feistel 结构逻辑如框图 2-2：

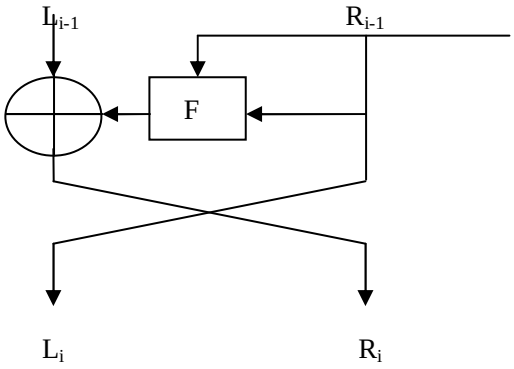


图 2-2 Feistel 结构逻辑框图

一个分组长度为 $2m$ 比特的 r 轮迭代 Feistel 结构密码，其中，加密过程可以描述为：明消息 $P = X$，记：$X=（L_0，R_0）$，L_0，和 R_0 分别是明消息 X 的高 m 位和低 m 位。设基本密钥 k，由它生成的 r 个子密钥表示成：$k_1,k_2,…,k_r$,加密算法的变换公式为：

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus F(R_{i-1}, k_i)$　　$I = 1、2、\ldots、r$

对 Feistel 结构有一些推广，得出许多变形的 Feistel 结构，如非平衡 Feistel 结构等，统称为广义 *F*eistel 结构。

在 *F*eistel 网络中，函数 $F(R_r, k_{r+1})$ 在已知 k_{r+1} 的条件下是不可逆的，它的可逆性与整体结构是否有逆无关。

2.2.1 SP 网络结构

SP 网络是典型的局部有逆结构分组密码算法。算法结构分为两层，一层为 S 混淆层，由密钥控制的非线性置换，通过并行查表实现。第二层 P 为扩散层，通常由与密钥无关的可逆线性变换实现。

Safer、Shark、及 AES 等分组密码算法都采用了此结构，受 AES 的影响，欧洲新世纪密码标准中提交的 17 个分组密码候选算法中有 13 个选用了此类结构。此外，在 Feistel 结构的轮函数设计中也大多采用 SP 网络结构，如图 2-3。

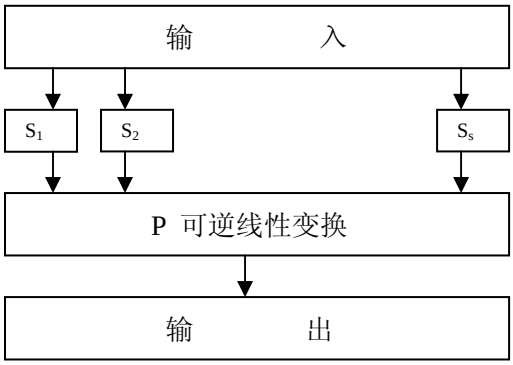


图 2-3 SP 网络结构

2.3 几个经典分组密码算法举例

分组密码算法出现了许多种不同的设计，其中常见的有 DES、AES、Camellia 等。

数据加密标准（Data Encryption Standard，DES）也被称为数据加密算法（DATA ENCRYPTION ALGORITHM，DEA），分别被 ANSI 和 ISO 标准化，全球广泛使用了近二十年的时间。1973 年，NIST 的前身国家标准局（National Bureau Standards, NBS）公开征集计算机通信数据的加密标准，虽然应征勇跃，但是专业领域的算

法很少。只有少数算法能够满足测试、验证、对于不同硬件环境适应性强。一年后 IBM 公司提出了 Lucifer 算法，NBS 请求国家安全局（National Security Agent, NSA）协助并通过公开方式进行评价。许多方面认为 NSA 对算法进行蓄意调整而留了陷门，而且把 128 比特的密钥长度减少到 56 比特，对算法设计原理进行保密。尽管面临许多质疑与批评[24]，美国政府仍然于 1976 年 12 月 23 日把 DES 采纳为联邦标准，授权可以在所有政府无密级数据通信中使用。对 DES 标准的描述可以参考[25]。DES 最新的版本是 NIST 标准，由 IBM 公司的专业研究人员设计的。对 DES 的使用与分析已经历了二十多年。

2.3.1 AES

AES 是目前典型的一种 SP 网络，由比利时密码学家 Joan Daemen 和 Vincent Rijimen 设计，是新一代的美国数据加密标准。对 AES 的介绍将侧重于 C 伪代码。

AES 的结构框图 2-4 如下：（*10≤N≤14*）

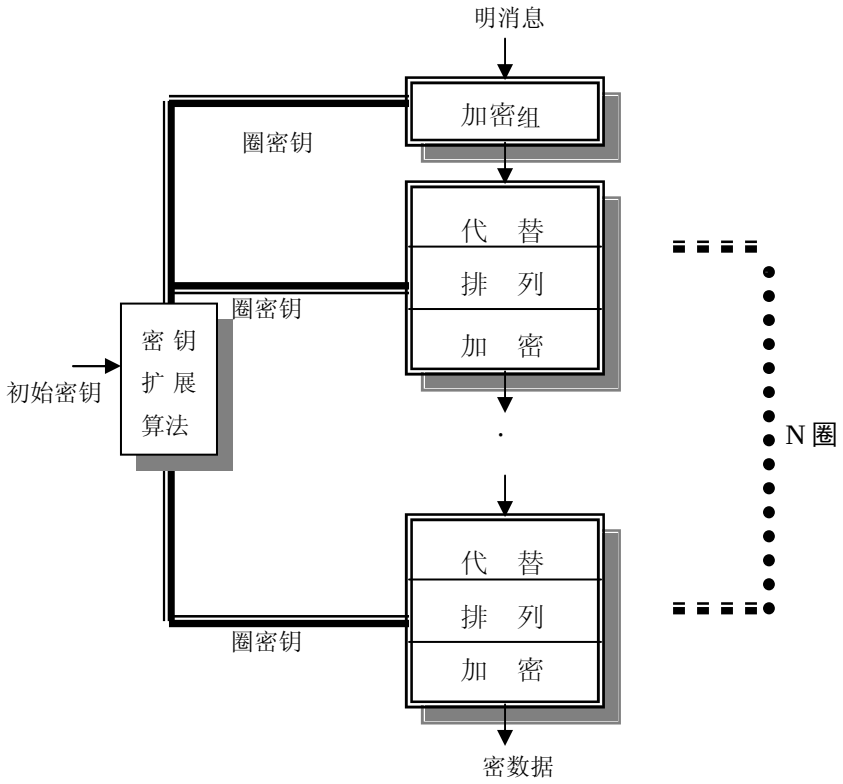


图 2-4 AES 总体结构

AES 仍基于香侬的混合与扩散原理[26][27]，设计初衷是尽可能简单，事实上，它确是一个非常简单的 S/P 网络结构密码。它在密码强度、运算速度、完成情况等

方面都有上乘的表现。

AES 对 128 比特分组，128、192、256 比特密钥进行运算，128 比特分组在加密过程中写成 4×4 字节的方块矩阵。加密迭代次数由 128 比特、192 比特、256 比特密钥分别确定为 10、12、14，在一圈密钥加法运算后，使用固定圈数的代替-排列网络运算（Substitution-Permutation Network, SPN）。其圈运算如图 2-5。加密可以描述为一串字节列的运算，其中一些运算可以在 GF（2^8）上描述，Rijndael 模多项式为 $X^8+X^4+X^3+X+1$。AES 由 10 至 14 圈 SPN 这样的运算组成，而且每圈的运算相同。

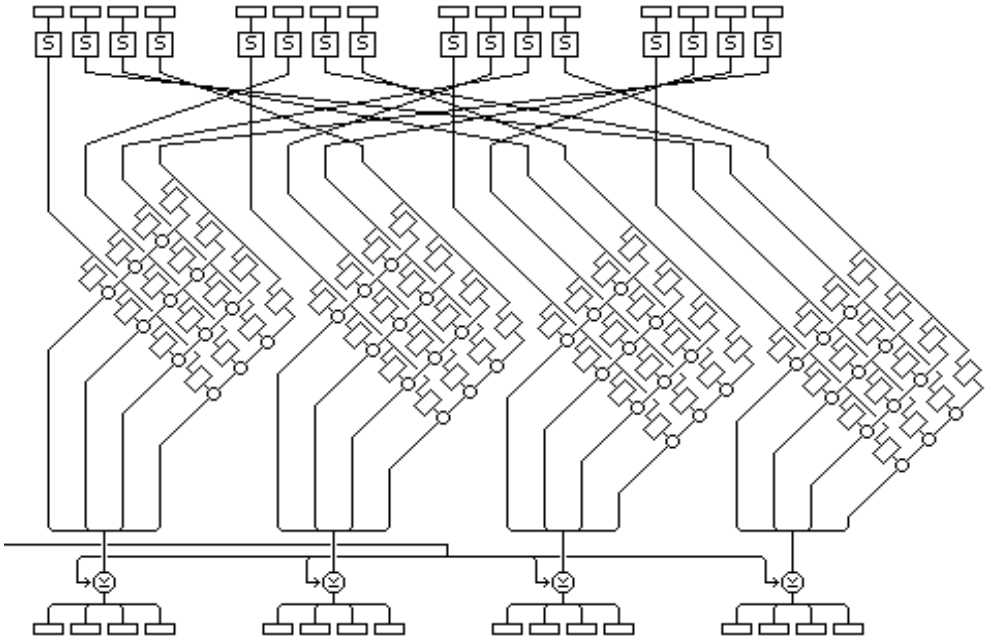


图 2-5 AES 轮函数

AES 算法包含 4 种面向字节的变换：

1、字节代替变换 SubBytes（）

$S_{ij} \rightarrow S_{ij}' = Sbox(S_{ij})$，$0 \le i, j < 4$ 其中 S 盒变换包括：任意 a、b、$c \in$ GF（2^8）

（1）逆运算 $b = a^{-1}$（$0 \rightarrow 0$）。

（2）仿射运算 $c_i = b_i + b_{(i+4)mod8} + b_{(i+5)mod8} + b_{(i+6)mod8} + b_{(i+7)mod8} + con$。

其中 con = ‘63’=“01100011”。

2、行移位变换 *ShiftRows*（）

$S_{ij} \rightarrow S_{ij}' = S_{i,(j+i)}$ $0 \le i, j < 4$。

3、列混合变换 MixColumns()

$S_{ij} \rightarrow S_{ij}'$ 的变换如下：$0 \le i, j < 4$

$$\begin{pmatrix} S_{0i}' \\ S_{1i}' \\ S_{2i}' \\ S_{3i}' \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} S_{0i} \\ S_{1i} \\ S_{2i} \\ S_{3i} \end{pmatrix} \quad (2\text{-}3)$$

4、轮密钥加密变换 AddRoundKey（）

$S_{ij} \rightarrow S_{ij} + W^r_{ij}$ ， $0 \le i, j < 4$，其中 $W^r \in GF(2^{128})$ 表示第 r 轮的轮密钥。

AES 密钥扩展算法，设初始密钥向量为 Nk 个字 $W_0W_1 \ldots W_{NK-1}$ ，其中：

$W_i = [W_{0i}, W_{1i}, W_{2i}, W_{3i}] \in GF(2^{32})\ 0 \le i \le Nk-1$

AES-128、AES-192 的密钥扩展算法：

$W_i = W_{i-Nk} + S(R(W_{i-1})) + [Rcon(i/Nk - 1), 00, 00, 00]$ 当 $i \equiv 0 \pmod{Nk}$

$W_i = W_{i-1} + W_{i-Nk}$ 否则

AES-256 扩展算法：

$W_i = W_{i-Nk} + S(R(W_{i-1})) + [Rcon(i/Nk - 1), 00, 00, 00]$ 当 $i \equiv 0 \pmod{Nk}$

$W_i = S(W_{i-1}) + W_{i-Nk}$ 当 $i \equiv 4 \pmod{Nk}$

$W_i = W_{i-1} + W_{i-Nk}$ 否则

其中，$R(a) = R([a_0, a_1, a_2, a_3]) = [a_1, a_2, a_3, a_0]$

$S(a) = [sbox(a_0), sbox(a_1), sbox(a_2), sbox(a_3)]$

$Rcon(i) = (x^i)_{m(x)}$

AES 加密过程 C 语言伪码表达如下（图 2-6）：

```
Rijndael(State, CipherKey)
// State 表示输入明消息，CipherKey 表示输出密数据
{
        KeyExpansion(CipherKey, ExpandedKey);
        AddRoundKey(State, ExpandedKey);
        For ( i=1; i<Nr; i++)
        Round(State, ExpandedKey+Nb×i);
        FinalRound(State, ExpandedKey+Nb×Nr);
}
```

图 2-6 AES 加密算法

上述算法中的 Key Expansion，可以预先进行计算出来，具体加密过程可以简化为（图 2-7）：

```
Rijndael(State,ExpandedKey)
//State 表示输入明消息
//ExpandedKey 表示每个 Round 使用的子密钥
{
    AddRoundKey(State,ExpandedKey);
    For( i=1 ; i<Nr ; i++ )
    {
        Round(State,ExpandedKey + Nb×i) ;
    }
    FinalRound (State, ExpandedKey + Nb×Nr);
}
```

图 2-7 AES 密钥扩展算法

各个子圈运算如下：

圈运算转换包含四个不同的步骤（如图 2-8）：

```
Round(State,RoundKey)
//State 表示输入明消息
//RoundKey 表示每个 Round 使用的子密钥
{
    ByteSub(State);
    ShiftRow(State);
    MixColumn(State);
    AddRoundKey(State,RoundKey);
}
```

图 2-8 AES 圈运算

AES 为了便于解密，最后一圈较其它圈有所区别。

算法中的最后一圈（如图 2-9）：

```
FinalRound(State,RoundKey)
//State 表示输入明消息，
//RoundKey表示每个Round使用的子密钥。
{
    ByteSub(State) ;
    ShiftRow(State) ;
    AddRoundKey(State,RoundKey);
}
```

图 2-9 AES 最后一圈运算

AES 有以下优点：

1、AES 可以嵌入在 Pentium 等计算机上，在表格大小与效率之间可以做取舍。

2、AES 可以实作在智能卡上，使用少量的 RAM，少量的程序代码；在 ROM 与效率之间可以进行优化。

3、在设计上，每圈的运算可并行处理。

4、加密不采用算术运算，不会因为不同处理器架构而有所偏差。

使用简单的设计完成安全强度要求高的算法[28]：

1、设计上不引用其它加密组件，如 S-box。

2、安全度不建立在一些分析不够明确的算术运算之上。

3、加密法紧凑，不易藏入陷门等程序代码。

2.3.2 Camellia

Camellia 是日本在新欧洲数字签名及加密活动（New Europe Scheme For Sigunature，Intergret and Encryption，NESSIE）中最后设计的分组密码算法，基于 128 比特分组、128、192、256 比特长度密钥，该算法最终获得认可。对 Camellia 的介绍将侧重于硬件实现模块，Camellia 的标准化进程也逐步完成，被大多数的国际组织采纳。

Camellia 分组密码算法设计目标是：

1、高强度的安全标准：算法设计能够抗差分分析、线性分析。Camellia 没有低于 2^{-128} 的差分或线性特征。同时，Camellia 的安全性能抗高阶差分分析[29]、插值分析[30]、相关密钥分析[31]、SLIDE 分析[32][33][34]、爆炸分析[35]、插值差

分分析[29][36]。

2、针对并行平台的高效运算：Camellia 设计分别适用于软件、硬件系统，包括门级硬件设计，SMART 卡的内存设计及并行平台设计。Camellia 包括 8 进 8 出代替表，逻辑操作能够有效的在多种平台上执行，这样对于低端 SMART 卡 8 比特处理器、PC 机的 32 比特、64 比特处理器都适用。但 Camellia 没有使用在 128 比特分组密码算法中常用的 32 比特整数加法和乘法，因为这类算法只便于软件实现。S 盒设计使得硬件尽可能小，4 个 S 盒仿射等价于 GF（2^8）上的逆变换。密钥变换简单，128 比特长度密钥由 32 字节 RAM 和 64 字节变换用于 192 比特和 256 比特 RAM。

3、标准化：2000 年，Camellia 设计之初既是定位于国际标准，按照 ISO/IECJTC1/SC 27 进行设计。

Camellia 算法的加解密硬件实现分为加/解密模块、密钥扩展模块、密钥表寄存器模块、输出寄存器模块四个部分，硬件实现时可运用。不妨设初始密钥为 K_L、K_R，中间密钥为 K_A、K_B。硬件开始执行时，首先把子密钥储存起来，子密钥分别由 K_L、K_A 逐轮计算，前两轮中，K_L 直接与中间结果进行异或。从第三轮开始，密钥针对 Feistel 网络结构进行变换。

图 2-10 是以加/解密速度为主要目的可编程门电路（Field Programmed Gata Array，FPGA）设计。

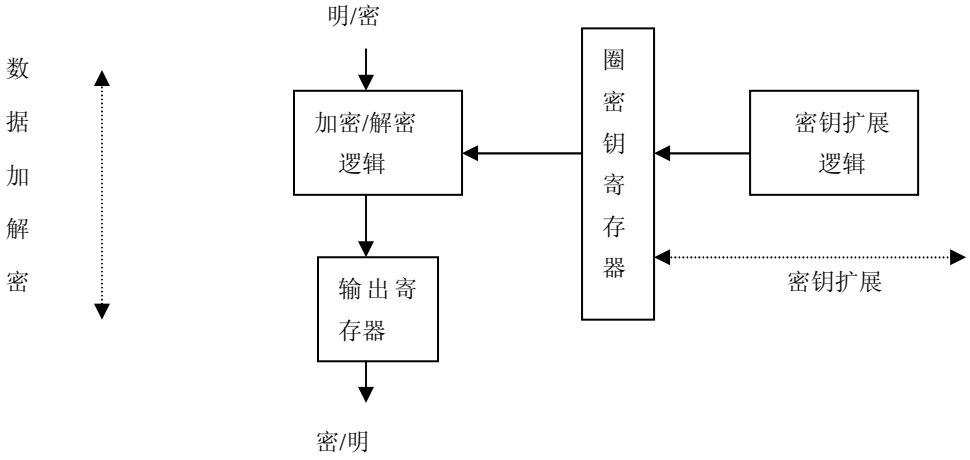


图 2-10 Camellia 算法加/解密硬件模块实现

密钥模块有 128 比特规模密钥和 192、256 比特规模密钥两种，运算如下：

128 比特密钥：

$$\begin{cases} (\text{右变换}) = F(K_{LL}, \sum_1) \\ (\text{左变换}) = F(K_{LR} \oplus (\text{右变换}), \sum_2) \end{cases} \tag{2-4}$$

192、256 比特密钥

$$\begin{cases} （右变换）= K_{RR} \oplus K_{RL}, \sum_1 ） \\ （左变换）= K_{RL} \oplus F（K_{LR} \oplus（右变换）, \sum_2 ） \end{cases} \quad （2\text{-}5）$$

其中常数为：

$\sum_{1(64)}$: 0xA09E667F3BCC908B

$\sum_{2(64)}$: 0xB67AE8584CAA73B2

$\sum_{3(64)}$: 0xC6EF372FE94F82BE

$\sum_{4(64)}$: 0x54FF53A5F1D36F1C

$\sum_{5(64)}$: 0x10E527FADE682D1D

$\sum_{6(64)}$: 0xB05688C2B3E6C1FD

密钥算法模块如图 2-11。

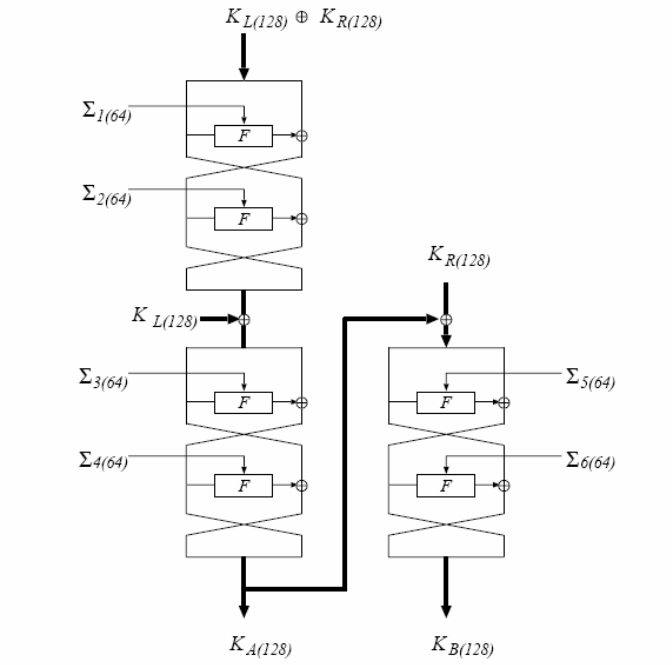


图 2-11 Camellia 密钥算法模块

K_L、K_R、K_A、K_B 不必保存，但生成子密钥时，需要保存旋转值。子密钥的值可以通过 16±1 比特的整数倍旋转来实现。如果使用的密钥不超过 128 比特，就不计算 K_B。F 函数的设计 E2[37]，E2 和 Camellia 的区别在于代替置换网络（Substitution-Permutation Network, SPN）采用的是 1 圈还是 2 圈。如果 1 圈 SPN

结构中采用的是 Feistel 网络，其抗线性分析、差分分析的理论安全性上界更加复杂，但是实际运算速度却加快。Camellia 包括基于比特的异或、与、或运算。

数据加密变换在 64 比特处理器上，实现 SP 运算可采用如下方法：

$SP_1(y_1) = (s_1(y_1), s_1(y_1), s_1(y_1), 0, s_1(y_1), 0, 0, s_1(y_1))$

$SP_2(y_2) = (0, s_2(y_2), s_2(y_2), s_2(y_2), s_2(y_2), s_2(y_2), 0, 0)$

$SP_3(y_3) = (s_3(y_3), 0, s_3(y_3), s_3(y_3), 0, s_3(y_3), s_3(y_3), 0)$

$SP_4(y_4) = (s_4(y_4), s_3(y_3), 0, s_4(y_4), 0, 0, s_3(y_3), s_3(y_3))$

$SP_5(y_5) = (0, s_2(y_5), s_2(y_5), s_2(y_5), 0, s_2(y_5), s_2(y_5), s_2(y_5))$

$SP_6(y_6) = (s_3(y_6), 0, s_3(y_6), s_3(y_6), s_3(y_6), 0, s_2(y_5), s_2(y_5))$

$SP_7(y_7) = (s_4(y_7), s_4(y_7), 0, s_4(y_7), s_2(y_5), s_2(y_5), 0, s_2(y_5))$

$SP_8(y_8) = (s_1(y_8), s_1(y_8), s_1(y_8), 0, s_1(y_8), s_1(y_8), s_1(y_8), 0)$

$$\bigoplus_{i=1}^{8} SP_i(y_i) \rightarrow (z_1', z_2', z_3', z_4', z_5', z_6', z_7', z_8')$$

对密码系统还可以采取如图 2-12 的实现方式，可以使加/解密芯片的面积达到最小。

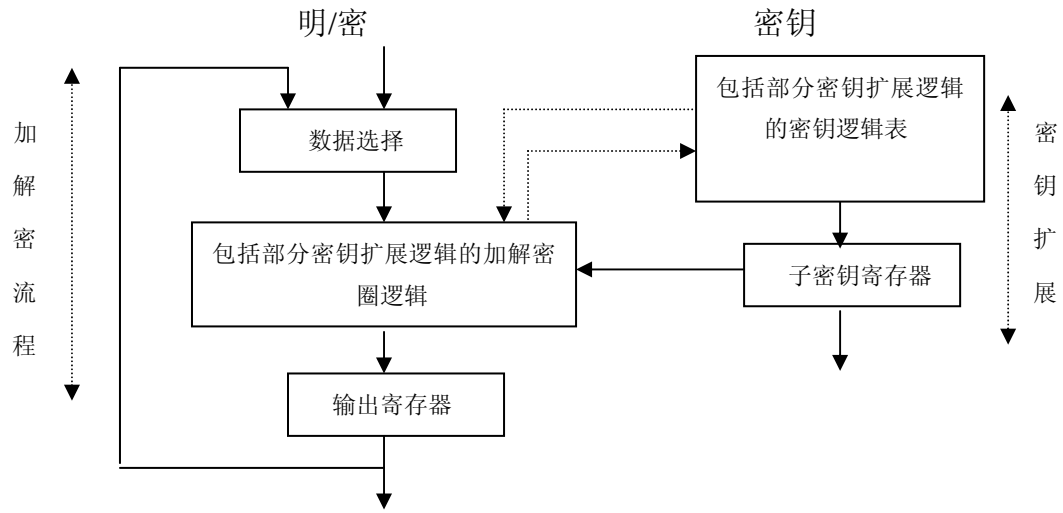


图 2-12 Camellia 算法加/解密硬件模块实现 2

图 2-13 的实现方式是子密钥直接写入 FPGA 内存的特殊情况，包括“输出寄存”、“子密钥内存”、“数据选择器”模块。“加/解密逻辑”模块包括：圈加密的循环结构；传送式结构设计；最优化 S 盒代替表设计，这样可以提高运算速度。具体硬件实现也与使用效果密切相关。

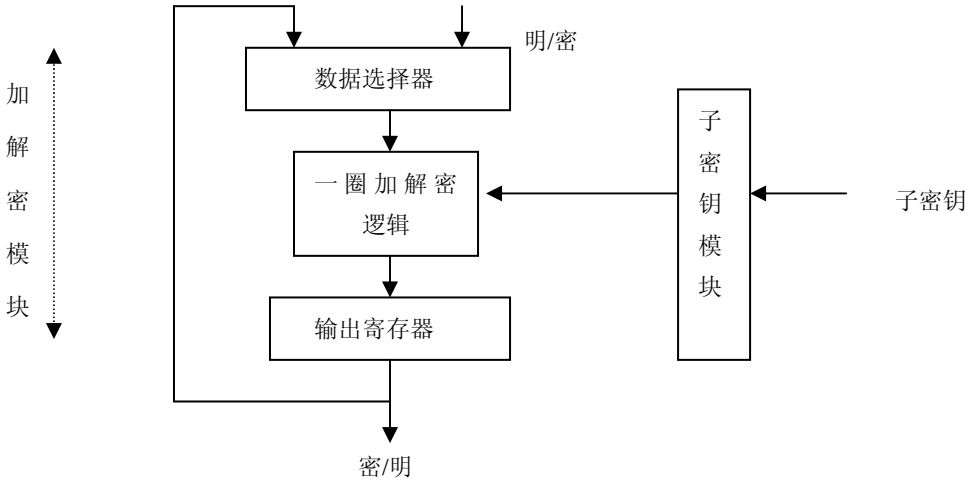


图 2-13 Camellia 算法加/解密硬件模块实现 3

如果不考虑硬件的逻辑结构，还可以使用传送结构来改进 FPGA 硬件设计以提高加/解密速度，如图 2-14。但是这种设计并没有考虑到反馈模式，如 CBC、CFB、OFB 等密码系统。

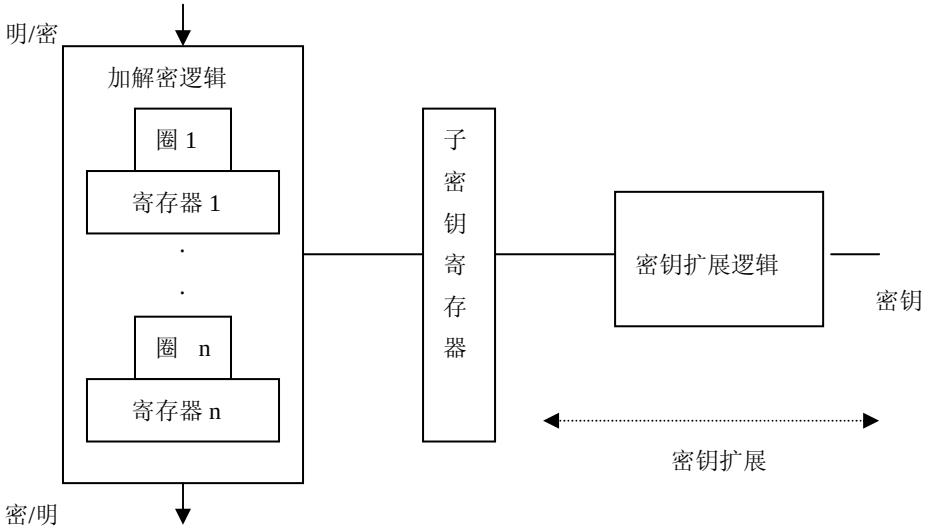


图 2-14 Camellia 算法加/解密硬件模块实现 4

Camellia 是典型的 Feistel 结构，其圈函数又带有 SP 结构的特征，是对两种结构的综合使用。从 Camellia 分组密码算法硬件结构设计可以看到：在硬件实现时，算法模块设计针对不同目的有不同的取舍。但是在算法安全前提下，提高运算速度是 INTERNET 对分组密码算法最基本的要求，工程上的细节能够使算法具备更强的实用性。

2.3.3 Anubis

Anubis 密码算法是巴西的 Paulo S.L.M Barret 和比立时的 Vincent Rijmen 所设计的分组密码算法，参选新欧洲数字签名活动。它是一个 128 比特分组，密钥长度可变的标准 SP 密码体制。解密运算仅仅在密钥方面与加密不同。Anubis 设计基于抗多种密码分析的策略。虽然最终没有成为 NESSIE 的推荐分组密码，但它的设计者在高级加密标准 Rijndeal 分组密码基础上有所前进，仍是一个值得关注的设计。

一、　Anubis 密码算法的总体结构如图 2-15：

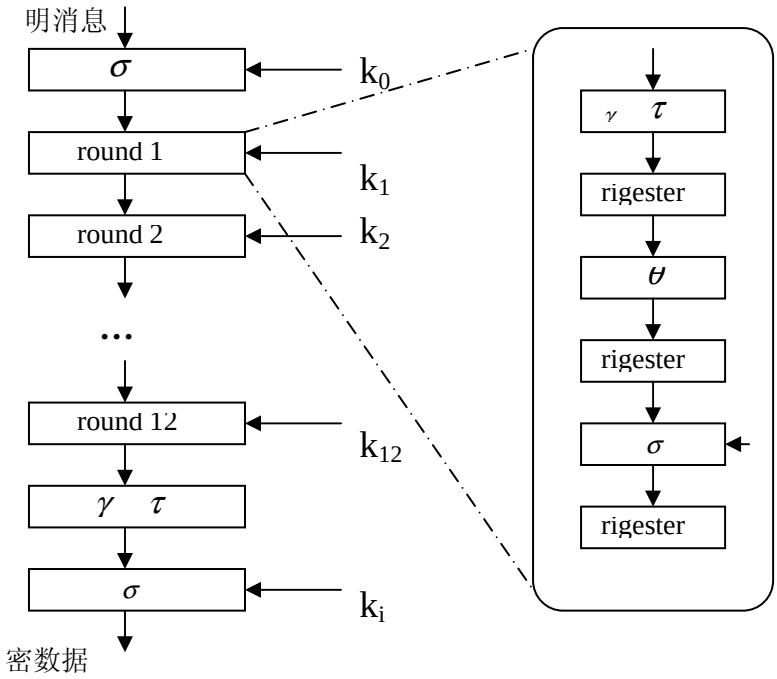


图 2-15 Anubis 分组密码算法结构图

其中每圈的函数结构为：$\rho(key)=\sigma_{key}(\theta(\tau(\gamma(x))))$

二、算法描述

阿力庇斯算法为回旋型分组密码算法，通过 128 比特分组、*32N*（*4≤N≤10*）可变密钥长度来进行独立的每轮加密，加密圈数为 12、13、14、15、16、17、18 可变。

1、输入、输出模块

128 比特的输入状态可以表示为 $M_{4\times4}$[GF（2^8）]上的矩阵，而密钥可以表示成为 $M_{N\times4}$[GF（2^8）]上的矩阵，128 比特初始状态通过映射与密钥对应。

μ：GF（2^8）^{4N} ，$M_{N\times4}$[GF（2^8）]及逆可实现上述功能。

$$\mu（a）=b \quad <=> \quad b_{ij}=a_{4i+j} \quad 0\le i\le N-1，0\le j\le 3$$

2、非线性变换 γ

函数 γ：$M_{N\times 4}[GF（2^8）]$，$M_{N\times 4}[GF（2^8）]$,$4\le N\le 10$，相当于一般分组密码的非线性代替 S 盒，$GF（2^8）$，$GF（2^8）$，$x\rightarrow S[x]$。

$$\gamma（a）=b \quad <=> \quad b_{ij}=S[a_{ij}] \quad 0\le i\le N-1，0\le j\le 3$$

S 盒是伪随机的，并且对于任意 $a\in GF（2^8）$，$S[S[a]]=a$。S 是一个置换。

3、τ 代替变换

τ 映射：$M_{4\times 4}[GF（2^8）]$,$M_{4\times 4}[GF（2^8）]$

$$\tau（a）=b \quad <=> \quad b_{ij}=a_{ji} \quad <=> \quad b=a^t，0\le i、j\le 3$$

4、线性混合层 θ

混合层 θ：$M_{N\times 4}[GF（2^8）]$，$M_{N\times 4}[GF（2^8）]$ $4\le N\le 10$，是基于[8，4，5]的可分最大距离码及生成矩阵 $G_H=[I\ H]$，

$$H=\begin{bmatrix} '01' & '02' & '04' & '06' \\ '02' & '01' & '06' & '04' \\ '04' & '06' & '01' & '02' \\ '06' & '04' & '02' & '01' \end{bmatrix}，\ 则：\theta（a）=b \quad <=> \quad b=a\cdot H$$

可以看出 H 是对称并且唯一的，所以 θ 是一个 $N=4$ 的回旋变换。

5、加乱函数 $\sigma[k]$

仿射加密函数 $\sigma[k]$ ：$M_{N\times 4}[GF（2^8）]$，$M_{N\times 4}[GF（2^8）]$，$4\le N\le 10$，密钥通过对应比特异或进行加密变换。

$$\sigma[k]（a）=b \quad <=> \quad b_{ij}=a_{ij}\oplus K_{ij} \quad 0\le i\le N-1，0\le j\le 3$$

6、圆排列 π

排列 π: $M_{N\times 4}[GF（2^8）]$ ，$M_{N\times 4}[GF（2^8）]$ $4\le N\le 10$

$$\pi（a）=b \quad <=> \quad b_{ij}=a_{(I-j)\ mod N,j} \quad 0\le i\le N-1，0\le j\le 3$$

7、密钥提取变换 ω

密钥提取函数 ω：$M_{N\times 4}[GF（2^8）]$，$M_{4\times 4}[GF（2^8）]$，$4\le N\le 10$ 是一个线性映射，基于[4+N，N，5]的 MDS 码，生成矩阵为 $G_v=[I\ V^t]$,$V=vdm_N$（‘01’，‘02’，‘06’，‘08’）

$$V=\begin{bmatrix} '01' & '01' & \cdots & '01' \\ '02' & '02'^1 & \cdots & '02'^{N-1} \\ '06' & '06'^1 & \cdots & '06'^{N-1} \\ '08' & '08'^1 & \cdots & '08'^{N-1} \end{bmatrix}$$ 因此：$\omega（a）=b <=> b=V\cdot a$

8、r 圈常数 C^r

r 圈常数是 $M_{N\times 4}[GF(2^8)]$，$4\le N\le 10$ 上的矩阵，定义为：

$$C^r_{0j}=S[4(r-1)+j], \qquad 0\le j\le 3,$$

$$C^r_{ij}=0, \qquad 0\le i\le N,\ 0\le j\le 3$$

9、密钥表

密钥表扩展密钥 $K\in GF(2^8)^{4N}$ $4\le N\le 10$ 为一系列密钥串，K^0，K^1，…，K^R，$K^r\in M_{N\times 4}[GF(2^8)]$：

$$k^0=\mu(K)$$

$$k^r=(\sigma[C^r]\cdot\theta\cdot\pi\cdot\gamma)(k^{r-1}),\ r>0$$

$$K^r=(\tau\cdot\omega\cdot\gamma)(k^r),\ 0\le r\le R$$

复合映射 $\psi(C^r)=\sigma[C^r]\cdot\theta\cdot\pi\cdot\gamma$，$\Phi\equiv\tau\cdot\omega\cdot\gamma$ 分别称作第 r 圈的密钥匙递归函数和密钥选择函数。初始变换 γ 仅简单用于计算 K^0，并非用于加密。

10、完整密码算法函数

Anubis 定义为密钥 $K\in GF(2^8)^{4N}$ 如下的变换，

$Anubis[K]: GF(2^8)^{16} \longrightarrow GF(2^8)^{16}$ 函数为：

$Anubis[K]\equiv\mu^{-1}\cdot\alpha_R[K^0,\ldots,K^R]\cdot\mu$，这里

$$\alpha_R[K^0,\ldots,K^R]=\sigma[K^R]\cdot\tau\cdot\gamma\cdot\left(\overset{r=R-1}{\underset{1}{O}}\sigma[K^r]\cdot\theta\cdot\tau\cdot\gamma\right)\cdot\sigma[K^0]$$

$32N$ 密钥加密的圈数为：$R=8+N$，$4\le N\le 10$。合成映射：

$\rho[K^r]=\sigma[K^r]\cdot\theta\cdot\tau\cdot\gamma$ 称为第 r 圈的圈函数。相应最后一圈映射 $\rho'[K^r]=\sigma[K^r]\cdot\tau\cdot\gamma$。

11、逆运算

Anubis 是一个回旋型分组密码，加密及逆运算区别仅在密钥的规模，以下给出几个定理：

引理 2-1：$\tau\cdot\gamma=\gamma\cdot\tau$

引理 2-2：$\theta\cdot\sigma[K^r]=\sigma[\theta(K^r)]$

定理 2-1：令 $\ddot{K}^0\equiv K^R$，$\ddot{K}^R\equiv K^0$，并且 $\bar{K}^r=\theta(K^{R-r})$，$0<r<R$，那么，

$$\alpha_R^{-1}[K^0,K^1,\ldots,K^R]=\alpha[\bar{K}^0,\bar{K}^1,\ldots,\bar{K}^R]$$

由此可见，Anubis 密码的解密运算仅仅在密钥表上有所不同。

虽然 NESSIE 的最终标准算法并没有包括 Anubis，但是设计人的影响力与对这个算法设计的初衷仍然准确地传达给了世界。而且，设计者在随后给出了 S 盒设计中的 TWIST 概念，使得该分组密码算法的非线性部分变化量与可选择性明显加强。

2.4 本章小结

本章介绍了分组密码算法的研究背景，相关概念、特点、常用结构和标准化内容。对本文的核心内容分组密码算法设计与评估现状进行了理论基础阐述，特别以 AES、Camellia、Aubis 为例从算法的框架、模块分析了目前几个重要的分组密码算法，分别通过软件伪 C 代码实现、硬件模块设计不同的侧重点讨论了上述算法的特征。对分组密码算法标准化及在不同网络环境下的使用情况做出概述。

第三章　分组密码算法设计与评估

分组密码是与计算机硬件、网络技术的发展息息相关的一类算法。从仅供商业和非国防性政府部门使用的 DES 开始，AES、NESSIE、ECRYPT 分组密码算法的设计与评估始终处于公开的状态。因此，对算法的分析成为全球密码学爱好者的共同目标，也是对算法评估的重要工具。分组密码算法的设计随着分析方法的进步而演变。

3.1 针对分组密码算法安全性评估

以下给出分组密码算法安全性评估中需要使用到的概念和基本定理。

定义 3-1：设 $X=(x_1,x_2,\cdots,x_n)\in GF^n(2)$，$W=(\omega_1,\omega_2,\cdots,\omega_n)\in GF^n(2)$，$X$ 和 W 的点积为：

$$W\cdot X=\omega_1x_1+\omega_2x_2+\cdots+\omega_nx_n \pmod 2 \qquad (3\text{-}1)$$

定义 3-2：$S_f(\omega)=1/2^n\cdot\sum_{x\in GF^n(2)} f(x)\cdot(-1)^{\omega\cdot x},\ \omega\in GF^n(2)$

$\{S_f(\omega)\mid \omega=0,1,2,\cdots,2^{n-1}\}$称为函数 $f(x)$ 的 Walsh 线性谱。显然，$S_f(\omega)$ 为 $GF^n(2)$ 到[-1，1]闭区间的一个映射。

$$S_{(f)}(\omega)=1/2^n\cdot\sum_{x\in GF^n(2)}(-1)^{f(x)+w.x},\ \omega\in GF^n(2) \qquad (3\text{-}2)$$

称为函数 $f(x)$ 的第二种 Walsh 变换，也称为 Walsh 循环谱。

引理 3-1：设 $W=(\omega_1,\omega_2,\cdots,\omega_n)\in GF^n(2)$ 是 n 维离散函数，则：

$$\sum_{x\in GF^n(2)}(-1)^{w.x}=\begin{cases}2^n, & \omega=0\\ 0, & \omega\neq 0\end{cases} \qquad (3\text{-}3)$$

证明：ω＝0 时，结论显然成立。

ω≠0 时，$W\cdot X=0$ 与 $W\cdot X=1$ 在 $GF^n(2)$ 中解的个数为 2^{n-2} 个，故 ω≠0 时，

$$\sum_{x\in GF^n(2)}(-1)^{w.x}=0$$

[证毕]

定理 3-1：设 $S_f(\omega)$ 和 $S_{(f)}(\omega)$ 分别是 n 元离散函数的 Walsh 线性谱和 Walsh 循

环谱，则他们之间有如下关系：

$$S_{(f)}(\omega) = \begin{cases} -2S_f(\omega), \omega \neq 0 \\ 1-2S_f(\omega), \omega = 0 \end{cases} \quad (3\text{-}4)$$

证明：由于 $(-1)^{W.X} = \begin{cases} 1, f(x)=0 \\ -1, f(x)=1 \end{cases} = 1-2f(x)$

故：$S_{(f)}(\omega) = 1/2^n \cdot \sum_{x \in GF^n(2)} (-1)^{f(x)+WX}$

$$= 2^{-n} \sum_{x \in GF^n(2)} [1-2f(x)](-1)^{f(x)+WX}$$

$$= 1/2^n \cdot \sum_{x \in GF^n(2)} (-1)^{WX} - 2 \cdot 2^{-n} \sum_{x \in GFn(2)} f(x) \cdot (-1)^{WX}$$

$$= \begin{cases} -2S_f(\omega), \omega \neq 0 \\ 1-2S_f(\omega), \omega = 0 \end{cases}$$

[证毕]

定理 3-2：设离散函数 $f(x)$，$X=(x_1,x_2,\cdots,x_n) \in GF^n(2)$ 的 Walsh 线性谱为 $S_f(\omega)$，Walsh 循环谱为 $S_{(f)}(\omega)$，则：

$$\sum_{x \in GF^n(2)} [S_f(\omega)]^2 = S_f(0) \quad (3\text{-}5)$$

$$\sum_{x \in GF^n(2)} [S_{(f)}(\omega)]^2 = 1 \quad (3\text{-}6)$$

证明：由 $S_f(\omega) = 1/2^n \cdot \sum_{x \in GF^n(2)} f(x) \cdot (-1)^{WX}$，则：

$$[S_f(\omega)]^2 = 2^{-2n} \cdot \sum_{x \in GF^n(2)} f(x) \cdot (-1)^{WX} \cdot \sum_{x \in GF^n(2)} f(y) \cdot (-1)^{WY}$$，令 $x+y=d$，

$$= 2^{-2n} \cdot \sum_{x \in GF^n(2)} \sum_{x \in GF^n(2)} (-1)^{Wd} \cdot f(x) \cdot f(x \oplus d)$$

$$\sum_{w \in GFn(2)} [S_f(\omega)]^2 = 2^{-2n} \cdot \sum_{x \in GF^n(2)} \sum_{x \in GF^n(2)} f(x) \cdot f(x \oplus d) \cdot \sum_{w \in GFn(2)} (-1)^{Wd};$$

由引理 3-1，可得：

$2^n \cdot \sum_{x \in GF^n(2)} [S_f(\omega)]^2 = \sum_{x \in GF^n(2)} f^2(x)$。令：$f(x) = (-1)^{f(x)}$，则：

$$\sum_{x \in GF^n(2)} [S_{(f)}(\omega)]^2 = 1$$

[证毕]

由定理 3-2 可知：Walsh 循环谱谱值一定有偏离 1/2 区间的情况。因此，离散

函数必然存在线性组合优势，只是优势大小会因为算法设计的不同而产生变化。Walsh 谱优势是直接导致密码算法产生信息泄露的原因。

3.1.1 对算法安全线性评估基本原理

密码算法线性分析（linear Cryptanalysis，LC）是 1993 年由日本人 M-Matsui 首先提出的，并有效的应用于 DES 分析。分组密码算法的线性分析是已知明消息的分析方法，其基本原理是通过寻找密码算法明消息、密数据与密钥之间的有效线性逼近式来破解密码系统。

密码算法线性分析的目的是寻找密码算法的线性逼近表达式。假设随机明消息 X、密钥 K 和相应的密数据 Y，它们对应的线性组合系数变量分别为：W、V、U，WX、UY、VK 表示变量之间的点积，则

$$WX \oplus UY = VK \tag{3-7}$$

即是密码算法的线性组合。如果（3-7）式成立的概率 P≠1/2，定义 $P'=|2P-1|$ 来刻画（3-7）式的有效性，此时，（3-7）称为密码算法有效线性逼近表达式。称取值最大的 P'为密码的最大线性偏差，该逼近式称为最佳线性逼近。

不妨假设明消息、子密钥变量是相互独立且均匀分布的。T 是 n 比特输入 m 比特输出的多输出函数，输入随机变量 $X \in Z_2^n$,输出为 $T(X) \in Z_2^m$，对于给定的 $W \in Z_2^n$、$V \in Z_2^m$，一个函数的线性偏差可以用多输出函数的广义循环 Walsh 谱来定义：

$$LP^T(V, W) = LP(WX \oplus VT(X)) = 2^{-n} \sum_{X \in Z_2^n} (-1)^{(WX \oplus VT(X))} \tag{3-8}$$

表示输入线性组合系数为 W、输出线性组合系数为 V 时函数 T 的线性偏差。

分组密码算法可看作输入为明消息、密钥，输出为密数据的多输出函数，当明消息 P、密钥 K、和对应的密数据 C 三者的线性组合系数分别为 W、U、V 时，密码的线性偏差记为：

$$LP(WP \oplus VK \oplus UC) = 2^{-(n+m)} \sum_{P \in Z_2^n, C \in Z_2^m} (-1)^{(WP \oplus VK \oplus UC)} \tag{3-9}$$

其中 n 为明消息长度，m 为密钥长度。

算法安全线性分析正是通过这样的线性逼近还原或相对还原分组密码算法。

3.1.1.1 Feistel 型分组密码算法线性偏差描述

对 Feistel 密码，记明消息及分组为 $P=(P_0, P_1)$，P_0 与 P_1 的长度为 e 比特，r 个长度为 e 比特的轮子密钥为 K_0、K_1、…、K_{r-1}，由密码的一轮迭代公式：

$$P_{i+2} = P_i \oplus F(P_{i+1} \oplus K_i) \qquad i=0，1，\ldots，r-1 \qquad (3\text{-}10)$$

得到 r 轮迭代后的输出为（P_r，P_{r+1}）。轮函数 F 是 e 比特输出的非线性函数。在 Feistel 密码设计中，为了保证加/解密结构一致，要采取密数据反序输出。

若明消息 P_0，P_1，子密钥 K_0，K_1，…，K_{r+1} 及 r 轮迭代后相应的输出为 P_r，P_{r+1} 的线性组合系数分别为：W_0，W_1，V_0，…，V_{r+1}，W_r，W_{r+1} 时，分组密码算法的线性偏差记为：

$$LP(W_0P_0 \oplus W_1P_1 \oplus V_0K_0 \oplus \ldots \oplus V_{r-1}K_{r-1} \oplus W_rP_r \oplus W_{r+1}P_{r+1}) \qquad (3\text{-}11)$$

以下将给出线性偏差的轮推导关系：

引理 3-2：$LP(W_0P_0 \oplus W_1P_1 \oplus V_0K_0 \oplus \ldots \oplus V_{r-1}K_{r-1} \oplus W_rP_r \oplus W_{r+1}P_{r+1}) = LP^F(W_{r+1}V_{r-1})\, LP(W_0P_0 \oplus W_1P_1 \oplus V_0K_0 \oplus \ldots \oplus V_{r-2}K_{r-2} \oplus W_{r+1}P_{r-1} \oplus (V_{r-1} \oplus W_r)P_r)$ （3-12）

证明：令 $a=2^{-e(r+2)}$，$a'=2^{-e(r+1)}$，i=0,1,…,r-1 则：

$$\begin{aligned}
&LP(W_0P_0 \oplus W_1P_1 \oplus V_0K_0 \oplus \ldots \oplus V_{r-1}K_{r-1} \oplus W_rP_r \oplus W_{r+1}P_{r+1}) \\
&= a \sum_{X_iK_i \in Z_2^e} (-1)^{(W_0P_0 \oplus W_1P \oplus V_0K_0 \oplus \cdots \oplus V_{r-1}K_{r-1} \oplus W_rP_r \oplus W_{r+1}P_{r+1})} \\
&= a \sum_{X_iK_i \in Z_2^e} (-1)^{(W_0P_0 \oplus W_1P \oplus V_0K_0 \oplus \cdots \oplus V_{r-1}K_{r-1} \oplus W_rP_r \oplus W_{r+1}(P_{r-2} \oplus F(P_r \oplus K_{r-1}))} \\
&= a \sum_{X_iK_i \in Z_2^e} (-1)^{(W_0P_0 \oplus W_1P \oplus V_0K_0 \oplus \cdots \oplus V_{r-1}K_{r-1} \oplus W_rP_r \oplus W_{r+1}P_{r-1} \oplus V_{r-1}X_r)} \sum_{K \in Z_2^e} (-1)^{(V_{r-1}(X_r \oplus K_{r-1}) \oplus W_{r+1}F(P_r \oplus K_{r-1}))} \\
&= LP^F(W_{r+1}，V_{r-1})\, a' \sum_{X_iK_i \in Z_2^e} (-1)^{(W_0P_0 \oplus W_1P \oplus V_0K_0 \oplus \cdots \oplus V_{r-2}K_{r-2} \oplus (W_r \oplus V_{r-1})X_r \oplus W_{r+1}P_{r-1})} \\
&= LP^F(W_{r+1}V_{r-1})\, LP(W_0P_0 \oplus W_1P_1 \oplus V_0K_0 \oplus \ldots \oplus V_{r-2}K_{r-2} \oplus W_{r+1}P_{r-1} \oplus (V_{r-1} \oplus W_r)P_r)
\end{aligned}$$

[证毕]

由上述引理，通过算法的 F 函数递推关系，可以推出：

定理 3-3：经过 r 轮迭代，Feistel 密码的线性偏差表达式为

1、当 r 为偶数，即 $r=2m$ 时，

$$\begin{aligned}
&LP(W_0P_0 \oplus W_1P_1 \oplus V_0K_0 \oplus \ldots \oplus V_{r-1}K_{r-1} \oplus W_rP_r \oplus W_{r+1}P_{r+1}) = \\
&\prod_{i=0}^{m-1} LP^F(W_r \oplus \sum_{j=i}^{m-1} V_{2j+1}, V_{2i}) \bullet \prod_{i=0}^{m-1} LP^F(W_{r+1} \oplus \sum_{j=i}^{m-2} V_{2j+2}, V_{2i+1}) \\
&\bullet LP((W_0 \oplus W_r \oplus \sum_{i=0}^{m-1} V_{2i+1})P_0 \oplus (W_1 \oplus W_{r+1} \oplus \sum_{i=0}^{m-1} V_{2i})P_1)
\end{aligned} \qquad (3\text{-}13)$$

2、当 r 为奇数，设 $r=2m+1$ 时

$$LP（W_0P_0 \oplus W_1P_1 \oplus V_0K_0 \oplus \ldots \oplus V_{r-1}K_{r-1} \oplus W_rP_r \oplus W_{r+1}P_{r+1}）=$$

$$\prod_{i=0}^{m-1} LP^F(W_{r+1} \oplus \sum_{j=i}^{m-1} V_{2j+1}, V_{2i}) \bullet \prod_{i=0}^{m-1} LP^F(W_r \oplus \sum_{j=i}^{m-2} V_{2j+2}, V_{2i+1})$$

$$\bullet LP((W_0 \oplus W_{r+1} \oplus \sum_{i=0}^{m-1} V_{2i+1})P_0 \oplus (W_1 \oplus W_r \oplus \sum_{i=0}^{m-1} V_{2i})P_1)$$

（3-14）

事实上，由于 P_0、P_1 相互独立、均匀分布，为使整体线性偏差不为 0，其线性组合必须为 0，上式中的系数关系可以化简为：

1、当 r 为偶数，即 $r=2m$ 时，

$$W_r = W_0 \oplus \sum_{i=0}^{m-1} V_{2i+1}，\ W_{r+1} = W_1 \oplus \sum_{i=0}^{m-1} V_{2i} \qquad （3\text{-}15）$$

2、当 r 为奇数，设 $r=2m+1$ 时

$$W_{r+1} = W_0 \oplus \sum_{i=0}^{m-1} V_{2i+1}，\ W_r = W_1 \oplus \sum_{i=0}^{m-1} V_{2i} \qquad （3\text{-}16）$$

代入定理 3-3 的表达式，有：

定理 3-4：对 r 轮迭代的 Feistel 密码，其线性偏差的表达式为：

1、当 r 为偶数，即 $r=2m$ 时，

$$LP（W_0P_0 \oplus W_1P_1 \oplus V_0K_0 \oplus \ldots \oplus V_{r-1}K_{r-1} \oplus W_rP_r \oplus W_{r+1}P_{r+1}）$$

$$= \prod_{i=0}^{m-1} LP^F(W_0 \oplus \sum_{j=0}^{i-1} V_{2j+1}, V_{2i}) \bullet \prod_{i=0}^{m-1} LP^F(W_1 \oplus \sum_{i=0}^{m-1} V_{2j}, V_{2i+1}) \qquad （3\text{-}17）$$

并且 $W_r = W_0 \oplus \sum_{i=0}^{m-1} V_{2i+1}$，$W_{r+1} = W_1 \oplus \sum_{i=0}^{m-1} V_{2i}$　以避免分组密码算法的线性偏差为零。

2、当 r 为奇数，设 $r=2m+1$ 时

$$LP（W_0P_0 \oplus W_1P_1 \oplus V_0K_0 \oplus \ldots \oplus V_{r-1}K_{r-1} \oplus W_rP_r \oplus W_{r+1}P_{r+1}）$$

$$= \prod_{i=0}^{m-1} LP^F(W_0 \oplus \sum_{j=0}^{i-1} V_{2j+1}, V_{2i}) \bullet \prod_{i=0}^{m-1} LP^F(W_1 \oplus \sum_{i=0}^{m-1} V_{2j}, V_{2i+1})$$　并且

$W_{r+1} = W_0 \oplus \sum_{i=0}^{m-1} V_{2i+1}$，　$W_r = W_1 \oplus \sum_{i=0}^{m-1} V_{2i}$　避免分组密码的线性偏差为零。

定理 3-3 与定量是等价的，*r* 轮迭代的 Feistel 型分组密码算法的线性偏差是 *r* 项轮函数 *F* 的线性偏差的乘积，定理 3-3 表出的是输出线性组合系数和子密钥组合系数的函数；定理 3-4 中表出的是输入线性组合系数和子密钥组合系数的函数。由于分组密码算法的对称性，定理 3-3 和定理 3-4 分别是子密钥按加密和解密的顺序放置，而输入与输出的线性组合系数对换。从形式上来看，定理 3-4 的表达方式更为简洁。

3.3.1.2 SP 型分组密码算法线性偏差描述

SP 网络的明消息输入没有经过分组，设 *e* 比特明消息为 P_0，*r+1* 个长度为 *e* 比特的圈子密钥为 K_0，K_1，…，K_r，则分组算法的一圈迭代表出为：

$$X_{i+1} = F（X_i \oplus K_i） \quad I = 0，1，…，r-1 \tag{3-18}$$

那么，*r* 轮迭代后的输出为 X_r ，由于 SP 结构局部有逆，在最后一轮中进行一次状态 X_r 与子密钥的异或作为出口处理，输出密数据 C 为 $X_r \oplus K_r$ 。设明消息 P_0 、子密钥 K_0，K_1，…，K_{r-1}，K_r 和 *r* 轮迭代后相应的密数据 $C=X_r \oplus K_r$ 的线性组合系数分别为 W_0，V_0，…，V_{r-1}，V_r，W_r 时，记该算法的线性偏差为：

$$LP（W_0P_0 \oplus V_0K_0 \oplus … \oplus V_{r-1}K_{r-1} \oplus V_rK_r \oplus W_r（P_r \oplus K_r））$$

把一轮 *F* 函数代入线性偏差，得到

引理 3-3：SP 型分组密码算法

$$LP（W_0P_0 \oplus V_0K_0 \oplus … \oplus V_{r-1}K_{r-1} \oplus V_rK_r \oplus W_r（P_r \oplus K_r））$$

$$=LP^F（W_r,V_{r-1}）LP（W_0P_0 \oplus V_0K_0 \oplus … \oplus V_{r-1}K_{r-1} \oplus （V_r \oplus W_r）K_r） \tag{3-19}$$

证明：令 $a=2^{-e(r+1)}$，$a'=2^{-er}$，i=0,1,…,r-1 则：

$$LP（W_0P_0 \oplus V_0K_0 \oplus … \oplus V_{r-1}K_{r-1} \oplus V_rK_r \oplus W_r（P_r \oplus K_r））$$

$$=a \sum_{X_iK_i \in Z_2^e} (-1)^{(W_0P_0 \oplus V_0K_0 \oplus \cdots \oplus V_{r-1}K_{r-1} \oplus V_rK_r \oplus W_r(P_r \oplus K_r))}$$

$$=a \sum_{X_iK_i \in Z_2^e} (-1)^{(W_0P_0 \oplus V_0K_0 \oplus \cdots \oplus V_{r-1}K_{r-1} \oplus W_rF(P_{r-1} \oplus K_{r-1}) \oplus (V_r \oplus W_r)K_r)}$$

$$=a \sum_{X_iK_i \in Z_2^e} (-1)^{(W_0P_0 \oplus V_0K_0 \oplus \cdots \oplus V_{r-1}K_{r-1} \oplus (W_r \oplus V_r)K_r)} \sum_{K \in Z_2^e} (-1)^{(V_{r-1}(P_{r-1} \oplus K_{r-1}) \oplus W_rF(P_{r-1} \oplus K_{r-1}))}$$

$$=LP^F(W_r，V_{r-1})\, a' \sum_{X_iK_i \in Z_2^e} (-1)^{(W_0P_0 \oplus V_0K_0 \oplus \cdots \oplus V_{r-2}K_{r-2} \oplus (W_r \oplus V_r)K_r \oplus V_{r+1}P_{r-1})}$$

$$=LP^F（W_r, V_{r-1}）LP（W_0P_0 \oplus V_0K_0 \oplus … \oplus V_{r-2}K_{r-2} \oplus V_{r-2}P_{r-1} \oplus （V_r \oplus W_r）K_r）$$

[证毕]

根据上述引理中 *F* 函数的递归关系，容易得到如下定理：

定理 3-5：r 轮的 SP 网络密码线性偏差表达式为：

$$LP（W_0P_0 \oplus V_0K_0 \oplus \ldots \oplus V_{r-1}K_{r-1} \oplus V_rK_r \oplus W_r（P_r \oplus K_r））$$

$$=LP^F（W_r，V_{r-1}）\cdot \prod_{i=0}^{r-2} LP^F(V_{i+1},V_i) \bullet LP((W_0 \oplus V_0)X_0 \oplus (W_r \oplus V_r)K_r) \quad (3\text{-}20)$$

其中最后一项是线性函数的线性偏差，由于变量 X_0 和 K_r 相互独立且均匀分布，如果整体偏差值不为 0，其线性组合系数必须为 0，即有：

$W_0 = V_0$ ，$W_r = V_r$ 代入定理 3-5

定理 3-6：r 轮迭代 SP 网络密码的线性偏差表达式为

$$LP（W_0P_0 \oplus V_0K_0 \oplus \ldots \oplus V_{r-1}K_{r-1} \oplus V_rK_r \oplus W_r（P_r \oplus K_r））$$

$$=\prod_{i=0}^{r-1} LP^F(V_{i+1},V_i) \quad (3\text{-}21)$$

并且有 $W_0 = V_0$ ，…，$W_r = V_r$，否则，密码的线性偏差为 0

由定理 3-5、定理 3-6 可以得到 r 轮迭代的 SP 网络密码线性偏差可以表示为 r 项轮函数 F 线性偏差的乘积。

以上给出了 Feistel 型、SP 型分组密码算法的线性偏差数学表出式。

3.1.2 最大线性偏差

考虑在分组密码算法中，唯密数据分析的情况：由于离散空间上针对算法的 Walsh 循环谱谱值总会出现随机偏离现象，如果关于明消息、密钥、密数据的离散函数偏离度达到一定水平 T，并且数据量足够丰富时，根据 T 值的测定，能够判断密钥的取值。通过线性分析，当信息泄漏超过标准，算法和密钥会被相对还原。因此，评估一个分组密码算法的安全强度时，T 值起到一个标准的作用。规定 T 的一个容忍范围，超出范围说明算法抗线性分析能力不强。

定理 3-7：二元离散空间上随机变量 ξ 服从二点分布。如果 ξ 是参数为（u，σ^2）的正态分布，其概率密度函数为：

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left\{-\frac{(x-u)^2}{2\sigma^2}\right\} \quad (3\text{-}22)$$

如果 $u=0$，$\sigma=1$，称 ξ 服从标准正态分布。

定义 3-3：偏离值 $T = |p-q| \times \sqrt{N} = |2p-1| \times \sqrt{N}$ （3-23）

通过定理 3-7、定义 3-3，对 T 进行标准化。

定理 3-8：在分组密码算法公开的条件下，分析明消息 M，密数据 C，密钥 K 之间的偏离值最小的线性表达式，设 S、T、W 分别表示 M、C、K 的系数，对以 XOR 方式结合的算法显然存在：

$$SM \oplus TC = WK \tag{3-24}$$

由（3-23）式（3-24）式、定理 3-4 可知：最坏情况下，在中间人唯密数据线性分析时，信息泄漏量可以作为还原密钥的判断条件。

定理 3-9：如果随机选取的 M、C、K 使等式（3-24）成立的概率 p 不随机，在 M、C 对总量为 N 时，偏离值 $|T|$ 表达式称为该密码算法的线性逼近，当 $|T|$ 值达到最大，称为最大线性偏差，此时的线性逼近为最佳线性逼近。当最佳线性逼近存在，仅从密数据将测试到密钥的信息泄漏；如果算法已知，可以通过明消息、密数据得到密钥信息。

3.1.2.1 最大线性偏差评估法及方法

由于分组密码算法的线性偏差可以表出为各个轮函数偏差的乘积，要使线性偏差取最大值，则表达式中的轮函数线性偏差有效项数尽可能多。约定输入、输出线性组合系数不为 0 的项数为活动项，均为 0 称为平凡项。因为输入、输出线性组合系数同时取 0 的项的系数尽可能多时，线性偏差值才不为 0；否则，如果仅其中之一为 0，那么线性偏差为 0。所以为使线性偏差达到最大，输入、输出的线性组合系数均不为零的系数要尽可能少。

确定分组密码算法线性偏差上界的关键在于求取最少轮函数活动项数——可以通过求线性方程组最小重量解的方法解决。求取最小重量解的方法可以通过计算机穷尽，利用对矩阵进行初等变换的方式实现：

将分组密码算法线性偏差表达式如定理 3-3、定理 3-5 表为输入明消息和密钥线性组合系数的线性组合，得到一个线性矩阵。穷尽假设分组密码算法线性偏差表达式中各线性偏差项中的活动项与平凡项。用平凡项对应的向量通过初等变换去化简活动项向量，若可将任一活动项对应的输入或输出系数化简为 0，说明假设错误，否则假设正确。在穷尽假设中，采取活动项数从小到大的顺序，一旦出现正确假设，此时的活动项数即为最少活动项数。

求最大线性偏差的具体方法如下：

1、按照各乘积项系数写出输入、输出组合系数各比特由明消息和密钥线性组合系数表示的向量，组成系数矩阵 B。实际上，对 i 比特输入 j 比特输出的函数来说，每个线性偏差项的输入或输出组合系数对应矩阵 B 中的某 i 或 j 行向量。

$$B = \begin{bmatrix} b_{0,0} & b_{0,1} & \cdots & b_{0,n-1} \\ b_{1,0} & b_{1,1} & \cdots & b_{1,n-1} \\ \cdots & \cdots & \ddots & \cdots \\ b_{m-1,0} & b_{m-1,1} & \cdots & b_{m-1,n-1} \end{bmatrix} \quad (3\text{-}25)$$

2、将矩阵 B 按假设的活动项和平凡项分割为两个矩阵。

平凡矩阵为

$$C = \begin{bmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,n-1} \\ c_{1,0} & c_{1,1} & \cdots & c_{1,n-1} \\ \cdots & \cdots & \ddots & \cdots \\ c_{i-1,0} & c_{i-1,1} & \cdots & c_{i-1,n-1} \end{bmatrix} \quad (3\text{-}26)$$

活动项矩阵为：

$$D = \begin{bmatrix} d_{0,0} & d_{0,1} & \cdots & d_{0,n-1} \\ d_{1,0} & d_{1,1} & \cdots & d_{1,n-1} \\ \cdots & \cdots & \ddots & \cdots \\ d_{n-i-1,0} & d_{n-i-1,1} & \cdots & d_{n-i-1,n-1} \end{bmatrix} \quad (3\text{-}27)$$

3、通过初等变换，将矩阵 C 化简为上三角矩阵 C’

$$C' = \begin{bmatrix} 1 & \cdots & 0 & \cdots & \cdots \\ 0 & \ddots & 0 & \cdots & \cdots \\ 0 & \cdots & 1 & \cdots & \cdots \\ 0 & \cdots & 0 & \cdots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 \end{bmatrix} \quad (3\text{-}28)$$

4、用矩阵 C’中的非零行向量去化简矩阵 D 的行向量，矩阵 D 自身不进行化简。如果矩阵 D 中某个输入或输出组合系数对应的几个行向量全部被化简为零，则假设错误，否则，假设正确。

3.1.2.2 最大线性偏差搜索算法

分组密码算法线性分析的关键在于寻找最大线性偏差和最佳线性逼近，但由于分组密码算法的分组长度大且加密轮数多，寻找最大线性偏差经常是密码年会讨论的重点，但有效的、能应用于实际的搜索算法并不多。

1994 年 M.Matsui 在欧洲密码年会上发表了一篇论文，提出了一种最大线性偏差的搜索算法[38]，以 DES 密码为例给出了计算机实现步骤。

引理 3-3[39]堆积引理：设 X_i（$1 \le i \le n$）是独立的随机变量，它的取值为 0 的概率是 P_i，为 1 的概率是 $1—P_i$，记 $P_i' = |2P_i-1|$ ，则：$X_1 \oplus X_2 \oplus \ldots \oplus X_n = 0$ 的概率

为：

$$1/2 + 2^{n-1}\prod_{i=1}^{n}(p_i - 1/2) \qquad (3\text{-}29)$$

线性偏差为 $\prod_{i=1}^{n} P_i'$

设 P_i、C_i、K_i 为随机变量，ΓP_i，ΓC_i,ΓK_i 表示变量 P_i、C_i、K_i 的组合系数，用符号 $P_i \cdot \Gamma P_i$ 表示 P_i 与 ΓP_i 的点积。定义：

$$（\Gamma P_i，\Gamma C_i）= |2P_r\{（P_i \cdot \Gamma P_i）= F（P_i，K_i）\cdot \Gamma C_i \}—1| \qquad (3\text{-}30)$$

$$[P_1，P_2，\ldots，P_r]= \prod_{i=1}^{t} P_i \qquad (3\text{-}31)$$

$$B_n = \max_{TY_i = TY_{i-2} \oplus Tx_{I-1}(3 \le I \le N)} [（\Gamma P_1，\Gamma C_1），（\Gamma P_2，\Gamma C_2），\ldots，（\Gamma P_n，\Gamma C_n）] \qquad (3\text{-}32)$$

事实上，组合系数的变化情况正是随分组密码算法的轮函数变化而变化的，如图 3-1。由堆积引理，分组密码算法的线性偏差为 $\prod_{i=1}^{n} P_i$ 。

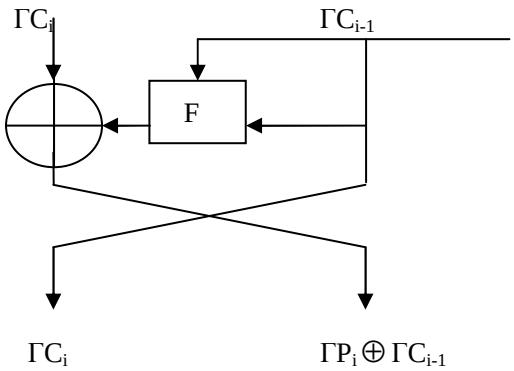


图 3-1 Feistel 结构线性偏差变化图

具体的搜索方法是一种归纳算法，搜索程序以加密轮数 n 从小到大的顺序执行，要求取 n 轮的最大线性偏差 B_n，需要求得 i 轮的最大线性偏差 B_i（$1 \le i \le n-1$）。一般说来，三轮以下的最大线性偏差容易得到，可以从 $n=4$ 开始。同时该方法还需要给定 B_n 的初始值 $\underline{B_n}$，虽然对满足 $\underline{B_i} \le B_i$（$1 \le i \le n-1$）中任意的 $\underline{B_i}$ 可以得到最后结果，但它的取值直接影响到搜索最大线性偏差的速度。如果值选取得过小，会影响到搜索最大线性偏差的速度。

通常的办法是选取特殊值得到一个 n 轮最大线性偏差，作为初始值 $\underline{B_i}$：

第一轮算法流程：

对每个候选的 ΓC_1，

令 $P_1=\max_{TX}(\Gamma C_1,\Gamma P)$；　　（3-33）

如果满足$[P_1，B_{n-1}]\geq \underline{B}_n$，进入第二轮流程。

第二轮流程：

对每个候选的 ΓC_2，ΓP_2，

令 $P_2=(\Gamma C_2,\Gamma P_2)$，　　（3-34）

如果满足$[P_1，P_2，B_{n-2}]\geq \underline{B}_n$，进入第二轮流程。

返回到上一轮流程。

第 i 轮流程（$3\leq i\leq n-1$）

对每个候选的 ΓP_i ，

令 $\Gamma C_i=\Gamma P_{i-1}\oplus \Gamma C_{i-2}, P_i=(\Gamma C_i,\Gamma P_i)$　　（3-35）

如果满足$[P_1，P_2，\ldots，P_i，B_{n-i}]\geq \underline{B}_n$（$1\leq i\leq n$），进入下一轮流程。

返回到上一轮流程。

在第 n 轮程序中，一旦出现一个更大的线性偏差值，就改写初始值 $\underline{B}_n$。流程结束时，$\underline{B}_n$ 就是 n 轮最大线性偏差 B_n。

由于 ΓP_i 和 ΓC_i 的取值范围非常大，采取穷尽的方法难以实现，按照 ΓP_i 和 ΓC_i 大小顺序的方法可以避免反复计算。

K-Ohta 等人提出了搜索方法的改进版本，降低了搜索复杂度。

方法 1：等价候选者

由于 DES 密码的对称性，其加密和解密算法的结构是一致的，不同的只是子密钥的使用顺序。在求取 n 轮的最大线性偏差时，n 轮的一组组合系数值确定，则线性偏差值也相应地确定。对所有 $i(1\leq i\leq n)$，将第 i 轮 F 函数的组合系数 ΓP_i 和 ΓC_i 替换为第（$n-i+1$）轮 F 函数的组合系数 ΓP_{n-i+1} 和 ΓC_{n-i+1} 所得到的线性偏差值必然相同，在流程中可以省略其中的一种情况，使运算量降低一半。

方法 2：不可能候选者

在 Matsui 的搜索算法中，由满足式$[P_1，P_2，\ldots，P_i，B_{n-i}]\geq \underline{B}_n$（$1\leq i\leq n$）求得的一组线性偏差值（$P_1，P_2，\ldots，P_n$）必然满足以下不等式组：

$$[P_2，P_3，\ldots，P_n]\leq \underline{B}_{n-1} \qquad (3\text{-}36)$$

$$[P_3，P_4，\ldots，P_n]\leq \underline{B}_{n-2} \qquad (3\text{-}37)$$

$$[P_n]\leq \underline{B}_1 \qquad (3\text{-}38)$$

这些不等式说明，对任意的 r<n ，如果一组候选组合系数对应的线性偏差值满足如下不等式，那么该组组合系数就不必穷尽。

$$[P_i，P_{i+1}，\ldots，P_{i+r-1}]>B_r \quad (1\leq i\leq n，i+r-1<n) \qquad (3\text{-}39)$$

这种改进方法利用了密码学的特征，也运用了一些程序上的技巧以提高效率。

改进方法在该问题的思想上并没有多少突破，而且对于分组大的算法，计算量过大，不能实施。从密码学的不同角度来看，分组密码算法的线性分析关键在于寻找最大线性偏差。但从密码分析角度来看，必须要求出最大线性偏差和最佳线性逼近。目的是在最大线性偏差足够大的情况下，利用明消息、密数据和密钥之间的有效线性逼近关系，在已知一定数量明密对的条件下获取部分密钥信息。分组密码算法的安全性分析要求该密码算法能够抵抗线性分析，证明线性偏差足够小，不必求得准确的最大线性偏差值和最佳线性逼近式。显然，上界值越接近最大线性偏差值越好，这样有利于算法设计中各个参数特别是加密轮数的选择，保证密码算法既安全又高速。对于分组长度大的加密算法分析，SLIDE 分析是不错的选择。在唯密数据分析时，通过对数据的仿真，可以及时发现算法的字节信息泄露。

3.1.3 针对算法安全非线性评估原则

密码算法差分分析（Differential Cryptanalysis, DC）是 1990 年由 Eli Biham 和 Adi Shamir 针对 DES 提出的分析方案。虽然 DES 的设计者说他们早已掌握这种方法，由于 NSA 的反对，没有公之于众。利用这种方法，Biham 和 Shamir 找到了一个选择明消息的 DES 分析方法，该方法比穷举分析有效，特别对于减轮的 DES，此方法可以很快分析成功。密码算法差分分析虽然是针对 DES 提出的，但它对其他类似有固定 S 盒的密码算法同样有效，它是迄今已知的分析迭代分组密码算法体制最有效的方法之一。自差分密码分析方法提出以来，每一个分组密码算法设计者都把能否抵抗差分分析作为衡量一个分组密码体制的安全性的重要指标。1991 年，来学嘉、James L. Massey 与 Sean Murphy 提出了马尔科夫密码（Markov Cipher，MC）的思想：若迭代密码算法是马尔科夫密码算法且子密钥统计独立，那么每轮的输出差分序列构成一条马尔科夫链，这是对密码算法差分分析的重要补充。在差分分析的基础上，密码学家又提出了许多新的差分类分析方法，如截断差分密码分析、不可能差分密码分析、高阶差分密码分析、Bommerang 分析等，这些方法对许多密码算法是有效的分析方法。具体评估结论需要视测试环境及测试要求而定。

3.1.3.1 差分密码分析的基本原理

对分组密码算法中分组长度为 n 的 r 轮迭代，将两个明消息或密数据的差定义为：

$$\Delta X_i = X_i \oplus X_i',\ 其中，\ \Delta X_i \ 、\ X_i \ 、\ X_i' \in Z^{2^n}，0 \le i \le r$$

若记第 i 轮的子密钥为 K_i，轮函数为 F，则 $X_i=F（X_{i-1},K_i）$

定义 3-4[22]：r-轮差分特征（r Round Differential Characteristic，rRDC）Ω_r 是一个差分序列，$\Omega_r=（\alpha_0，\alpha，\alpha_1，\ldots，\alpha_r）$，$\alpha_0$ 是明消息对 P_0 、 P_0'的差分，α_i 是密数据对 C_i 、 C_i'的差分（$1 \le i \le r$）。

定义 3-5[22]若 r-轮差分特征 $\Omega_r=（\alpha_0，\alpha，\alpha_1，\ldots，\alpha_r）$ 满足：明消息对 P_0 、P_0'的差分，α_i 是密数据对 C_i 、 C_i'的差分（$1 \le i \le r$），则称明消息对 P_0 、 P_0'的差分差分特征 Ω_r 是正确对，否则称是错误对。

定义 3-6：r-轮差分特征 Ω_r 的概率是指在明消息 X_0 和子密钥 K_1、K_2、…、K_r 独立，均匀随机分布时，明消息对 P_0 、 P_0'的差分为 α_0 的条件下，第 i（$1 \le i \le r$）轮输出 C_i 、 C_i'的差分为 α_i 的概率，记作：$P^{\omega_r} = d(\alpha_0,\alpha,\alpha_1,\alpha_2,\cdots,\alpha_r) = P（\Delta X_r=\alpha_r，\ldots，\Delta X_1=\alpha_1 | \Delta X_0=\alpha_0）$ (3-40)

设 Ψ 是 n 比特输入、m 比特输出的非线性变换，记为 y=Ψ（x）,用符号

dΨ（α，β）= P（⊿Y=β|⊿X=α）表示 Ψ 的输入输出差分概率，其中 ⊿X 为输入差分，⊿Y 为输出差分，简化记为 dΨ（⊿X，⊿Y）表示 Ψ 的输入输出差分概率。由概率的定义，其数学关系式可表示为：

$$d_\Psi（\Delta X，\Delta Y）= 2^{-n}\sum_x \delta（\Delta Y \oplus \Psi（x）\oplus \Psi（x \oplus \Delta X））\qquad （3\text{-}41）$$

其中：

$$\delta(x)=\begin{cases}1, x=0\\ 0, x=1\end{cases}，是\ \text{Kronecker delta}\ 函数$$

在 Ψ 明确的情况下，也用 $d(\Delta X，\alpha,\Delta Y)$表示 Ψ 的输入输出差分概率。

若记第 i-轮差分的概率为：

$$D_F（\alpha_{i-1}，\alpha_i）= P（\Delta X_i=\alpha_i | \Delta X_{i-1}=\alpha_{i-1}）\qquad （3\text{-}42）$$

则 r 轮差分特征 Ω_r 的概率可用

$$\prod_{i=1}^{r} D_F（\alpha_{i-1}，\alpha_i）$$

来近似代替。

密钥作用下的轮函数 F 具有如下性质：对于 $C_i=F（C_{i-1},K_i）$ 和 $C_i'=F（C_{i-1}',K_i）$

从已知的 ΔX_{i-1}、X_i、X_i'中可获取子密钥 K_i 的信息（或部分信息），那么，差分分析对 F 函数是有效的。

一般在迭代分组密码算法设计中，轮函数的设计很难做到具有强抗差分分析特性，因此在轮函数较弱的情况下，若密数据对已知，并且在最后一轮的输入对的差分能以某种方法得到，获取最后一轮的子密钥信息或一部分信息是可行的。第 r 轮的输入对的差分通常是通过寻找概率最大或几乎最大的 $r-1$ 轮差分特征来预测的。

3.1.3.2 S 盒线性偏差

定义 3-7：若一个分组密码算法的轮函数的非线性部分是由 S 盒实现，并且 S 盒是固定的，且子密钥由二元域上线性置入，则称此分组密码算法为并行查表分组密码算法（Parallel Table Lookup Block Cipher，PTLBC）。

设 T 为 S 盒（并行查表）变换，即由 s 个小的查表变换并列组成。

若 T 的输入为 $x=x_1x_2\ldots x_s$, $x_i\in Z_2^l$（$1\le i\le s$）,输出为 $y=y_1y_2\ldots y_s\in Z_2^m$（$1\le i\le s$）则 T 表示成：

$$T：\quad Z_2^{l\times s} \quad\rightarrow\quad Z_2^{m\times s} \tag{3-43}$$

$$（x_1，x_2，\ldots，x_s）\quad\rightarrow\quad（y_1，y_2，\ldots，y_s） \tag{3-44}$$

$T（x\rightarrow y）=t_1（x_1\rightarrow y_1）\times t_2（x_2\rightarrow y_2）\times\ldots\times t_s（x_s\rightarrow y_s）$ 其中 t_i: $Z_2^l\rightarrow Z_2^m$（$1\le i\le s$）即是 S 盒的定义。

子密钥 K 的置入方式一般有两种：

方法 1：在查表置换 T 之前置入，此时，$K\in Z_2^{l\times s}$；

方法 2：在查表置换 T 之后置入，此时，$K\in Z_2^{m\times s}$

根据该定义 DES、AES 都属于并行查表分组密码算法。

对于 SP 型分组密码算法，其轮函数可以表示为：

$$Y=F（X，K）=（L\cdot T）（X，K），X、Y、K\in Z_2^n \tag{3-45}$$

其中 L 为模 2 域上的可逆线性变换。

对于 Feistel 型分组密码算法，若分组长度为 $2n$，密数据分组为（X_i，X_{i+1}），$0\le i\le r-1$，子密钥为 K_0，K_1，…，K_{r-1}，X_i、$K_i\in Z_2^n$。若子密钥置入方式为 1，则其轮函数可以表示为：

$$X_{i+2}=X_i\oplus F（X_{i+1},K_i）=X_i\oplus L_i(T(L_i'(X_{i+1}))\ \oplus\ K_i)) \tag{3-46}$$

其中 L_i'为模 2 域上的线性变换，L_i 为模 2 域上的可逆线性变换。而且上述定义

中每一轮的线性变换可以不同。

对于 T 为 s 个 S 盒的并行变换，对于其差分概率有如下定理：

定理 3-10：$d_T(\Delta X, \Delta Y)=\prod_{i=1}^{s} d_{Ti}(\Delta X_i, \Delta Y_i)$　　（3-47）

关于并查表分组密码算法的马尔科夫密码，有如下定理：

定理 3-11：若子密钥与明消息独立且均匀随机，则并行查表分组密码算法在差分定义为两个密数据的异或时是马尔科夫密码。

证明：为了表述简洁，以 SP 型的并行查表分组密码算法为例，设子密钥的置入方式为 1；

设轮函数为：

$$Y=F(X, K)=L(T(X\oplus K)),\ X、Y、K\in Z_2^n \qquad (3\text{-}48)$$

记 T 的输入输出分别为 X'，Y'，则 $X'=X\oplus K$，$Y'=L^{-1}(Y)$。T 的输入输出差分分别为 $\Delta X'=\Delta X$，$\Delta Y'=L^{-1}(\Delta Y)$。那么对于所有可能的 α，β（$\alpha\neq 0$，$\beta\neq 0$）及任意 γ，有：

$$\begin{aligned}
&P(\Delta Y=\beta|\Delta X=\alpha, X=\gamma)\\
=&\sum_{\gamma} P(\Delta Y=\beta, K=\lambda|\Delta X=\alpha, X=\gamma)\\
=&\sum_{\gamma} P(\Delta Y=\beta|\Delta X=\alpha, X=\gamma, K=\lambda)P(K=\lambda|\Delta X=\alpha, X=\gamma)\\
=&\sum_{\gamma} P(\Delta Y=\beta|\Delta X=\alpha, X=\gamma, K=\lambda)P(K=\lambda)\\
=&1/2^n\sum_{\gamma} P(\Delta Y=\beta|\Delta X=\alpha, X=\gamma, K=\lambda)\\
=&1/2^n\sum_{v} P_T(\Delta Y'=L^{-1}(\beta)|\Delta X'=\alpha, X'=v)
\end{aligned} \qquad (3\text{-}49)$$

由于上式中 K 均匀随机，故 $P(K=\lambda)=1/2^n$。

因此，$P(\Delta X_{i+1}=\beta|\Delta X_i=\alpha, X_i=\gamma)$ 与 γ 无关。

同理，对于 Feistel 型并行查表分组密码算法也可以证明该结论。所以并行查表分组密码算法在差分定义为异或时是马尔科夫密码。

在并行查表差分密码中，定义并行查表变换 T 的输入差分：

$\Delta X=\Delta X_1\Delta X_2\ldots\Delta X_s$ 中的每一个 l 比特长 ΔX_i（$1\le i\le s$）为一个输入字。定义输出差分 $\Delta Y=\Delta Y_1\Delta Y_2\ldots\Delta Y_s$ 中的每一个 m 比特长 ΔY_i（$1\le i\le m$）为一个输出字。即每一个 S 盒的变换 $t_i: Z_2^l\rightarrow Z_2^m$（$1\le i\le s$）的输入输出差分定义为一个字。

对一个字 a，定义特征函数如下：

$$\delta(a)=\begin{cases}1, a\neq 0\\ 0, a=0\end{cases} \tag{3-50}$$

定义 3-8：如果 $\Delta X=\Delta X_1\Delta X_2\ldots\Delta X_s$ 中的每一个 l 比特长 ΔX_i（$1\le i\le s$）为一个输入字，定义 $\hat{C}$（ΔX）=（$\delta(\triangleright x_1),\delta(\triangleright x_2),\cdots,\delta(\triangleright x_s)$）为 ΔX 的字特征（Byte Characteristic Weight，BCW）。$\hat{C}$（ΔX）的 Hanming 重量为 ΔX 的字特征重量（Byte Characteristic Weight，BCW）,记作 $\hat{C}W$（ΔX）。

例：若 AES—128 的某轮变换中，经过扩展变换 E 后输出差分（即 S 盒的输入差分）为 ΔX=（0，0，4，0，8，0，0，4，0，0，4，0，8，0，0，4）（其中每一字长度为 16byte），则其字特征为 $\hat{C}$（ΔX）=（0，0，1，0，1，0，0，1，0，0，1，0，1，0，0，1），字特征重量为 $\hat{C}W$（ΔX）=6。

对于 S 盒的差分概率，有如下性质：

性质：设 α，β 分别为 t_i 的输入输出差分，

1、若 $\alpha=0$，$\beta\neq 0$，则 d_{tj}（α，β）=0； （3-51）

2、若 $\alpha=0$，$\beta=0$，则 d_{tj}（α，β）=1。 （3-52）

对于并行查表变换 T 的差分概率有如下定理：

定理 3-12：若所有 S 盒的差分概率最大值为 λ，T 的输出字特征重量为 $\hat{C}W$（ΔY），则：

$$d_T(\Delta X,\Delta Y)\le\lambda^{CW(\Delta Y)} \tag{3-53}$$

证明：由定理 3-9 可知：d_T（ΔX，ΔY）=$\prod_{i=1}^{s} d_{Ti}$（ΔX_i，ΔY_i），又由上述性质当 ΔX_i，ΔY_i 同时为 0 时，d_{tj}（ΔX_i，ΔY_i）=1，当 $\Delta Y_i\neq 0$ 时，d_{tj}（ΔX_i，ΔY_i）$\le\lambda$。

$\hat{C}W$（ΔY）表示 $\Delta Y_i\neq 0$ 的个数，故有：d_T（ΔX，ΔY）$\le\lambda^{CW(\Delta Y)}$

[证毕]

约定，若 S 盒的输入输出差分不为 0，则称此 S 盒是活动的（Active）。由上述推导，输出字特征重量代表 T 的活动 S 盒个数。

以下对 Feistel、SP 型分组密码算法的差分特征概率数学表达式进行数学描述：

设 Feistel 型并行查表分组密码算法的输入为（P_0，P_1）第 i 轮输出为（P_i，P_{i+1}），子密钥为 K_0，K_1，…，K_{r-1}，$P_i\in Z^{2^n}$，$K_i\in Z^{2^n}$，。其 r 轮差分特征记为：

$$\Omega_r=((\Delta P_0，\Delta P_1)\alpha\Delta P_2，\ldots，\Delta P_{r+1}) \quad (3\text{-}54)$$

对于连续两轮变换，当子密钥置入方式为方式 1 时，有：

$$P_{i+2}=P_i\oplus F(P_{i+1},K_i)=P_i\oplus L_i(T(L'(P_{i+1}) \oplus K_i)) \quad (3\text{-}55)$$

$$L_i^{-1}(P_{i+1}\oplus P_i)=T(L_i'(P_{i+1}) \oplus K_i) \quad (3\text{-}56)$$

差分概率：$d_F((\Delta P_i，\Delta P_{i+1})\rightarrow\Delta P_{i+2})=d_T(L'(\Delta P_{i+1})，L_i'(\Delta P_{i+2}\oplus\Delta P_i))$ (3-57)

当子密钥置入方式为 2 时，有：

$$P_{i+2}==P_i\oplus F(P_{i+1}，K_i)=P_i\oplus L_i(T(L'(P_{i+1}) \oplus K_i)) \quad (3\text{-}58)$$

$$L_i^{-1}(P_{i+2}\oplus P_i L_i'(K_i))=T(L_i'(P_{i+1})) \quad (3\text{-}59)$$

差分概率 $d_F((\Delta P_i，\Delta P_{i+1})\rightarrow\Delta P_{i+2})=d_T(L'(\Delta P_{i+1})，L_i'(\Delta P_{i+2}\oplus\Delta P_i))$

由此可推出：

定理 3-13：$d_F((\Delta P_i，\Delta P_{i+1})\rightarrow\Delta P_{i+2})=1$ (3-60)

当且仅当：

$$L'(\Delta P_{i+1})=0，\Delta P_{i+2}\oplus\Delta P_i=0 \quad (3\text{-}61)$$

考虑密钥作用下的 r 轮差分特征 Ω_r，假设子密钥均匀随机且统计独立，由马尔科夫密码的特征有：

定理 3-14：r 轮差分特征 Ω_r 的概率为：

$$P^{\Omega r}=\prod_{i=0}^{r-1} d_T(L'(\Delta P_{i+1})，L_i'(\Delta P_{i+2}\oplus\Delta P_i)) \quad (3\text{-}62)$$

由定理 3-13、定理 3-14 可以得到，当 T 函数的输入输出差分项满足下述表达 $L'(\Delta P_{i+1})=0，\Delta P_{i+2}\oplus\Delta P_i=0$ 的项数越多，$P^{\Omega r}$ 的值越大，当 T 的输出差分项满足 $\Delta P_{i+2}\oplus\Delta P_i\neq 0$ 时，乘积项 $d_T(L'(\Delta P_{i+1})，L_i'(\Delta P_{i+2}\oplus\Delta P_i))$ 对结果起作用：如果 $L'(\Delta P_{i+1})=0，\Delta P_{i+2}\oplus\Delta P_i\neq 0$，则必有 $P^{\Omega r}=0$，这种情况为平凡情况，不予以考虑。因此非零项乘积中 T 的输出差分的字特征重量之和越小，$P^{\Omega r}$ 的值越大；若最小字特征重量之和为 W，所有 S 盒的差分概率最大值为 λ：

$$P^{\Omega r}\leq\lambda^W \quad (3\text{-}63)$$

Feistel 型并行查表分组密码算法的差分概率上界的求取需要进行如下工作。

定义 3-9：将式（3-62）的右边乘积项中 r 的输出差分的字特征重量之和定义为 Ω_r 的字特征重量，记作：$\hat{C}W(\Omega_r)$。并且，记 $(\zeta_i，\eta_i)$（$0\leq i\leq r-1$）式（3-63）右边乘积项中 T 的输入输出差分对；$(u_{ij}，v_{ij})$（$0\leq i\leq r-1，1\leq j\leq s$）为第 i 轮 T 中 S 盒 t_j 的输入输出差分对，则式（3-63）可以表示为：

$$\mathbf{P}^{\mathbf{\Omega r}}=\prod_{i=0}^{r-1} d_T(\zeta_i,\ \eta_i)=\prod_{i=0}^{r-1}\prod_{j=1}^{s} d_{tj}(u_{ij},\ v_{ij}) \tag{3-64}$$

这样，$\hat{C}\mathrm{W}(\Omega_r)=\sum_{i=0}^{r-1}\hat{C}\mathrm{W}(\eta_i)=\sum_{i=0}^{r-1}\sum_{j=1}^{s}\bar{\delta}(v_{ij})$ （3-65）

定理 3-15：若所有 S 盒的差分概率最大值为 λ，则差分特征 Ω_r 的概率满足：

$$P^{\Omega r}\le\lambda^{CW(\Omega r)} \tag{3-66}$$

需要求取 $\hat{C}\mathrm{W}(\Omega_r)$ 的最小值，由最小值定义差分特征的概率的上界。

$(\zeta_i,\eta_i)(0\le i\le r-1)$中，$\zeta_i=L'(\ \Delta P_{i+1})$，$\eta_i=L_i'(\ \Delta P_{i+2}\oplus\Delta P_i)(0\le i\le r-1)$ （3-67）

或表示为：

$\zeta_i\oplus\ L'(\ \Delta P_{i+1})=0$，$\eta_i\oplus\ L_i'(\ \Delta P_{i+2}\oplus\Delta P_i)=0$，$(0\le i\le r-1)$

（3-68）

以 DES 为例，由式（3-68）可知，ΔP_0，ΔP_1，…，ΔP_s，ζ_0，η_0，…，ζ_{r-1}，η_{r-1} 构成了 GF（2^{32}）上的 $r\times2$ 个方程。通过求解，使得 $\hat{C}\mathrm{W}(\Omega_r)=\sum_{i=0}^{r-1}\hat{C}\mathrm{W}(\eta_i)$ 取最小值。具体步骤如下：

将 ΔP_0，ΔP_1，…，ΔP_s，ζ_0，η_0，…，ζ_{r-1}，η_{r-1} 总共 $3r+1$ 个变量展开成比特，形成有（$3r+1$）$\times n$ 个的比特元，记为如下的向量形式：

$$Z^{\omega}=(\Delta P_0^{(0)},\ \Delta P_0^{(1)},\ \ldots,\ \eta_{r-1}^{(n-2)},\ \eta_{r-1}^{(n-1)}) \tag{3-69}$$

简记为：

$$Z^{\omega}=(\Delta P_0,\ \ldots,\ \Delta P_s,\ \zeta_0,\ \eta_0,\ \ldots,\ \zeta_{r-1},\ \eta_{r-1}) \tag{3-70}$$

定义 $\mathrm{Z}^{\omega\mathrm{T}}$ 为 Z^{ω} 的转置，E 为单位矩阵，C 如下：

$$\mathrm{C}_{[r\times2\times n\times(r+1)\times n]}=\begin{bmatrix}
B_0 & 0 & B_0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0\\
0 & A_0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0\\
0 & B_1 & 0 & B_1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0\\
0 & 0 & A_1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0\\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\
0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & B_{r-1} & 0 & B_{r-1}\\
0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & A_{r-1} & 0
\end{bmatrix} \tag{3-71}$$

将线性变换 L_i' 用矩阵表示为 A_i，L_i^{-1} 用用矩阵表示为 B_i，则（3-67）、（3-68）为：

$$[\mathrm{C}_{[r\times2\times n\times(r+1)\times n}\ \mathrm{E}_{[r\times2\times n]\times[r\times2\times n]}]\ \mathrm{Z}^{\omega\mathrm{T}}=0^{\omega}{}_{r\times2\times n} \tag{3-72}$$

对式（3-72）做方程组系数矩阵初等行变换，将其中的分块矩阵 B 化成上三

角矩阵，形式如下：

$$\begin{bmatrix} 1 & \cdots & \cdots & \cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ & 1 & \cdots & \cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ & & o & o & o & o & o & M \\ & & & 1 & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ & & & & e_{00} & e_{01} & \cdots & e_{0q-1} \\ & & & & e_{10} & e_{11} & \cdots & e_{1q-1} \\ 0_{[(r+1)\times n]\times[(r+1)\times n]} & & & & M & M & o & M \\ & & & & e_{h-10} & e_{h-11} & \cdots & e_{h-1q-1} \end{bmatrix} \quad (3\text{-}73)$$

其中 h=r×n，q=（r×2）×n。

记:

$$S_{h\times q}=\begin{bmatrix} e_{00} & e_{01} & \cdots & e_{0q-1} \\ e_{10} & e_{11} & \cdots & e_{1q-1} \\ M & M & o & M \\ e_{h-10} & e_{h-11} & \cdots & e_{h-1q-1} \end{bmatrix} \quad (3\text{-}74)$$

$y^{\omega}=(\zeta_0^{(0)}, \zeta_0^{(1)}, \ldots, \zeta_0^{(N-1)}, \eta_0^{(0)}, \eta_0^{(1)}, \ldots, \eta_0^{(N-1)}, \ldots, \zeta_{r-1}^{(0)}, \zeta_{r-1}^{(1)}, \ldots, \zeta_{r-1}^{(N-1)}, \eta_{r-1}^{(0)}, \ldots, \eta_{r-1}^{(N-2)}, \eta_{r-1}^{(N-1)})$ （3-75）

求取差分特征概率上界的数学模型如下：

$$S_{h\times q}Y^{\omega}=0$$

$$\hat{C}W(\Omega_r)=\sum_{i=0}^{r-1}\hat{C}W(\eta_i)\text{取最小且}Y^{\varpi}\neq 0^{\varpi} \quad (3\text{-}76)$$

求解此问题与求解“背包问题”相似，是一个 NP 问题。针对特定的分组密码算法体制，根据结构特点可以找到一个在工程上可实现的方法来求解。

对于 SP 型并行查表分组密码算法，同样可以建立如上模型。但对于具体运算需要进行进一步工作。

定义 3-10[40]：对于一个线性变换 L，若其输入为 $x=x_1x_2\ldots x_s$，$x_i\in Z_2^m$（$1\le i\le S$），输出为 $y=y_1y_2\ldots y_s$，$y_i\in Z_2^m$（$1\le i\le S$）,将每一个 m 比特的串看做是一个字，其分枝数（Branch Number，BN）可定义为：

$$\phi=\min_{x\neq 0}(\hat{C}\omega(x)+\hat{C}\omega(y))$$

对并行查表分组密码算法，其线性变换的分枝数越大，则差分特征的最小字特征重量越大，因此，差分特征的概率上界越小。

显然，对输入输出分别由 S 个字组成的线性变换，最大分枝数为 S+1。

在并行查表分组密码算法的设计中，对线性变换的选择必须保证其分枝数达到最大或在工程实现可行的前提下达到最大。

在 SP 型并行查表分组密码算法中，若 P 置换的分枝数为 b，S 盒的最大差分概率为 λ，则 r 轮差分特征的最小字特征重量 W 满足

$$W \geq \begin{cases} \frac{1}{2} \times b, r = 2k \\ \frac{r-1}{2} \times b + 1, r = 2k+1 \end{cases}$$，K 为整数

任意差分特征的概率$\leq \lambda^W$，这是差分概率的一个粗略上界。

定义 3-11[41]：对一个映射 $t: Z_2^l \rightarrow Z_2^m$，其差分分布矩阵为：

$$D_{l \times m}^{(t)} = \begin{bmatrix} \triangleright_{00} & \triangleright_{01} & \cdots & \triangleright_{02^m-1} \\ \triangleright_{10} & \triangleright_{11} & \cdots & \triangleright_{12^m-1} \\ M & M & O & M \\ \triangleright_{2^l-10} & \triangleright_{2^l-11} & \cdots & \triangleright_{2^l-12^m-1} \end{bmatrix} \tag{3-77}$$

其中 $\triangleright_{\alpha\beta} = \sum \delta(\beta \oplus t(x) \oplus t(x \oplus \alpha)), 0 \leq \alpha \leq 2^l - 1, 0 \leq \beta \leq 2^m - 1$

差分分布矩阵刻画了变换 t 的动态变化行为，差分密码分析的关键在于充分利用 S 盒的差分分布矩阵中的特殊元素，如果某些元素值明显大于其余各元素值，则这些元素的位置对差分分析是重点分析对象。

对 SP 型并行查表分组密码算法设输入为 P_0，第 i 轮输出为 P_i，子密钥为 K_0，K_1，…，K_{r-1}，$P_i \in Z^{2^n}$，$K_i \in Z^{2^n}$'。其 r 轮差分特征记为：

$$\Omega_r = (\Delta P_0, \alpha \Delta P_1, \ldots, \Delta P_r) \tag{3-78}$$

对于连续两轮变换，当子密钥置入方式为方式 1 时，有：

$$P_{i+1} = F(P_i, K_{i+1}) = L_i(T(P_i \oplus K_{i+1})) \tag{3-79}$$

$$L_i^{-1}(P_{i+1}) = T(P_i \oplus K_{i+1}) \tag{3-80}$$

差分概率：$d_F(\Delta P_i, \Delta P_{i+1}) = d_T(\Delta P_i, L_i'(\Delta P_{i+1}))$ （3-81）

当子密钥置入方式为 2 时，有：

$$P_{i+1} = F(P_i, K_{i+1}) = L_i(T(P_i) \oplus K_i)) \tag{3-82}$$

$$L_i^{-1}(P_{i+1}) \oplus K_i = T(P_i) \tag{3-83}$$

差分概率 $d_F(\Delta P_i, \Delta P_{i+1}) = d_T(\Delta P_i, L_i'(\Delta P_{i+1}))$

由此可推出：

定理 3-16：$d_F(\Delta P_i, \Delta P_{i+1}) = 1$ （3-84）

当且仅当：

$$\triangle P_i=0，\triangle P_{i+1}=0 \tag{3-85}$$

考虑密钥作用下的 r 轮差分特征 Ω_r，假设子密钥均匀随机且统计独立，由马尔科夫密码的特征有：

定理 3-17：r 轮差分特征 Ω_r 的概率为：

$$P^{\Omega r}=\prod_{i=0}^{r-1} d_T（\triangle P_i，L_i^{'}（\triangle P_{i+1}）） \tag{3-86}$$

由定理 3-16、定理 3-17 可知，当 T 函数的输入输出差分项满足 $\triangle P_i=0，\triangle P_{i+1}=0$ 的项数越多，$P^{\Omega r}$ 的值越大，T 的输出差分项满足 $\triangle P_{i+1}\neq 0$ 时，乘积项 $d_T（\triangle P_i，L_i^{'}（\triangle P_{i+1}）)$ 对结果起作用：若 $\triangle P_i=0，\triangle P_{i+1}\neq 0$，则必有 $P^{\Omega r}=0$，这种情况为平凡情况，不予以考虑。

因此非零项乘积中 T 的输出差分的字特征重量之和越小，$P^{\Omega r}$ 的值越大；若最小字特征重量之和为 W，所有 S 盒的差分概率最大值为 λ，可以得到：

$$P^{\Omega r}\leq\lambda^W$$

可见，SP 型分布式查表分组密码算法与 Feistel 型分布式查表分组密码算法的差分分析结构是相同的。

定义 3-12[42]：令 $S（x）=（f_1（x）,\ldots,f_m（x））:F_2^l\rightarrow F_2^m$ 是一个多输出函数，若

$$\delta=\frac{1}{2}\max_{a\in F_2^l a\neq 0}\max_{\beta\in F_2^m}|\{x\in F_2^l : S(x\oplus\alpha)\oplus S(x)=\beta\}| \tag{3-87}$$

就称 S（x）是差分 δ 均匀的。δ 称为 S（x）的差分均匀性。

在并行查表分组密码算法的设计中，必须保证 S 盒的差分均匀性尽量小，差分均匀性可用来衡量一个分组密码函数抗差分分析的能力。上述理论推导与证明已经在具体的算法实现与分析中得到应用。

3.1.3.3 分组密码算法扩散性测试评估原则

分组密码算法的扩散性测试评估主要是建立在统计学原理之上的。

设 ξ 为一随机变量，数学期望为 E（ξ），称 ξ 的一阶矩 $T=E（|\xi-E（\xi）|）$ 为 ξ 的偏差。T 反映了随机变量与其中心的偏离程度。由于在统计学上，绝对值的处理不方便，所以对 T 进行放大，用 $D=E（\xi-E（\xi））^2$，即方差来反映随机变量与中心的偏离程度，称为 ξ 的二阶矩。

在统计假设检验中，对 ξ 的 n 个独立样本的偏差取统计平均，记为 TN。显然，TN 是一个随机变量，数学期望等于 ξ 的均差，由 TN 的分布，可以求出在某置信

度下的置信区间，根据此进行假设检验，称为偏差分析。

在实际分析分组密码算法的非线性扩散性时，可采用这种偏差分析，比如在分组密码算法依赖性分析中的具体应用。

关于分组密码算法的依赖性分析，文献[11]中阐述了这种方法，它与分组密码算法的 X^2 检验不同。

设 F 是一个 n 比特输入 m 比特输出变换函数，输入向量 $X=(x_1, x_2, \ldots, x_n)$ 其中 $x_i \in \{0,1\}, i=1,2,\ldots,n$ 仅改变 x 的第 i 比特后的输入向量记为 $X^{(i)}$，$i=1, \ldots, n$；则对应的输出向量可记为二元域上的向量 $F(x)$、$F(x^{(i)})$。

设函数 F 的输入变量取自样本集合 $X \subset Z_2^n$,记：

$a_{ij}=\#\{x \in X | (F(x))_j \neq F(x^{(i)})_j\}$（其中 $i=1,2,\ldots,n, j=1,2,\ldots,m$）表示 X 中的输入向量 x 和 $x^{(i)}$对应的输出向量之间的第 j 比特不同的个数。

$b_{ij}=\#\{ x \in X | W_H(F(x) \oplus F(x^{(i)}))=j\}$（其中 $i=1,2,\ldots,n, j=0,1,\ldots,m$）表示 X 中的输入向量 x 和 $x^{(i)}$ 对应输出向量之间差分汉明重量为 j 的个数。

设用 d_1，d_2，d_3，d_4 来度量算法非线性扩散的程度[11]：

$$d_1 = \frac{1}{n}\sum_{i=1}^{n}\left(\frac{1}{\#x}\sum_{x \in X} W_H(F(x) \oplus F(x^{(i)}))\right) \tag{3-88}$$

是雪崩效应程度的度量。

$$d_2=1-\#\{(i,j) \mid a_{ij}=0, i=1,2,\cdots,n; j=1,2,\cdots,m\}/(nm) \tag{3-89}$$

是完全程度的度量。

$$d_3=1-\frac{1}{n}\sum_{i=1}^{n}\left|\frac{1}{\#x \times m}\sum_{j=1}^{m} 2jb_{ij}-1\right| \tag{3-90}$$

是雪崩函数的一种度量。

$$d_4=1-\left(\sum_{i=1}^{n}\sum_{j=1}^{m}\left|\frac{2a_{ij}}{\#x}-1\right|\right)/(nm) \tag{3-91}$$

是严格雪崩的度量。

[43]中指出，若 $d_1 \approx m/2$、$d_2=1$、$d_3 \approx 1$、$d_4 \approx 1$，则说明密码算法满足非线性扩散的基本要求，即可以认为加密函数具有良好的完全性和雪崩效应，满足严格雪崩准则。

以下就上述结论中的各项系数进行讨论。

统计量 a_{ij} 的数学分布有如下定理成立：推导中讨论的#X 设为偶数，$F(\cdot)$ 输

出随机。

定理 3-18：

1、 a_{ij}～B（$\#X$，$1/2$）。记 $prob$（$a_{ij}=z$）$=P_z=C_{\#x}^{z}/2^{\#x}$。（3-92）

2、令 $T=|a_{ij}-E(a_{ij})|$表示 a_{ij} 的偏差，显然 $T\in\{0，1，…，\#X/2\}$。由（3-92）式可得：$E\{a_{ij}\}=\#X/2$，若设离散随机变量 z∈{0，1，…，$\#X/2$}，则有：

$Z=0$ 时，$prob$（$T=z$）$=prob$（$z=0$）$=prob$（$a_{ij}=\#x/2$）$=P_{\#x/2-z}$

$Z\neq0$ 时，$prob$（$T=z$）$=prob$（$a_{ij}=E\{a_{ij}\}\pm z$）$=2prob$（$a_{ij}=\#X/2-z$）$=2\,P_{\#x/2-z}$

因此，T 具有如下的分布：$prob(T=z)=\begin{cases}2P_{\#x/2-z}, 0<T\le \#x/2\\ P_{\#x/2-z}\end{cases}$（3-93）

当#X 足够大时，$2T/\sqrt{\#X}$ 近似服从于单边正态分布。

3、设 u 服从单边标准正态分布，即 u 的分布密度函数为：

$$F(u)=\sqrt{\frac{2}{n}}e^{-\frac{u^2}{2}},u>0 \qquad (3\text{-}94)$$

若记 $V=2T/\#X$，则 V 具有分布：

$$Prob(V=z)=prob(T=z\#X/2)$$

且：　$E\{V\}=E(u)/\sqrt{\#x}$，$Var\{V\}=Var\{u\}/\#X$　(3-95)

4、设有 N 个独立样本 V_1，V_2，…，V_N，N 足够大，则由中心极限定理可以近似得到：

$$\frac{\sum_{i=1}^{N}V_i-N\times E(V)}{\sqrt{N\times Var(V)}} \qquad (3\text{-}96)$$

服从标准正态分布。记 $VN=\frac{\sum_{i=1}^{N}V_i}{N}$，则 VN 的分布如下：

$$Prob(VN<z)=\phi\left(\frac{N\times(z-\frac{E(u)}{\sqrt{\#x}})}{\sqrt{N\times Var(u)/\#x}}\right)=\phi\left(\sqrt{\frac{N}{Var(u)}}(z\times\sqrt{\#x}-E(u))\right) \qquad (3\text{-}97)$$

显然，统计量 V 反映了随机变量的偏差，统计量 VN 是多个独立同分布样本的统计平均值。

令 $U=\sum_{j=1}^{m} jb_{ij}$，有以下定理成立：

定理 3-19：下列等式成立

1、$U\sim B(\#X, 1/2)$。记 $prob(U=z)=P_z=C_{\#x\times m}^{z}/2^{\#x\times m}$ （3-98）

2、用 $W=|2U/(m\times\#X)-1|$表示随机变量 U 的归一化偏差，同式（3-99）的分析，W 具有如下分布：

$$Prob(W=z)=\begin{cases}2P_{(1-z)\times m\times \#x/2}, 1\geq W>0\\ P_{(1-z)\times m\times \#x/2}, W=0\end{cases} \quad (3\text{-}99)$$

且 $E(W)=E(u)/\sqrt{m\times\#X}$，$\mathrm{Var(W)}=\dfrac{\mathrm{var}(u)}{m\times\#X}$ (3-100)

3、设有 N 个独立样本 $W_1, W_2, \ldots, W_N$，N 足够大，则由中心极限定理可近似认为：

$$\frac{\sum_{i=1}^{N} W_i - N\times E(W)}{\sqrt{N\times Var(W)}} \quad (3\text{-}101)$$

服从标准正态分布。记 $WN=\dfrac{\sum_{i=1}^{N} W_i}{N}$，则 WN 的分布如下：

$$Prob(WN<z)=\phi\left(\frac{N\times(z-E(W))}{\sqrt{N\times Var(W)}}\right)=\phi\left(\sqrt{\frac{N}{Var(u)}}(z\times\sqrt{m\times\#x}-E(u))\right) \quad (3\text{-}102)$$

显然，统计量 WN 是多个独立同分布样本的统计平均值。

如果函数 $F()$ 是随机变换，则 $F()$ 变换具有很好的完全性和雪崩效应，满足严格雪崩准则，可以近似认为 a_{ij}，b_{ij} 是独立同分布的。

若随机变量 $B\sim B(m,1/2)$,则 $E(B)=m/2$，$Var(B)=m/4$。设 $B_1, B_2, \ldots, B_N$ 为 N 个独立同分布样本，N 足够大，则由中心极限定理：

$\dfrac{\sum_{i=1}^{N} B_i - N\times E(B)}{\sqrt{N\times Var(B)}}\sim N(0, 1)$，记 $BN=\dfrac{\sum_{i=1}^{N} B_i}{N}$，那么 BN 的分布服从：

$$Prob(BN<z)=\phi\left(\frac{N\times(z-E(B))}{\sqrt{N\times Var(B)}}\right)=\phi\left(\sqrt{\frac{N}{m}}(2z-m)\right) \quad (3\text{-}103)$$

由上述讨论可知道，*1- d_3* 具有与 *W* 同分布的 *n* 个独立随机变量的统计平均值；*1-d_4* 与 *V* 具有同分布的 *n* 个独立随机变量的统计平均值，设显著性水平为 *α*，用 $Z_{\alpha/2}$ 表示标准正态分布的 *α/2* 分位点，于是有：

1、*E*（d_1）=*m/2*，由式（3-99）其置信区间为：

$$(\frac{m}{2}-\frac{z_{\alpha/2}}{2}\sqrt{\frac{m}{\#x}},\frac{m}{2}+\frac{z_{\alpha/2}}{2}\sqrt{\frac{m}{\#x}})$$

2、由式（3-92）得：*prob*（d_2=*1*）=$12^{-\#x}\rightarrow 1.00$

3、E（d_3）=*1-E*（*W*）=*1-0-E*（*u*）/$\sqrt{m\times\#X}$，由式（3-99）知 d_3 的置信区间为

$$(E(d_3)-z_{\alpha/2}\sqrt{\frac{Var(u)}{n}}\sqrt{\frac{1}{m\times\#x}},E(d_3)+z_{\alpha/2}\sqrt{\frac{Var(u)}{n}}\sqrt{\frac{1}{m\times\#x}})$$

4、*E*（d_4）=*1—E*（*V*）=*1—E*（*V*）=*1-0-E*（*u*）/$\sqrt{\#x}$。由（3-96）式可知，d_4 的置信区间为：

$$(E(d_4)-z_{\alpha/2}\sqrt{\frac{Var(u)}{n}}\sqrt{\frac{1}{m\times\#x}},E(d_4)+z_{\alpha/2}\sqrt{\frac{Var(u)}{n}}\sqrt{\frac{1}{m\times\#x}}) \qquad (3\text{-}104)$$

其中 *E*（*u*）和 *Var*（*u*）可以从 *u* 的单边正态分布函数求出，分别为：$\sqrt{\frac{2}{\pi}}$ 和 1。

由 d_1，d_2，d_3，d_4 四个统计量的定义，如果 *F*（）是随机变换，则给定假设条件

P（*j* | *i*）= *1* 与不给定假设条件相比，二者关于各个统计量的差值 Δd_k，*k=1,2,3,4* 可以计算出来：

$$\Delta d_1=1/2n，\Delta d_2=0，\Delta d_3=1/nm，\Delta d_4=1/nm \qquad (3\text{-}105)$$

在给定显著性水平 α 时，统计量 d_1，d_2，d_3，d_4 的置信区间长度 sl_k，*k=1,3,4* 可计算出如下结论：

$$Sl_1=z_{\alpha/2}\cdot\sqrt{\frac{m}{\#x}}\,,\ Sl_3=2z_{\alpha/2}/\sqrt{nm\cdot\#x}\,,\ Sl_4=2z_{\alpha/2}/\sqrt{nm\cdot\#x} \qquad (3\text{-}106)$$

引用统计量 d_1，d_2，d_3，d_4 做扩散性分析时，应在给定显著性水平 *α* 的条件下，选取大样本量，满足 *P*（*j* | *i*）= *1* 的关系对（*i*，*j*）能在检测结果中被区别出来。

3.2 分组密码算法设计

3.2.1 相关概念

常见的离散空间是二元域 $F_2=\{0、1\}$和整数模 m 环 $Z_m=\{0、1、2、\ldots、m-1\}$等以及它们组合派生出来的空间，如 F_2^n 和 Z_m^n，有时还有其他一些置换群、可逆矩阵乘法群等。一般，当离散空间 X 和 Y 各自具有明确的代数运算时，记 $f: X\rightarrow Y$，规定从 X 到 Y 的的映射 f 为离散函数。分组密码算法的明消息空间和密钥空间是该密码的定义域，密数据空间是值域。目前出现的分组密码算法都是基于离散空间上的密码函数。类似，分组密码算法中的置换作为一类特殊的函数也是离散的。其代数表达式也是基于离散空间的。

3.2.2 设计基本原理

1949 年，Shannon 发表了“保密通信的信息理论”一文，该文用信息论的观点对信息保密问题作了全面的阐述。Shannon 以概率统计的观点对消息元、密钥元、接收和截获的消息进行数学描述和分析，用不确定性和唯一解距离度量密码体制的保密性，阐明了密码系统、完善保密性和实际保密性等概念，将密码学的研究纳入了科学的轨道。为了使密码算法抵抗统计分析，Shannon 建议采用“混乱”和“扩散”法来使密数据和明消息的关系复杂化，并将每一位明消息数字的影响尽可能迅速散布到多个输出的密数据数字中，以便隐蔽明消息数字的统计特性。基于信息论的理论基础体系一直是密码学中相关应用的根据，较有限域等代数方面的理论更切合密码设计与分析的使用。

到目前为止，混乱和扩散原则仍然是分组密码算法设计总的基本原则。

Shannon 通过“乘积”与“迭代”实现分组密码算法良好的混乱和扩散效果，现在使用的分组密码算法还在使用这两种方案：乘积密码（Product Cipher, PC）是若干个简单密码算法的复合，以达到安全性更强的算法；迭代密码（Iterated Cipher, IC）是一种特殊的乘积密码，以一个简单的轮函数（Round Function, RF）为基础，通过密码变换，在密钥控制下以迭代方式进行加密变换来实现混乱和扩散原则。

一个好的迭代分组密码算法是以一类密码学特征良好的基础置换为轮函数来构造，每一轮置换应该有清晰的数学结构和合适的密码学性质，其轮数选择需要由安全性分析最终确定。而且，在现有的计算机及网络技术下便于软硬件实现。加/解密可以用同样器件来实现，整体结构尽量使用规则结构。轮函数使用子块为

运算单元，并尽量采用简单运算来实现，子块长度面向软件编程，运算部件易于硬件实现。总而言之，分组密码算法设计中应采取“理论前导、技术优先、工程前瞻、实践选择原则”。在强调安全性的同时，密钥作用的有效性、算法实现的简捷性、算法使用的灵活性都是衡量一个分组密码算法是否优秀的标准。

3.2.2.1 Feistel 结构分组密码算法设计

Feistel 网络结构由 Horst Feistel 在设计 Lucifer 分组密码算法时首先提出，并在 DES 中得以应用。许多分组密码算法如 GOST、FEAL、RC5、Camellia 等都采用了 Feistel 网络。

Feistel 网络分组密码算法的外观特征是对明消息进行部分变换、逐步混乱与扩散。DES 是 Feistel 型分组密码算法的代表作，此类的设计多是参照 DES 的结构对细节进行部分改进而成。这类设计仍然需要能够抗各种已知的分析。本文重点讨论 SP 型分组密码算法的设计与评估，对 Feistel 型分组密码算法的设计情况可以参照其他章节。

3.2.2.2 SP 结构分组密码算法设计

SP 结构分组密码算法的概况在第二章已经提及，以下以 AES 为例按算法层次进行讨论。

AES 采用宽轨迹设计。宽轨迹策略主要致力于线性扩散层的设计，保证轮函数有很宽的线性轨迹和差分轨迹，对 S-盒的要求则仅仅是使其具有足够小的相关重量和足够小的限制重量，并不要求 S 盒达到最优。

AES 扩散层选用了线性非时移变换（Linear Shift-Invariant Transformation, LSIT），是细胞自动机（Cellular Automata, CA）的一种，具有并行实现结构和良好的扩散特性，保证了 AES 算法的快速实现以及很强的抗线性密码分析和抗差分分析能力。

使用细胞自动机[44][45]进行密码算法的实现是目前密码学中的一种选择：用于描述具有并行结构的离散时间系统。离散时间系统是一系列变换的乘积，将输入序列的规律掩盖变换为输出序列。设序列中元素位置的集合为 I，各元素都取值于集合 A，如果用 q^t 表示 t 时刻的输入序列，则离散时间系统在 t 时刻的变换可以表示为：$F^t: A^l \to A^l$

$$q^{t+1} = F^t(q^t) \tag{3-107}$$

当 F^t 由若干并行的 $f_i^t : A^l \to A$ 组成时，既：

$$F^t = \bigcup_i f_i^t$$

则该离散系统为一细胞自动机，简称为 CA。

定义 3-13：细胞：序列中的每个元素称为一个细胞。

配置：某个时刻所有的细胞的取值称为配置，全体配置的集合 A^l 称为配置集，记为 Q。记初始配置为 q^0、t 时刻的配置为 q^t，一个 CA 是由 q^0 衍生出 q^1，q^2，…，配置 q 在位置 I 处的细胞值用 q_i 表示。

邻元投影（Neighborhood Projector, NP）定义为:设 $q \in A^l$ 为一配置，细胞集合 $q_{i+V} \in A^V$ 称为配置 q 在位置 I 的邻元投影，记作 $q|_I$。局部映射（LOCAL MAP, LM）：局部映射反映一个细胞的变化过程，是 $A^l \rightarrow A^l$ 的映射，可由全局函数表示。全局映射是若干局部映射的并联，即 t 时刻的全局函数 F^t 可表示为：

$$F^t = \bigcup_i f_i^t \qquad (3\text{-}108)$$

当局部映射与时间无关时，全局映射也与时间无关，此时简记为 F。

典型的 CA 其局部函数与时间 t 和位置 I 无关,即具有同质的空间和时间行为，称这样的 CA 为非时移变换。一维的非时移变换可用三元组（A，V，f）表示，其中 A 为有限状态集，V 为邻元模式，f 为局部函数。

例：设一维 CA{{0，1}，{-1，0，1}，f}的局部函数为 $f(q_{i-1},q_i,q_{i+1}) = q_{i-1} + q_{i+1}$ ，初始配置为：q^0 = 000000100000…，则其演化过程如下：

q^1：…000001010000…

q^2：…000010001000…

q^3：…000101010100…

q^4：…001000000010…

…

AES 的扩散层包括行移位变换和列混合变换两部分。由于 AES 面向字节操作，而字节被当作了由 F_2 上的不可约多项式 $m(x) = x^8+x^4+x^3+x+1$ 定义的域 GF（2^8）上的元素，将 AES 的行扩展为无线序列，则行移位变换相当于 GF（2^8）平凡的线性时移变换，同样，将列扩展为无限序列，则列混合变换为 GF（2^8）上非平凡的线性非时移变换。在 AES 算法中，列混合变换选用的多项式，即线性非时移变换的局部函数为：

$$A(x) = [03]x^3 + [01]x^2 + [01]x + [02]$$

因为满足：

$$gcd(A(x), x^4+1) = 1$$

故其在（GF（2^8））^{4}上可逆，其逆函数为：

$$B^{-1}（x）= \{0b\}x^3 + \{0d\}x^2 + \{09\}x + \{0e\}$$

因为 $W（A（x））=4$，即扩散因子为 4，说明一列中的一个活动字节可以扩散到该列的全部四个字节上；分枝数为 5，达到了上界值 D+1。在行移位变换方面，其参数经过选择，保证一个列上的字经过行移位变换，分别在不同的列上。

结合行移位变换和列混合变换，可以看到：AES 经过一轮变换的扩散层后，输入与输出至少有 5 个字节不同，即任一 2 轮轨迹至少有 5 个活动 S 盒，同理，任意 4 轮轨迹至少有 25 个活动 S 盒。因为 SP 型密码的线性差分轨迹和差分轨迹的重量等于活动 S 盒的重量之和，即：线性轨迹的相关系数为活动 S 盒相关系数的乘积，差分轨迹的扩散率近似为活动 S 盒扩散率的乘积，已经知道 AES 的任意四轮差分轨迹的最大扩散率为 2^{-150}，任意四轮线性轨迹的最大相关系数为 2^{-75}。

由此可见，采用宽轨设计策略的 AES，其抗线性分析能力和抗差分分析能力主要依赖于扩散层的设计。由于采用线性非时移变换，AES 扩散层具有良好的扩散性能及能够并行实现的特点，这使的 AES 能同时兼顾安全性和实现速度的需求。

3.2.2.3　S 盒设计与可证明性安全

定义 3-14：设 $f（x）：F_2^n \rightarrow F_2$，$L_n=\{ux+v|u \in F_2^n, v \in F_2\}$表示 F_2 上所有线性布尔函数的集合（称为线性布而函数类）。称：

$$N_f = \min_{l(x)\in l_n} d_H(f(x), l(x))$$ 为 $f（x）$为非线性度。其中 d_H （$f（x）$，$l（x）$）表示 $f（x）$与 l（x）间的汉明距离，即：

$$d_H(f(x), l(x)) = |\{x \in F_2^n | f（x）\neq l（x）\}| \qquad （3\text{-}109）$$

非线性度反映了 F 的抗线性密码分析能力，其值越大，F 的抗线性密码分析能力越强。

对任何 n 元布尔函数 $f（x）：F_2^n \rightarrow F_2$，可以唯一表示成如下形式：

$$f（x）= a_0 + \sum_{\substack{1\le i_1<\cdots<i_k\le n \\ 1\le k\le n}} a_{i_1 i_2 \cdots i_k} x_{i_1} x_{i_2} \cdots x_{i_k} \qquad （3\text{-}110）$$

其中，$x=（x_1,x_2,\ldots,x_n）$，a_0，$a_{i1i2\ldots ik} \in F_2$，称为代数形式。

定义 3-15[46]：设 $f（x）：F_2^n \rightarrow F_2$，称 $f（x）$代数正规形式中最高项的次数为 $f（x）$ 的次数，记为：$deg（f）$；$f（x）$代数正规形式中 I 次项的个数称为 $f（x）$的 I 次项数，所 $I（0\le i\le n）$次项数之和称为 $f（x）$的项数。

定义 3-16[47]设 $F（x）=（f_1（x），f_2（x），…，f_m（x））：F_2^n \rightarrow F_2^m$，定义：

$$D（F）=min\{deg（\beta F）|\beta \neq 0，\beta \in F_2^m\}$$

$$= min\{deg(\sum_{i=1}^{m} b_i f_i(x))|\beta \neq 0，\beta=（b_1,…,b_m）\in F_2^m\} \quad （3\text{-}111）$$

为 $F（x）$的代数次数。当 $D（F）=k$ 时，称 $F（x）$为 k 次函数。

设计一个理想的随机置换 $S：F_2^n \rightarrow F_2^n$，其每个分量函数的代数次数最佳为 $n-1$，每个分量函数的 I 次项数应接近于 $C_n^i/2$。若代数次数太低，无法抗差分分析；若项数太少，有可能提高插值分析的成功率。

对 S 盒的其它要求还有严格雪崩准则、扩散准则、可逆性、没有陷门等。

1、S 盒的构造方法

实际中 S 盒的构造准则中有些相互制约，根据设计标准，需要对某些指标作出协同设计。SP 型分组密码算法中的 S 盒，可以降低对其扩散性的要求，把这一部分任务在扩散层 P 完成。构造 S 盒的方法有：

随机选取并测试：随机选取的小规模的 S 盒在安全性缺乏保障。但是 S 盒的规模越大，随机产生的 S 盒密码性能越好[48]。随着 n 的增大，F_2^n 上置换均趋向与非退化置换，如果 S 盒随机，又依赖于密钥，则强度会更高。通常采取随机选取，通过某些测试根据特殊要求进行筛选。当计算能力足够强大，消耗足够的时间总会选定合适的 S 盒，并且可以使用户相信没有陷门。

按照规则构造和测试：该方法通常以已有的条件优越的 S 盒为基础，以一种简单而确定的方式构造满足需要的 S 盒。其中之一是使用数学函数，例如指数和对数函数、有限域 GF（2^n）上的逆映射、有限域上的幂函数等；使用不同群中数学函数的复合对抵抗插值分析和高阶差分分析有效。

AES 的 S 盒，其设计主要考虑到抗差分密码分析与抗线性密码分析的需求，同时还关注到抗代数计算分析，例如插值分析的要求，设计基于如下考虑：

可逆性。

最大扩散率尽可能小。

最大输入输出相关系数尽可能小。

在 GF（2^8）中代数表示的复杂性。

表达式的简单性。

由于 AES 的宽轨迹设计策略，在抗线性分析和抗差分分析方面，对 S 盒没有重点关注。S 盒采取的 GF（2^8）上的求逆变换有非常简单的表达式，这使得代数

分析容易实施。同时设计在求逆的基础上加入了 F_2 上的仿射变换作为掩码，增加了代数表出的复杂度；仿射变换中的常数保证 S 盒既没有不动点，也没有逆不动点。

AES 的 S 盒求逆变换表示如下：

$$F（x）=\begin{cases} x^{-1}, x \neq 0 \\ 0, x = 0 \end{cases} \quad （3\text{-}112）$$

具有以下性质[48]：

$$N_F \geq 2^{n-1}-2^{n/2} \quad （3\text{-}113）$$

$$\mathrm{Deg}（F）=W_h（2^n-2）=n-1 \quad （3\text{-}114）$$

n 为奇数时，F 的差分均匀度有冗余，可能在与 n 有关的多项式时间内计算出 x^{-1}，所以通常选择偶数的 S 盒。

域上求逆映射作为 S 盒的方法被许多著名分组密码算法所采用，原因在于算法简单易于表出，并且非线性度、差分均匀性及代数次数表现符合通常采用的设计标准。分组密码中 S 盒的构造原则。S 盒作为分组密码的非线性部分，主要提供分组码的混乱作用。一般，一个分组密码的安全强度取决于 S 盒的密码强度。构造好的 S 盒是一个分组密码必须考虑的问题。S 盒本质上是一个简单的代替：将 m 位输入映射到 n 位输出，也称为 $m \times n$ 位的 S 盒。在算法中，S 盒通常情况下是仅有的一个非线性步骤。S 盒越大，发现在差分分析和线性分析中统计关系异常难度就越大，并且容易找到强的 S 盒。大多数随机的 S 盒是非线性的，非退化的，能够抗线性分析，当入口位减少时，这些特性不会很快减少。M 的大小比 n 的大小更为重要，增加 n 的大小抗差分分析能力增强，但抗线性分析能力减弱。在 S 盒的设计中必然会涉及到离散函数的研究。为了保证强度，S 盒中的离散函数必须满足：非线性、非仿射性，甚至不能接近线性或仿射性。0 、1 平衡性，在不同的位组合中没有相关性。

A、随机选择。显然小的 S 盒是不安全的，大的 S 盒可以确保强度。有 8 个或更多个输入的随机 S 盒是相当强的。1 2 位的 S 盒具备更高的强度。如果 S 盒随机且与密钥相关，那么 S 盒强度更大。

B、折衷测试。设计随机的 S 盒，根据需要的特征指标来测试。

C、人为构造。直接产生随机的 S 盒，这种方法不失为一种快速、捷径的构造方法。

D、数学方法构造。根据数学原理来产生 S 盒，使得能抗差分分析和线性分析。

E、人为构造、数学构造相组合。随机选择的S盒采取尽可能大的措施来抵抗各种分析，数学构造抗已知分析，对未知分析的效果无法考虑。本项目主要采取这种方式对 S 盒进行研究。

2、S 盒的入口变换原则与几种设计

雪崩效应：当一些S盒的输入位发生改变时，S盒的输出位改变量的程度。离散函数能够在某些条件下满足雪崩特性，但构造雪崩函数非常困难。严格雪崩准则保证了当一个输入位发生改变时输出为将有一半发生改变。

设入口位为 m，出口位为 n，当 $n \geq 2^m - m$，那么，在S盒的输入与输出位中存在一个线性关系。如果 $n \geq 2^m$，仅在S盒的输出位中存在线性关系。S盒公认的设计原则体现为：随机选择。显然小的S盒是不安全的，大的S盒可以确保强度。有 8 个或更多个输入的随机S盒是相当强的。1 2 位的S盒具备更高的强度。如果S盒随机且与密钥相关，那么S盒强度更大。

3、S盒的模函数设计，模运算的简化问题

多个分组密码中都采用了在 n 元域上求逆运算后进行置换的算法对S盒进行设计的数学方法构造，由于S盒在模整数域上进行，模函数自然成为设计重点。分组密码使用环境多为计算机网络，模运算设计会针以字节进行，通常在 $G(2^8)$ 上，为了确保逆运算的存在性、唯一，选择的模多项式是不可约多项式。8 次不可约多项式有 30 个，理论上来讲：这些多项式都是可用的。

4、不同模运算与不同入口变换组合后，S盒的密码强度估计，运算速度分析

在以上的数学构造进行后，把多种模运算与设计的S盒入口变换进行组合,进行人为设计，在该阶段，每种设计产生不同的运算结果，同时运算速度也将随算法的改变而改变。每种算法的抗线性分析、差分分析的能力也会有所区别。最后得到算法最终密码学指标、运算指标，通过对结果的分析，建议在高保密强度、高运算速度之间选择。

对 SP 结构进行框架、S 盒、替代置换函数之间的设计原理、运算强度的分析比较。特别是对高级加密标准 AES 算法进行详细分析可以看出，AES 的保密、速度方面的要求与密钥长度是有关系的。设计以密钥长度为自变量的选择函数，即使用密钥长度的 128 比特、192 比特、256 比特做为 S 盒组选择的标准。以此把设计的S盒组嵌入到 AES 中。

关于 S-盒的可证明安全性，以两种典型的例子作为说明：

CRYPTON 是韩国作为 AES 候选算法而提出的分组密码，其 S 盒的设计沿用了分组密码算法 MISTY 的思想，使用了两个互逆的八进八出 S-盒——S_0，S_1，采

用 P_0，P_1，P_2 三个四进四出 S-盒三圈 Feistel 结构生成方式生成（如图 3-2、图 3-3）。

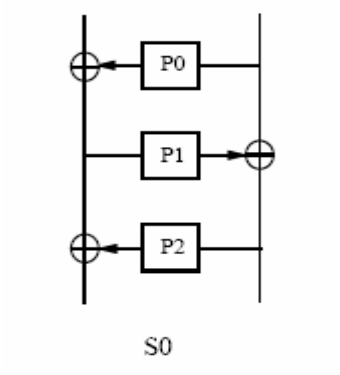


图 3-2 八进八出 S 盒 S_0

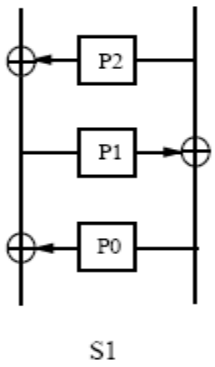


图 3-3 八进八出 S 盒 S_1

具体定义为：$y = S_0(x)$，$x = x_1||x_2$，x_1，$x_2 \in \{0, 1\}^4$，$y_1 = x_1 \oplus P_1(x_2 \oplus P_0(x_1))$，$y_2 = x_2 \oplus P_0(x_1) \oplus P_2(y_1)$，$y = y_1||y_2$。$S_1$ 可以直接由 S_0 派生，$y = S_1(x)$，$x = x_1||x_2$，x_1，$x_2 \in \{0, 1\}^4$，$y_1 = x_1 \oplus P_1(x_2 \oplus P_2(x_1))$，$y_2 = x_2 \oplus P_2(x_1) \oplus P_0(y_1)$，$y = y_1||y_2$。$S_1(x) = S_0(x)^{-1}$，$x \in \{0, 1\}^8$。因此，对于一个完全随机函数 $F^* \in (0, 1)^8$，m 块的数据加密，$Adv_A(S_i, F^*) \leq m(m-1)/16$。

设 S 盒的 2^n 个输入、输出集合分别为 X、Y，则：

$$DP_S = \max_{\triangleright x \neq 0, \triangleright y} \frac{\#\{x \in X \mid S(x) \oplus S(x \oplus \triangleright x) = \triangleright y\}}{2^n} \tag{3-115}$$

$$LP_S = \max_{\Gamma x, \Gamma y \neq 0} \left(\frac{\#\{x \in X \mid x \cdot \Gamma x = S(x) \cdot \Gamma y\} - 2^{n-1}}{2^{n-1}}\right)^2 \tag{3-116}$$

·为面向 *bit* 乘法。

这种类型的 S 盒具有特征：如果 P_i 是一一映射，且满足

$$DP_{Pi} \leq p，则\ DP_{Si} \leq 2p^2、L\ P_{Si} \leq 2p^2 \tag{3-117}$$

具体的数据可以参考 S 盒具体的 P_i 真值表进行计算。用 4×4 S 盒生成 8×8 S 盒便于在硬件实现。

AES 的 S 盒的数学表达式为：$S=f \cdot g$，其中映射 g 把 0 变换为 0，f 把非 0 元变换为逆。具体的，任意 x，y，z，为 GF^8（2）上的元，则 S 盒相应的变换可表示为：$z=S(x)=f(g(x))$。根据 S 盒的定义，显然有：$x \neq 0$，则 $1=xy$。AES 的 S 盒是 $\{0, 1\}^8 \rightarrow \{0, 1\}^8$ 的八进八出置换。虽然这种 S 盒的代数表达式非常简单，但是映射的定义域、值域空间相对较大。

因此，更普遍的情况下是把逆变换看作是 F_2^8 上的映射，在密码设计与实现时采用固定的 256×256 方表进行查表运算。对于这种 S 盒有如下特征：

性质 3-1：对 S 盒的非线性函数 f_i（x），I=0，1，…，7，有 $D_{fi}\leq 7$

性质 3-2：对 S 盒的非线性函数 f_i（x），I=0，1，…，7，当 $D_{fi}=7$，达到 S 盒的最大非线性度

性质 3-3：AES 的 S 盒的最大线性偏差概率 P_{MLA} 的变化区间为：[1/64，1/8]

性质 3-4：AES 的 S 盒代数次数为 7

性质 3-5：AES 的 S 盒如果记为 F（x）=（f_1（x），f_2（x），…，f_8（x）），那么 f_1（x），f_2（x），…，f_8（x）之间相互仿射等价：存在 F_2 上的 $n\times n$ 矩阵 D、常量 c，及 F_2^8 上常量 a、b，使得：f_1（x）= f_2（$Dx+a$）+ bx + c

由于 AES 采取的设计策略中 S 盒的代数表达式非常简单，并且可以通过线性变换形如

$$x^i=x^{i+1}y\,,\quad y^i=xy^{i+1}\ (1\leq i\leq 128)$$

来增加 S 盒的表达式数量。因此，AES 的 S 盒可以视数据条件表示成多个布尔函数。显然 S 盒的表出式很简单，算法主要通过高次迭代增加算法的复杂度。

在可证明性安全的领域，对分组密码算法的外部轮廓已经进行了一些工作，但是对 S 盒的可证明性安全的工作几乎没有系统的结果。S 盒的设计是密码算法非线性的关键，并且与硬件发展水平相对应。因此，对 S 盒进行可证明性安全的工作可以使其在非线性程度得以度量的同时，保证算法通过量化达到最合理的设计指标。事实上，国际上经常采用的几种典型 S 盒设计明显能够保证安全，只是结构复杂性上有所区别。当然，可证明安全性也是有时间等条件的限制。在 DES 设计之初，虽然设计者已经掌握差分分析技术，但就普通分析者而言算法是安全的。本文提出针对 S 盒可证明安全性的工作应主要从 S 盒的多项式代数表出式次数、相对与完全随机的优势度、线性偏差概率、非线性偏差概率等方面加以描述。S 盒的设计是涵盖在整个密码算法之内的，所有的安全性指标还需要与扩散、迭代圈数等其他因素相互结合形成最终的可证明性结论。

3.2.2.4 正形置换

正形置换（Orthornorphic Permutation, OP）是分组密码算法设计中较常用的一种方法，在国际上被多个国家的军方资金所资助。

正形置换是一种完全映射（Complete Mapping, CM）。

定义 3-17：一个群、拟群、圈的完全映射是 G 到 G 的双射：θ：$x\rightarrow\theta$（x）使得 φ（x）=$x\cdot\theta$（x）仍然是 G 上的一个双射。

定义 3-18：一个 Z_2^m 上的正形置换是一个一一映射 σ $Z_2^m\rightarrow Z_2^m$，满足：

$$\{x \oplus \sigma(x)\} = Z_2^m$$

定义 3-19：一个 2^m 阶正形拉丁方 $L^0(e_{ij})$ 是一个 $2^m \times 2^m$ 方阵，它的第 I 行第 j 列的元素为

$$e(I,j) = I \oplus j, I,j \in Z_2^m$$

定义 3-20：一个 2^m 阶正形拉丁方 $L^0(e_{ij})$ 的截集是从该拉丁方中选取的 2^m 个单元的集合，每行、每列一个，任意两个单元的符号都不相同。一个 2^m 阶正形拉丁方的截集 $T \in S_{2^m}$，截集的全体记作 $S^0(m)$。

定理 3-20：一个 Z_2^m 上的正形置换 $P \in S_{2^m}$，它满足：$P \in S^0(m)$。即一个 2^m 次正形置换是 2^m 阶正形拉丁方的截集。

证明：显然。

以向量表示一个 2^m 次正形置换 P:

$$P=(\sigma(0), \sigma(1), \ldots, \sigma(2^m-1))$$

恒等置换记为：$I=\{0, 2, \ldots, 2^m-1\}$

定义 3-21：一个 2^m 次正形置换 P^0 是 S_{2^m} 中的一个置换，满足：

$$P^0 \oplus I \in S_{2^m}$$

称 $P^{0'} = P^0 \oplus I$ 为 P^0 的补置换，记

$$P^0 = (\sigma'(0), \sigma'(1), \ldots, \sigma'(2^m-1))$$

其中，$\sigma'(i) = \sigma(0) \oplus I, I=0,1,\ldots, 2^m-1$-

S_{2^m} 中正形置换的总体记做 $S^0(m)$。

显然，正形置换有如下性质：

1、 $P^{0'} \oplus P^0 = I$，因此在 S_{2^m} 中正形置换成对出现，$|S^0(m)|$为偶数。

2、 $(P^0)^{-1} \in S^0(m)$

3、 $P^{0'} \oplus r \in S^0(m)$，$r \in Z_2^m$，并且：$|S^0(m)| \equiv 0 \mod 2^m$。由一个正形置换能够生成 2^m 个正形置换。

4、 若 $P_1^0(n_1) = \{r(i) | I=0,1,\ldots, 2^{n1}-1\} \in S^0(n1), n1>1$

$P_1^0(n_1) = \{t(i) | I=0,1,\ldots, 2^{n1}-1\} \in S^0(n2), t1>1$

$N1+n2=m$

则有： $P^0(m) = \{\sigma'(j) | j=0,1,\ldots, 2^m\} \in S^0(m)$

其中，

$\sigma'(j) = r(j_1) + t(j_2) \times 2^{n1}, j = j_1 + j_2 \times 2^{n1}, j_1=0,1,\ldots, 2^{n1}-1, j_2=0,1,\ldots, 2^{n1}-1$

记 $\sigma_m = (r_{n1}, t_{n2})|_{m=n1+n2}$，更一般有：$\sigma_m = (\sigma_{n1}^1, \sigma_{n2}^2, \ldots, \sigma_{nk}^k)$，

$$m = \sum_{k\geq 0} n_k \qquad (3\text{-}118)$$

定理 3-21：S_n 中的一个置换 P 可唯一分解为互无公共元素，彼此可交换的若干个轮换圈的积：$P=C_{11}C_{12}C_{13}\ldots C_{1k}$ 。C_{1i} 表示长度为 L_i 的轮换圈，称 L_i—轮换，若上式中恰有 K_j 个 j-轮换（$1\leq j\leq n$）,则称 P 为 $1_{k1}2_{k2}3_{k3}\ldots n_{kn}$-置换，这里 K_j 满足

$$K_1+2K_2+\ldots nK_n = n,\ K_j > 0，\ 1\leq j\leq n$$

显然，有如下性质：

5、 $K_1=1$，正形置换的圈表示中，恰有一个 I-轮换，即只有一个不动点（$\sigma'(x)=x$）

6、 $K_2=0$, 正形置换的圈表示中，不存在 2 轮换。

若不然，必有 $x\in Z_2^m$：$x\to\sigma'(x)\to x$ ，这样，$P'\oplus I\notin S_n$，与正形置换定义矛盾。

7、 $K_n=0$，正形置换的圈表示中，不存在 n-轮换。

因此，正形置换属于 $1^12^03^{kn}\ldots(n\text{-}1)^{kn-1}n^0$-置换类。求 $1^{j1}\ldots k^{jk}$ 型所有置换的个数

$$h(1^{j1}\ldots k^{jk}) = \frac{n!}{j_1!\,j_2!\cdots j_k!\,1^{j1}2^{j_2}\cdots k^{j_k}} \qquad (3\text{-}119)$$

利用上述公式可以求出对$|S^0(m)|$上界的估计。

目前，正形置换的计数问题尚未解决，已经有的结果如下：

$|S^0(1)|=0$

$|S^0(2)|=8=2^2!!$

$|S^0(3)|=384=2^3!!$

利用计算机，按定义搜索，可以得到：

$|S^0(4)|=2^4!!(23+32/45)$

从组合论容错原理的角度，求含 r 个不动点的 n 次置换的个数 $N(r)$ 计算问题，

$$N(r) = \frac{n!}{r!}\sum_{r\leq k\leq n}\frac{(-1)^{k-r}}{(k-r)!} \qquad (3\text{-}120)$$

而 $e^{-1} = \sum_{k\geq 0}\frac{(-1)^k}{k!}$，因此，$N(0)\approx\frac{n!}{e}$

一个正形置换是只有一个不动点的置换，S_{2^m} 中 N（1）个只有一个不动点的置换中有非正性置换，因此：

$$|S^0（m）|< \frac{2^m!}{e} \quad (3\text{-}121)$$

从拉丁方的角度，给出下界为：

$$|S^0（m）| \geq 2^{2^m}, m>1$$

F_2 上的 n 次本原多项式能够生成 Z_2^n 上极大自同构正形置换（Maximal Automophic Orthomorphism, MAO）。若函数 X_{n+1} 能够递归调用，并且 $X_k=f（x_{k-n},\ldots,x_{k-1}）$ 产生完整的正形映射，称它为极大的，是 1^1m^1 型的，$m = 2^n -1$。函数 $f（x_1,\ldots,x_n）$ 可以看作极大正形置换的生成函数。

一个 Z_2^n 上的极大正形置换是一个线性双射，因此是一个线性双射，因此是自同构的，其生成函数为 F_2^n 上的本原多项式。Z_2^n 上 n 次本元多项式

$$F（X_0，X_1，\ldots，X_{n-1}）= \sum a_i x^i$$

$a_0=1$，$a_{n-1}=1$，$a_i \in Z_2^n$，作为生成函数，能迭代生成正形置换。对于正形置换的应用在 eSTREAM 算法征集中已经可以看到一些趋势。

3.2.2.5 对称置换设计

分组密码算法在扩散层设计时，一定要考虑到上述分析特性。但是由于分组密码算法所使用的环境决定了在抗分析的同时还需兼顾密码运算速度和密码芯片大小。由于 SP 型分组密码算法的扩散层结构较 Feistel 型分组密码算法有优势，因此重点以 SP 网络结构为例并设计一个基于对称置换的 SP 型分组密码算法。SP 网络结构的轮变换分为两层：第一层为 S 混乱层，是由密钥控制的非线性置换，通常由并行查表实现；第二层为 P 扩散层，通常由与密钥无关的可逆线性变换实现。SP 结构分组密码的抗线性分析和抗差分分析的能力容易衡量，而且扩散速度快，因此许多著名的密码算法都采用了 SP 结构：如高级加密标准 AES。传统的 SP 网络结构通常用文献[45]的方法构造 S 盒，并且用与密钥无关的可逆置换实现 P 结构。

分组密码算法的设计，由于其网络的使用环境，要求有应用数学、密码学、工程实现等方面的系统指标。对密码算法强度和执行效率之间的取舍视安全要求级别而定。本文就对称置换作为分组密码扩散部分，论述圈枝结构基本特征，及此种设计的可行性和优势。

在两类分组密码设计中，置换是必备的一个环节。讨论对称置换的密码学理论基础如下：设 A 为有限集，S_n 为 A 上的 n 元置换群。

定义 3-22：置换 σ 称为对称置换，若 $\sigma^2=e$ 为恒等置换，记为 R_n。$R_n=\{\sigma|\sigma^2=e$，

σ∈S_n}。

定义 3-23[49]：设 σ∈S_n，a_1，a_2，…，a_r（$r \le n$）为 A 中的 r 个不同元素，并且 $\sigma(a_i)=a_{i+1}$，$I = 1，2，…r-1$，$\sigma(a_r)=a_1$，其他元素为 σ 置换不动点，称 σ 为 A 上长为 r 的一个轮换，记为：$\sigma=(a_1，a_2，…，a_r)$。

定义 3-24：当 s、$t \le n$，如果两个轮换（$a_1，a_2，…，a_s$）、（$b_1，b_2，…，b_t$）满足：

$$(a_1，a_2，…，a_s) \cap (b_1，b_2，…，b_t) = \varnothing$$

则称这两个轮换是独立的。

定义 3-25：任意 σ_1、$\sigma_2 \in S_n$，$\sigma_1 \cdot \sigma_2$ 为两个置换的复合：$\sigma_1=(a_1，a_2，…，a_r)$、$\sigma_2=(b_1，b_2，…，b_r)$，$\sigma_1 \cdot \sigma_2=(c_1，c_2，…，c_r)$，$c_i$ 为 b_{s+1}，$b_r=a_i$。

性质 3-6：在不考虑排列顺序意义下，任何非恒等置换能够唯一的表成若干个独立轮换之积。

性质 3-7：任意 σ_1、$\sigma_2 \in S_n$，$\sigma_1 \cdot \sigma_2$ 与 $\sigma_2 \cdot \sigma_1$ 有相同的轮换结构。

对于对称置换有如下性质：

性质 3-8：若 $\sigma \in R_n$，则：$\sigma^{-1}=\sigma$。

性质 3-9：对称置换的任一轮长都小于或等于 2

定理 3-22 对称置换的记数：对称置换的个数 $|R_n|=\sum_{r,s \ge 0, r+2S=n}(n!)/(r!\cdot s!\cdot 2^S)$

证明：由性质 3-4，若 σ 为 n 元对称置换，则：

σ 中不动点的个数与 n 有相同的奇偶性 （3-122）

将 n 个相异的元素分成 t 组，其中含一个元素的有 r_1 组，…，含有 k 个元素的有 r_k 组，显然：

$$r_1+r_2+\ldots+r_k=t \quad (3\text{-}123)$$

$$r_1+2r_2+\ldots+kr_k=n \quad (3\text{-}124)$$

则分组的方法共有

$$(n!)/(r_1!r_2!\ldots r_k!(1!)^{r1}(2!)^{r2}\ldots(k!)^{rk})\text{种} \quad (3\text{-}125)$$

（3-123）与（3-124）可得：对称置换的个数为

$$|R_n|=\sum_{r,s \ge 0, r+2S=n}(n!)/(r!\cdot s!\cdot 2^S) \quad (3\text{-}126)$$

[证毕]

定理 3-23：存在 σ，$\sigma \in R^2$，轮长为 n。

证明：1、当 n 为偶数时，不妨设 $n=2t$，构造：

$$\sigma_1=(a_1a_{t+1})(a_2a_{t+2})\ldots(a_{t-2}a_{2t-2})(a_{t-1}a_{2t-1})(a_t)(a_{2t})$$

$$\sigma_2=(a_{t+1}a_2)(a_{t+2}a_3)\ldots(a_{2t-2}a_{t-1})(a_{2t-1}a_t)(a_{2t}a_1)$$

则：$\sigma_2\sigma_1=(a_1a_2\ldots a_{t-1}a_ta_{2t-1}a_{2t-2}\ldots a_{t+2}a_{t+1}a_{2t})$　　（3-127）

2、当 n 为奇数时，不妨设为 $n=2t+1$，构造：

$\sigma_1=(a_1a_{t+1})(a_2a_{t+2})\ldots(a_{t-1}a_{2t-1})(a_ta_{2t})(a_{2t+1})$

$\sigma_2=(a_{t+1}a_2)(a_{t+2}a_3)\ldots(a_{2t-1}a_t)(a_{2t}a_{2t+1})(a_1)$

则：$\sigma_2\sigma_1=(a_1a_2\ldots a_{t-1}a_ta_{2t+1}a_{2t}a_{2t-1}\ldots a_{t+2}a_{t+1})$　　（3-128）

只需令 $\sigma=\sigma_2\sigma_1$ ，显然 $\sigma\in R^2$，轮长为 n ，定理成立。

同理，通过构造，可以使 $\sigma\in R^2$，轮长分别为{1，2，…，n}。

[证毕]

定理 3-24：轮长为 n 的 $R_n\times R_n$ 中的元素的个数共有 $n!$ 个。

证明：1、当 n 为奇数时，不妨设 $n=2t+1$；R_n 中含有 1 个不动点的置换 σ_1 有：$n!/(t!2^t)$ 个。由定理 3-24，对每一个这样的置换 σ_1，R_n 中满足 $\sigma_2\sigma_1$ 轮长为 n 的不同的置换 σ_2 的个数：对于 σ_1 的 t 个轮换中的 2 个元素任选一个作为 σ_2 的不动点，选择方法共有 $t!2^t$ 种。

因此，n 为奇数时轮长为 n 的 $R_n\times R_n$ 中的元素的个数共有：

$n!/(t!2^t)\times t!2^t=n!$ 个。

2、当 n 为偶数时，不妨设 $n=2t+2$；R_n 中含有 2 个不动点的置换 σ_1 有：$n!/(2!\,t!2^t)$ 个，0 个不动点的置换 σ_1 有：$n!/((t+1)!2^{t+1})$ 个；同理，由定理 3-24，对每一个这样的置换 σ_1，R_n 中满足 $\sigma_2\sigma_1$ 轮长为 n 的不同的置换 σ_2 的个数：方法共有 $t!2^t$、$(t+1)!2^t$ 种。

因此，n 为偶数时轮长为 n 的 $R_n\times R_n$ 中的元素的个数共有：

$n!/(2!\,t!2^t)\times t!2^t+n!/((t+1)!2^{t+1})\times(t+1)!2^t=n!$个。

由（3-123）、（3-124）可得，定理 3-24 成立。

[证毕]

由定义，如果对称置换中的元素 N_i 映射到 N_j，那么：元素 N_j 必然映射到 N_i。显然，对称置换中的一半元素就可以决定置换全体。这样，算法的加/解密硬件实现电路可以简化、运算速度得以提高。和由定理 3-23、定理 3-24 可知，对称置换虽然自身结构简单，但是通过多次迭代，置换的轮换扩张能力较强。由定理 3-24 可知，对称置换有广泛的选择范围。对称置换在分组密码设计中使用时，必须考虑算法在混乱与扩散中的效率。以现行网络使用的 128 比特标准分组来看，存在 16！即 $2\text{-}09\times10^{13}$ 种对称置换可供选择。事实上，从 $2\text{-}09\times10^{13}$ 个对称置换中选取高效、扩散速度快的置换工程量很大。以下是通过选择得到的一个对称置换在 SP 结构分组密码中的应用以及与高级加密标准 AES 扩散性能比较。

对某一 128 比特 SP 结构分组密码算法进行对称置换设计，单轮加密如图 3-4。

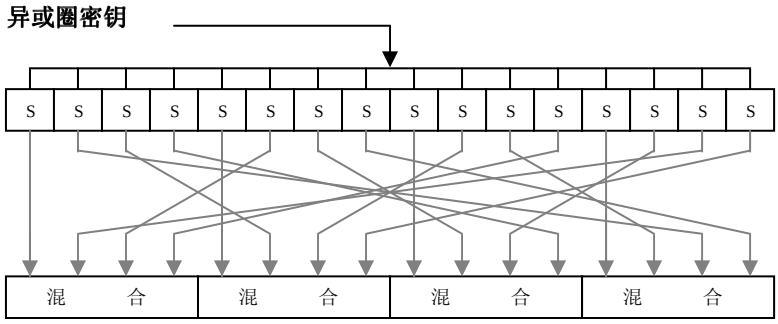


图 3-4 SP 结构分组密码单轮加密图

单轮加密步骤为：

1、 其每圈结构在进行圈密钥异或

2、 采用八进八出 S 盒设计

3、 S 盒替换后的分组以字节为单位进行对称置换

4、 置换结果再进行混合运算

加密圈数根据密钥规模而定，在本文中不做讨论。

可以看出，该对称置换有 4 个字节不动点。若以 N_i（$0\le i\le 15$）来表示经过圈密钥异或与 S 盒置换后的 16 个字节状态，则上图置换形式可以写成如下：

$$\begin{pmatrix} N_0 & N_1 & N_2 & N_3 & N_4 & N_5 & N_6 & N_7 & N_8 & N_9 & N_{10} & N_{11} & N_{12} & N_{13} & N_{14} & N_{15} \\ N_0 & N_{14} & N_5 & N_{11} & N_4 & N_2 & N_9 & N_{15} & N_8 & N_6 & N_{13} & N_3 & N_{12} & N_{10} & N_1 & N_7 \end{pmatrix}$$

若把 16 个字节按照 4×4 的矩阵排列，该对称置换可以表述为：

$$\begin{matrix} \mathbf{0} & 4 & 8 & 12 \\ \mathbf{1} & 5 & 9 & 13 \\ \mathbf{2} & 6 & 10 & 14 \\ \mathbf{3} & 7 & 11 & 15 \end{matrix} \quad \Rightarrow \quad \begin{matrix} \mathbf{0} & 4 & 8 & 12 \\ 14 & \mathbf{2} & 6 & \mathbf{10} \\ 5 & 9 & 13 & \mathbf{1} \\ \mathbf{11} & 15 & \mathbf{3} & 7 \end{matrix}$$

显然，上述设计中的每个字节的信息可以均匀扩散到其余 16 个字节中。以 N_0 字节为例，其信息扩散轨迹如下：

第一圈:N_0 —S 盒→ N_0 — 置换 → N_0 —混乱→ $N_0\,N_1\,N_2\,N_3$

第二圈:$N_0\,N_1\,N_2\,N_3$ — S 盒 → $N_0\,N_1\,N_2\,N_3$ — 置换 → $N_0 N_{14} N_5 N_{11}$ →混乱所有字节。

第三圈运算后 N_0 字节信息已经完全溶入各个字节。

采用上述对称置换的设计，从扩散的角度与原有 AES 具备相同级别强度的效果。而且无论在软件实现或硬件实现时，运算速度提高、硬件空间减小。更重要的是：采取对称置换设计的分组密码在一定程度上破坏了原有的代数特征，而使算法抗线性分析性能加强。

对称置换的乘积圈结构与其不动点的个数、位置以及轮换的位置、连接结构有关。在迭代过程中圈结构具备多样性。分组密码的迭代设计方法恰好克服了对称置换本身圈结构的简单化。由于对称置换只需一半的映射关系就可反映所有特点，在加/解密时使用同一非线性变化。因此，在分组密码设计中使用对称置换可以使算法在硬件实现时节约空间，同时能够提高加、解密速度。把这种设计嵌入标准分组密码中替换其原有的置换算法，可以得到一个新的分组算法。通过检测，可以证明这种设计具备抗差值分析、线性分析、差分分析和代数分析能力。就目前公开的分组密码算法来看，对称置换并不被经常使用，但这种置换确实可以在硬件开销方面为算法增加一点优势。

3.3 分组密码算法硬件模块设计与评估

3.3.1 相关概念

在 1998 年，Paul Kocher,、Joshua Jae 和 Benjamin Jun 提出了能量分析法。简单能量分析法（Sample Power Attack ，SPA）直接对在加解密过程中能量消耗进行分析解释，得出算法的相关信息甚至是密钥。差分能量分析（Differential Power Attack ，DPA）功能更强，可以在信号相对较低的情况下获取系统泄漏的较多信息。与 SPA 相似，DPA 对测量设施的要求并不高，更精确以及更高的采样频率会取得更好的效果。针对代替、置换 SP 类分组密码的特殊性，进行了抗能量分析模块结构分析研究。

密码芯片的传统设计思想一般认为分析者仅能获取输入消息和输出消息，而其他有关密钥的信息则无法获取。而密码设备运算时的实际信息泄漏情况却并非如此。最基本的旁路分析能够成功是由于与密钥相关的处理设备在运算过程的中间状态能量消耗被捕获。DPA 使用了加密算法步骤中相关密钥与能量消耗之间的关系。分组密码是网络上广泛使用的一类密码，是国际上公开密码算法中最活跃的一个分枝。其设计理念是保密依赖于密钥，而算法大多公开。SP 结构因为其混乱和扩散速度优于 Feistel 网络结构设计而逐渐成为该领域的主流设计方案。针对

密钥的 DPA 分析是分组密码分析的特有的方法。

3.3.2 分组密码算法硬件模块保护设计

通常对于分组密码芯片的抗能量分析设计采用添加掩码的方式。通过随机数掩码使得明消息分组在加密之前随机化，在解密之后能够去掉掩码而彻底还原出明消息。并且通过对掩码的分析计算模式来达成对掩码的纠错。但是，代价是硬件实现时芯片面积会加倍。另外一种保护模式通过掩码及掩码数据的管道计算，添加一个 128Bit 的移位寄存器。实际上，第一种方法并不比第二种方法使用更多的元件，而且保护措更加直接。当然，对于掩码的设计从产生算法到掩码的硬件实现方面就工程上的实现需要进一步讨论。

SP 分组密码自身的结构就一圈看来，可分为线性结构与非线性结构。其中，线性结构包括 S 盒中仿射变换、列混合、行扩散及密钥异或；非线性结构包括 S 盒中的逆运算。自然的，对线性、非线性结构采取不同的方式分别进行保护会减少信息泄露。由于网络上现行的国际标准数据多是以 128Bit 为分组单位，密钥至少为 128Bit，根据安全强度要求的不同，还有例如 192Bit、256Bit 密钥的标准。以下的讨论基于 128Bit 分组，128Bit 密钥规模的分组密码算法。

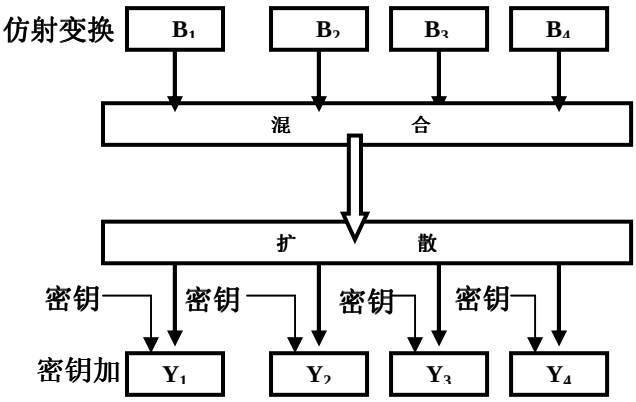


图 3-5 SP 结构部分线性变换

128Bit 分组的 SP 结构分组密码可视作四组 32Bit 字的变换。每一个字的线性变换部分（图 3-5）。每次变换包括 32Bit 明消息、32Bit 密钥共 64Bit 的输入，32Bit 密数据的输出。

当对线性部分进行过掩码保护后，可能会使原始信息产生误码，对误码的探测（Differential Faulty Attack, DFA）与纠正也非常关键。直观的方法就是对原始加密信息进行预先运算与线性保护后的加密信息进行异或，显示出错误率及错误发

生的位置。但是代价表现在预运算部分在储存空间的开销。对 $Y_1 \oplus Y_2 \oplus Y_3 \oplus Y_4$ 的线性预先计算在容错范围内可以作为原始加密信息的签名。这样，当密码芯片出现故障时，能够被及时发现。而且通过累加运算后实现过程变得简便与节省。

总之，对 SP 结构分组密码线性部分的保护仍然使用线性码对明消息分组随机化。当时间与空间允许时，直接使用预先运算的原始序列进行错误探测与纠正。通过对每一个分组中的字结构做适当的变换，也可以达到检错的目的，同时节省时间与空间。

SP 结构分组密码的非线性变换体现在 S 盒结构的求逆运算中。

定义 GF（2^8）上的乘法为：当 X 不等于零，$X \cdot X^{-1}=I_8$（I_8 为 GF（2^8）上单位元），当 $X=0$，$X \cdot X^{-1}=0$。因此，AES 及使用类似 S 盒的分组密码在非线性部分都存在一个 0 不动点，即 0 的逆仍然为 0。针对这个特点，仅在掩码处测试 0、1 值（图 3-6）。

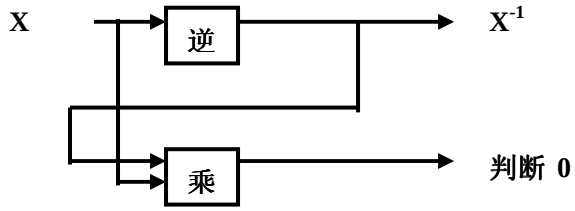


图 3-6 非线性模块保护

这样，形成了对非线性部分的保护。同时对这部分信息达到签名保护错误监测的效果。对八进八出的 S 盒，设任意 r（$r<9$），GF（2^8）中向量与自身逆元乘法之后，单位向量 I_r 产生错误的概率等于向量空间向量求取逆元出现错误的概率（因为求逆运算的结果也依赖于输入向量）。设 E_B、E_r 分别为逆运算及乘法部分产生的错误，X 为输入向量，$\mathbf{X}$、$\mathbf{E_B} \in$ GF（2^8），$E_r \in$ FG（2^r）有：

$$[X^{-1} \oplus E_B] \cdot X = I_r \oplus E_r$$

由上述处理方法，乘法有 16Bit 的输入，在 X 非 0 的情况下产生 8Bit 的‘1’值。产生 rBit 错误时探测不到的概率为 2^{-r}，探测到的概率为 $1-2^{-r}$。通过 m 次随机处理之后概率变被动变为 2^{-rm}。

同时，在上述方法之上还可以对 X 进行与线性部分相同的随机化处理。但是 X 更复杂的变换不包括在保护部分。

对 SP 结构分组密码抗能量分析芯片的设计以往多采用在明消息入口处进行随机化设计。由于 SP 结构分组密码在 S 盒求逆运算时存在零不动点，所以只针对非线性模块的保护设计在一定程度上能对密码芯片产生保护作用。由于涉及范围小、

附加算法简单，使得只针对密码芯片非线性部分保护的规模能得到控制。当对算法非线性、线性部分模块都采取适当的保护时，芯片在算法的两个不同方面进行了抗能量分析设计。显然，以上两种保护方法在安全强度、电路规模上会有所区别。并且，分组密码模块保护方法在对非线性、线性算法模块保护设计在抗能量分析的同时，对数据进行了签名与正确性检测。

因此，针对 SP 结构分组密码芯片进行分别保护设计，能使芯片抗能量分析设计在线性保护、非线性保护及两种保护组合应用中灵活选用，可以控制加密硬件的复杂度，同时达到使电路能量消耗趋于平衡的目的。

对于完全依赖密钥保密的分组密码算法，密钥与明消息结合部分的防止能量泄露特别关键。如果当任何门电路的输入都不能改变电路中能量的稳定性，这样的芯片设计可以有效的防止能量分析。使用随机掩码对加密算法进行处理，特别是本文中提出的选用线性部分、非线性部分模块保护的算法，可以根据使用要求的安全级别，采用线性保护、非线性保护以及线性与非线性模块保护三种方式对电路实施防能量泄露处理，以保证不同安全级别的密码芯片安全。

提出的设计方法也适用于算法非线性、线性部分模块能够独立分开的一类密码芯片。模块保护设计能够从多个角度实施抗能量分析。同时，对密码算法芯片线性部分与非线性部分提供简单验证、监测。

3.4 分组密码算法密钥及结合模块设计

分组密码算法因为自身的公开性，安全性侧重在密钥设计上。目前公开的分组密码算法中密钥扩展部分多是基于加密算法中已有的部分，通过非线性变换及相关变换进行密钥运算。国际标准化组织也在一个公开分组密码算法确定之后的若干年内进行运算模式的研究与征集。

3.4.1 密钥设计方法研究

分组密码算法中密钥设计的关键是空间开销的问题，如果加密和解密运算使用相同的程序，算法中的轮密钥部分就需要一定空间进行存储。以下分别讨论几种典型分组密码算法的密钥设计方案。

AES 的密钥扩展运算借用了加密算法中的非线性 S 盒部分，一次生产出一组明消息 Nr 轮加密所需要的密钥。随着分组密码算法的高次迭代密钥初始向量因素逐步产生作用。由于算法公开，分组密码算法中密钥使用协议的严谨程度直接对

整个密码系统的可信度产生影响。以下就 AES 对密钥扩展算法的细节与主加解密函数的结合方式进行讨论。

3.4.2 密钥结合模式研究

由于分组密码算法保密依赖于密钥，所以对密钥算法本身的设计需要重点研究以外，在密钥与密码算法本身结合部分如果进行设计上的改进，会使分组密码算法使用时更加安全。为了在使用基于网络使用的分组密码算法时不需要更多的专业密码方面的知识，密钥的相关协议也能够产生积极的作用。本小节将就密钥结合模式进行讨论，提出一种带比特延迟的密钥结合模式，充分掩盖密钥算法的生成特性，设计如图 3-7。

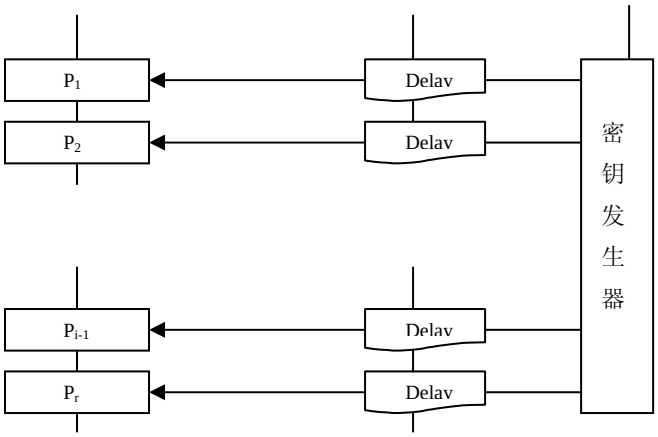


图 3-7 带比特延迟的密钥结合方式

具体的结合方式可以参照下节的运算模式。

3.5 分组密码算法的几种运算模式

分组密码算法由于其使用环境的宽泛性，较其他密码而言，在强调密码学性质的同时，还要求工程实现上的高速。为了硬件设计在时效上的经济性，其密钥在安全上依赖密码算法本身的一些函数；在密钥结合及密码运算模式上的一些设计可以弥补分组密码算法自身的某些缺陷，而且能够提高速度和安全。以下介绍常用的几种分组密码算法运算模式，这些运算模式在 DES 阶段就被广泛的使用，随着 AES，NESSIE 分组密码算法标准的推出，模式标准化工作也在得到发展。这项工作已经引起广泛的关注。

电码本模式（Electronic Book Code Mode, ECB），其工作方式如图 3-8：

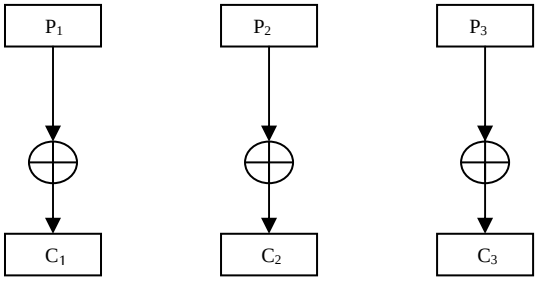


图 3-8 分组密码算法 ECB 运算模式

密数据分组链接模式（Cipher Block Chain Mode, CBC）图 3-9：

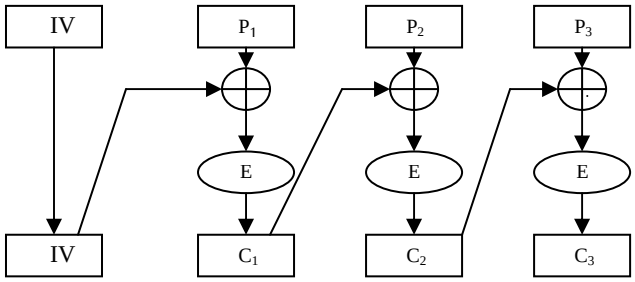


图 3-9 分组密码算法 CBC 运算模式

明消息进行加密之前与前面的密数据进行异或。IV 为初始值。

密数据反馈模式（Cipher Feedback Mode, CFB）图 3-10

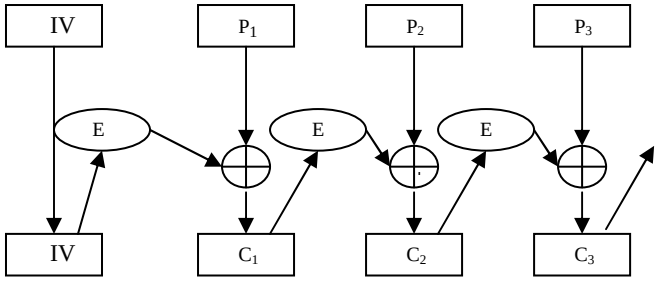


图 3-10 分组密码算法 CFB 运算模式

此时的分组密码算法作为一个密钥流产生器，在 J 比特密数据反馈下，每次输出 J 比特密钥对输入的 J 比特明消息进行并行加密。如果考虑 CFB 能在更宽的程度使用，并且具备更强的抗唯密数据分析特性，可对 CFB 模式进行如下设计：

1、带比特延迟的密数据反馈模式（Cipher Feedback Delay Mode, CFBD）

延迟的字数需要根据实际情况中运算速度和芯片内存大小而定，配合安全所需要的强度：如果对安全强度要求较高，则增加延迟的字数；如果对加密速度更

加看中，则可不对延迟启动。量化的指标因不同的分组密码算法不同（图 3-11）。

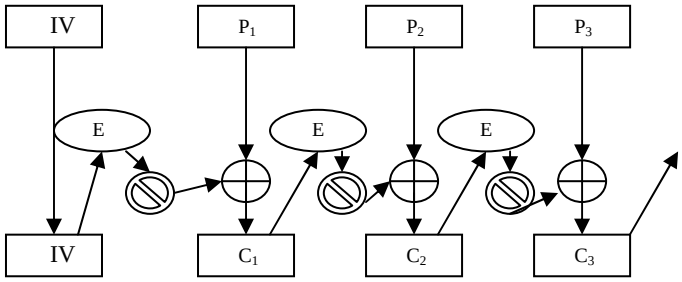


图 3-11 分组密码算法 CFBD 运算模式

2、输出反馈模式（Output Feedback Mode, OFB）如图 3-12

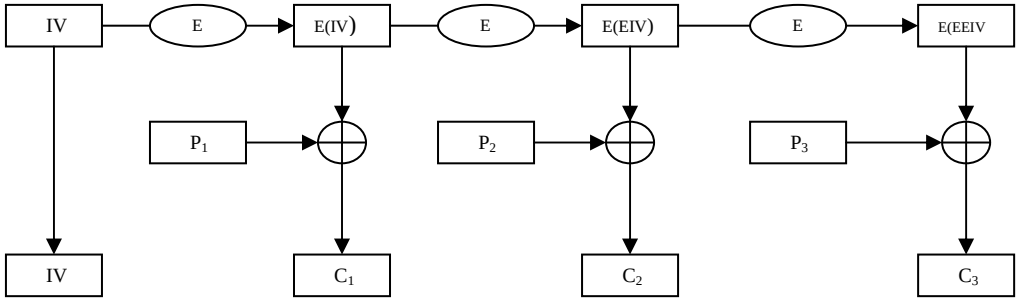


图 3-12 分组密码算法 OFB 运算模式

分组密码的运算模式[50]是利用分组密码解决实际问题的密码方案。好的运算模式可以弥补分组密码的某些缺憾；相反，不好的运算模式可能带来安全隐患。运算模式的研究始终伴随着分组密码的研究历史，新的分组密码标准的推出，都会伴随着相应运算模式的研究。从针对 DES 的 ECB、CBC、CFB、和 OFB，到针对 AES 的 CTR、CCM、CMAC、GCM 和 AESKW，分组密码运算模式经历了二十年的变化。在 AES 即将诞生之际，2001 年 NIST 公布了 AES 用于保密的 5 种运算模式，分别是：ECB、CBC、CFB、CTR。其中 CTR 模式是与前四种惯用的模式不同的运算模式。

3、CTR 模式

以下是 CTR 模式的具体介绍：

给定计数序列 T_1，T_2，…，T_{t-1}, T_t，对于明消息 X_1，…，X_{t-1}，X_t（其中 X_1，…，X_{t-1} 为 n 比特，X_t 为 u 比特），CTR 的加密过程为：

$$O_i=E_k（T_i），I=1，2，…，t；$$

$$Y_i=X_i⊕ O_i，I=1，2，…，t-1；$$

$$Y_i=X_i\oplus MSB_u（O_t）$$

CTR 的解密过程为：

$$O_i=E_k（T_i），I=1，2，…，t；$$

$$X_i=Y_i\oplus O_i，I=1，2，…，t-1；$$

$$X_i=Y_i\oplus MSB_u（O_t）$$

其中 $MSB_u（O_t）$ 表示 O_t 的高 u 比特。

CTR 可以并行，并可通过预处理提高速度，其安全性至少和 CBC 一样好，可加密任意长度的消息，但没有完整性，对错误没有冗余度。

3.6 三种新的运算模式及可证安全性

可证安全性（Provable Security, PS）理论最早应用于公开密码体制及单向散列函数中，对安全协议框架证明而采取的一种方法，这一阶段的研究者是一些计算机科学领域的学者。1979 年，Rabin 密码体制利用了大素数分解数学难题而证明了安全性。随后 Goldwasser 和 Micali 给出了两种更严格的定义：一是可证安全的概念是基于语义安全的，这也是选择密数据分析的前身；另一种是普遍的安全性证明，包括了 Naor-Yung 和 Rackoff-Simon 的选择密数据分析的思想，这两种可证明安全的概念有很强的相关性。第二次的理论进展是 1980 年数字签名的安全性证明——Goldwasser 和 Micali 把选择密数据分析发展成为了选择消息分析，用存在伪造的观点代替了语义安全性和普遍性。这一时期的安全性概念包括的执行运算时间、能量消耗、电磁泄露、逻辑错误、消息错误。90 年代两个最大的贡献在于 Bellarehe Rogaway 的“随机预言机制”与“面向应用的可证安全性”理论。因为他们的贡献可证安全性理论得到了极大范围的认可与发展。可以看出：对于以数学难题为基础的公钥体制的非对称密码体制和单向散列函数，在可证安全性领域进行了很多的工作；但是就对称密码体制而言，这方面的工作几乎没有进行。

运算模式是分组密码算法的加解密过程中非常必要的一种手段，国际上许多的密码学家已经讨论了多种模式。为此，国际标准化组织 NIST 在高级加密算法 AES 确定的同时，专门进行了加密模式的标准与制定。但是，国内除了少数对 NIST 标准的执行模式的讨论之外，国内在可证安全性对方面的研究与实际应用还没有公开研究结论。先对分组密码算 *CTR*,*CCM*,*CMAC* 法加密模式进行一定的描述，再用可证安全性理论对他们进行可证安全性研究。最后是对于前面的一些证明在不同通信环境下使用的一些结论。

设 M 是一个集合，C 为该集合上的密码体制，F 是作用在这个集合上的密码函数；D 为一个可能发生的事件，设标准值 $d \in D$。事件 D 不发生的概率记为：$\Pr(\overline{D})$。记 $|M|$ 为 M 所包含的元素的个数；使用穷尽的方法寻找 F 与其线性逼近（或其它）构造的完全随机仿真函数 F^* 的偏差（或距离）定义为：$AdvF^{ATC(d)} = \max_D\{Adv_d^{ATC(d)}(F, F^*)\}$；使用穷尽的方法寻找 C 与其逼近构造的完全随机仿真的密码系统 C^* 的偏差（或距离）定义为：$AdvC^{ATC(d)} = \max_D\{Adv_d^{ATC(d)}(C, C^*)\}$。通常约束这两个值来限定一个密码体制或密码函数的逼近仿真。

若密码体制的运算模式为 $Mode(C)$，在该密码体制的作用下，消息块数 $mess$ 在 d 块加密过程后的最佳随机预言机优势记为：$Adv^{ATC(d|mess)}(Mode(C))$；满足条件 A 的最佳随机预言优势为：$Adv^{ATC(d|q)}(Mode(C) \mid A)$。

分组密码算法运算模式在 DES 时期的标准有 ECB、CBC、DFB、OFB 四种。2001 年的 800-38A 中确定了 AES 的五种运算模式：ECB、CBC、CFB、OFB 和 CTR；2004 年 5 月公布的 SP800-38C 中建议了认证保密模式 CCM；2005 年 5 月公布的 SP800-38B 中加入了认证模式——CMAC。事实上，各种运算模式都存在各自的不足之处，因此在不同的使用环境选择恰当的运算方式能够使得密码算法的安全功能达到最好的效果。由于 ECB、CBC、DFB、OFB 四种保密模式在多种场合进行深入的研究。以下叙述 AES 标准中新增加的 CTR、CCM、CMAC 模式。

1、加密计数模式（Counter Mode Encryption，CTR）及可证安全性（图 3-13）

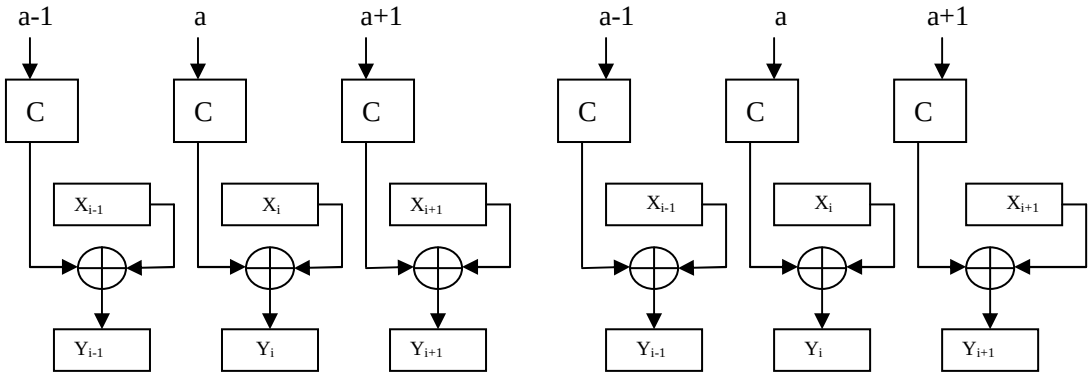


图 3-13 分组密码算法 CTR 运算模式的加解密过程

加密计数模式是 Diffie Hellman 在 1979 年提出的，直到在 AES 运算模式的征集中才由于其简单和高速的优点而得以使用。

CTR 模式是 OFB 模式的一种变形，该模式引用了一个由初始密钥产生的随机记数序列 Counter。$K_i = C(counter(i))$，设明消息 $X = x_0 x_1 \cdots$，密数据 $Y = y_0 y_1 \cdots$，

加解密形式为：$y_i = x_i \oplus K_i, x_i = y_i \oplus K_i$。

定理 3-25：F^*是集合M上的完全随机函数，$ATC, mess, d(d \geq mess)$如前所定义，那么下式成立：

$$Adv^{ATC(d|mess)}(CTR[F^*]) \leq \frac{mess \cdot d}{|M|} \tag{3-129}$$

证明：设$C_1 = CTR[F^*], C_2 = C^*$是$M$上的完善密码体制。如果分析者获得了如下的明、密对：$X_j = x_{j1}x_{j2}, \cdots, x_{jn_j}, Y_j = y_{j1}y_{j2}, \cdots, y_{jn_j}$，$1 \leq j \leq mess$，$n_1 + n_2 + \cdots + n_{mess} = d$，$n_j$为消息的块数。$D_k$是一系列事件成立，如果：

$(u,a) \neq (v,b), 1 \leq u, v \leq k, 1 \leq a \leq n_u, 1 \leq b \leq v \Rightarrow y_{u,0} + a \neq y_{v,0} + b,$

即明消息不同，则密数据必不同。假设$D_0 = 1, D = D_{mess}$。

如果D_k成立，并且$y_{ka} = F^*(y_{k0} + a) \oplus x_{ka}$是随机序列，$C^*, CTR[F^*]$之间的距离可以忽略。如果两组不同的明消息$Y_m, Y_n, m < n$会产生碰撞当且仅当存在一组常数（$a,b$）使得$Y_m + a = Y_n + b$。那么，$Y_n$的碰撞存在当且仅当$Y_{n0} > Y_{m0} - t_n, Y_{n0} < Y_{m0} + t_m$，并且，$Y_m, Y_n, m < n$可能碰撞的次数为：$t_n + t_m - 1$。$Y_n$仅在前一块数据产生碰撞的概率为：

$$\Pr[\overline{D_k} \mid D_{k-1}] \leq \frac{\sum_{m=1}^{n=1}(t_m + t_n - 1)}{|M|} = \frac{(n-1)(t_n - 1) + \sum_{m=1}^{n-1} t_m}{|M|}$$

因此：

$$AdvC^{ATC(d|mess)}(CTR[F^*]) = \Pr[\overline{D}] = \Pr[\overline{D_{mess}}]$$

$$\leq \sum_{m=1}^{mess} \frac{(m-1)(t_m - 1) + \sum_{n=1}^{m-1} t_n}{|M|} \leq \sum_{m=1}^{mess} \frac{mt_m}{|M|} + \sum_{m=1}^{mess}\sum_{n=1}^{m-1} \frac{t_n}{|M|}$$

$$= \sum_{m=1}^{mess} \frac{mt_m}{|M|} + \sum_{n=1}^{mess}\sum_{m=1}^{mess-1} \frac{t_n}{|M|} = \sum_{m=1}^{mess} \frac{mt_m}{|M|} + \sum_{m=1}^{mess} \frac{(mess - m)t_m}{|M|}$$

$$= \sum_{m=1}^{mess} \frac{mess \cdot t_m}{|M|} = \frac{mess}{|M|} \sum_{m=1}^{mess} t_m = \frac{mess \cdot d}{|M|} \quad \text{[证毕]}$$

定理 3-26：设F是一个密码函数，$F: M_1 \to M_2$，$ATC, mess, d(d \geq mess)$如前所定义，那么：$Adv^{ATC(d|mess)}(CTR[F]) \leq Adv^{ATC^+(d)}(F) + \frac{d \cdot mess}{|M|}$。

定理 3-27：设 $F*$ 是集合 M 上的完全随机函数，$CPA,mess,d(d \geq mess)$ 如前所定义，那么下式成立：

$$Adv^{CPA(d|mess)}(CTR[F*]) \geq (1-\frac{1}{e})(1-\frac{1}{|M|})\frac{mess \cdot d}{|M|} \qquad (3\text{-}130)$$

证明：针对 CTR 运算模式 d 方向上的分别分析：

1、生成一个消息 $mess$ $X_k = x_{k1}x_{k2}\cdots x_{kn_q}(1 \leq k \leq mess.\sum_{k=1}^{q} n_k = d)$ 在所有的块中都有相同的值。即：$\exists v \in M : \forall k,a : x_{ka} = v$

2、*For k=1* to *mess do*

2-1 Get $Y_k = y_{k0}y_{k1}\cdots y_{kn_q} = C(X_k)$，$C$ 是 $CTR[F*]orC*$

3、如果 $\exists u,v \leq mess,a < n_u,b < n_v,(u,a) \neq (v,b) : y_{u0} + a = y_{v0} + b$

3-1 如果 $y_{ua} = y_{vb}$ 那么输出"*accept*"

4、输出"*reject*".

D_k, D 如同定理 3-23 的定义，如果 CTR 运算分别分析发现了碰撞，则预言机制结束。记数 $Counter$ 的初始向量可以随便产生，碰撞发生的概率是相同的。假设输出为 i 的碰撞产生的概率为 P_i，$P_i = \frac{1}{|M|^d}\sum_{X,Y} 1_{(X,Y)\in D}[F_i]_{X,Y}^d$，那么：

$$p_0 = \Pr[\overline{D}], p_1 = \Pr[\overline{D}]\frac{1}{|M|},$$

$$|p_0 - p_1| = \Pr[\overline{D}](1-\frac{1}{|M|})$$

$$\Pr[D_k \mid D_{k-1}] \leq \frac{|M| - \sum_{t=1}^{k-1} n_t}{|M|} = 1 - \frac{\sum_{t=1}^{k-1} n_t}{|M|}$$

因此：

$$\Pr[D] = \Pr[D_{mess}] = \prod_{k=1}^{mess}\Pr[D_k \mid D_{k-1}] = \prod_{k=1}^{mess}(1-\frac{\sum_{t=1}^{k-1} n_t}{|M|}) \leq \prod_{k=1}^{mess} e^{-\frac{\sum_{t=1}^{k-1} n_t}{|M|}}$$

$$= e^{-\sum_{k=1}^{mess}\frac{\sum_{i=1}^{k-1} n_i}{|M|}} = e^{-\frac{\sum_{i=1}^{mess}\sum_{k=1}^{mess-1} n_t}{|M|}} = e^{-\frac{\sum_{i=1}^{mess}(mess-t)n_t}{|M|}} \leq e^{-\frac{\sum_{i=1}^{mess} mess \cdot n_t}{|M|}} = e^{-\frac{mess \cdot d}{|M|}}$$

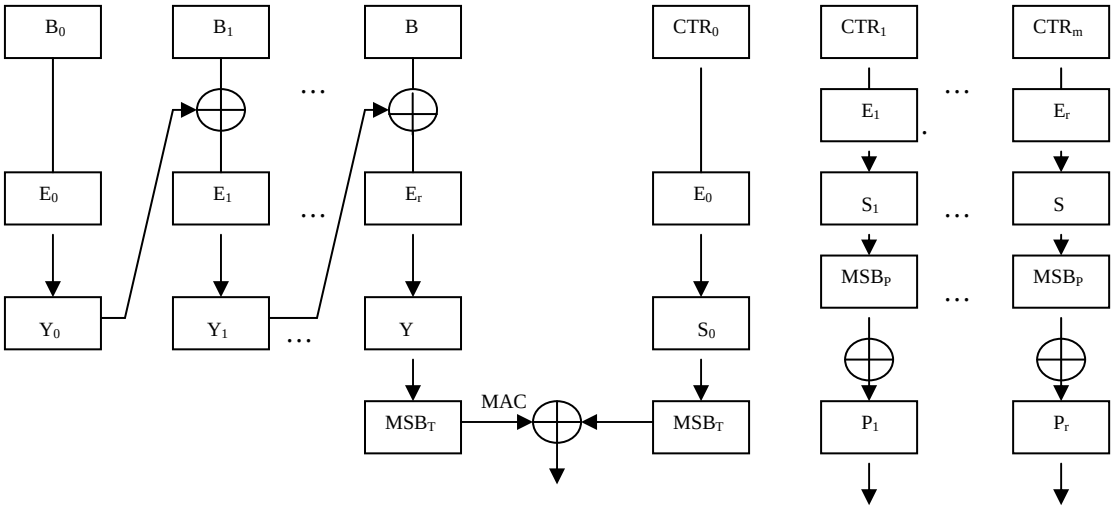
$$\Pr[\overline{D}] = 1 - \Pr[D] \geq 1 - e^{-\frac{mess \cdot d}{|M|}} \geq (1 - \frac{1}{e}) \frac{mess \cdot d}{|M|}$$

$$Adv^{CPA(d|mess)}(CTR[F^*]) \geq (1 - \frac{1}{e})(1 - \frac{1}{|M|}) \frac{mess \cdot d}{|M|} \quad (3\text{-}131)$$

[证毕]

通过认证模式的运算过程可以看出：每个密数据块之间没有信息重叠。

2、认证保密模式（Counter with Cipher Block Chaining-Message Authentication Code，CCM）及可证安全性（图 3-14）：



$$C = (P \oplus MSB_{|P|}(S)) \| (MAC)$$

图 3-14 分组密码算法的 CCM 运算模式

认证保密模式即是在 $SP800-38C$ 中采用的分组密码算法运算模式，也是 $IEEE802.11$ 的无线局域网的运算模式，并且通过 $RFC3610$ 进行标准化。尽管对 CCM 存在一些争论，但是两大标准对其的认可说明这种运算方式具备优势。图中分组密码算法 E，密钥 K，记数 $Counter$ 的生成函数为 g，格式函数 f 及 MAC 的长度为 τ；输入随机数 N，消息 P 和相关数据 A。如果预先处理过程为：

$$f(N, A, P) = B_0 \| B_1 \| \cdots \| B_r, |B_i| = n, 0 \leq i \leq r \text{。}$$

可以看出 CCM 运算模式是 CTR 运算模式加上 CMAC 验证码，但分别是两种算法调用加密函数次数的和。

定理 3-28：设 F^* 是一个 M 上的完美函数，$ATC \in \{CPA, ACPA\}$ 是传统意义下

的选择明消息分析与已知明消息分析，$d,mess$ 是整数 $(mess \le d)$，那么

$$AdvC^{ATC(d|mess)}(CCM[F^*]) \le \frac{d^2}{2|M|} \qquad (3\text{-}132)$$

证明：证明：设 $C_1 \coloneqq CCM[F^*]$，并且 $C_2 = C^*$。假设分析者已知明、密数据对：$X_j = x_{j1}x_{j2},\cdots,x_{jn}$，$Y_j = y_{j0}y_{j1}y_{j2},\cdots,y_{jn}$，$1 \le j \le q$，并且 n_j 是分组数，$n_1 + n_2 + \cdots + n_q = d$。

设所有 y_{jl}，$1 \le j \le q$，并且 $0 \le l < n_k$，因此，y_k 定义为序列的第 K 个元素，

$$y_k = y_{ab}$$

设 α 是使下列等式成立的最大整数，$\sum_{j=1}^{\alpha-1} n_j \le k, b = k - \sum_{j=1}^{\alpha} n_j$。假设 x_k 为明消息，经过分组密码算法加密后变换为 y_k，假设 D_k 为使下列条件成立的事件：

$$u,v < k, u \ne v : y_u \oplus x_{u+1} \oplus MAC_u \ne y_v \oplus x_{v+1} \oplus MAC_v$$

$$u \ne v, y_u \oplus x_{u+1} \oplus MAC_u \oplus k_i \ne y_v \oplus x_{v+1} \oplus MAC_v \oplus k_i, i = 1,2$$

函数 F^* 的输入明消息不同，则输出一定不同。规定 $D_{-1} = 1, D = D_{d-1}$。

设 CCM 运算模式下在第 K 个元发生第一次碰撞的概率为：

$$\Pr[\overline{D_k} \mid D_{k-1}] = \Pr[\exists u < k : y_k = y_u \oplus x_{u+1} \oplus x_{k+1} \oplus MAC_u \oplus MAC_k \mid D_{k-1}]$$

$$= \Pr[\exists u < k : F^*(y_{k-1} \oplus x_k \oplus MAC_k) = y_u \oplus x_{u+1} \oplus x_{k+1} \oplus MAC_u \mid D_{k-1}] = \frac{k}{|M|}$$

如果发生碰撞的元为 y_{a0}，上述表达式为：

$$\Pr[\overline{D_k} \mid D_{k-1}] = \Pr[\exists u < k : y_{a0} = y_u \oplus x_{u+1} \oplus x_{k-1}] = \frac{k}{|M|}$$

则：

$$AdvC^{ATC(d|mess)}(CCM[F^*]) = \Pr[\overline{D}] = \Pr[\overline{D_{d-1}}] \le \sum_{k=0}^{d-1} \Pr[\overline{D_k} \mid D_{k-1}]$$

$$= \sum_{k=0}^{d-1} \frac{k}{|M|} = \frac{d^2}{2|M|}$$

[证毕]

定理 3-29：设 F^* 是集合 M 上的完全随机函数，$CPA, mess, d, d \ge mess$ 如前所定义，那么下式成立：

$$Adv^{CPA(d|mess)}(CCM[F*]) \geq (1-\frac{1}{e})(1-\frac{1}{|M|})\frac{mess \cdot d}{|M|} \qquad (3\text{-}133)$$

证明类似于定理 3-28。

3、认证模式（Cipher-based Message Authentication Code，CMAC）及可证安全性（图 3-15）：

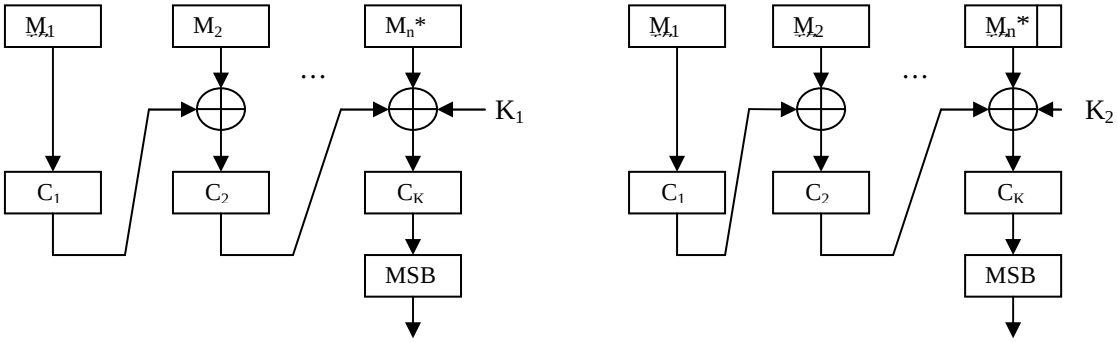


图 3-15 分组密码算法 CMAC 运算模式的加密过程

CMAC 是分组密码算法通过运算代替 HASH 函数功能的一种模式（如图 3-5-5），算法依赖对称密钥分组密码算法的选择，提供数据完整性和差错检测的保障。对于给定的密钥，分组密码算法由两种运算方式决定：如果消息分组正好满足整块，使用密钥 K_1 来进行运算；如果消息分组有剩余，则使用填充码填成一组后在使用 K_2 进行运算。作为单向函数的使用，因此 CMAC 模式没有考虑逆函数。

定理 3-30：设 F^* 是一个 M 上的完美函数，$ATC \in \{CPA, ACPA\}$ 是传统意义下的选择明消息分析与已知明消息分析，$d, mess$ 是整数 $mess \leq d$，那么

$$AdvC^{ATC(d|mess)}(CMAC[F^*]) \leq \frac{d^2}{2|M|} \qquad (3\text{-}134)$$

证明：设 $C_1 := CMAC[F^*]$，并且 $C_2 = C^*$。假设分析者已知明消息：$X_j = x_{j1}x_{j2},\cdots,x_{jn}$，密数据：$Y_j = y_{j0}y_{j1}y_{j2},\cdots,y_{jn}$，$1 \leq j \leq q$，并且 n_j 是分组数。因此，$n_1 + n_2 + \cdots + n_q = d$。

设所有 y_{jl}，$1 \leq j \leq q$，并且 $0 \leq l < n_k$，因此，y_k 定义为序列的第 K 个元素，

$$y_k = y_{ab}$$

设 α 是使下列等式成立的最大整数，$\sum_{j=1}^{\alpha-1} n_j \leq k, b = k - \sum_{j=1}^{\alpha} n_j$。假设 x_k 为明消息，

经过分组密码算法加密后变换为 y_k，假设 D_k 为使下列条件成立的事件：

$$u,v<k,u\neq v: y_u \oplus x_{u+1} \neq y_v \oplus x_{v+1}$$
$$u\neq v, y_u \oplus x_{u+1} \oplus k_i \neq y_v \oplus x_{v+1} \oplus k_i, i=1,2$$

函数 F^* 的输入明消息不同，则输出一定不同。规定 $D_{-1}=1, D=D_{d-1}$。

事件 D 发生，保证了所有密码输入不会产生碰撞，则所有密码分组 y_{ab} 是完全随机的。因此，使用分别分析的方法对于 $CMAC[F^*]$ 与 C^* 都不能产生根本的作用。设 $CMAC$ 运算模式下在第 K 个元发生第一次碰撞的概率为：

$$\Pr[\overline{D_k} \mid D_{k-1}] = \Pr[\exists u<k: y_k = y_u \oplus x_{u+1} \oplus x_{k+1} \mid D_{k-1}]$$
$$= \Pr[\exists u<k: F^*(y_{k-1} \oplus x_k) = y_u \oplus x_{u+1} \oplus x_{k+1} \mid D_{k-1}] = \frac{k}{|M|}$$

如果发生碰撞的元为 y_{a0}，上述表达式为：

$$\Pr[\overline{D_k} \mid D_{k-1}] = \Pr[\exists u<k: y_{a0} = y_u \oplus x_{u+1} \oplus x_{k-1}] = \frac{k}{|M|}$$

则：

$$AdvC^{ATC(d|mess)}(CMAC[F^*]) = \Pr[\overline{D}] = \Pr[\overline{D_{d-1}}] \le \sum_{k=0}^{d-1} \Pr[\overline{D_k} \mid D_{k-1}]$$

$$= \sum_{k=0}^{d-1} \frac{k}{|M|} = \frac{d^2}{2|M|}$$

[证毕]

定理 3-31：设 C^* 是 M 上的完善密码体制，$ATC \in \{CPA, ACPA\}$ 是传统意义下的选择明消息分析与已知明消息分析，$d, mess$ 是整数 $mess \le d$，那么

$$AdvC^{ATC(d|mess)}(CMAC \mid C^*) \le \frac{d^2}{|M|} \quad (3\text{-}135)$$

显然。

定理 3-32：设 F^* 是一个 M 上的完美函数，$d<\sqrt{2M}$，$mess\ (mess \le d)$ 是一个整数，则：

$$Adv^{CPA(d|mess)}(CMAC[F^*]) \geq (1-\frac{1}{e}-\frac{1}{|M|})\cdot\frac{d^2}{2|M|} \qquad (3\text{-}136)$$

证明类似于定理 3-31。

当且仅当发生一个碰撞时，能够从C^*中得出$CMAC[F^*]$。当选择明消息范围大时，产生碰撞的概率较大；当碰撞的机会增加时，$\frac{d^2}{2|M|}\to 1$，$d\approx\sqrt{|M|}$，

$$AdvC^{CPA(d|mess)}(MCAC[F^*]) \geq (1-\frac{1}{e})(\frac{d^2}{2|M|})^2=\frac{1}{4}(1-\frac{1}{e}) \qquad (3\text{-}137)$$

对于分组密码算法运算模式最简单的就是把消息分成块后直接加密。CTR 模式是在这种方案基础上忽略密钥长度与消息分块长度之间的区别，按照消息分块标准直接选取密钥块的高位进行加、解密，这样减少了密钥的存储量并加快了运算速度。CCM 运算模式由于其运算过程中调用了双倍的加密算法，因此效率与速度都遭到质疑。但是从运算模式可以看出 CCM 很出色的保证了消息的完整性和安全性，从 FIP 与 RFC 标准均采用这种运算模式则可以证明这两大标准的认可。CMAC 是 MAC 运算模式的一种改进，借用了 CTR 模式的一些运算思想，本质上的作用与 MAC 没有根本的区别。如果分析者能够在界限之内发现合适的消息与密数据对构造出碰撞的条件，说明该分组密码系统存在安全问题。对于设计者，缩小上界与下界的标准是对分组密码系统的改进。

3.7 本章小结

本章讨论了分组密码算法安全性评估与设计应用研究：包括算法线性部分分析基本原理，最大线性偏差、最大线性偏差评估法，最大线性偏差搜索算法，针对算法非线性设计模块安全性评估原则，差分密码分析基本原理，S 盒线性偏差，分组密码算法扩散性测试评估原则；分组密码算法讨论了设计基本原理——Feistel 结构分组密码算法设计，SP 结构分组密码算法设计，正形置换设计，S 盒设计、S 盒的代数次数和项数分布，S 盒的非线性度、S 盒常见构造方法。重点对 SP 型分组密码算法进行了置换部分的设计与研究；对密钥的生成与密码结合方式进行深入讨论；对分组密码算法芯片抗 DPA 分析进行模块保护设计。

第四章　分组密码算法相关标准与协议

分组密码算法主要在互联网络和无线网络使用，算法本身对数据的作用可以体现在加密、验证、抗抵赖等方面。但是各种功能都是在算法公开、密钥保密的基础上进行的，因此，对密钥的保护与密钥分发对分组密码算法的使用是最关键的一部分。安全协议进行实体间的认证，在实体之间安全分配密钥或其他各种秘密信息，确认发送及接收的消息的不可抵赖性。设计一个安全协议的难度在于安全度与冗余度之间的平衡。

分组密码算法通过协议实现网络上的安全数据交换，针对标准结构不同层次下的数据设计保密传输协议。国际标准组织制定的 ISO 7498-2[51]提供了基本的安全模型，1991 年国际电信联盟 CCITT 在 X.800 协议文件中采用了该模型[52]作为局域网的安全保障。ISO/IEC 在 1996 和 1997 年推出的七层网络安全结构标准 10181[53][54]，同时 ITU.T 推出 X.810、X.816 标准。ITU-T 的安全结构主要针对端对端系统，如 X.805。

4.1 安全协议简介

分布式网络的密钥难度在于如何秘密地把分组密码算法所使用的密钥安全地分发到目的地。1976 年，Diffie 和 Hellman 设计的基于大数分解难题的密钥交换协议使得密码的使用进入新纪元。

分组密码算法属于对称密码算法体制。而对称密码算法体制中，如果实体 I 希望同实体 J 建立秘密联系，但是不希望有其他方加入，此类问题可归结到密钥交换难题（Authenticated Key Agreement,AKA）。显然，由于密钥分发问题中还添加了身份认证部分，因此，这种问题比密钥广播更具难度。

与 Diffie-Hellman 协议相关的一些技术[55][56]用于解决 AK 难题。部分协议在设计和使用初期并发现不到哪些漏洞，但是随着使用时间的推移，没有被发现的问题会不断出现[57][58][59][60]。处于 AK 问题层面时，I 仅希望与 J 分享秘密数据，并不涉及是否证实 J 得到消息与否。如果需要回执，则要另外的盲协议。I 想知道 J 是否通过计算得到了密钥，把密钥确认加入分发协议中，称为直接认证协议，这类协议被称作带密钥认证回执的密钥认证协议（Athenticated Key Agreement with

Key Confirmation, AKC）。在 AK 协议之上加入密钥证实实际上是把 I 与 J 联系的回执补充到 AK 协议；这类协议还可以弱化建立在使 J 能够计算出密钥的基础上，而不是仅仅强调确认 J 已经计算过。

AK、AKC 协议是分布式网络中的对称密钥分发安全的保障，除了 IEEE 1363[61]已经对对称密钥分发做出各种标准化的建议外，还有一些对称算法的协议也在讨论和使用[62][63][64][65]。这些协议促使了对称密码算法广泛使用，因此对 AK、AKC 协议的设计与验证不仅伴随对称密码算法设计与使用，而且是对对称密码算法使用安全性的重要补充。

通常，安全的协议生产需要五个步骤：

1、 模型描述。

2、 模型内定义的目的。

3、 提出各种假设。

4、 协议描述。

5、 证明在模型框架内协议能够达到的目的。

对协议的安全性证明建立在适当的协议模型、适当的安全性假设之上。针对协议的分析，是证明协议安全的必要途径；并且还需要求协议分析的方法能够成立，结论足够可靠。通常针对分组密码算法的协议有两种类型：

被动分析：分析者通过监测真正的接受者而阻止协议分发正常完成。

主动分析：对手主动对协议通信进行各种方式的破坏，包括：重放消息分析、插入假消息分析、消息篡改分析等。

显然，在分布式网络中的密钥分发协议需要抵抗被动分析和主动分析。在协议设计中通常假设的最坏情况有：

1、会话密钥已知。协议设计者需要考虑到之前的会话密钥已经被分析者获取。

2、完全向前保密。如果一方或多方的长期密钥受到威胁，以前的会话密钥不受影响。

3、密钥分享未知。实体 *I* 不会被强迫与之前不相关的实体 *J* 共享密钥。例如 *I* 认为 *L* 是秘密共享方，而 *L* 与 *J* 不是同一实体。

4、密钥承诺假冒。假设 *I* 的私钥值被泄露，如果分析者 *J* 得到 *I* 的私钥值，并且协议明确该值是 *I* 私有。通过对私钥值的计算，那么 *J* 就能够假冒 *I*。但是即使如此，*J* 仍然不能假冒其他方与 *I* 通信。

5、信息损失影响。对分析者保密的额外信息协商不会影响到协议的安全，例

如 DIFFIE-HELLMAN 型密钥交换协议中，*I* 的长期密钥损失不影响整个协议体系的安全。

6、消息独立。协议中两个诚实的实体相互独立的信息交换不会彼此影响。

在一些应用中，某些协议需要通过多方证明，而协议的任意一方都不能单独对密钥选择产生影响。但是，事实上最先选择密钥的一方会认为协议不公平，因为其他方有机会通过使用的密钥计算出所使用的私钥。

4.2 分组密码算法与无线网络标准

由于无线网络本身物理结构的特点，运行在无线网络上的各种信息的安全需要进行安全保证，密钥需要协议管理。现在国际上已经把分组密码算法用于无线网络上的信息安全保障，中国也已经通过国家密码管理局公布了用于无线网络加密的分组密码算法 SMS4。

密码共享认证：这种认证使用标准的询问和应答模式，包含一个用于请求的认证的共享密钥。具体过程如图 4-1：

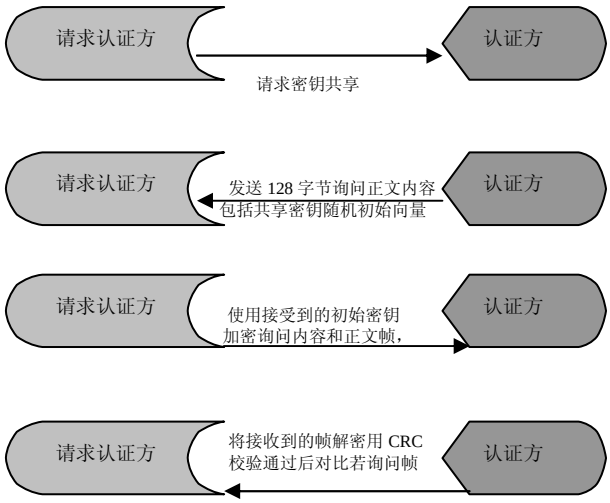


图 4-1 密码共享认证

针对无线网络的安全认证如下：

开放系统认证：开放系统认证系统是 802.11 标准系列中的认证协议，该协议对任何认证请求都会通过，显然，该协议是空协议，不具备更深的意义。这种协议更象是对硬件兼容性的认可。同时，这种硬件管理帧在网络中可以随意传输。

密钥管理：802.11 系列标准，对密钥管理没有严格的方案，一些密码产品会

有产品开发商定义部分自身的一些密码管理和密码协议。密钥管理会因为密码产品使用的安全级别而有所不同。

为了使共享密钥的安全机制更具鲁棒性，在分配和使用时，密钥需要更好的保护。通常的无线网络中使用的 WEP 加密体制提供如下两种信息安全功能：一是防止信息窃听；二是防止未得到授权的设备进入网络。密钥管理是密码体制中最关键的一环，WEP 将这一问题留给了商家。由于密钥是静态的，并且需要手工维护，扩展能力差，管理和配置起来工作量比较大。在大部分网络中使用单一密钥在区域内共享，一个用户丢失密钥会使整个网络面临危机。初始向量为了便于用户使用，长度会有所限制，但是如果协议不够严谨，密钥会产生重复使用的情况。WEP 帧中的完整性是用循环校验码生成的 CRC 校验和来完成的，用来检测数据在传输过程中是否被篡改。在最近的 802.11 协议中，校验数据与信息一起被加密，降低了通过利用 CRC 的线性关系还原信息的可能。

随着无线网络在全球逐步被广泛纳入移动办公范畴，信息安全问题成为薄弱和受关注的一环[66][67]。无论是使用防火墙或是入侵检测，无线网络都存在明显的漏洞。许多无线网络上使用的安全协议主要是 WEP 协议，密钥长度为 64 或 128 比特的 RC4 加密算法。而实际协议中的密钥长度是 40 和 104 比特长。这些都是由 24 比特初始向量来产生实际的加密密钥。在繁忙的网络环境中，密钥可能经常重新启动 24 比特初始向量，从而产生大量相同的密钥。一旦两个使用相同密钥的加密数据被截获，通过统计分析就可得到 WEP 的加密密钥。WEPCrack 和 AirSnort 就是针对 WEP 协议分析和密钥求取的软件。另外，WEP 没有提供用户身份证明和密钥管理。一旦移动终端被盗，管理员没有更改各个终端和网络入口的网络口令，整个无线网络就可能遭到威胁。同时 WLAN 面临的其他分析还包括：

1、基于通信的分析：WEP 的通信漏洞让截取者能够获得加密数据。分析者可以被动窃听或主动研究无线局域网的弱点进行将来的分析。入侵者可进行重放、篡改等分析。另一种是无线电波干扰，分析者利用合法资源以接近无线电流频点建立非法通信联系。

2、无线局域网络分析：合法的无线局域网可能遭到两种分析，一种是由于认证机制的脆弱性而导致入侵者进入局域网从事非法的活动。另一种是在无线局域网执行过程中，网络管理与用户端之间的通信非常简单，入侵者直接通过连接轻易的进入局域网，获得相关信息。

3、客户端分析：无线局域网客户端在局域网防火墙之外，许多网络结构的威胁来自于网络内部。分析者可以利用内部客户控制、分析无线网络。在 802.11 协

议中，客户端可以直接进行连接，这些都提供给分析者多个分析渠道。

为了保证无线网络的安全，接下来设计了高保真接口保护协议。该协议仍然使用 RC4 加密算法，但比 WEP 有所提高。加强的部分包括提供用户认证的 802.1*x* 扩展认证协议，用于自动加密密钥管理的临时密钥完整协议。48 比特的初始向量加长了密钥长度，避免密钥重复使用的机率。WPA 还使用了数据完整性检测来确保传输数据的完整性。但是 WPA 使用的加密算法 RC4 对于当前的计算能力已经过时。业内人士希望能通过分布式计算分析 RC4 加密算法。另外，密钥更换需要较大空间，PDA、条码扫描和 IP 电话不容易使用 WPA 协议。新的 802.11*i* 数字协议提供数据机密性、数据源真实性、重放保护。协议要求每个进程使用新密钥。密钥管理使用经授权认可、提供认证过的接入信道进行密钥分发。结构体系密钥证明。目前，协议使用 *802.1x/EAP* 的规格为用户提供 AES 加密认证和完整性检测。802.11*i* 提供以 *TKIP* 备份为 *WPA* 协议进行互操作的反向兼容。但是，提供反向兼容的代价是协议中不得不使用 RC4 加密算法，该算法已经发现有明显缺陷。基于 AES 的 802.11*i* 协议特殊进程安装在无线网络设备上。802.11*i* 中的数据安全通过对用户提供密钥 K 加密传输数据帧来实现。加密过程可归纳为：

1、计算校验和：在信息 *M* 上计算一个完整的校验和 *c（M）*，通过 *P*<=*M*，*c（M*）获得一个明码文本，作为第二步输出，*c（M*）和 *P* 不依赖于密钥 K。

2、加密：对明消息 *P* 使用 AES 加密。选择一个初始向量用加密算法产生密钥流作为 *v*、*K* 的函数，设为 AES（*v*，*K*）计算：

$$C=P\oplus \ \mathrm{AES}(v，K)$$

C 即为密数据。

3、传输：通过无线网络传输 *v*、密数据。

$$A\rightarrow B：v，(P\oplus \ \mathrm{AES}(v，K))$$

其中 *P*=<*M*，*c（M*）>，该式表明由源站 A 到接收站 B 的密数据传送方式。 解密即是对加密过程简单的倒置

802.11i 中数据加密协议的密钥初始向量长度加强为 48 比特，其中前 4 比特指示传输质量级别，后 44 比特用于记数，如果传输级别在解密/完整性检测后改变则检测失败。加密算法使用基于 OCB 模式的高级加密标准 AES，较 RC4 而言显然增强了数据安全强度。

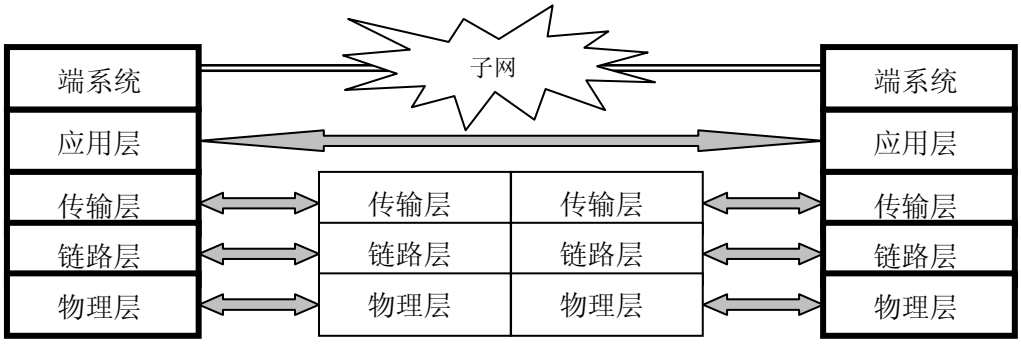
虽然初始向量长度由 24 比特加长为 48 比特后，重复使用的机率由 $1/2^{24}$ 减少到 $1/2^{48}$，但是由于无线网络的各种通信故障会造成不断的重新启动密钥，依然可能使用相同的初始向量，共享密钥 K 一般很少变化，使如下分析得以成功：

当初始向量使用重复、共享密钥相同时，造成加密乱源相同。此时，两份无线通信密数据的和能够反映它们的明消息和的形式。

$$P_1 \oplus \text{AES}(v, K) \oplus P_2 \oplus \text{AES}(v, K)$$
$$= P_1 \oplus P_2 = C_1 \oplus \text{AES}(v, K) \oplus C_2 \oplus \text{AES}(v, K)$$
$$= C_1 \oplus C_2 \quad (4\text{-}1)$$

通过这种方式，可以得到无线网络通信协议加密使用的框架情况。无线网络技术的广泛使用导致信息安全的危机。采用 AES 为加密算法的 802.11*i* 协议在信息加密方面强度增加。但是如果初始向量没有专业的管理、使用手段，仍然有可能使重放分析得以实现。

无线传感网络和有线网络具备相同的层次结构（图 4-2）：由于无线环境的开放性，使得中间人容易窃听到消息原语，再进行相应分析。



4-2 无线网络结构图

与 TCP/IP 的架构相同，无线传感网络同样分为物理层、链路层、传输层和应用层，消息的传输与对话只能在对等层进行[68][69][70]。物理层包括智能天线和传感器网络硬件，用于支持正确的能量计算和信号衰减检测；消息的传输和会话在链路层进行：封装、传输已经由安全协议 802.1*X* 系列进行了标准化；有线网络上的 IPSEC 协议包通过与无线网络标准的接口可以进行消息的认证和授权；应用层通过异常检测签名、变化检测签名和通信分析机制保证消息原语的完整性、不可篡改性、安全性和可用性。这种分层的结构使无线传感网络用合理的方式接入互联网。通过研究无线传感网络目前的安全保障系统，设计出一种改进的基于活动分组密码算法作为消息身份认证的协议，接口上完全与国际标准相同，并能证明协议的安全性。无线传感按照网络节点、网络分析方法有相应的分类：节点分类包括电源探测、运算功率探测、内存探测和能量消耗探测等。按组网形式分为无线网络（Wireless Networks, WNs）探测、Ad Hoc 探测和其它形式探测。

较有线网络而言，这种网络需要更简单的密钥管理与生产模式：对网络中的虫洞部分进行安全加密时必须考虑到使用不同的密码方案，消息封装包应该更小。在使用密码保证的传统安全领域之外，无线传感网络在设计安全系统时还要考虑抗击另外几种分析方案：拥塞分析、重放分析、包延迟分析、包阻塞、恶意节点以及其他一些影响网络的分析。链路层上密钥预先管理、消息完整语义、消息安全语义、消息认证语义，在 802.1*x* 系列协议进行了说明。具体的安全认证结构（图 4-3）为：对访问控制的接入、消息原语完整性验证、安全消息原语验证。访问控制对非授权的用户进行限制，并且，在传送过程中必须保证不被窃听与不被篡改。

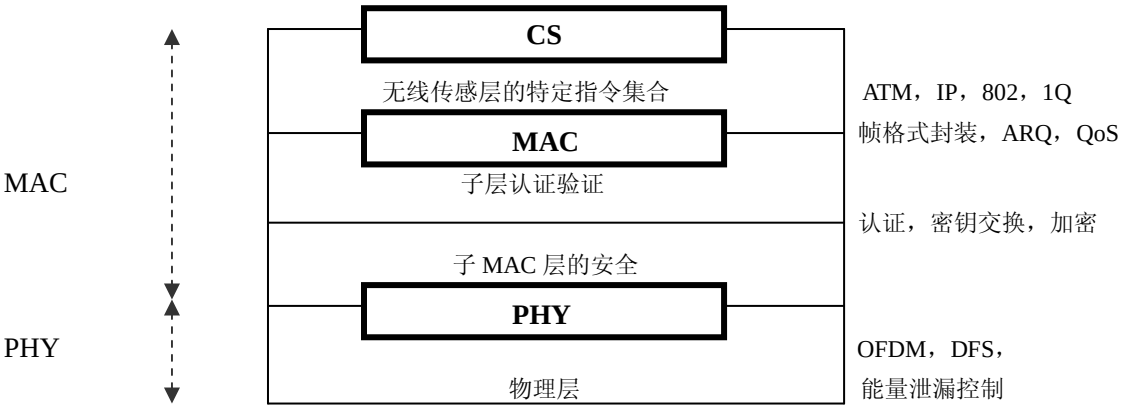


图 4-3 无线传感网络的安全结构

上述功能采用的安全手段分别为：访问控制原语与消息完整原语使用消息认证码（Message Authentication Code, MAC）实现，消息安全原语使用加密机制实现。通过密钥、密码算法、密码协议等安全措施进行完整性、安全性、不可篡改的功能设计。目前基于四次握手协议的密钥管理采用的是对密钥的预分配策略。无线传感网络的不同层次有不同的标准体系，因此关注的焦点是密码系统的设计与使用[71][72][73]。

密钥预先处理机制可以在传感网络节点的注册信息中加以选择和设置。把密钥的更新设定置于原语加密之外，可以提高节点传送的效率，同时兼容性、可扩展性较好。预先密钥分发方案有三种执行形式：1、全网络密钥预先分发：一个密钥在使用启动前发送给网络中所有节点或机站，使得这些节点都具备消息的都可以获得消息加密原语。这种密钥分发的优点是直观、简单。2、指定节点密钥预先分发：密钥对只分发给指定的节点。例如特定的 n 个节点，分发密钥量为 C_n^2。虽然每个节点需要存储 C_n^2 个密钥，但是这种分发使特定节点的端对端通信安全性强。如果有新的节点加入，整个特定通信网络必须全部重新分发密钥。3、J-群安

全密钥分发：把 n 个节点分成 m 个群，每个群可以通过基站相互联系（图 4-4）。

对每一个节点群，分发密钥 K_i，群与群之间的通信通过基站进行交换。如果这种结构继续分为树状，形成一个公钥基础设施（Public Key Infrastructure, PKI）的构造。

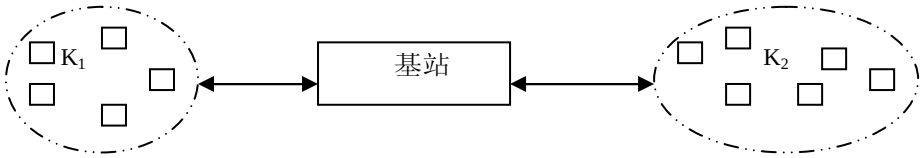


图 4-4 J-群密钥分发模式

无线传感网络分为 WN 和 Ad hoc，这两种网络对安全的要求并没有本质的差别。无论那种组网形式，把无线传感网络的传输条件分为：子网内部传送、跨网传送。不同网络层次消息封装由低到高分为：IP 层封装、链路层封装和应用层消息原语直接加密，网间和网内的颗粒细度根据具体要求和情况而定。当进行网内传送时，密钥的选用与分发可以不通过基站，因此协议相对简单。这种情况下，密码算法的选择安全强度大、速度稍慢一类，比如 128 比特分组、128 比特密钥及强度更大的一些算法。进行网间传送时，路由选择比较复杂，选用分组和密钥规模小的算法以提高速度。对新成员接入无线传感网络的进展是使用可选择的活动分组密码算法，使分组密码算法较流密码的优势得到充分应用。建议使用不同类型的分组密码算法对上述情况加以实现，称这种方式为活动分组密码选择。假设活动分组密码算法用 AE 表示，消息原语为 d，算法的 $Hash$ 模式由 AE_{Hash} 表示，单向函数值表示为 h（d）则：一个消息经过 En 封装之后，蕴涵的信息为（d，E_n（d），AE_{Hash}（d）），消息有效时间为 T。这样点 A 对点 B 的通信过程及可证安全性（图 4-5、图 4-6）为：

步骤一、身份认证过程

1、$B \longrightarrow A$：ID_B，h（K_B，T）	B 产生身份认证私钥 b，计算 $K_B=g^b$。 B 使用消息时间戳计算 K_B 的 Hash 值， 发送身份认证码 ID_B 到 A
2、$A \longrightarrow B$：ID_A，h（K，K_A，T）， K	A 产生身份认证私钥 a，计算 $K_A=g^a$。 A 使用消息时间戳计算 K_A 的 Hash 值， 发送身份认证码 ID_A 到 B

图 4-5 消息密钥的传送与验证

步骤二、无线传感网络进行消息交换与认证

1、$A \longrightarrow B$：ID_A，K_A	A 发送认证码与步骤一相同的 ID_A 和 K_A 到 B
2、$B \longrightarrow A$：ID_B，K_B，E_{ABHash}（ID_B，N_B，h（K，K_B，T））	B 使用 K 和 h（K，K_A，T）认证 K_A。B 计算出 h（g^{ab}）共享密钥 K_{AB}。B 选择一个随机数 N_B 并计算认证码 h（K，K_B，T）。使用 K_{AB} 和认 ID_B 认证和密数据。同时传送 ID_B、K_B 和消息加密原语一起发送 A
3、$A \longrightarrow B$：E_{ABHash}（ID_A，N_A，N_B，T）	A 接收 K_B，计算出 h（g^{ab}）共享密钥 K_{AB}。A 读取随机数 N_B 并计算认证码 h（K，K_B，T）。 选取随机数 N_A，使用时间戳和 K_{AB} 产生 ID_A，N_A，N_B 为消息验证原语和加密原语
4、$B \longrightarrow A$：N_A	B 使用 K_{AB} 和时间戳读取随机消息 N_A，并发送给 A

图 4-6 消息原语的加密传送与认证

A 和 B 同时计算他们的会话密钥 K_{Hash}（A，B，T）并可以作为认证码使用。

步骤一是传统的 DH 协议密钥交换，使用非对称密码体制实现。在双方通信中引入了时间戳机制进行密钥的加密传送。步骤二的消息认证码和消息加密原语的产生的密码算法 E_{AB} 用了可选择的方式，E_{AB} 的强度保证上述可证安全性过程成立，使用对称密码体制实现消息的安全传送。活动分组密码算法建议使用 AES 和欧洲分组密码标准 Camellia。这两种算法分别是 SP 型和 Feistel 型分组密码算法的代表：消息分组长度分别为 128 比特、192 比特、256 比特；密钥长度支持 128 比特、192 比特和 256 比特。事实上，对不同的分组长度与密钥长度在各种环境下的运算应该采取哪种加密手段分别进行了统计与测试。在安全级别要求允许时，只需使用 128 比特消息分组、128 比特长度密钥就可以完成对无线网络的安全保障。

无线传感网络中消息的安全传送与验证一直是密码学界关注的领域，各个标

准的制定最初都把服务质量作为第一目标，移动终端的多样性、使用的灵活性与便捷是较有线网络的突出优势。无线网络的分析手段促使标准化组织不断进行修订安全方案，同时通信界也采取了更多补充的方式自行对网络标准加以完善——尤其是在一些要求自主技术作基础的使用环境下。通过上述研究提出使用可选的分组密码算法进行通信安全保密方面的工作是可行的。活动分组密码算法虽然消耗一些存储空间，但是不同使用环境下选择运算速度不同的算法可以提高通信质量，并保证安全和效率。

4.3 分组密码算法在网络环境应用建议

1969 年，美国国防部远景研究规划局（Advanced Research Projiects Agency,ARPA）为军事用途建立了 ARPARNET，其设计目标是当网络中的一部分因战争原因遭到破坏时，其余部分仍能正常运行。现在网络已经进入商业化阶段。由于网络使用人群的扩展，分组密码算法成为安全保障的公开方式。在互联网环境中，分组密码算法主要应用于身份认证。身份认证(Identify Authentication Protocol, IAP)包括：认证、授权、审计。一般的，安全系统都必须有身份认证这一环节，防止非法用户的侵入，对合法用户根据访问控制权限限制其行为。从对身份认证的实现手段来划分：基于口令的认证方式；基于智能卡的认证方式；基于生物特征的认证方式。事实上，上述三种方式都有各自的应用领域。最常用的还是基于口令的认证方式，这一方式优点是不需要其他设备，可以与现有系统无缝集成，对用户而言也较为透明。访问控制也是网络中确保信息合法存取的技术。通常使用的身份认证协议会因为网络配置商家的不同而有所区别，而对协议的研究虽然不断在进行，但是关于协议的最终制定仍然掌握在大的资本手中。以下主要介绍 Raduius 协议和 Kerberos 协议。

就目前的理论来看，网络连接中认可的身份认证协议主要有 Raduius（Remote Authentication Dial in User Service, Raduius）协议。对远程用户，Radius 协议采用分布式客/服（Client/Server, CS）结构完成分组密码算法的集中管理和身份认证功能。用户登陆请求接网络连接，由网络访问服务器（Network Access Server, NAS）提示键入用户名和口令字，NAS 向安全服务器提出请求；安全服务器按照一定规则处理，返回响应，响应中包含是否同意用户连接请求。

当用户登录网络时 NAS 要求进行用户名及口令的身份认证，并向安全服务器发送请求。请求信息中包括各种属性配置信息，诸如 IP，子网掩码等。安全服务

器按照一定的规则处理并返回响应信息，使用户及时明确是否被验证通过。如果验证通过，信息中还包括 NAS 对用户的配置信息，最终由安全服务器返回给用户的配置信息才是最终使用的值，完全可以屏蔽 NAS 的属性值。RADIUS 协议在 RFC2138、RFC2139 中定义，同时 NAS 供应商也可以对这些标准中的具体数据进行相应规定。

自从 MIT 在它的 ATHENA 项目中开发出了 Kerberos 身份认证协议以来，该认证系统一直在 UNIX 系统中采用，通常使用的是第四和第五版。MICROSOFT 公司在 WINDOWS 2K 中实现了这一认证系统。该协议的使用背景是大量匿名工作站和较少的独立服务器：服务器提供文件存储、打印、邮件等服务，工作站用于交互及计算；服务器能够进行流量控制、验证服务请求。在这样的环境中面临的威胁有：

用户有访问特定工作站并且伪装成其它工作站用户的能力。用户能够改动工作站的网络地址，这样改动过的工作站发出的请求不能被证实。用户能利用重放分析进入服务器破坏操作并在交换过程中窃取消息。ATHENA 的计算环境与目前的网络环境非常类似，对安全的需求也适用于大部分实际的网络。为减轻服务器的负担，Kerberos 把身份认证集中在身份认证服务器（Authentication Server，AS）上执行。AS 中存有所有用户的口令。另外，为使用户输入口令的次数最小化，在 Kerberos 认证体制中，还增加了授权服务器（Ticket-Granting Server，TGS）。

用户 C 登录系统，并表明访问某系统资源。由 AS 从用户口令产生一个密钥 K_{as}，传输给用户一个可以访问 TGS 的票据 T_{tgs} 以及用于 K_{as} 加密的密钥 K_{tgs}。如果用户 C 获得口令，则可以利用口令产生一个密钥 K_{as}，解密后获得 K_{tgs}，用户请求服务时发送 T_{tgs}、私人信息到 TGS；TGS 认证后发送给 C 一个可以访问某个服务器的票据 Ts 及用 K_{tgs} 加密的密钥 K_s。C 把用 K_{tgs} 解密得到的 K_s 和私人信息发送到 SERVER。SERVER 对信息加以认证后，为 C 提供相应服务。

定义 4-1：票据是一种用户身份识别的证明和私人信息，服务器能够使用这些信息来确认使用票据的客户与发送票据的目的客户是同一身份。Kerberos 的票据格式如下：

$$T_s = s，\{c，a，v，K_s\}\ K_s \qquad (4\text{-}2)$$

S 代表服务器，C 代表客户，a 是客户的网络地址，v 是票据的有效起止时间，K_s 是服务器和客户之间的共享秘密密钥，这些信息都使用 K_s 加密，其他人由于不知道 K_s 无法对其中的内容解密或篡改。用户可以将加密的票据递交给服务器，服务器用自己的私钥解密后得到用户的信息，用户和服务器共享的密钥，从而能够

与用户进行通信。

定义 4-2：鉴别码是与票据一起发送的，请求服务器服务的标记。包括用户名、时间标记、可选附加会话密钥、使用服务器与客户间共享的密钥加密。与票据不同的是，鉴别码只能使用一次。鉴别码的格式如下：

$$A_s=\{c，t，key\}K_s \quad (4\text{-}3)$$

鉴别码包括一些由会话密钥加密的明消息，表明鉴别码的发送者知道该密钥；其次，由于包括了时间标记，防止了记录和重放分析。

Kerberos 具体认证过程中的三个步骤为：

1、用户 C 由 AS 获得访问 TGS 的票据 TGT

用户向 AS 发送申领票据的请求，包括用户 ID、TGS 的 ID、时间、一次性随机值，用户所在的 DNS 等信息，不包括用户的私有密钥。

AS 收到用户 C 的申请后，首先查找该用户的 ID，如果该客户的信息在数据库中，根据用户口令生成一个用户密钥 K_s，同时生成票据（Ticket Granting Ticket, TGT）用于与 TGS 通信。AS 使用它与 TGS 之间的共享密钥加密 TGT。

AS 将上述两个信息发送给用户。因为用户知道自己的口令，可以生成 K_s 并且对消息解密得到 K_{tgs}。非法用户不可能从窃听的消息中得到任何信息，防止了非法访问。一般说来，在进行第一步时，系统才向用户提示输入口令，在使用口令解密相关消息之后可以将口令销毁，这样口令在内存中生存周期非常短。

2、用户 C 由 TGS 获得访问 SERVER 的票据 T_s

用户向 TGS 发起请求，并使用上一步解密得到的密钥 K_{tgs} 对鉴别码加密，用户还将上一步得到的 TGT 发送给 TGS。TGS 接收到用户请求后，用自己的秘密密钥解密 TGT，然后再用 TGT 中的会话密钥解密鉴别码，比较鉴别码和 TGT 中的信息是否一致，如果一致则允许处理该请求。TGS 向用户返回一个用户与服务器之间的共享密钥 K_s，使用 K_{tgs} 加密，TGS 还为用户产生一个用于访问服务器的票据 T_s，使用 TGS 和服务器之间的共享密钥加密 K_s,使用 K_{tgs} 加密。

3、用户 C 把 T_s 想 SERVER 提交并获取得到服务资格

C 产生一个鉴别码，用 K_s 加密，连同上一步得到的 T_s 提交给 SERVER；与 TGS 相同，SERVER 对鉴别码和 T_s 解密并比较其中的内容，如果一致则认为用户是合法的。SERVER 向用户返回一个包含时间标记的消息，并使用 K_s 加密，这证明 SERVER 知道用户的密钥而且能够解密票据和鉴别码。于是 SERVER 也向用户证明了自己的身份。在 Kerberos 的认证过程中，用户只需要向 AS 提交一次口令，之后在 TGT 的有效期内用户不需再次提交。并且口令并不在网上传播，即使是口

令的加密形式也并不传输。整个系统中所用的秘密密钥也并不在网上传输，用户和服务器之间的认证基于：双方均能解密对方发送来的消息，双方均拥有共享的秘密密钥。

Kerberos 的两级授权机制可方便地划分安全域，除 AS 必须存储所有用户的 ID 和口令及所有 TGS 秘密密钥外，TGS 不需存储任何用户信息，只需存储该 TGS 本身和它所管理的服务器的秘密密钥，提供服务的服务器只需存储与 TGS 共享的秘密密钥即可。这样很大程度减少了密钥的存储开销。一个 TGS 管理的区域可视为一个安全域，不同的 TGS 之间互不干扰，某个 TGS 被攻破不会影响到其他服务器，也不会影响到 TGS 和 AS 的安全。Kerberos 存在的主要问题在于：用户和 AS 共享密钥 K_{as}，这由用户的口令导出，一个有窃听能力的分析者可以采用离线方式分析用户口令，如果用户口令被破获，系统的安全性受到威胁，Kerberos 使用的票据方式降低了通行字的使用频度；其次，系统安全基于对 AS 和 TGS 的绝对信任，且实现软件不可被篡改。

4.4　下一代互联网中分组密码算法使用简介

通常，网络体系结构是已知网络设计技术的高层次设计原则[74]，特别针对各种协议机制与算法。一个网络体系结构必须包括以下几点：

1、某一状态出现的地址、现状、演变趋势。

2、怎样处理实名。

3、实名、地址、路由功能是怎样相互关联的，是如何运做的。

4、沟通功能是怎样模块化的，例如，用“层次”构成“协议包”。

5、网络资源怎样在不同流量之间分配，终端系统怎样对这个划分进行反映，例如公平竞争和拥塞控制。

6、安全边界是怎样划分的，是怎样强制执行的。

7、怎样管理边界划分、选择性贯通。

8、怎样达到不同的 QOS 要求。

一个应用层结构（Application Level Framing, ALF）典型的假想的结构例子是 ALF90。ALF 不是一个完整的结构，只是基于特殊用途的一个结构部件：代价很低，执行灵活，更多功能的操作在不同结构下完成。能有效支持广泛应用要求。ALF 说明了即使是短时的利益仍需要长期的结构设计。

现行的互联网络的结构设计是典型的军事化的产品。为了使国防部能够使用

COTS 技术，网络地址解析（Network Address Translation ，NAT）在设计上必须有通用性，这样一来军用和商用的目标可以相互协调。对于网络上的安全技术，需要注意如下几点：

1、NAT 设计与 IPSEC 加密标准兼容。使得网络安全切实可行。

2、传输网页与安全包（Secure Sockets Layer, SSL）或 IPSEC 认证不兼容。

3、诊断工具无法判断传输层的相互作用。

4、NAT 设计需要诸如 TCP 之类的协议来规范地址的控制。

新的应用软件协议因为防火墙的缘故进展受到一定阻力，先行的协议与防火墙之间有冲突。

同时，在网络结构设计中还有经济、政治方面的背景。需要达到如下要求：

1、现行的 INTERNET 能够接入新的网络。

2、鲁棒性：INTERNET 通信必须不间断，除非路由或网络连接出现故障。

3、兼容性：新的结构设计可应用于各种网络结构。

4、分布式管理：互联网必须要求分布式管理它所涉及的资源。

5、开销：互联网需要合理的开销。

6、便于添加附件：使主机可以用很低的代价增加附件。

7、可解释：应用于互联网的结构必须是可以解释的。

随着互联网的发展，一些新的元素加入设计要求，如：可移动性、自动分配、高次可变资源等功能。当卫星通信、光纤通信和网络通信三网达成一致协议，人们更为关注基于 IP 的网络协议及相关技术，使得下一代网络构架成为人们关注的焦点。电信网络从承载单一业务的独立网络向承载多种业务的统一的下一代网络的演进正成为不争的事实，运营商必须设法改变其现有网络的设计，以适应迅速增长的数据通信业务。这种改变的核心是利用分布式的体系结构，将语音和数据汇聚在同一个无缝网络中，通过将接入、呼叫控制和电信应用程序分离的三层结构，使运营商利用现有网络提供更灵活的适应性和更强的管理能力，这种网络结构就是下一代网络的基本框架。与目前的 IP 长途电话类似，当前 NGN 核心技术仍然是分组话音及其控制信令，但 NGN 旨在真正将语音融合到数据网络中，在数据网络的统一平台上构筑电信级的话音大网，与以节省长途费用为主要目的的 IP 电话有本质区别。NGN 的一个核心思想是媒体与业务分离、媒体与控制分离，从而使媒体层的设备不需要知道业务逻辑和控制智能，以降低媒体层设备的成本，并使网络具备可扩展性和快速部署新业务的能力。

下一代网络在功能上可分为如下四层：

1、接入和传输层：将用户连接至网络，集中用户业务将它们传递至目的地，包括各种接入手段。

2、媒体层：将信息格式转换成为能够在网络上传递的信息格式。例如：将话音信号分割成 ATM 信元或 IP 包。此外，媒体层可以将信息选路至目的地。

3、控制层：提供呼叫控制和连接控制功能，实现各种信令协议的互通和转换。

4、网络服务层：提供增值业务逻辑、业务开发平台和第三方可编程接口。

每个平面均包含多个网络元素，主要有软交换、信令网关、媒体网关、应用服务器、媒体资源服务器以及智能终端等。

NGN 是目前运营商和设备厂商都在讨论的热点技术，也是国外许多标准化组织和论坛包括 ITU-T 的第 11 和 16 工作组，IETF 的 IP Telephony 工作组、信令传输工作组、媒体网关控制工作组，ETSI 的 Tiphon，国际软交换协会，3GPP，3GPP2，MPLS 论坛，ATM 论坛，DVB，DSL 论坛，PARLAY 等的研究工作重点。ITU-T 认为 NGN 是全球基础设施 GII 的具体实现，NGN 代表了网络融合的发展趋势，其实现方式是多种多样的，网络互通和业务互通是 NGN 研究的关键内容，NGN 的体系架构将是层次化的，其控制和管理之间的界面日益模糊，在技术上将解决现有网络存在的问题。NGN 是全球基础设施 GII 的具体实现，ITU-T 第 13 研究组将开始准备和组织 NGN 标准化项目的实施，2002 年 11 月完成项目的定义阶段。ITU-T 和 ETSI 认为，有关 NGN 应研究以下关键的技术领域：

1、体系结构和协议：研究确定 NGN 网络体系和参考模型；研究 NGN 的协议分层体系，以体现 NGN 业务和网络分离的特性；研究基于 GMPLS 的控制和协议体系；研究光 VPN 的体系结构和协议；考虑使用通用的参考模型来标识运营商内或运营商间支持 NGN 所需要的通信流程；定义与传统终端所需要的互通功能；定义 BICC 协议用于中继层面；确定跨越异构网络如何支持端到端业务、呼叫控制和用户移动性。根据终端软件升级机制和版本协商等因数定义 NGN 类终端的功能。

2、网络控制和端到端的 QoS：研究和定义 QoS 业务量工程要求；研究基于 GMPLS 以太网传送的 OAM 和链路控制协议；完成用于话音的端到端 QoS 等级，研究用于端到端多媒体业务 QoS 的等级要求及其各自媒体组件的 QoS 等级要求；研究如何使用网络低层的 QoS 机制获得高层 QoS；研究运营商间网络低层 QoS 控制机制；研究 QoS 的端用户规则；研究传输网规模对 QoS 的影响和接入网上传输呼叫对 QoS 的影响等。

3、业务平台：定义包括 API 和代理因素的业务要求和业务控制体系；完善跨越多网络的业务互联和用户漫游所需要的业务支撑和提供机制；开发支持用户控

制和客户化业务的机制，研究用户移动性的业务平台的影响等。

4、网络管理：实现 NGN 网络的一个重要条件是必须有一个适当的网络管理解决方案，由于 NGN 是基于开放式接口并且允许不同种类的业务进入一个网络，网络管理必须在多厂商和多业务的环境下进行，因此有必要定义适用于 NGN 要求的基本网络管理业务和接口；研究光网络的 FCAPS 模型；完善和增强核心网络管理的体系等。

5、网络安全：NGN 网络的一个特点是开放式接口增多，安全性方面的风险也相应增大，因此有必要开发 NGN 的安全性体系和操作安全性规则；开发 NGN 所需的特定安全性协议，API 和工具，例如加密、信息摘要和数字签名等。

6、其它问题：研究会晤和呼叫管理，研究支持紧急呼叫业务和优先服务的机制，研究 NGN 网络的编址等。

与传统的 PSTN 网只需要功能单一的电话机/传真机不同，NGN 可以提供多种业务，也需要多种不同功能、不同层次的终端，比如：MGCP/H-248，H-323，SIP 终端，IAD，以及软终端等。目前，各类终端种类少、供电方式单一，且价格较高。另外，很多终端制造厂家对协议理解不同，各类终端之间互通存在各种各样的问题，限制了业务的发展。要解决终端匮乏的问题的关键是必须统一相关的技术标准和规范，而在 NGN 终端规范化的进程中运营商大规模的网络建设方案以及对相关终端制造厂家的技术和设计引导将扮演相当重要的角色。

QoS 是运营商网络运营和业务发展的永恒主题，保证 NGN 网络的 QoS 可以从两个方面着手解决：首先是承载网的 QoS 骨干网的 QoS：可以建立基于 MPLS 的骨干数据承载网，并根据业务需求划分不同的 VPN，以保证骨干网的 QoS。接入网的 QoS：在 IAD 和二层交换机上，对数据分组和语音分组打上不同的 VLAN 标签。对不同的 VLAN 标签可以设置不同的优先级，对不同的优先级送入不同的发送队列，从而可以达到向语音分组提供较高优先级的目的。在和二层交换机相连的三层交换机上，将不同的 VLAN 标签映射到 IP 包头中的 DSCP 字段中，对不同 DSCP 字段提供不同的处理优先级，从而保证了接入网的 QoS。目前，在全球范围内，各运营商对 NGN 网络都还处于技术试验或者商用试验阶段，还没有大规模成功商用的实际案例。这主要是因为虽然软交换提供的 C4 业务已经成熟，但在提供 C5 业务方面仍缺乏必要接入安全和控制的机制。

根据上述介绍，分组密码算法仍然适合下一代互联网环境下部分数据的安全目的。但是通信模式的变化会导致网络安全与数据安全在许多网络层次上的变化。

4.5 一种针对可信网络连接的数据安全算法设计

当网络环境发生变化，可信计算环境成为网络安全研究者理想的目标。除了传统意义上所说的“黑客”，以个人行为或民间组织行为来对互联网进行破坏和分析外，还有来自别国的政府及军事机构通过各种手段获取敏感有用信息。可信计算平台[75]（Trusted Computing Module, TCM）通常包括：可信计算构架、移动计算、服务器、软件存储、存储设备、可信网络连接六个部分。可信网络连接[78]（TRUSTED NETWORK CONNECT，TNC）决定网络连接的合理性、安全性。TNC[76]结构提供基于系统完整性、唯一性的端设备注册统一架构，其特征是：基于完整性、唯一性两个基本概念。完整性用于描述终端的“鲁棒性”、构造，如同普通 IT 意义下的定义。例如系统如果保持预先确定的策略，确定系统没有在非正常或恶意的环境。唯一性确保系统被授权用户使用，TCM 的客户提供附加安全通过硬件来确定身份。TCM 也提供信赖导入机制，在不被探测到的情况下帮助根过滤工具包。TNC 的另外一些重要特征集中在产品更新换代形成的各种卖方不同种类的工作环境中。TNC 支持会提高许多已经存在的产品。用户可以因为使用了 TNC 工具快速获利。这个构架基于存在的一些标准，诸如：EAP、TLS 和 IPSEC 和 802.1X 等成熟技术。从可信计算组所提供的标准来看[77]，数据安全与身份认证完全依赖于整个可信平台的逐级密钥分发。对于可信计算组成员的对等通信安全没有涉及，也没有专业的密码小组，因此在安全协议与认证方面明显还可以进行许多有益的改进。可信计算涉及的部分概念如下：可信计算组核心功能（TCG Core Service，TCS），可信计算服务供应商（TCG Service Provider，TSP），网络接入认证（Network Access Authority，NAA）。IF—IMV 由一个或多个可信网络连接服务器（Trusted Network Connect Severs, TNCS）及一个或多个完整性验证方案（Integrity Measurement Verifiers, IMVs）组成。还有一些逻辑主机，TNCS 与 IMVs 一般存在于同一主机，IF—IMVs 相当于 TNCS 与 IMVs 的中间件。多数远程分布式终端是安全管理的薄弱环节。TNC 怎样把一个传统的网络通过加强端点安全策略，扩展成为一个带有接入控制检查的网络。通过这个例子，一个要求接入的用户（the Access Requestor, AR）试图连接安全网络。网络通过策略加强端（Policy Enforcement Point, PEP）进行策略决定端的询问（Policy Decision Point, PDP）进行策略决定端的询问的答复是否可以全部接入。这是现在典型的网络，但是 AR 和 PDP 都包括了上述附加软件元件。AR 包括了 TNC 客户端和插入组件——完整性度量收集（Integrity Measurement Collectors, IMCs），从反病毒和其他安全包中搜集完整性测

量标准。PDP 包括一个 TNC 服务器和插入组件完整性测量证实——IMVs。证明这些完整性测量可以对抗安全策略。同样，可信计算平台也会面临一些威胁。对于 IF—IMV 所面临的安全威胁可以采取如下方法：

支持 TNC 的技术：网络接入技术包括 802.1X, VPNs, PPP；消息传递机制包括 EAP 保护机制, TLS 和 HTTPS；服务器认证技术（Authentication Sever, AS）包括 Radius，Diameter。

安全考虑包括：分别包括 TNC 客户端和 TNC 服务器端，AR 到 PDP 之间的完整性及以下诸多方面：

1、AR 与 PDP 之间的安全信道。

2、对 TNC 客户/服务器与 IMV—IMC 的认证。

3、AR 和 PDP 的自身完整性。

4、补救措施的安全性。

5、界面的信息资源保护。

6、界面威胁的保护。

其中，秘密信息的保护包括：

1、需要支持匿名保护。

2、所有者的控制策略。

3、泄露控制策略。

4、IMC 选项。

5、敏感信息加密。

目前针对可信计算平台新出现的恐吓软件机制包括：支持 Raduius 协议，是网络接入的安全机制。支持几乎所有的网络接入机制，包括 WAN 和 VPN。认证[78][79](Authentication Protocol, AP)是保证数据安全的第一道屏障，包括：认证、授权、审计。一般的，安全系统都必须有认证这一环节，防止非法用户的侵入，对合法用户根据访问控制权限限制其行为。认证技术是可信计算平台、可信网络平台、可信连接标签、代理活动和交易活动都在使用的代理认证技术。包括数字签名、电子印鉴、标签认证、代理认证、数字证书管理、密钥管理等系统。网络环境下认证系统以逻辑参数作为鉴别的主要依据。

4.5.1 一种基于虚拟中间件的可信网络连接身份生存系统

考虑认证的方式即算法，可以分为如下几类：明消息用户名/口令传输；例如

原始的 telnet 和 ftp 协议中的认证过程就属于此类，这类方式是最不安全的，只是比不加任何方式的安全认证稍微有一些保障。基于口令散列的方式；这类是使用最为广泛、普遍的方式，几乎所有操作系统都使用这一方式，如 UNIX、WINNT 等。这类方式是将用户名明消息传送，同时发送一个经散列后的口令值，服务端将散列值与预先保存的口令散列互相比较，如果相同则通过验证。通常，为了防止窃听，有时口令在散列之前要加上证明的种子。挑战、应答方式；服务端向用户端发出“挑战”，通常是随机串 nonce，客户端将其与口令结合后，经过单向函数计算出“应答”，同时，服务端也进行同样的计算，如果结果相同则可认为该用户通过验证。这类方式抗第三方窃听，较单纯基于口令散列更加安全。基于公钥的认证方式；公钥公开，私钥保密，拥有用户公钥的一方可以发送消息，然后通过私钥解密。这种方式中通常会存在可信第三方对用户和公钥进行管理。

在可信网络连接中认可的认证协议主要有 Radius[80][81]协议，文献[82]对 Radius 在多种场合的特征有详细的描述。对远程用户，Radius 协议采用分布式客/服结构完成密码的集中管理和身份认证功能。用户登陆请求接网络连接，由网络访问服务器（Network Access Server, NAS）提示键入用户名和口令字，NAS 向安全服务器提出请求；安全服务器按照一定规则处理，返回响应，响应中包含是否同意用户连接请求。

可信计算组所定义的可信模块如图 4-7：

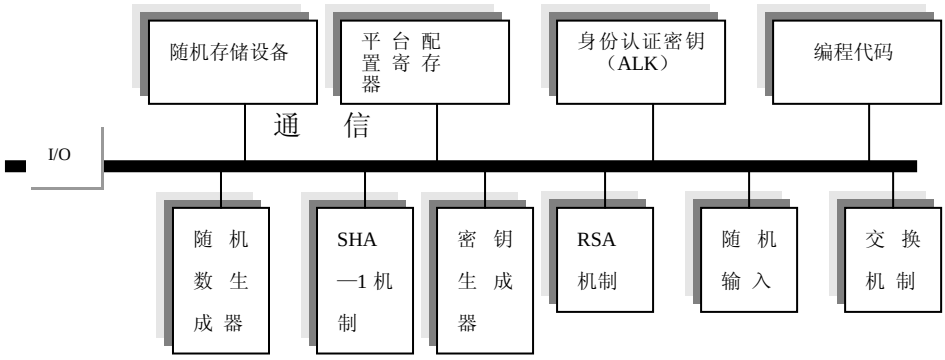


图 4-7 可信平台模块

认证技术是可信计算平台、可信网络平台、可信连接标签、代理活动和交易活动都在使用的技术。包括数字签名、电子印鉴、标签认证、代理认证、数字证书管理、密钥认证管理等系统。网络环境下认证系统以逻辑参数作为鉴别的主要依据。考虑认证的方式即算法，可以分为如下几类：明消息用户名/口令传输；例如原始的 telnet 和 ftp 协议中的认证过程就属于此类，这类方式是最不安全的，只

是比不加任何方式的安全认证稍微有一些保障。基于口令散列的方式；这类是使用最为广泛、普遍的方式，几乎所有操作系统都使用这一方式，如 UNIX、WINNT 等。这类方式是将用户名明消息传送，同时发送一个经散列后的口令值，服务端将散列值与预先保存的口令散列互相比较，如果相同则通过验证。通常，为了防止窃听，有时口令在散列之前要加上证明的种子。挑战、应答方式；服务端向用户端发出“挑战”，通常是随机串 nonce，客户端将其与口令结合后，经过单向函数计算出“应答”，同时，服务端也进行同样的计算，如果结果相同则可认为该用户通过验证。这类方式抗第三方窃听，较单纯基于口令散列更加安全。基于公钥的认证方式；公钥公开，私钥保密，拥有用户公钥的一方可以发送消息，然后通过私钥解密。这种方式中通常会存在可信第三方对用户和公钥进行管理。

如果采用基于分组密码的认证算法，把随机数生成、SHA—1 机制、密钥生成机制三种数据安全方式用分组密码算法的不同运算模式完成。通过对数据分组之后，用 ECB 模式进行加密。由于分组密码的设计初衷就是便于计算机数据字长的处理，并且易于硬件实现，因此可信计算平台采取分组加密算法是经济、简便、安全的方式。在 ECB 模式加密数据的同时，再把数据用 CBC 模式进行累加，最后的出与分组长度相同的认证代码。此处采用基于椭圆曲线求解难题的 ECC 机制来进行密钥交换，以替换原来可信计算平台的基于大数分解难题的 RSA 机制。ECC 明显的优势是在相同安全强度要求下，节省运算空间，减少门电路，降低可信平台面积。上述设计如上图 4-8。

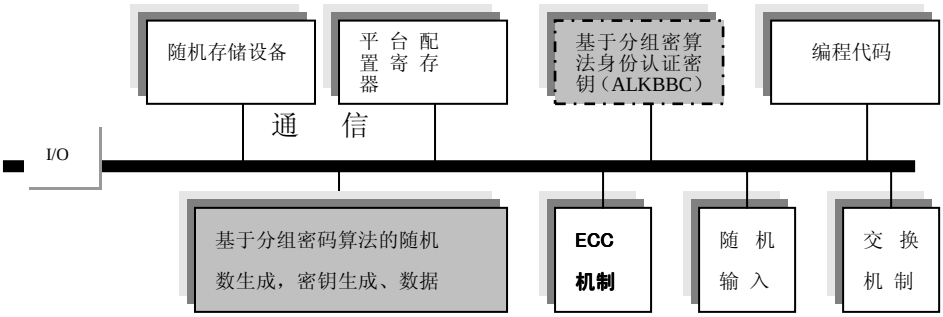


图 4-8 一种可信平台模块数据安全算法模块

对数据加密算法及发方 A 与接收方 B 对等身份认证的安全性证明：

步骤 1、A 采用 ECC 机制与 B 交换密钥 K，由于 ECC 算法的计算困难性，可以保证在非对称条件下把用于产生分组密码算法认证的初始向量传送至 B。此处无需向 B 要求回执进行身份验证，把时间节约出来在算法的最后一步与数据同时得

到证明。

步骤 2、A 发送数据 D，分别采用约定好的分组密码算法 ECD、CBC 模式对 D 进行加密同时向 B 通信，传送加密数据 E（D）、数据 HASH 值 H（D）。

步骤 3、B 接收到 A 的加密数据 D 及数据 D 的认证代码，使用相同的分组密码算法对 D 进行解读。如果能够得到正确的语意，说明 B 使用了正确的密钥，第一步的身份验证成功。把解出的语意使用 CBC 模式再进行 HASH 得到 $H^{'}$（D）。把 HASH 值与收到的 H（D）进行对比，如果两个 HASH 值相等，向 A 返回解读后的固定长度信息。

通过步骤 3，B 可以通过对比数据 HASH 值来验证 A 的身份同时证明数据的通信质量、通信中是否被篡改。A 可以通过 B 发回的固定位置语意信息，以证明 B 的确收到了 A 发送的密钥，使 B 的身份得到验证。同时也确认数据的安全通信完整性。该设计关系着加密算法、加密模式，还涉及 ECC 曲线的选取等方面，在该文章中不作重点关注。在对等条件下发送方 A 与接收方 B 就握手、分组密码算法选择还有一个预先通信过程，何以使用现成的可信计算组中规定的协议完成（如图 4-9）：

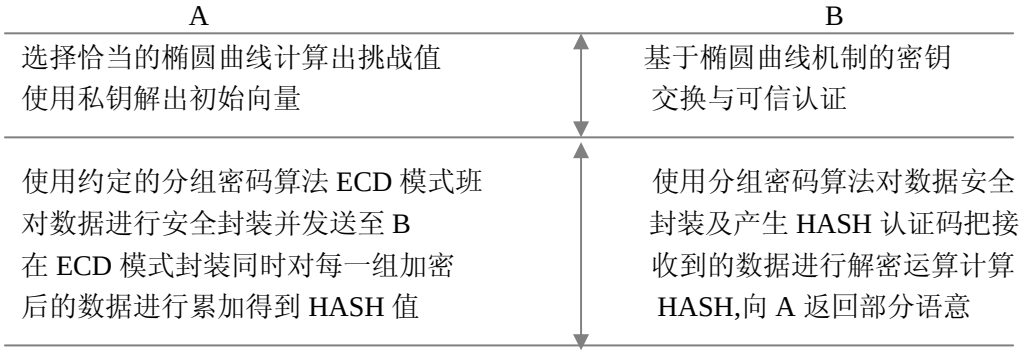


图 4-9 可信计算中对等关系安全数据通信及认证算法

在可信计算平台标准组的基础上，通过数据认证过程可以保护数据来源并且确认数据不被修改。如果通过解密后能够还原语意，既可以证明解密方掌握了真实的密钥，并且在数据得到确认的同时保证对方身份得到证明。这又关系着加密算法、加密模式，还关系这上一步中的非对称密钥交换算法。对身份认证选择公开使用的分组密码 CBC 模式，并用 ECB 模式对数据传送提供加密选择。可信网络连接（Trusted Network Connect，TNC）决定网络连接的合理性、安全性。TNC 结构提供端设备注册统一架构，其特征是：基于完整性、唯一性两个基本概念。

完整性用于描述终端的“鲁棒性”,其构造如同普通 IT 意义下的定义。例如系统如果保持预先确定的策略，确定系统没有在非正常或恶意的环境。唯一性确保系统被授权用户使用，TCM 的客户提供附加安全通过硬件来确定身份。TCM 也提供信赖导入机制，在不被探测到的情况下对根过滤工具包进行帮助。TNC 的另外一些重要特征集中在产品更新换代形成的各种不同种类的工作环境中。TNC 支持会提高许多已经存在的产品。用户可以因为使用了 TNC 工具快速获利。这个构架基于已经存在的一些标准，诸如：EAP、TLS 和 IPSEC 和 802.1X 等成熟技术。认证(Authentication Protocol, AP)是保证数据安全的一种方法。

虚拟中间件构架(图 4-10)提供原始的虚拟中间件作为软件开发的对象，使软件设计者有相当程度的灵活性。

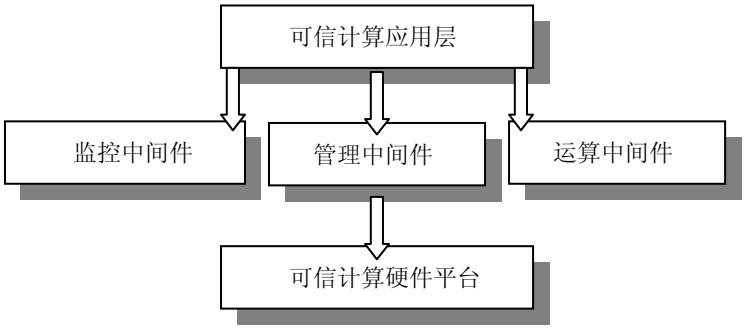


图4-10 可信计算中间件结构

使用虚拟中间件技术对可信计算平台进行适当的技术改进研究，是对分组密码算法在可信计算平台中的实际应用研究的一个分枝。当传统的虚拟中间件技术已经成熟，而且对 JAVA 虚拟中间件（Java Virtual Middleware, JVM）已有大量深入的研究。JVM 的目标是提供一个基于抽象规格描述的计算机模型，为解释程序开发人员提供很好的灵活性，同时也确保 Java 代码可在符合该规范的任何系统上运行。由于 JVM 有足够的灵活性，这使得将字节码翻译为机器代码的工作具有较高的效率，完全能满足运行速度要求较高的应用程序，从而也能很好地保证可移植性和高性能。使用虚拟中间件技术，把真实的物理 CPU 和内存封装起来，通过一系列的可信认证后，由管理虚拟中间件划分为若干个虚拟中间件。根据每个虚拟中间件上运行的应用软件不同的安全等级要求，管理虚拟中间件给相应的虚拟中间件配置合适的“虚拟 CPU”和“虚拟存储器”。每个“虚拟 CPU”和“虚拟存储器”只服务于它们对应的虚拟中间件，完全独立于其他虚拟中间件的“虚拟 CPU”和“虚拟存储器”，它们之间不能相互关联，更不能互操作。选择虚拟中间件加反篡改芯片可以相对容易实现高质量的可信计算。

4.5.2　一种 RFID 在可信计算平台的安全接入方案

随着计算无处不在的理论推广，可信计算平台的接入范围更广——几乎所有网络应用层的数据都可以进行可信接入。无线射频识别技术（Radio Frequency Identification, RFID），是非接触式自动识别技术的一种,也会被接入到可信计算平台。RFID 由传感标记、阅读器、相应数据的远程应用系统组成,通常使用低频、高频或甚高频。与传统条形码依靠光电效应不同的是，RFID 标签无须人工操作，在阅读器的感应下可以自动向阅读器发送商品信息，从而实现商品信息处理的自动化。RFID 采用无线信号进行无接触的双向信息传输，在使用方便和灵活的同时，增加了信息被窃取的风险。与有线信道不同，无线信道是一个公开的传输平台，任何人只要拥有相应频段的接收设备，就可以对无线信道进行监听。因此和有线信道相比，无线信道更容易被中间人分析，而且不容易被发现。事实上，针对 RFID 安全性的研究与标准化问题一直处于低端状态：由于经常使用的是廉价的功能，没有专门进行安全方面的研究。本文主要就 RFID 产品的可信计算平台接入，结合分组密码算法的不同使用特征，对 RFID 的完整性、安全性及未经授权不可篡改性进行讨论。

基于可信平台互联网安全接入的 RFID 结构如图 4-11：

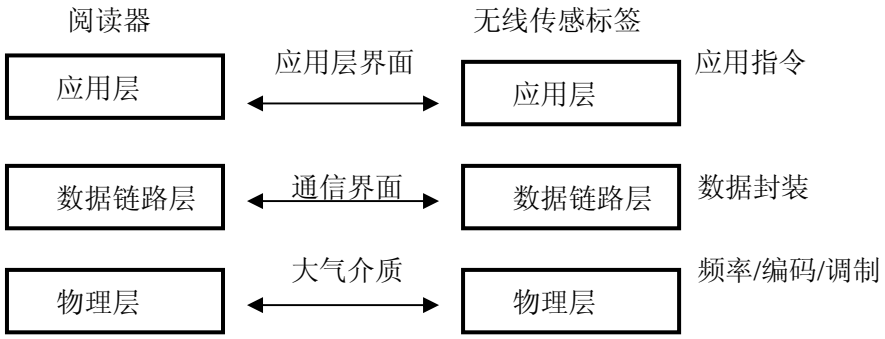


图 4-11 RFID 在不同网络层的结构及功能

就 RFID 本身使用等级来看，在商品供应链的层面，现存的体制都能保证其安全。但是如果作为身份识别或秘密载体，考虑到可信计算平台中网络的安全接入，需要使用软件和硬件的标准化程度较高的分组密码算法进行安全性的加强。

RFID 所遇到的安全问题，要比通常的计算机网络安全问题要复杂。在较新的 UHF 式 RFID 标签中，也发现到该漏洞，它可对关键的 RFID 系统造成的影响，就连更精密、可以四段速操作的“第二代 RFID”也一样难以应对分析。RFID 的数据通信链路是无线通信链路。与有线连接不一样，无线传输的信号本身是开放的。开放

链路通常遭到的分析包括：截取通信数据；业务拒绝式分析，即非法用户通过发射干扰信号来堵塞通信链路，使得阅读器过载，无法接收正常的标签数据；利用冒名顶替标签来向阅读器发送数据，使得阅读器处理的都是虚假的数据，而真实的数据则被隐藏。在阅读器中，除了中间件被用来完成数据的遴选、时间过滤和管理之外，只能提供用户业务接口，而不保障用户自行提升安全性能。中间件可以灵活运用于多种通信标准与现实环境中。

回避 RFID 风险的方法是根据其使用环境决定的[83]，并且使用对象的不同采取的标准也不同（图 4-12）。

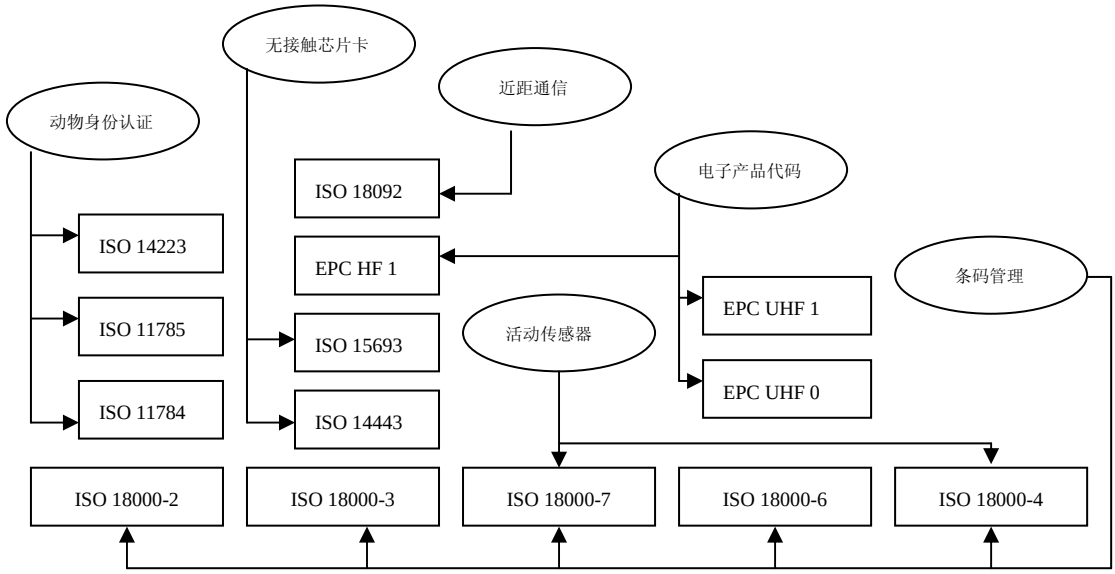


图 4-12 不同使用频段的 RFID 标准

采用不同工作频率、天线设计、标签技术和阅读器技术可以限制两者之间的通信距离，降低非法接近和阅读标签的风险，但是这仍然不能解决数据传输的风险。在高度安全敏感和互操作性不高的情况下，通常会采用实现专有通信协议。它涉及到实现一套非公有的通信协议和加解密方案。基于完善的通信协议和编码方案，可实现较高等级的安全。在金融网络及其他敏感数据——包括高端标签，智能卡的场合，可以通过专用的数据网关来操作，在不需要阅读和通信的场合，这是一个主要的保护手段。另外，使用适当的应用操作口令可以直接对进程中断处理而到达回避风险的目的。但是这需要有一系列的监控保障以选择适当的时机进行中断或保护。在协议、网络硬件、操作口令的层面上，协议通常掌握在国际、国家等级别的标准组织内，网络硬件可以通过生产商固化，而操作口令则需要依据实际情况而定。

通常的RFID系统没有相关的身份认证环节，使用PIN码是简洁而安全的方法，构成 PIN 码识别技术与硬件认证结合模式。RFID 的使用也可以分布在不同的安全层次，与可信计算的可信根结构是一致的。只需要根据 RFID 的标准，按照可信网络的标准选择合适的安全级别对 RFID 信息进行相应的加密与认证，能够保证安全使用。事实上，已经有较多的观点倾向与直接使用可信根结构进行 RFID 的安全系统密钥分发。由于分组密码算法在征集时就伴随标准化的过程，而且能够根据不同的安全程度进行密钥的控制。考虑到 RFID 系统的普及特性，采用分组密码算法的 CBC 运算模式代替 SHA-1 进行 PIN 码消息认证并进行可信计算平台的接入。在对 RFID 进行可信平台接入的同时，也使得可信计算的模块变得更简单。这里提出的设计关系着加密算法、加密模式，适用于对等关系的数据安全通信，可以在无线局域网与互联网络中使用，是对于可信计算组现行的逐级认证方式的补充。算法的设计初衷是节省可信计算平台硬件开销、使安全与可信计算执行速度更加优化。采用了为各种网络环境使用的分组密码算法作为可信计算平台的安全模块，与可信计算组目前所规定的用于无线局域网的 EAP、用于 Web Severs 的 TLS 及 HTTP 协议能够完全兼容，便于被标准化，也容易进行硬件实现。

4.6 分组密码算法在量子密钥分发中的使用建议

在 70 年代和 80 年代初期，几个调查人员包括 Wiesner、Feynam 等开始从理论上调查是否比特信息可以用两个方向上的量子表示。垂直偏振态和水平偏振态分别表示“0”“1”。通过 heisenberg 不确定原理和重叠原理。事实上，量子有六种存在的状态（图 4-13）。量子物理为信息科学引入了几个新观念：一般的，量子比特或昆比特既不能完全复制也不能实行监视，试图进行这些工作必然会使原来信息产生变化。这些特征对量子信息在密码学中的应用非常有启发，在1984年Charles Bennett和 Gilles Brassard提出了量子通信具备信息安全能力而且能够达到传统信息理论无法达到的效果这一思想。量子通信及保密由会话双方通过量子和普通通信方式合成,产生安全通信所必须的共享密钥，随机比特流。这个过程的安全性是通过毫无争议、完善的量子物理基础原理和信息理论的相互作用来保证的。

目前，量子密钥分发（Quantum Key Distribution, QKD）能够在光纤通道或数公里的空间通道中实现。除了满足独立应用，QKD 能够在物理层整合[84]，光通信为安全的通信提供物理层加密保障。更多实验表明：包括完整 QKD 协议的通信过程仅仅把目标定在缩短量子密码基础体系实现与完全保密理论的距离上，更多

的学术工作应在理论保密方面进行。但是随着成熟的物理实验促进技术进步，可以看到 QKD 肯定能够显著的对通信安全进行保障，而不去一味强调在物理实现中的完全保密性的不可实现。以 MD5 为代表的一类 Hash 函数宣称告破，对需要以该类算法作为信息保密、防篡改、抗否认、完整性验证的安全体制提出了挑战。分组密码算法以其分组及密钥的灵活性，能够以更强的保密性完成 Hash 的功能。

QKD 作为一个完整的信息安全及通信系统，在技术足够成熟后来满足未来需要。光通信基础中 QKD 有两个基本的作用[85]：作用一、“QKD 密钥分发模式”：对普通密钥分发功能的加强，支持对称密码体制的密钥产生和分发。作用二、“QKD 加密模式”：一种新的物理层加密技术。量子密钥分发的协议在 1984 年由 Bennett 和 Brassard 建立，通常称为 BB84 协议。A 和 B 产生一个公共密钥：不是由 A 创建一个密钥发送给 B，而是由 A 和 B 各自构建一个随机串，并在公共信道上承认相互的内容。BB84 是最为广泛使用的量子密钥分发协议，使用了量子的四种状态（图 4-14），它的一些细节还未公开。条件为一个抗干扰的公共信道时，并且假设量子信道是不安全的[86]，步骤如下：

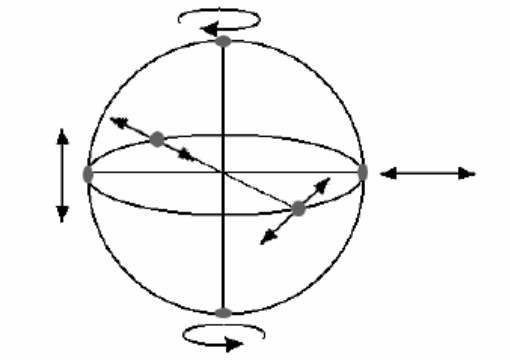


图 4-13 量子的六种状态

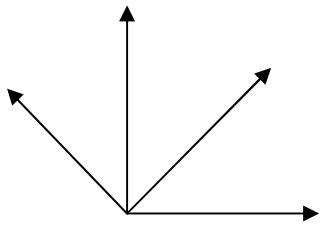


图 4-14 BB84 中量子的非正交态

1、A 和 B 协商一个可以接受的差错率，一般在 20%左右。

2、A 发送给 B 一串粒子，每个粒子的状态是四种偏振态中的一种。

3、B 每接收到一个粒子都测量它的偏振角度和纠缠率。B 记录这些状态，并且同时度量这些设置。

4、B 公开它的设置，不仅针对公共信道上对 A 的状态测量。

5、A 通过公共信道通知 B，他的哪一部分设置是正确的。A 与 B 通信前已经约定好错误率。

6、A 和 B 通过偏振态分离他们的数据。例如：平行、垂直、45°、135°。

7、如果 B 使用了错误的设置，那么 A 和 B 都不使用这些粒子。假设没有窃

听者，A 和 B 就得到了正确的偏振态。

8、A 和 B 从粒子设置中选择固定个数的 m、n 量子，并计算错误率，如果每个错误率都低于约定率，那么没有窃听发生，否则，A 和 B 需要放弃他们的数据并且从第一步重新开始。

9、A 和 B 使用这些结果数据去产生密钥。

但是在实际应用中，BB84 协议存在一些问题。首先，真实的量子探测总是伴随着噪音，即使没有窃听者，A 和 B 获得的量子序列也是不相同的；第二，以现在的技术，产生单个量子是不可信的。事实上，量子发生器是以每个脉冲产生量子数 m 来工作的，而不必要以单位时间的确切量子来记数。显然，当 m＞1，窃听者 E 有机会分离脉冲，窃取一个量子而使剩余的部分继续无干扰地分发到 B。如果 m＜1，那么窃听者能够分离脉冲的可能性有 $m^2/2$，在这种情况下，E 仍然能获得量子密钥的片段而不被发现。

分组密码算法在设计思想上仍然基于香侬关于信息的混乱与扩散原理，通过简单函数进行若干圈迭代使得明消息规律被充分掩盖；其优点是：密钥可以在一定时间内固定，不必每次变换，因此给密钥配发带来了方便。但是，由于分组密码存在着密数据传输错误在明消息中扩散的问题，因此在信道质量较差的情况下无法使用。针对量子密钥分发信道的纠错问题本文不做进一步讨论，通过分组密码的运算模式能够对错误扩散进行控制。1992 年，Bennett、Bessette、Brassard、Salvaid 和 Smolin 发表文章，提出克服量子密钥分发中错误扩散缺点的方案。在该协议中，A 和 B 先通过公开讨论协调他们的数据，对 E 仅仅只有在量子交换时的信息泄露。然后用所谓的“秘密放大”机制，A 和 B 提取一部分的虽然数目小，但是保密性强得多的密钥。A 和 B 协商数据在公共信道上进行，E 可能听到所有过程。A 和 B 在同样的密钥产生之前要尽可能少的泄露信息。由于 E 的窃听以及分析技术的不断进步，须要在进行块奇偶校验之前，对数据块进行加密。针对量子通信的技术发展特点，在现阶段采取的方法一般是 Hash 压缩。由于分组密码算法支持长度为 128、192、256 的信息分组，因此使用分组密码算法在量子通信中用做一种抗检测的高次压缩函数，来减少信息泄漏，其抗分析程度是 128 比特的 SHA-1 所无法比较的。当对数据进行完加密后，对加密序列进行排列、按大小 b 进行序列分组，常数 b 的选择是确保每块数据的错误数不会超过 1 个。BBBSS 执行的时候，b 多是根据经验来选择的而非通过理论计算而得到。A 和 B 比较每个块的奇偶性，如果发现奇偶性不同，则把块进行更小的分割。继续比较奇偶性，直到没有错误的匹配。为了不让 E 在这个过程得到信息，A 和 B 丢掉他们透露的每

个奇偶块的最后一个比特。

完成一次对话过程后，A 和 B 将继续比较块的奇偶性，由于比较后的块都要去掉 1 比特，所以，发现错误的概率会随之降低。在对 A 和 B 分块方面，还可以采取对数据块的子集进行划分的方法，进一步进行奇偶性检测。从 BB84 公开发表以后，在量子通信和量子密码的基础理论研究都经历了巨大的发展。1991 年 Ekert 展示了利用奇特的量子纠缠态的机器能够大大提高量子保密水平。在 90 年代早期和中期，实验量子物理和量子技术都取得了很大的发展，这给在实验室进行量子信息实验提供了基础。特别针对一类量子密码协议进行了多种实验，主要集中在量子密钥分发上。通过这些实验，新的对量子密码理论体系认知达到了一个新的水平，激发了绝大多数国际发达国家对这个领域的高度重视、空前研究热情和资金支持。不论这 20 年的历史多么显著，量子密码还有许多工作需要继续[87] [88] [89] ，要达到量子信息安全在现实中的应用要求：

1、还有一些剩余的完整性理论需要证明。

2、考虑理想保密、量子信息理论概念、理论量子实现之间的差距。

3、专线通信已经进行了 QKD 实验，对在网络环境下传统通信和精确量子信息共存的论点没有具体论断。

4、量子密码信息保密系统相对与普通通信保密而言其潜在使用要更加难以实现。

5、对 QKD 在点对点以外的协议几乎没有引起注意。

6、对 QKD 以外的量子协议几乎没有进行。

与这些相伴的有，在日益庞大的网络国际，政府及商业行为都需要有可靠的信息安全保障，虽然传统的安全形式能够满足这些要求，但是也面临着日益增加的技术挑战：

7、在数学、高性能计算上不可预知的发展，可能的大规模量子计算威胁今天的通信安全。

8、日益增加的网络通信安全复杂度要求支持多层次用户安全动态接口。

9、要求发射更高安全的宽频段。

量子密码有可能遭遇到这些潜在的威胁，也会为未来通信保密工具集合中添加新的工具。可以看到信息安全保障能够与传统方法进行评估和参照。对量子密钥分发安全性进一步研究的目的是在基础和应用以及系统工程方面，保证量子密码在将来的几十年从“物理+信息理论”发展到“量子信息安全”纪元。这些因素会使新手段在将来的信息安全机制中与传统手段结合而成为一个整体，促使量子通信

中密码学真正能够参与进来。由于量子通信的质量问题，数据需要不断进行纠错。这样使得中间人进行分析的机会增大，截获数据序列的机会也随之加大，所以对量子序列进行加密传输是保证信息安全的必然手段。虽然量子通信在信号传送方式、传送质量上都存在局限性，但目前通信界与信息安全界普遍看好这一新型传输介质。在量子通信安全保障方面，随着压缩函数的一一告破，分组密码算法的以其快速、安全、经济等优势，相对于流密码算法、单向压缩算法更值得推荐，在量子密钥分发中应成为首选加密算法。同时，量子通信的完善使网络密码在物理层得以实现。

4.7 本章小结

本章主要对分组密码算法所使用的协议环境及标准进行了研究。由于分组密码算法主要使用于无线网络与互联网络，因此该两类网络的使用密钥分发协议与标准对于数据的安全起关键作用。对可信计算平台、RFID 技术及量子密钥分发方案中分组密码算法的运用也进行了论述。一个好的分组加密算法不仅在设计上需要满足硬件实现、软件工程方面的要求，还需要好的使用协议到达算法最佳的发挥。当然，信息安全中最核心的部分是密码算法本身，协议的薄弱会对安全产生威胁。通过应用，展示了分组密码算法在多种协议环境下的各种不同方式的用途。

第五章 结 论

5.1 全文总结

作为对称密码算法中公开的一部分，无线网络与互联网络中逐步推广使用的分组密码算法成为国际上研究的热点。DES 公开征集、使用后，各种机构对分组密码算法给予了越来越多的关注。随后的 NESSIE 标准征集为密码的应用打开了更广阔的前景，eSTREAM 对流密码的再次鳞选证明了：信息安全领域的公开竞争是不可避免的趋势。中国无线网络使用的分组密码算法也首次由官方公布，这标志着随着信息全球化，中国信息安全领域核心密码设计最终从算法保密走到算法公开。也表明在分组密码算法设计方面已经具备足够的信心对抗算法已知条件下的多种分析。

本文先后论述了分组密码算法的理论基础，从抗分析的角度对算法进行加强设计。包括：抗线性分析设计、抗非线性分析设计、抗 DPA 硬件设计、运算模式设计、密钥生成及基于无线网络和互联网络的分组密码算法相关标准、协议设计。重点关注了分组密码算法的概念、特点、常用结构和标准化内容。对本文的核心内容分组密码算法设计与评估现状进行了阐述，特别以 AES、Camellia 为例，从算法的框架、模块分析了当前几个重要的分组密码算法。同时分别通过软件、硬件不同的侧重点讨论了上述算法的特征。对分组密码算法标准化及在不同网络环境下的使用情况做出概述。讨论了分组密码算法安全性评估与设计，具体包括算法线性部分分析基本原理，最大线性偏差、最大线性偏差评估法、最大线性偏差搜索算法应用研究；针对算法非线性设计模块安全性评估原则应用研究；差分密码分析基本原理、S 盒线性偏差、分组密码算法扩散性测试评估原则应用研究；分组密码算法设计讨论了 Feistel 结构分组密码算法设计基本原理、SP 结构分组密码算法设计基本原理；正形置换设计、S 盒设计、S 盒的代数次数和项数分布、S 盒的非线性度、S 盒常见构造方法等部件的设计原理。重点对 SP 型分组密码算法进行了置换部分的设计与研究；对密钥的生成与密码结合方式进行深入讨论。

以信息安全协同作为背景，研究了各个层次所使用的分组密码算法的设计与使用。在基于 IP 的三网合一标准下，对国际公开标准与协议进行讨论，使分组密码算法的作用发挥到更加合理的限度。提出了分组密码算法相关协议的设计与评

估是基于密钥的。特别，从可信计算角度分析了协议的安全性以及存在的漏洞，使用层次划分的方法进行安全协议设计并且给出安全强度证明。研究了现行公开使用的分组密码算法标准，提出分组密码算法设计框架在安全前提下，简洁设计更适合于网络化的使用环境；在密码强度与运算速度的取舍中需要具有冗余度，以应对网络中的各种不同类型故障。对分组密码算法非线性模块设计、评估做出量化，运算并证明最低安全标准值。给出几个设计与分析方案；对线性模块提出基于运算速度及基于安全强度的设计思路，列举几个创新性设计方案。对密钥提出唯速度与硬件标准设计方案。对密钥与密码结合方式进行研究，提出了相应的硬件实现策略。对目前研究热点——可信计算平台、RFID 应用、量子通信中的分组密码算法也进行了一定的创新设计与应用，进一步证明了：分组密码运算模式的灵活，可以用做单向函数、流密码等多种用途。

5.2 公开方向展望

分组密码算法是公开类密码设计中强调速度及工程实现的一类，因此在密码算法设计中需要充分考虑到硬件具体实现的安全性、合理性及经济性，硬件的布线拓普结构设计是一个需要研究的方面。对分组密码算法的分析手段与计算技巧、能力也是需要不断研究之处，特别是对非线性模块分析的研究逐步成为加强设计的依据。同时对分组密码算法在纯理论上的研究还包括正形置换的圈枝结构、计数研究等。由于主要使用于网络之上，本文对下一代网络的体系结构研究、网络密钥分发协议也给予了一定的关注。

致　谢

感谢导师魏正耀院士、秦志光教授、范明钰教授和教研室的张凤荔教授、何兴高、周世杰、陆庆老师及同窗好友。通过博士阶段的学习，我能以开阔的心胸和客观的眼界看待、处理周围的事物，有自信面对未来的挑战。感谢电子科技大学学报和 IEEE 等出版物的编辑们，他们给予我了耐心的帮助，使我的研究工作能够更完美的呈现出来。

感谢电子科技集团三十所现代通信国家重点实验室的学者，感谢曾给予我机会和支持的国际、国内同行。

参考文献

[1] American National Standards Institute. ANSI X3, 1983, American National Standard for Information Systems. Data Encryption Algorithm-Modes of Operation:106-1983

[2] W.Diffe M.E.Hellman，New Directions in Cryptography，IEEE Trans Information Theory，Vol.IT22，1967:644-654

[3] NBS，Data Encryption Standard，FIPS PUB 46，National Bureau of Standards，Washington，D.C,1977

[4] M.Matsui, Linear Cryptanalysis Method for DES Cipher. In T. Helleseth, editor, Advances in Cryptology—EUROCRYPT'93, Volume 765 of Lecture Notes in Computer Science. Springer-Verlag, Berlin, Heidelberg, New York, 1994:386-397

[5] 吴文玲，冯登国，分组密码的运算模式的现状研究，计算机学报，2006、1

[6] International Organization for Standardization. ISO 8372:1987,Information Processing. Modes of Operation for a 64-bit Block Cipher Algorithm,1987

[7] International Organization for Standardization. ISO/IEC TR 13594: 1995, Information technology. Lower layers security, 1995

[8] International Organization for Standardization. ISO/IEC 10181.4*:* 1997, Information technology. Open Systems Interconnection. Security frameworks for open systems. Part 4: Non-repudiation framework, 1997

[9] Paul Kocher, Joshua Jaffe, Benjamin Jun. Differential Power Analysis [C], 1999,Proceeding of Advances in Cryptography (CRYPTO99):386-397

[10] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1997

[11] European Telecommunications Standards Institute (ETSI). 3GPP TS 33.105, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Cryptographic Algorithm Requirements, June 2001

[12] European Telecommunications Standards Institute (ETSI). 3GPP TS 35.202, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification, June 2002

[13] European Telecommunications Standards Institute (ETSI). 3GPP TS 35-201, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: f8 and f9 Specification, June 2002

[14] National Institute of Standards and Technology, U.S Department of Commerce. Data Encryption Standard, 1999.NIST FIPS PUB :46.3

[15] National Institute of Standards and Technology (NIST). Federal Information Processing Standards Publication 46-3 (FIPS PUB 46-3): Data Encryption Standard, October 1999

[17] American National Standards Institute- ANSI INCITS (R1998), Data Encryption Algorithm (formerly ANSI X3.92. 1981 (R1998)), 1998:92-1981

[18] National Institute of Standards and Technology (NIST). Federal Information Processing Standards Publication 197 (FIPS PUB 197): Specification for the Advanced Encryption Standard (AES), November 2001

[19] National Institute of Standards and Technology（NIST）NIST Special Publication 800-38A,Recommendation for Block Cipher Modes of Operation:Methods and Techniques, December 2001

[20] W.E.Burr, Selecting the Advanced Encryption Standard. IEEE Security and Privacy, March/April 2003 *1*(2):43-52

[21] C.Giraud. DFA on AES Cryptology ePrint Archive. http://eprint.iacr.org 10,2005

[22] 胡玉濮，张玉清，肖国镇，对称密码学，机械工业出版社，2002:47-56

[23] 阮传概，孙伟，近世代数及其应用，北京邮电大学出版设，2002:20-30

[24] N.Courtois, G.Castagnos, and L.Goubin. What do DES S-boxed say to each other ? http://epirnt.iacr.org/2003/184

[25] National Bureau of Standards, U.S Department of Commerce. Data Encryption Standard（DES）, FIPS 46, 1977

[26] C.E.Shannon，Communication Theory of Secrecy Systems，Bell System Technology Journal, Vol-28，n.4，1949:656-715

[27] W.Stallings. Data and Computer Communications. Prentice Hall, 7th edition, 2004

[28] E.Danielyan Goodbye DES, welcome AES. The Internet Protocol Journal, June 2001, 4(2):15.21

[29] L. R. Kmudsen. Truncated and Higher Order Differentials. In B. Prencel. Editor. Fast Software Encryption—Second International Workshop, Volume 100 of Lecture Notes in Computer

Science. Springer-Verlag, Berlin, Heidelberg, New York,1995:196-211

[30] T. Jakobsen, L. R. Kundsen. The Inerpolation Attack on Block Cipher. In E. Biham, editor, Fast Software Encryption—4th Intermational Workshop, FSE'97, Volume 1267 of Lecture Notes in Computer Science, pp.28.40, Berlin, Heideberg, New York, 1997, Springer-Verlag

[31] E.Biham. New Types of Cryptanalytic Attacks Using Related Keys. Journal of Cryptology, Vol-7, No.4, 1994:229-246

[32] A.Biryukov, D.Wagner. Advanced Slide Attacks. In S.Baudenay, editor, Adeances in Cryptology—EUROCRYPT2000, Volume 1807 of Lecture Notes in Computer Science, Berlin, Heidelberg, New York, 2000- Springer-Verlag :589-606

[33] A.Birynkov D.Wagner, Slide Attacks. In L.Knudesen, editor, Fast Software Encryption—6th International Workshop, FSE'99, Volume 1636 of Lecture Notes in Computer Science, Berlin, Heidelberg, New York, 1999. Springer-Verlag :245-259

[34] 罗岚，大规模自变量函数的差分密码分析，解放军信息工程大学硕士学位论文，2004

[35] D.Wagner. The Boomerang Attack. In L.R..Knudsen, editor, Fast Software Encryption—6th International Workshop, FSE'99, Volume 1636 of Lecture Notes in Computer Science, Berlin, Heidelberg, New York, 1999- Springer-Verlag:156-170

[36] M.Matsui T. Tokita. Cryptanalysis of a Reduced Version of the Block Cipher E2. In L. Knudsen, editor, Fast Software Encryption—6th International Workshop, FSE'99, Volume 1636 of Lecture Notes in computer Science, Berlin Heidelberg, New York, 1999. Springer-Verlag :71-80

[37] M.Kanda, S. Moriai, K.Aoki, H.Ueda, M.Ohkubo, Y. Takashima, K. Ohta, T. Matsumoto. A New 128-bit Block Cipher E2. Technical Report ISEC98.12. The Institute of Electronics, Information and Communication Engineers, 1998

[38] M.Matsui , On Correlation Between the Order of S-boxes and the Strength of DES, Advances in Cryptology Eurocrypto'94, 1994:157-170

[39] M.Matsui, Linear cryptanalysis method for DES cipher. Advances in cryptology-Eurocrypt'93, LNCS 765, Springer-Verlag, 1994:17-26

[40] J.Daemen, V.Rijmen, AES proposal Rijndael,1998

[41] 王育民，刘建伟，"通信网的安全——理论与技术"，西安电子科技大学出版社，2000

[42] 冯登国，吴文玲，分组密码的设计与分析，清华大学出版社，2001:3-5

[43] B.Preneel, evaluation by the NESSIE Project on the AES Finalists, AES Round 2 public assesse, 5.2000

[44] T.Toffoli, N.Margolus, Invertible Cellulat Automata: A Review Physica D.Vol45, 1995:229-253

[45] W.V.Dam, Quantum Cellular Automata. Master thesis. Department of Mathematics and Computer Science, University of Nijmegen, The Netherlands, August, 1996

[46] 冯登国，密码分析学，清华大学出版社，广西科学技术出版社，2000:19-22

[47] 温巧燕，钮心忻，杨义先编著，现代密码学中的布尔函数，科学出版社，2000

[48] L.Connor, Enumerating nondegenerate permutations- Advances in cryptology Eurocrypt'91, Springer-Verlag,1991:368-377

[49] 王树禾，离散数学引论[M]，中国科技大学出版社，2001，18-22

[50] 吴文玲，冯登国，卿思汉，简评美国公布的 15 个 AES 候选算法，软件学报。1999，10（3）：225-230

[51] International Organization for Standardization. ISO 7498-2: 1989, Information processing systems. Open Systems Interconnection. Basic Reference Model. Part 2: Security Architecture, 1989

[52] International Telecommunication Union. CCITT Recommendation X.800 (1991), Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure and Applications Security Architecture for Open Systems Interconnection for CCITT Applications, 1991

[53] International Organization for Standardization. ISO/IEC 10181.1: 1996, Information technology . Open Systems Interconnection. Security frameworks for open systems: Overview, 1996

[54] International Organization for Standardization.ISO/IEC 10116:1997,Information Technology. Security Techmiques.Modes of Operation for an n-bit Block Cipher,2nd edition,1997

[55] T.Matsumoto, Y.Takashima, H.Imai. On seeking smart public-key-distribution systems. The Transactions of the IECE of Japan, 1986, E69:99-106

[56] N.Alexandris, M.Burmester, V.Chrissikopoulos, D.Peppes. Key agreement protocols: two efficient models for provable security. In S.K.Katsikas, D.Gritzalis, editors, Information Systems Security, Facing the Information Society of the 21st century, IFIP SEC'96, Chapman & Hall,1996: 227-236

[57] M.Just S.Vaudenay. Authenticated multi-party key agreement. In Advances in Cryptology: Asiacrypt'96,1996:36-49

[58] J.H.Moore. Protocol failure in cryptosystems Chapter 11 in Contemporary Cryptology; the Science of Information Integrity,IEEE Press,1992, G.J.Simmons, editor:541-558

[59] Bennett,C.H G.Brassard , "Quantum cryptography : Public Key distribution and coin

tossing ”[J] , in Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India（IEEE, New York, 1984）:175-179

[60] K.Nyberg. Differentially uniform mappings for cryptography[J], Advances in Cryptology Proceedings Eurocrypt’93, LNCS 765 , T.Helleseth, Ed., Springer-Verlag,1994:55-64

[61] IEEE p1363 Standard for Public-key Cryptography. July 1997. Working Draft

[62] M.Bellare , P.Rogaway. Entity authentication and key distribution. In Advances in Cryptology: Crypto’93,1993. A full version of the paper is available at http://www.cse.ucsd.edu/users/mihir : 232-249

[63] M.Bellare , P.Rogaway. Provably secure session key distribution—the three party case. In Proceedings of the 27th- ACM Symposium on the Theory of Computing,1995:57-66

[64] M.Burmester. On the risk of opening distributed keys. In Advances in Cryptology: Crypto’94,1994:308-317

[65] Foley, S.N.; Li Gong; Xiaolei Qian A security model of dynamic labelling providing a tiered approach to verification; Security and Privacy, 1996. Proceedings, 1996 IEEE Symposium on 6-8 May 1996 Page(s):142 – 153

[66] W.Diffie, P.C.van Oorschot, M.J.Wiener. Authentication and authenticated key exchanges- Designs, Codes and Cryptography, 1992:107-125

[67] Wireless Application Protocol (WAP) Forum[S]: http://www.wapforum.com 2005.4

[68] Dierks, C.Allen, The TLS Protocol Version 1.0 [S] RFC.2246, 1999.1

[69] PKCS standards and PKI related information[S]: http://www.reasecurity.com/rsalabs/pkcs/index.html 2005.5

[70] National Institute of Standards and Technology, FIPS PUB140-2 Annex A: Security Requirements for Cryptographic Modules[S], http://www.nist.gov/cmvp 2006.5

[71] 卿思汉，冯登国，信息和通信安全——CCICS‘99。北京：科学出版社，1999

[72] 卿思汉，周展飞，Kailar 逻辑的缺陷。软件学报，1999，10（12）：1238-1245

[73] 杨义先，孙伟，钮心忻，现代密码新理论，科学出版社，2002

[74] Shi, W. Lee, H.H.S.; Ghosh, M.; Lu Architectural support for high speed protection of memory integrity and confidentiality in multiprocessor systems, C.Parallel Architecture and Compilation Techniques, 2004. PACT 2004. Proceedings-13th International Conference on 29 Sept.3 Oct. 2004 :123 – 134

[75] Trustedcomputinggroup: Trusted Computing Module[R]. http://www.trustedcomputinggroup.org 2005-12-1

[76] Trusted computing group , trusted network connect to ensure endpoint integrity[R]. http://www.trustedcomputinggroup.org 2005.12.1

[77] T.Roe, M.Casey, Integrating cryptography in the trusted computing base,Computer Security Applications Conference, 1990, Proceedings of the Sixth Annual 3-7 Dec. 1990:50 – 56

[78] B.Clifford Neuman: Proxy-Based Authorization and Accounting for Distributed Systems[J]. Proceedings of the 13th International Conference on Distributed Computing Systems, May 1993: 283-291

[79] B.Clifford Neuman Theodore Ts'o. Kerberos : An Authentication Service for Computer Networks[M], IEEE Communications, September 1994, 32(9):33-38

[80] C. Rigney, S. Willens Livingston, A. Rubens Merit, W. Simpson Daydreamer : Remote Authentication Dial In User Service (RADIUS) http://www.ietf.org/rfc/rfc2865.txt 2003.12

[81] C. Rigney, S. Willens Livingston, A. Rubens Merit, W. Simpson Daydreamer : Remote Authentication Dial In User Service (RADIUS)[R] http://www.ietf.org/rfc/rfc2865.txt 2004

[82] G. Zorn Microsoft Vendor. specific RADIUS Attributes[R] http://www.freeradius.org/rfc/rfc2548.html 2003.10

[83] International Organization for Standardization. ISO/IEC FCD 18033-3, Information technology . Security techniques. Encryption Algorithms. Part 3: Block Ciphers, 2003

[84] Bennett,C.H , G.Brassard , C.Crepeau, U.M.Maurer "Generalized privacy amplification"[J] IEEE Transactions on Information Theory 41, （1995）:1915--1923

[85] D.Aharonor, M.Ben "Fault tolerant computation with constant error"[J] , 1997,In proceedings of the Twenty. Ninth Annual ACM Symposium on the Theory of Computing ： 176-188

[86] N.Gershen feld I.Chuang , Quantum computing with molecules[J], Scientific American , Jun 1998

[87] Discovery[J], Vol-23, n.5, May 2002

[88] Hisket,P.A.,Bonfrate, G.Buller, G.s. Townsend, P.D, "Eighty kilometer transmission experiment using an InGaAs/IP-based quantum cryptography receiver operating at 1-55μm"[J], Jorunal of Modern Optics, Vol-48, n-13, 2001

[89] Eleanor Rieffel and Wolfgang Polak, "An Introduction to Quantum Computing for Non-Physicists"[J], ACM Computing Surveys, September 2000 quantph, 32(3):300-335

攻博期间取得的研究成果

一、 参与科研工作情况

［1］2006 自然科学基金项目： 60673075

［2］2006 科技部 863 项目：2006AA01Z428

［3］2007 年新技术与应用中的安全技术国际研讨会审稿

［4］2007 年 CISP2008 国际会议审稿人

［5］2008 年 International Journal of Information and Computer Security，International Journal of Computer Science and Engineering Systems，International Journal of Information Analysis and Processing 审稿人

二、 发表论文情况

[1] Luo, Lan, Qin, ZhiGuang, Wang, Juan, Intelligent Application Conversion of Block Ciphers for Different Network Layers, International Journal of Innovative Computing, Information and Control，Volume 3, Issue 1, 2009.3（SCI，EI 检索源刊）

[2] Lan Luo, Zehui Qu, Chaoming Song, Precise Transformation of Feistel to SP Fuse into LFSR: China Communications, VoL 6, No.4, 2009.11（SCI检索源刊）

［3］Luo, Lan, Notes to Grain128_p2 of eSTREAM Phases 3, International Journal of Computer Sciences and Engineering Systems, 2008.3

[4] Lan Luo, A Note to Modes of Block Cipher as Stream Cipher without Information Loss, International Journal of Computational Cognition, 2008.9

［5］罗岚、瞿泽辉、张凤荔、秦志光、魏正耀，一种带比特延迟的分组密码算法密钥结合模式设计，电子科技大学学报，Vol.36, No.3, 2007.3（EI 检索源刊, EI 检索号：073010707211）

［6］罗岚, 秦志光, 万国根, 魏正耀，分组密码算法认证运算模式的注记及可证安全性，电子科技大学学报，Vol.38, No.4, 2009.7（EI 检索源刊）

[7] Luo, Lan, Qin, ZhiGuang, Jiang, ShaoQuan, The Intelligent Secure Structure Based on Active Block Ciphers for Application Layer of Internet. The 2008 International Congress on Image and Signal Processing, IEEE proceeding, 2008.5（EI 检索号: 083911598698）

[8] Luo, Lan, Qin, ZhiGuang, Zhou, ShiJie, Jiang, ShaoQuan, Wang, Juan, A

Middleware Design for Block Cipher Seamless Connected into Stream Cipher Mode, The 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008 IEEE proceeding, 2008.8（EI 检索号：084311653450）

[9] Luo，Lan, Qin，ZhiGuang, Jiang，ShaoQuan, A Key Delay Design Operation Model of Block Cipher Algorithm in Networks, ISKE2007, 2007.10（ISTP 检索国际会议, DOI:10.2991/iske.2007.78）

[10] Luo，Lan, Zhang，Fengli, Zhou，ShiJie, A Design Of Data Security Algorithm To Trusted Network Connect and Comment to Its Security, Proceedings of 2006 Symposium on Information, Electronics, and Control Technologies, 2006.9（国际会议）

［11］罗岚、魏正耀、蒋绍权，分组密码圈结构设计及可证安全性，通信技术，2007.6（国内核心源刊）

［12］罗岚、范明钰、魏正耀、王光卫、瞿泽辉，分组密码对称置换算法设计，计算机应用研究，2007. 1（国内核心源刊）

［13］罗岚、魏正耀、范明钰，分组密码芯片模块保护设计，信息安全与通信保密，2006. 7

［14］罗岚、魏正耀、秦志光、石竑松、唐寅，分组密码算法两种 S 盒设计的可证安全性注记，信息安全与通信保密，2007. 3

［15］罗岚、魏正耀、秦志光、申兵、周世杰，一种基于分组密码算法使新成员接入无线传感网络的认证协议及可证安全性，第一届中国传感器网络学术会议，2007.9

［16］罗岚、魏正耀、秦志光，分组密码算法链接模式构造单向函数的可证安全性，第十届保密通信年会，2007.8.8

［17］罗岚、魏正耀、张凤荔、申兵、周世杰，一种基于分组密码算法认证模式的 RFID 在可信计算平台的安全接入方案，第一届中国高校通信类院系学术研讨会，2007.8

［18］罗岚、瞿泽辉、秦志光、魏正耀，分组密码算法抗线性分析设计策略，第十一届全国青年通信学术会议论文集，2006. 8

［19］罗岚、张凤荔、秦志光、唐寅、魏正耀，对基于分组密码算法的量子密钥分发方案注记，第十四届遥测遥控会议，2006. 11

［20］罗岚，一种收缩流密码算法非线性结构偏差的方法及可证安全性，中国科技论文在线，http://www.paper.edu.cn，2007.6.6