第 29 卷 第 1 期
2006 年 1 月
计 算 机 学 报
CHINESE JOURNAL OF COMPUTERS
Vol. 29 No. 1
Jan. 2006

分组密码工作模式的研究现状

吴文玲 冯登国
（中国科学院软件研究所信息安全国家重点实验室 北京 100080）

摘 要 分组密码工作模式是利用分组密码解决实际问题的密码方案.好的工作模式可以弥补分组密码的某些缺憾;相反,不好的工作模式可能带来安全隐患.工作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,都会伴随着相应工作模式的研究.从针对 DES 的 ECB、CBC、CFB 和 OFB,到针对 AES 的 CTR、CCM、CMAC、GCM 和 AESKW,作者以各种模式标准为主线,介绍分组密码工作模式的设计理念、安全模型、二十多年的研究成果以及发展现状.

关键词 工作模式;分组密码;加密;认证;Hash 函数
中图法分类号 TP309

The State-of-The-Art of Research on Block Cipher Mode of Operation

WU Wen-Ling FENG Deng-Guo
(*State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing* 100080)

Abstract A mode of operation, or mode, for short, is an algorithm that features the use of a symmetric key block cipher algorithm to provide an information service, such as confidentiality or authentication. A good mode can remedy some weaknesses of block cipher, on the other hand, a poorly designed mode may be insecure even though the underlying block cipher is good. The research of mode always goes with the development of block cipher. With the advent of new block ciphers, there is a need to update long-standing modes of operation and an opportunity to consider the development of new modes. From the ECB, CBC, CFB and OFB modes of DES to CTR, CCM, CMAC, GCM and AESKW modes of AES, the authors introduce the design rationales, security model, research results and the state-of-the-art of research on block cipher mode of operation in this paper.

Keywords mode of operation; block cipher; encryption; authentication; hash function

1 引 言

分组密码是最基本的密码技术之一,其处理消息的长度是固定的,如 DES 为 64 比特、AES 为 128 比特,但是在实际中需要处理的消息通常是任意长的,且要求密文尽量不确定,而分组密码自身不能做到,因此,引出了如何利用分组密码处理任意长度消息的问题.解决这个问题的技术就是分组密码工作模式.既然是分组密码的工作模式,所以它的研究始终伴随着分组密码的研究历史.1980 年,美国国家标准局(现在的 NIST)公布了 4 种 DES 的工作模式[1],它们分别是 ECB、CBC、CFB 和 OFB.在文件 FIPS 113 中,公布了 DES 的认证模式 CBC-MAC.在文件 FIPS 46-3 中,公布了 Triple-DES 的 7 种工作模式,它们同时也被包含进 ISO 的相关文件中[2~4].

收稿日期:2005-10-25.本课题得到国家自然科学基金(60373047)和国家"九七三"重点基础研究发展规划项目基金(2004CB318004)资助.
吴文玲,女,1966 年生,博士,研究员,博士生导师,目前主要从事密码学与信息安全方面的研究工作.E-mail: wwl@is.iscas.ac.cn.
冯登国,男,1965 年生,博士,研究员,博士生导师,目前主要从事信息与网络安全方面的研究与开发工作.

在 AES[5] 即将诞生之际，2000 年 3 月 NIST 为 AES 公开征集保密工作模式，NIST 在第一阶段征集到了 15 个候选工作模式，它们分别是 2DEM、ABC、CTR、IACBC、IAPM、IGE、KFB、OCB、PCFB、PMAC、RMAC、XCBC（MAC）、XCBC、XEBC（MAC）和 AES-Hash. 为了推进模式标准的征订工作，NIST 分别在 2000 年 10 和 2001 年 8 月召开了两次国际会议，讨论征集到的候选工作模式，并于 2001 年秋季在文件 800-38A[6] 中公布了 AES 用于保密性的 5 种工作模式，它们分别是 ECB、CBC、CFB、OFB 和 CTR. ECB、CBC、CFB 和 OFB 的用法类似 DES，CTR 是唯一选定的新保密工作模式. 除了保密模式，随后 NIST 继续在认证模式和认证保密模式方面做了大量的工作，在 2005 年 5 月公布的文件 SP 800-38B[7] 中给出了认证模式的建议标准——CMAC；在 2004 年 5 月公布的文件 SP 800-38C[8] 中给出了认证保密模式的建议标准——CCM. 到目前为止，NIST 公布了 AES 的三个模式建议标准，但是相关工作尚未结束，NIST 将会陆续推出其它特殊用途的模式，目前成熟的有 GCM 和 AESKW. GCM 被计划用于强认证的环境，AESKW 被计划用于特殊数据（如密钥）的认证加密.

除了上述 NIST 的建议标准外，其它的标准化组织和相关行业也推出了一些模式标准，如 ISO/IEC 19772 中的 OCB[9]，3GPP[10] 中的 f8 和 3GPP-MAC 等等. 近几年，国外对分组密码工作模式的研究非常热，研究成果很多. 工作模式已不局限于传统意义上的保密工作模式、认证模式（MAC），另外还包含认证保密模式、可变长度的分组密码以及如何用分组密码实现杂凑技术等等. 形成这种现状的原因有三：一是应用需求，比如网络上要求高速的保密方案，过去的方案满足不了要求；二是技术的成熟，理论密码学可以对设计提供安全的证明技术；三是 NIST 对 AES 工作模式的征集激发了研究人员设计新方案的兴趣，推动了整个方向的发展. 与国外相比，国内对工作模式关注的程度不够，无论从研究方面还是标准的制定方面，都需要继续努力. 因此，为了让更多的国内学者了解相关工作的研究现状，本文简要介绍分组密码工作模式的设计思想及典型工作模式.

2 分组密码工作模式的设计理念

2.1 评价指标

为了阐述分组密码工作模式的设计理念，我们首先介绍如何评价一个分组密码工作模式. 工作模式的评价指标有三个方面：安全性、性能、模式/执行特点.

安全性评价指标包括：抵抗现有攻击的能力；可证明安全性，在合理的假设下，是否有安全性的证明结果；和类似模式安全性的比较，和现在用的模式（如 CBC）的比较；随机性，输出的统计特性；是否拥有合理的数学背景等.

性能评价指标包括计算的有效性、空间需求、可并行性和预处理能力等.

模式/执行特点评价指标包括可提供的密码服务、灵活性、错误特性、模式本身抗错性和简单性等.

安全性是所有评价指标中最重要的，因为其它性能的评估相对容易、相对直观. 安全性评价中的第一条类似于分组密码中目前流行的做法，评价的是工作模式的应用安全性，有时和具体分组密码有关，分析模式在实际应用中对强力攻击、中间相遇攻击、潜信道攻击等的抵抗力. 安全性中的第二条评价的是模式的理论安全性，与具体分组密码无关；通常假定分组密码是“理想”的，研究工作模式自身的安全性. 模式的理论安全性是设计者应当考虑的首要问题，也就是在假定好的基本模块存在的条件下，如何设计各种性能的工作模式，比如用于保密的工作模式、用于认证的 MAC、Hash 等. 理论安全性是目前对设计工作模式最基本的要求，它保证在工作模式这一层没有安全隐患，没有降低分组密码的安全性.

2.2 理论基础

模式的理论安全性的研究源于 Goldwasser 和 Micali 在 1984 年提出的可证明安全的概念[11]，最早用于非对称加密的研究，随后被扩展到其它领域，比如伪随机性[12,13] 和数字签名[14]. Bellare[15~21] 等人将其引入对称密码体制的研究. 安全模型是理论密码学的基础，它的建立、规范是理论密码学的核心，它使得理论密码学的研究工作具有系统性和科学性，而安全模型应能反映实际中遇到的安全问题. 分组密码的安全性使用伪随机置换模型化，即如果一个分组密码作为置换与真正的随机置换是不可区分的，我们就称之为伪随机置换. 相应地如果一个函数类的随机实例的输入/输出的行为和随机函数的输入/输出的行为是计算不可区分的，则称此函数类是伪随机函数. 伪随机函数和伪随机置换是对称密码方案设计中的主要工具，它们可以模型化分组密码，使得分析基于分组密码的密码方案的安全性成为可能. 分组密码工作模式就是用分组密码解决实际问题的对称密码方案，对称密码方案要解决的安

全问题主要是保密性和认证性，因此下面我们简要介绍反映对称密码方案的保密性和认证性的安全模型.

2.2.1　保密性——选择明文攻击下的不可区分性

通俗地讲，保密性就是从密文得不到明文的信息，或者从密文恢复明文很困难（这种说法不科学、不严密）. 为了提炼出保密性的正式定义，我们想象一个攻击者（没有密钥）选取了两个长度相同的明文，送给加密方案，加密方案随机地选取其中之一加密，然后将密文返给攻击者，如果攻击者很难辨别哪个明文被加密了，则说加密方案是安全的. 事实上可以给攻击者更大的权利，攻击者选取一组明文对 $(M_{1,0},M_{1,1}),(M_{2,0},M_{2,1}),\cdots,(M_{q,0},M_{q,1})$，其中每个明文对的两个明文是等长的，加密方案或其他人随机选取一个"challenge"比特 b，加密方案加密 $(M_{1,b},M_{2,b},\cdots,M_{q,b})$，返回给攻击者一组密文 $(C_1,C_2,\cdots,C_q)$. 攻击者需推测比特 b，也就是攻击者需决定加密的是 $(M_{1,0},M_{2,0},\cdots,M_{q,0})$ 还是 $(M_{1,1},M_{2,1},\cdots,M_{q,1})$. 需要注意的是：加密方案每次加密完后需更新状态或加入随机信息，这样保证同一个信息在不同次加密的结果是不同的. 这里的选择明文可以是非适应的、也可以是适应的.

下面形式化上面的说法：

对加密方案 $\varsigma\varepsilon=(K,E,D)$，其中 K 是密钥生成算法，E 是加密算法，D 是解密算法；定义左右加密问答机 $E_K(LR(\cdot,\cdot,b))$：

问答机 $E_K(LR(\cdot,\cdot,b))$

　　$//b\in\{0,1\}$ 且 $M_0,M_1\in\{0,1\}^*$

　$C\leftarrow E_K(M_b)$

　返回 C

问答机加密两个消息中的一个，至于选取哪一个消息依据比特 b. 对一个加密方案，在区别 $b=0$ 和 $b=1$ 两种情况时，如果"合理"的攻击者没有"显著"的优势，则称加密方案对选择明文攻击是安全的；正式称为在选择明文攻击下是不可区分的，简写为 ind-cpa.

定义 1.　令 $\varsigma\varepsilon=(K,E,D)$ 是一个对称加密方案，$b\in\{0,1\}$，A 可以访问问答机，且问答机的输入是一对等长的比特串，输出是一个比特串；我们考虑下面的实验：

Experiment $Exp_{\varsigma\varepsilon,A}^{\text{ind-cpa-}b}$

$\kappa\xleftarrow{R}K$

$d\leftarrow A^{E_\kappa(LR(\cdot,\cdot,b))}$

Return d

A 的 ind-cpa-优势定义为

$$Adv_{\varsigma\varepsilon,A}^{\text{ind-cpa}}=P[Exp_{\varsigma\varepsilon,A}^{\text{ind-cpa-1}}=1]-P[Exp_{\varsigma\varepsilon,A}^{\text{ind-cpa-0}}=1].$$

对任意 t,q 和 μ，定义 $\varsigma\varepsilon=(K,E,D)$ 的 ind-cpa-优势：

$$Adv_{\varsigma\varepsilon}^{\text{ind-cpa}}(t,q,\mu)=\max_A\{Adv_{\varsigma\varepsilon,A}^{\text{ind-cpa}}\}.$$

最大值是针对所有时间复杂度为 t、对 Oracle 的询问不超过 q 次、询问的总比特数不超过 μ 比特的 A 而言.

上述对攻击者 A 定义了区分优势，不同攻击者会有不同的优势，有两个原因可能导致一个攻击者比另一个的优势大：一个是他"聪明"，在询问问题和处理回答的过程中更有技巧；另一个原因就是他的权限大，资源丰富；他询问的次数更多或处理回答信息的时间多. 我们想知道的是，对给定的有限资源，最聪明的攻击者的优势. 注意这里的资源参数是可变的，我们将"安全性"的衡量指标看成了以资源参数为变量的优势函数. 这一点和现实是相符的，在现实世界中安全是相对的，不是绝对的，原则上所有现代密码系统都是可破的，问题取决于需要花费的代价. 因此直观上，密码方案是"安全的"是指在合理的资源参数下，它的优势函数的值是"低"的；用复杂性理论定义为对任意具有多项式资源的攻击者，其优势是可忽略的.

2.2.2　认证性——选择明文攻击下的不可伪造性

认证模式的任务是能够检测出攻击者对传输数据的任何修改. 认证模式 $MA=(K,T,V)$ 通常由三个算法组成：密钥生成算法 K、MAC 生成算法 T 和验证算法 V. 直观上，对认证模式的要求是，即使已知许多消息及相应的 MAC 值，伪造一个新消息的 MAC 值也是"困难的". 为了给出正式的定义，我们首先了解一下攻击的分类及"破译"的含义.

依据攻击所用的信息，对认证模式的攻击可以分为

(1) 已知消息攻击. 攻击者能知道一些消息及相应的 MAC 值.

(2) 选择消息攻击. 攻击者能选取一些消息，并得到相应的 MAC 值.

(3) 适应性选择消息攻击. 攻击者先选取一消息，并得到相应的 MAC 值；下一个消息的选取依赖以前的消息和 MAC 值.

"破译"意味着：

(1) 存在性伪造. 攻击者对一个消息伪造了 MAC 值，并知道以几乎为 1 的概率通过验证；这个消息有可能是无意义的，但是在存在性伪造下，也说

此认证模式是不安全的.

(2)选择性伪造. 攻击者可以选取某个消息,伪造 MAC 值,并知道以几乎为 1 的概率通过验证.

(3)密钥恢复. 意味着攻击者能确定密钥,如此破译是最彻底的,攻击者可以对任意消息计算 MAC 值.

由此看出适应性选择消息攻击是最强的,它赋予攻击者最大的权限,而存在性伪造是破译中最弱的,可能构成的危害最小. 我们下面讨论认证模式的安全性就是要求最强的,也就是在适应性选择消息攻击下,没有存在性伪造,或者存在性伪造出现的概率充分小.

定义 2. 令 $MA=(K,T,V)$ 是认证模式,A 是具有一个问答机的攻击者,考虑下面的实验:

Experiment $Exp_{MA,A}^{\text{uf-cma}}$

Let $\kappa \xleftarrow{R} K$

Let $(M,\sigma) \leftarrow A^{T_\kappa(\cdot)}$

If $V_\kappa(M,\sigma)=1$ and M was not a query of A to its oracle

Then return 1 else return 0

令 $Adv_{MA,A}^{\text{uf-cma}}=\Pr[Exp_{MA,A}^{\text{uf-cma}}=1]$,

对任意 t,q 和 μ,

$$Adv_{MA}^{\text{uf-cma}}(t,q,\mu)=\max_{A}\{Adv_{MA,A}^{\text{uf-cma}}\}.$$

最大值是针对所有时间复杂度为 t、对 oracle 的询问不超过 q 次、询问的总比特数加上输出消息 M 的比特数不超过 μ 比特的 A 而言的.

对于攻击者 A,用伪造优势反映他的伪造能力,如果对最聪明的攻击者,在一定的资源下,伪造优势是充分小的,我们就称认证模式是安全的.

2.2.3 Hash 模式的安全性

因为 Hash 函数的安全性有抗碰撞性、抗二次碰撞性和单向性之分,因此,对于基于分组密码的 Hash 模式,文献[22]在黑盒子模型下,利用攻击者的优势定义了 Hash 模式的抗碰撞性、抗二次碰撞性和单向性.

3 典型分组密码工作模式

3.1 记号

$E_K(X)$:在密钥 K 作用下加密算法对明文块 X 的加密.

$E_K^{-1}(Y)$:在密钥 K 作用下解密算法对密文块 Y 的解密.

$0x$:表示十六进制.

$[x]_s$:表示将非负整数 x 写成长度为 s 的二元序列,其中 $x<2^s$.

$|X|$:表示比特串 X 的比特长度.

$\lceil x \rceil$:表示不小于实数 x 的最小整数.

$X \| Y$:表示两个比特串 X 和 Y 的连接.

$LSB_\tau(X)$:表示比特串 X 的最右边 τ 比特.

$MSB_\tau(X)$:表示比特串 X 的最左边 τ 比特.

在描述工作模式时,$P_1,\cdots,P_i,\cdots$ 表示明文,每个 P_i 是 n 比特块,n 是所用密码的分组长度;$C_1,\cdots,C_i,\cdots$ 表示相应的密文.

3.2 保密模式

3.2.1 ECB、CBC、OFB 和 CFB

ECB、CBC、OFB 和 CFB 是1980年 NBS 为 DES 推出的保密模式,随后,被包含在 ISO 的 64-比特的模式标准中. 为了尽可能地利用以前的标准,降低成本,NIST 也将这 4 个模式列为 AES 的模式标准. 因为大家对这 4 个模式都很熟悉,所以下面仅简要介绍它们的优缺点及研究进展.

(1)ECB 模式

加密变换为 $C_i=E_K(P_i)$,

解密变换为 $P_i=E_K^{-1}(C_i)$.

ECB 模式的优点是可并行运算,速度快,易于标准化. 缺点是分组加密不能隐蔽数据模式,即相同的明文组蕴含着相同的密文组;不能抵抗组的重放、嵌入、删除等攻击;加密长度只能是分组的倍数. 许多人建议 ECB 模式不应该包含在 AES 的标准中,因为此模式对长度多于一块的消息不可用.

(2)CBC 模式

加密变换为 $C_i=E_K(P_i \oplus C_{i-1})$.

解密变换为 $P_i=E_K^{-1}(C_i) \oplus C_{i-1}$,$C_0$ 是初始向量.

CBC 模式的优点是引入了随机的初始向量,如果 E 是伪随机的,则输出具有一定的随机性,避免了 ECB 的缺点;隐蔽了明文的数据模式,在一定程度上能防止数据篡改. 缺点是出现错误传播,而且加密的消息长度只能是分组长度的倍数,不是任意长度的消息.

CBC 是应用最广、影响也最大的一个模式,Bellare[23]等在 1997 年给出了 CBC 模式的安全性证明,证明假设初始向量是秘密的(仅由合法的收方和发方知道). 在 CBC 模式基础上 Jutla 提出了 IACBC 模式[24];Gligor 和 Donesa 提出了 XCBC 模式[25]. IACBC 模式在非适应性模型下是可证明安全的,但在适应性模型下似乎不安全,Joux 在文献[26]

中给出了攻击方法. 为了抵抗上述攻击，Fouque 在文献[27]中提出了 DCBC 模式. Bellare 等在文献[28]中提出了 HCBC 和 HPCBC 模式. HCBC 模式在适应性模型下对选择明文攻击是安全的，但对选择密文攻击是不安全的，HPCBC 模式与 HCBC 的不同之处在于分组密码的输入输出都得到伪装，作为在线的分组密码对选择密文攻击是安全的. 同样为了适应磁盘扇区加密的需要，Halevi 与 Rogaway 在 CBC 基础上设计了 CMC 模式[29].

(3)OFB 模式

加密变换为 $Z_i=E_K(Z_{i-1})$，$C_i=P_i\oplus Z_i$，$\boldsymbol{Z}_0$ 为初始向量.

解密变换为 $Z_i=E_K(Z_{i-1})$，$P_i=C_i\oplus Z_i$，$\boldsymbol{Z}_0$ 为初始向量.

OFB 模式的主要优点是错误传播小，密文中的 1 比特错误只导致明文中的 1 比特错误；可以预处理；消息长度是任意的；可在线处理(随时处理明文)等. 缺点是系统要求通信双方必须同步，否则难于解密.

(4)CFB 模式

加密变换为 $C_i=E_K(C_{i-1})\oplus P_i$，$\boldsymbol{C}_0$ 为初始向量.

解密变换为 $P_i=E_K(C_{i-1})\oplus C_i$，$\boldsymbol{C}_0$ 为初始向量.

CFB 模式的主要优点是具有自同步能力；可以处理任意长度的消息，同时具有 CBC 的优点. 基于 CFB 的相关工作有 OCFB[30]模式、openPGP CFB[31]模式等. OCFB 模式是由 Ammar Alkassar 针对 CFB 的效率问题提出的改进版，在保证自同步能力的前提下提高效率，并且是可证明安全的. openPGP CFB 是在 RFC2004 描述的模式，它主要用在签名和加密邮件，在商业加密产品中得到广泛应用. SCFB 模式[32]是 CFB 模式和 OFB 模式的混合体，作为密钥流生成器，具有自同步能力并且效率比 CFB 高，吸取了 CFB 和 OFB 的优点，充分利用了 OFB 的速度和 CFB 保持同步的能力.

3.2.2　CTR(Counter Mode Encryption)

CTR[33]由 Diffie 和 Hellman 于 1979 年提出，在征集 AES 保密模式的过程中，Rogaway 等人强烈推荐此模式.

给定计数序列 $T_1,\cdots,T_{t-1},T_t$，对明文 $P_1,\cdots,P_{t-1},P_t$(其中 $|P_1|=\cdots=|P_{t-1}|=n$，$|P_t|=u$)，CTR 的加密过程如下：

$$O_i=E_K(T_i),\ i=1,2,\cdots,t;$$
$$C_i=P_i\oplus O_i,\ i=1,2,\cdots,t-1;$$
$$C_t=P_t\oplus MSB_u(O_t).$$

CTR 的解过程：

$$O_i=E_K(T_i),\ i=1,2,\cdots,t;$$
$$P_i=C_i\oplus O_i,\ i=1,2,\cdots,t-1;$$
$$P_t=C_t\oplus MSB_u(O_t).$$

其中 $MSB_u(O_t)$ 表示 O_t 的高 u 比特.

由于 CTR 模式具有很多优点，2001 年 SP 800-38A 文件发布之后，在随后设计的许多模式中都有 CTR 模式的影子，比如双重 CTR 模式，是 NSA 为 IP 包开发的高速加密模式，它混合了 ECB 模式和 CTR 模式；另外还有 CCM[34]，EAX[35]，CWC[36]，GCM[37]等模式. 其中 CCM 是把 CTR 模式与 CBC-MAC[38]融为一体. EAX 是 CCM 的一个改进，比 CCM 更简单、更有效. CWC 模式是利用 CTR 模式加密，在认证中引进了泛 Hash 函数，优点是可并行运算. GCM 模式的保密部分也是以 CTR 为基础的，我们将在后面详细描述.

3.2.3　f8

f8 是 3GPP 的模式标准，它是 OFB 的改进版，3GPP 的文件中曾给出了 f8 的安全性证明，这些结果随后发表在 2001 年的亚密会上[39]；不过，2003 年 Iwata 等[40]指出文件中的安全性证明是不正确的，原因是 f8 的两个密钥之间的相关性，其中第二个密钥是由第一个密钥异或一个常数得到. 随后在假设所用分组密码是安全的 PRP-RKA 的条件下，他们给出了 f8 的安全性证明[41]. f8 使用的分组密码是 KASUMI，Biham 在文献[42]中指出 KASUMI 对相关密钥-矩阵攻击是不免疫的；这说明 3GPP 中的加密系统不具备可证明安全性. f8 具体如下：

$m\leftarrow\lceil|M|/64\rceil$
$Y[0]\leftarrow 0^{64}$
$A\leftarrow COUNT\parallel BEARER\parallel DIRECTION\parallel 0^{26}$
$A\leftarrow E_{K\oplus KM}(A)$
For $i=1$ to m do：
　$X[i]\leftarrow A\oplus[i-1]_{64}\oplus Y[i-1]$
　$Y[i]\leftarrow E_K(X[i])$
$C\leftarrow M\oplus MSB_{|M|}(Y[1]\parallel\cdots Y[m])$
Return C

其中 COUNT、BEARER 和 DIRECTION 是格式化常量.

除了上述的标准外，近几年推出的保密模式还有 2DEM(Two Dimensional Encryption Mode)、ABC(Accumulated Block Chaining)、KFB(Key Feedback Mode)和 PCFB(Propagating Cipher Feedback)等. 限于篇幅，这里不再一一介绍.

3.3 认证模式

认证模式(或基于分组密码构造消息认证码-MAC)的思想距今已有 28 年的历史,先后涌现了许多 MAC. 基于 DES 的 CBC-MAC 是最早出现的,先后被包含在许多标准文件中,比如 FIFS Pub. 81 (Us Federal Standard)、ANSI X9.19(US Banking Standard)、ISO 8730、ISO 9807 和 ISO/IEC 9797-1. Bellare 等证明了 CBC-MAC 对长度固定为 mn 的消息是安全的[43],但是在输入长度变化的情况下是不安全的. 为了克服 CBC-MAC 的安全性缺陷,人们先后对 CBC-MAC 进行了改进,推出了一批 CBC-MAC 的变体,这些改进主要集中在 3 个方面:

(1)padding(当信息长度不是 n 的倍数时,怎么办?).

(2)length-variability(因为 CBC-MAC 处理可变信息长度是不安全的,因此,如何改进它?).

(3)Key-search strengthening(如何使得抵抗穷搜索的能力更强?).

针对 CBC-MAC 的安全缺陷,Bellare 先后提出三种改进方法,其中第三种方法不需要提前知道消息的长度,更容易在线进行 MAC 计算. 基于第三种方法,Bellare 推出了 EMAC,随后被包含进了 ISO 标准中. 它的具体构造是

$$EMAC_{K_1,K_2}(M)=E_{K_2}(CBC_{E_{K_1}}(M)),$$

其中 K_1 和 K_2 是两个不同的密钥.

本质上 EMAC 是用一个密钥执行 CBC-MAC,最后再用另外一个密钥加密一次. EMAC 需要执行两次密钥编排. Petrank 和 Rackoff[44] 分析了它的安全性,结果显示 EMAC 在消息是分组长度整数倍时是安全的. 为了使 CBC-MAC 能够更有效地处理任意长度的消息,Black 和 Rogaway 使用三种方法改造了 EMAC,相应地推出了 ECBC、FCBC 和 XCBC[45],其中 XCBC 递交给 NIST 作为候选算法. XCBC 主要是从第二方面出发对 CBC-MAC 进行改进,它需要三个密钥,增加了存储空间;XCBC 的主要缺点是不可并行. 鉴于 XCBC 需要三个密钥的缺陷,Kurosawa 和 Iwata 提出了 TMAC[46](Two-key CBC MAC),改进之处是第三个密钥由第二个密钥诱导而来. Kurosawa 和 Iwata[47,48] 进一步对 TMAC 做了改进,提出了 OMAC(One-key CBC MAC),OMAC 只用一个密钥,其它两个子密钥均由种子密钥诱导而来,和 TMAC 相比,OMAC 降低了密钥个数,代价是多调用一次分组密码.

对 EMAC 的另一个推广是 RMAC[49](Randomized MAC):

$$RMAC_{K_1,K_2}(P)=(E_{K_2\oplus R}(CBC_{E_{K_1}}(P)),R).$$

R 是随机的 n 比特串,它将作为 MAC 的一部分. RMAC 有两个版本,主要的不同点在于明文的 padding 方式. 第一版本是不论明文长度是否是 n 的倍数,都要添加 10^*,也就是说当明文是 n 的倍数时,有一分组块 10^{n-1} 都是添加的. 第二版本是仅对明文长度不是 n 的倍数时,添加 10^*. RMAC 曾被 NIST 考虑作为一个标准,不过 RMAC 易受相关密钥攻击[50,51],Knudsen 在文献[52]提出了对 RMAC 的部分密钥恢复攻击.

除了上述针对 CBC-MAC 的改进算法外,值得一提的是 Bellare 等人在 Crypto'95 上推出的 XOR-MAC[53]. 该算法有一些很好的特性,比如可并行、增量式、支持乱序验证、安全性高于 CBC-MAC 等. 该算法的缺点是索引信息引起的消息扩展,导致加密次数的成倍增加. 鉴于此,Gligor 和 Donescu 对 XOR-MAC 进行了改进,设计了 XECB-MAC,并提交给 NIST 作为候选模式. 随后,Black 对 XOR-MAC 也进行了改进,在 Eurocrypt'2002 上推出了 PMAC[54],PMAC 继承了 XOR-MAC 的很多优点,并且改进了 XOR-MAC 的缺陷,但是该算法受专利保护,不能免费使用. 限于篇幅,下面重点介绍几个典型的算法.

3.3.1 CBC-MAC

商定分组密码 E、分组长度 n、密钥 K 及 MAC 的长度 τ,算法如下.

CBC-MAC 的生成算法.

输入:消息 P

输出:长度为 τ 的 MAC-T.

1. Padding 消息 P 使其变成分组长度 n 的整数倍,并将其分成 n 比特的块:$P_1,P_2,\cdots,P_m$.

2. Let $C_0=0$.

3. For $i=1$ to m, let $C_i=E_K(C_{i-1}\oplus P_i)$.

4. Return $T=MSB_\tau(C_m)$.

CBC-MAC 的验证算法.

输入:消息 P 和收到的 MAC T'

输出:$VALID$ 或 $INVALID$

1. 用 MAC 生成算法计算 $T=CBC\text{-}MAC(K,P)$.

2. If $T=T'$, return $VALID$; else, return $INVALID$.

CBC-MAC 的优点是构造简单,底层加密算法可以方便地进行替换. 缺点是与其它的 MAC 相比速度慢,在输入长度变化的情况下是不安全的,不能并行计算.

3.3.2　CMAC

CMAC 是 NIST 在 2005 年 5 月公布的文件 SP 800-38B 中建议的一个认证模式，CMAC 表示基于密码的消息认证码(Cipher-based Message Authentication Code)，相对于 HMAC，基于 Hash 消息认证码(Hash-based MAC). CMAC 本质上是 Iwata 和 Kurosawa 提交的 OMAC(One-Key CBC-MAC).

商定分组密码 E、分组长度 n、密钥 K 及 MAC 的长度 τ；

输入密钥 K，输出子密钥 K_1 和 K_2 的子密钥生成过程如下：

1. Let $L=E_K(0^n)$.
2. If $MSL_1(L)=0$, then $K1=L\ll 1$;
   else $K1=(L\ll 1)\oplus R_n$.
3. If $MSL_1(K1)=0$, then $K2=K1\ll 1$;
   else $K2=(K1\ll 1)\oplus R_n$.

其中 $R_{128}=0^{120}10000111$，$R_{64}=0^{59}11011$.

输入消息 P，输出长度为 τ 的 MAC 生成过程：

1. 利用子密钥生成过程和密钥 K 产生子密钥 K_1 和 K_2.
2. If $|P|=0$, let $m=1$; else let $m=\lceil |P|/n\rceil$.
3. Let $P=P_1 \| P_2 \| \cdots \| P_{m-1} \| P_m^*$，其中 $|P_1|=\cdots=|P_{m-1}|=n$.
4. If $|P_m^*|=n$, let $P_m=K1\oplus P_m^*$; else, let $P_m=K2\oplus(P_m^* \| 10^j)$, 其中 $j=mn-|P|-1$.
5. Let $C_0=0^n$.
6. For $i=1$ to m, let $C_i=E_K(C_{i-1}\oplus P_i)$.
7. Let $T=MSB_\tau(C_m)$.
8. Return T.

前 4 步可以说是消息的格式化或 padding 阶段，和原来不同的是使用了密钥信息，这样做的原因是保证其可证明安全性.

CMAC 的验证算法.

输入：消息 P 和收到的 $MAC\text{-}T'$

输出：$VALID$ 或 $INVALID$

1. 用 MAC 生成算法计算 $T=CMAC(K,P)$.
2. If $T=T'$, return $VALID$; else, return $INVALID$.

3.3.3　3GPP-MAC

3GPP-MAC(又称 f9)是 EMAC 的一个变体. 它同 EMAC 有两点不同：一是 3GPP-MAC 使用一对密钥 K，K'，其中 K' 是由 $K\oplus const$ 得到的，而不是通过加密明文 0 和 1 得到的；二是最后一块的计算. 这两点导致两个 MAC 在安全性证明时的差异. 3GPP-MAC 的安全性证明最早由文献[55]给出，2003 年 Iwata 和 Kurosawa[40] 指出了证明中的错误，并在文献[41]给出新的证明. 目前对 3GPP-MAC 最有效的攻击是 Knudsen 等人在文献[56]中给出的结果.

3.3.4　PMAC(Parallelizable Message Authentication Code)

PMAC 是 Black 和 Rogaway 提出的一个消息认证码，和 CBC-MAC 相比，PMAC 的优点在于可并行性和可处理任意长度的消息. 对明文 P_1，P_2，…，P_{m-1}，P_m，算法如下：

$L=E_K(0^n)$

For $i=1,2,\cdots,m-1$ do

　$Y_i=E_K(P_i\oplus\gamma_i\cdot L)$

$\Sigma=Y_1\oplus Y_2\oplus\cdots\oplus Y_{m-1}\oplus P_m 10^{n-|P_m|-1}$

If $|P_m|=n$ then $X_m=\Sigma\oplus L\cdot X^{-1}$

　　else $X_m=\Sigma$

$Tag=E_K(X_m)$[first τ bits]

Return Tag

PMAC 可以看成是 XOR-MAC 的改进，它也采用了异或的方法来得到 MAC，正是因为这种方法保证 PMAC 支持消息的添加、截短和替换以及可并行性. 和 XOR-MAC 的不同点在于：一是所加密的内容. XOR-MAC 所加密的内容是消息连接上一个索引信息；而 PMAC 使用的是消息和不同的串进行异或之后的值. 二是对最后一块消息的处理. XOR-MAC 并不对最后一块消息进行特殊处理，而 PMAC 并不直接加密最后一块，而是先填充，然后和前面块的加密结果进行异或之后再分情况处理，最后再加密一次. 这就保证了它的安全性.

3.4　认证保密模式

上面介绍了保密模式和认证模式，事实上，大多数的应用是既需要保密也需要认证服务的，过去的做法是简单地结合保密模式和 MAC 技术达到实际需求，比如 SSL/TLS 的密码组件就结合了 CBC(基于 3-DES)和 HMAC(基于 SHA-1). 关于这些结合方式，文献[16,57]给出了详细讨论，有些是安全的(先加密后认证)，有些虽然加密模块和认证模块是安全的，但蹩脚的结合使得整个方案很容易被攻破. 近几年，同时提供加密认证的分组密码工作模式成为一个很活跃的研究方向，原因除了应用需求外，技术的成熟也是一个很重要的原因，涌现了一些具有可证明安全的认证加密方案. 最早出现的是 2000 年 Jutla 设计的 IAPM[58]，此模式利用一个伪装生成器伪装明文，避免了 ECB 模式的缺陷. 随后 Rogway 等人又对 IAPM 做了进一步的改进，得到 OCB 模式. 2001 年，IEEE 802.11 旨选 OCB 为无线局域网的标准，但是一些活跃人士对 OCB 有负面的声音，主要是源于 OCB 的知识产权. 为了避免 OCB 的专

利问题，802.11 的三个参与者 Ferguson，Housley 和 Whiting 决定设计新的算法——CCM. CCM 调用分组密码的次数是 OCB 的两倍，但是设计者称：在许多环境下这不是一个问题，并将在 IEEE 802.11 标准中采用 CCM，并提交给 IETF 和 NIST. 尽管存在对 CCM 的诸多批评[59,60]，在 2004 年 5 月公布的文件 SP 800-38C 中，NIST 仍然将 CCM 列为 AES 的认证保密模式的建议标准，同时 CCM 也被 IEEE 指定为用于无线局域网的标准（IEEE 802.11），并被包含在 RFC 3610 中. 在最近的讨论中，NIST 计划增加两个特殊用途的认证保密模式：GCM 和 AESKW[61]. GCM 计划用于强认证的环境，AESKW 计划用于特殊数据（如密钥）的认证保密，其中为了密钥分配和存储的需要，算法设计不能用“nonce”. 与 GCM 竞争的是 CWC，两者的设计思路很类似，但是 GCM 在某些方面有明显的优点. 除了上述 NIST 的建议标准，另外一个就是 ISO/IEC 19772 中的 OCB，它由 Rogaway 等在 2001 年推出[62]. 下面我们介绍这几个标准.

3.4.1 CCM

商定分组密码 E、密钥 K、$Counter$ 生成函数 g、格式函数 f 及 MAC 的长度 τ；输入 $nonce$ N、消息 P 和相关数据 A，输出密文 C 的加密过程如下：

$f(N,A,P)=B_0 \| B_1 \| \cdots \| B_r, |B_i|=n, 0\le i\le r.$

$Y_0=E_K(B_0).$

For $i=1$ to r, do $Y_i=E_K(B_i\oplus Y_{i-1})$.

令 $T=MSB_\tau(Y_r)$.

利用 $Counter$ 生成函数 g 生成计数块 $Ctr_0, Ctr_1, \cdots, Ctr_m$，其中 $m=\lceil |P|/n \rceil$.

For $j=0$ to m, do $S_j=E_K(Ctr_j)$.

令 $S=S_1 \| S_2 \| \cdots \| S_m$.

返回 $C=(P\oplus MSB_{|P|}(S)) \| (T\oplus MSB_\tau(S_0))$.

输入 nonce N、相关数据 A 和密文 C，输出消息 P 或 $INVALID$ 的解密验证过程如下：

如果 $|C|\le\tau$，则输出 $INVALID$.

利用 $Counter$ 生成函数 g 生成计数块 $Ctr_0, Ctr_1, \cdots, Ctr_m$，其中 $m=\lceil (|C|-\tau)/n \rceil$.

For $j=0$ to m, do $S_j=E_K(Ctr_j)$.

令 $S=S_1 \| S_2 \| \cdots \| S_m$.

令 $P=MSB_{|C|-\tau}(C)\oplus MSB_{|C|-\tau}(S)$.

令 $T=LSB_\tau(C)\oplus MSB_\tau(S_0)$.

如果 N, A 或者 P 是无效的，则返回 $INVALID$；否则，令 $f(N,A,P)=B_0 \| B_1 \| \cdots \| B_r$.

$Y_0=E_K(B_0)$.

For $i=1$ to r, do $Y_i=E_K(B_i\oplus Y_{i-1})$.

如果 $T\ne MSB_\tau(Y_r)$，则返回 $INVALID$；否则，返回 P.

3.4.2 GCM

GCM 的设计动机是硬件实现非常高效、软件性能好、可证明安全、没有专利的一个认证保密模式，主要需求是网络上的某些对速度要求很高的应用环境. GCM 的设计思路和 CWC 非常类似，基于 CTR 模式和泛 Hash 设计的 MAC. 和 CWC 不同的是，GCM 的泛 Hash 是二元域上的运算，而 CWC 是 127 比特整数域上的运算. 二元域上乘法的硬件实现代价小、速度快；而且软件实现更容易. 在硬件实现中：相对于 AES 的实现代价，GCM 增加的其它费用是可以忽略的；OCB 也具有相同的优点，但是它需要实现 AES 的加密和解密，而 GCM 只用到 AES 的加密算法. CWC 也可以高速实现，但是它的费用高. 比如 AES 的 CTR 加密机需要 90K 门，在相同的环境下，GCM 只需再增加 30K 门；而 CWC 需再增加 100K 门. 软件速度：GCM 比 CWC、CCM 和 EAX 快；对于长度小于 64B 的消息，GCM 比 OCB 快一点；但是对长消息，OCB 比 GCM 快，对相同长度的消息，GCM 所需时间不高于 OCB 的 4/3. GCM 的基本模块的安全性得到了深入的研究，文献[15]证明了保密模块 CTR 的安全性，文献[63]研究了认证模块的安全性. GCM 的安全性证明依赖这些结果，但是有所区别，原因是用于认证的密钥是由主密钥生成的. 在假设 AES 是伪随机置换时，文献[64]证明了在适应性选择明文攻击下，GCM 的保密性和不可伪造性.

GCM 的加密过程：基本上是先用 CTR 加密，然后用泛 Hash 认证.

$H=E_K(0^{128})$,

$$Y_0=\begin{cases} IV \| 0^{31}1, & |IV|=96 \\ GHASH(H,\{\},IV), & \text{其它} \end{cases}$$

$Y_i=incr(Y_{i-1})$, for $i=1,2,\cdots,n$.

$C_i=P_i\oplus E_K(Y_i)$, for $i=1,2,\cdots,n-1$.

$C_n^*=P_n^*\oplus MSB_u(E_K(Y_n))$.

$T=MSB_\tau(GHASH(H,A,C)\oplus E_K(Y_0))$.

函数 $incr$：$\{0,1\}^{128}\rightarrow\{0,1\}^{128}$ 将每一 128 比特输入看成一个 96 比特串 I 和一个 32 比特串 J 的连接，即输入为 $I \| J$；将 J 看成一个非负整数，其中最右边的比特为最低位；则 $incr(I \| J)=I \| (J+1 \bmod 2^{32})$.

函数 $GHASH$ 定义为：$GHASH(H,A,C)=X_{m+n+1}$.

输入 $H=E_K(0^{128})$，$A=A_1 \| A_2 \| \cdots \| A_{m-1} \| A_m^*$，$C=C_1 \| C_2 \| \cdots \| C_{n-1} \| C_n^*$，$X_i$ $(i=0,1,\cdots,$

$m+n+1$)如下定义：

$$X_i=\begin{cases}0, & i=0\\ (X_{i-1}\oplus A_i)\cdot H, & i=1,2,\cdots,m-1\\ (X_{m-1}\oplus(A_m^*\parallel 0^{128-v}))\cdot H, & i=m\\ (X_{i-1}\oplus C_{i-m})\cdot H, & i=m+1,\cdots,m+n-1\\ (X_{n+m-1}\oplus(C_n^*\parallel 0^{128-u}))\cdot H, & i=m+n\\ (X_{m+n}\oplus([|A|]_{64}\parallel[|C|]_{64})\cdot H, & i=m+n+1\end{cases}$$

GCM 的解密过程：基本上是先用泛 Hash 认证，然后用 CTR 解密. 如果 $T'=T$，继续解密，输出明文；否则，输出 $INVLID$.

$H=E_K(0^{128})$,

$$Y_0=\begin{cases}IV\parallel 0^{31}1, & |IV|=96\\ GHASH(H,\{\},IV), & \text{其它}\end{cases}$$

$T'=MSB_\tau(GHASH(H,A,C)\oplus E_K(Y_0))$.

$Y_i=incr(Y_{i-1})$, for $i=1,2,\cdots,n$.

$P_i=C_i\oplus E_K(Y_i)$, for $i=1,2,\cdots,n-1$.

$P_n^*=C_n^*\oplus MSB_u(E_K(Y_n))$.

3.4.3　AESKW

一般地讲，有两种建立密钥的技术：一种是基于非对称密码技术，另一种是基于对称密码技术. 在现实中，经常是混合使用这两种技术，用公钥技术建立密钥加密密钥 KEK(Key Encryption Keys)，然后用 KEK 建立其它的对称密钥. AESKW(AES Key Wrap)正是 NIST 公布的利用 AES 解决这一问题的方案，它的设计要求是对明文(密钥及相关的认证信息和数据)提供安全保护，也就是在密钥管理系统中保证密钥的安全. AESKW 加密的是密钥数据，所以一般不会很长，比如对 AES，最长为 256 比特的密钥；但是为了适应更广泛的应用环境，AESKW 没有限制明文长度的上界，但是限制了下界，要求明文最少为 128 比特. AESKW 由两个算法组成，一个是密钥的包装算法(也就是加密算法)，另一个是密钥的开包算法(也就是解密算法). AESKW 计划用于特殊数据(比如密钥)的认证加密，其中为了密钥分配和存储的需要，算法设计不能用“nonce”. 处理每块数据，AESKW 大概调用 12 次分组密码，它也被包含在 RFC 3394 中.

密钥的包装算法.

输入：明文——m 块 64-bit 串$\{P_1,P_2,\cdots,P_m\}$,
　　密钥——K，即密钥加密密钥 KEK

输出：密文——$m+1$ 块 64-bit 串$\{C_0,C_1,C_2,\cdots,C_m\}$

1. 初始化

Set $A^0=IV$, 其中初始值 IV 的默认值是 $OX(a6a6a6a6a6a6a6a6)$.

For $i=1,2,\cdots,m$,

$R_i^0=P_i$.

2. 计算中间值

For $t=1,2,\cdots,s$, where $s=6m$,

$A^t=MSB_{64}(AES_K(A^{t-1}\parallel R_1^{t-1}))\oplus t$,

For $i=1,2,\cdots,m-1$,

$R_i^t=R_{i+1}^{t-1}$,

$R_m^t=LSB_{64}(AES_K(A^{t-1}\parallel R_1^{t-1}))$.

3. 输出结果

Set $C_0=A^t$.

For $i=1,2,\cdots,m$,

$C_i=R_i^t$.

密钥的开包算法.

输入：密文——$m+1$ 块 64-bit 串$\{C_0,C_1,C_2,\cdots,C_m\}$,
　　密钥——K，即加密密钥 KEK.

输出：$INVALID$ 或
　　明文——m 块 64-bit 串$\{P_1,P_2,\cdots,P_m\}$

1. 初始化

Set $A^s=C_0$, where $s=6m$

For $i=1,2,\cdots,m$,

$R_i^s=C_i$.

2. 计算中间值

For $t=s,\cdots,1$,

$A^{t-1}=MSB_{64}(AES_K^{-1}((A^t\oplus t)\parallel R_m^t))$,

$R_1^{t-1}=LSB_{64}(AES_K^{-1}((A^t\oplus t)\parallel R_m^t))$

For $i=2,3,\cdots,m$,

$R_i^{t-1}=R_{i-1}^t$.

3. 输出结果

If $A=OX(a6a6a6a6a6a6a6a6)$,

then

For $i=1,2,\cdots,n$,

$P_i=R_i^0$,

else return $INVALID$.

上述 AESKW 要求明文必须是 64 的倍数，这是源于 AESKW 是为 AES 的密钥设计的安全方案，AES 的密钥限制为 128，192 和 256 比特，符合 AESKW 对明文的要求.(虽然没有限制明文的长度，但是其它应用不是它的主要对象). 上述 AESKW 是 2002 年 NIST 公布的一个方案. 那么很自然想到：对于不是 64 倍数的密钥 AESKW 如何提供安全保护？美国标准委员会的密钥包装标准草案(ANS X9.02)中改进了 AESKW，使得它可以对任意长度的数据提供保护. 另外 ANS X9.02 中给出了针对 64 比特分组的分组密码(TDES)的密钥包装标准 TDKW、AKW1 和 AKW2，其中 TDKW 的结构和 AESKW 类似，只是块长度为 64 比特；AKW1 用了两层 CBC 模式；AKW2 用了 CBC 模式和 CBC-MAC. 2004 年 11 月至 2005 年 5 月是美国

标准委员会留给公众的评论期，但是反应不多.

3.4.4 OCB(Offset Codebook)

OCB 模式是 IAPM 的改进版，这类模式保留 ECB 模式的优点，利用一个伪装生成器，用其输出来伪装明文，避免 ECB 模式的缺陷，并且是可证明安全的. 和 IAPM 相比，OCB 的优点是明文长度不必添加为 n 的倍数，密文长度短；和 ECB 相比，有效性几乎最佳；对初始值的要求低，仅要求它不重复使用；只有一个密钥，降低了密钥编排的时间和存储的空间.

在给出具体方案之前，我们先规定几个符号：$ntz(i)$ 是 i 的二元表示中最低位 0 的个数，比如 $ntz(7)=0$，$ntz(2)=1$. 如果 $A=a_{n-1}\cdots a_1 a_0\in\{0,1\}^n$，则 $str2num(A)=\sum_{i=0}^{n-1}2^i a_i$. 如果 $a\in[0\quad 2^n-1]$，则 $num2str_n(a)$ 是满足 $str2num(A)=a$ 的 n 比特串 A. 对 $B\in\{0,1\}^*$，$len_n(B)=num2str_n(|B|)$. 对 $A_1\in\{0,1\}^l$，$A\in\{0,1\}^n$，$l<n$，则 $A_1\oplus A=A_1\oplus MSB_l(A)$.

$$L\cdot x=\begin{cases}L\ll 1, & MSB_1(L)=0\\ (L\ll 1)\oplus 0^{120}10000111, & MSB_1(L)=1\end{cases}$$

$$L\cdot x^{-1}=\begin{cases}L\gg 1, & LSB_1(L)=0\\ (L\gg 1)\oplus 10^{120}1000011, & LSB_1(L)=1\end{cases}$$

$L(j)=L\cdot x^j$，$j\geq -1$，$\gamma_i\cdot L=(\gamma_{i-1}\cdot L)\oplus L(ntz(i))$，其中 $\gamma_1\cdot L=L$.

输入初始值 N 和明文 $P_1,P_2,\cdots,P_{m-1},P_m$（其中 $|P_1|=\cdots=|P_{m-1}|=n$，$|P_m|=u$ 比特），选定校验值的长度 τ，输出 $\rho=C\parallel T$（密文 C 和校验值 T）的加密过程如下：

$L=E_K(0^n)$；$R=E_K(N\oplus L)$；
For $i=1,2,\cdots,m$ do
  $S_i=\gamma_i\cdot L\oplus R$
For $i=1,2,\cdots,m-1$ do
  $C_i=E_K(P_i\oplus S_i)\oplus S_i$
  $X_m=len(P_m)\oplus L\cdot x^{-1}\oplus S_m$
  $Y_m=E_K(X_m)$
  $C_m=Y_m\oplus P_m$
  $C=C_1C_2\cdots C_m$
  $Checksum=P_1\oplus P_2\oplus\cdots\oplus P_{m-1}\oplus C_m0^*\oplus Y_m$
  $T=E_K(Checksum\oplus S_m)[first\tau bits]$

输入初始值 N 和明文 $\rho=C\parallel T=C_1\cdots C_mT$，加密和验证过程如下：

$L=E_K(0^n)$；$R=E_K(N\oplus L)$；
For $i=1,2,\cdots,m$ do
  $S_i=\gamma_i\cdot L\oplus R$
For $i=1,2,\cdots,m-1$ do
  $P_i=D_K(C_i\oplus S_i)\oplus S_i$
  $X_m=len(C_m)\oplus L\cdot x^{-1}\oplus S_m$
  $Y_m=E_K(X_m)$
  $P_m=Y_m\oplus C_m$
  $P=P_1P_2\cdots P_m$
  $Checksum=P_1\oplus P_2\oplus\cdots\oplus P_{m-1}\oplus C_m0^*\oplus Y_m$
  $T'=E_K(Checksum\oplus S_m)[first\tau bits]$
If $T=T'$ then return M
  else return $INVALID$

除了上述提到的几个认证保密模式 OCB、CCM 和 GCM 外，另外还有 IACBC、IAPM、IGE[65]、EAX[66] 和 CWC.

3.5 大分组密码模式

基于小分组密码构造大分组密码的研究一直伴随分组密码的研究. 本质上，利用 Luby 和 Rackoff 关于 Feistel 结构的研究，就可以从 n 比特构造 $2n$ 比特分组的密码；类似的工作有 Naor 和 Reingold[67] 的从 n 比特构造 $2n$ 分组的密码；Iwata 等人基于 Misty 型[68~71] 结构的构造；Wu 基于 Camellia 和广义 Feistel 型结构的研究[72~74]；但这些工作所处理的都是分组的整数倍消息，未能实现真正意义上的可变输入长度. 在真正实现可变输入长度方面，Bellare 和 Rogaway[75] 利用节俭函数与模式给出了一个结构并证明了伪随机性；之后，Patel 等[76] 对此结构进行了改进，利用伪随机置换、Hash 函数和 CTR 模式构造了一个结构，并证明了其为超伪随机的. 另外近几年还推出了 XCB、ABL[77]、CMC、EME[78,79]、HCBC、HPCBC 和 HCTR[80] 等模式. 目前，这类模式的作用主要体现在存储加密，尤其是磁盘扇区加密上. 针对磁盘扇区加密的特点，2002 年，Liskov、Rivest 和 Wagner 提出了 Tweakable 分组密码[81] 的概念，它的输入除了消息和密钥外，还有一个“Tweak”. “Tweak”的作用类似于 CBC 模式中的初始向量和 OCB 模式中的 nonce，使得对不同的 Tweak，Tweakable 分组密码就代表两个不同的分组密码，优点主要体现在改变 Tweak 比改变密钥代价小. 因为改变密钥，就意味着要重新进行密钥编排. 当然，Tweakable 分组密码要想在实际中起作用，应该必须有两个支撑点：(1) Tweakable 分组密码的设计是容易的；(2) 将分组密码变成 Tweakable 所花的代价不大. 对 Tweakable 分组密码的研究已有一些成果[82,83]. 为了推动相关工作，也为了标准化用于存储加密的密码方案，2002 年 8 月，IEEE 启动了 P1619 项目[84]，预计到 2006 年 12 月结束. 目

前已形成了 Key Backup Format，Tweakable Narrow-block Encryption 和 Tweakable Wide-block Encryption 三个草案.

3.5.1 小分组的 Tweakable 加密方案——LRW-AES

磁盘通常被分成固定长度的扇区(一般是 512 字节)，如果要对一个扇区加密，假设此扇区所处的位置是 j，那么对应的待加密的 512 字节消息按如下方式分成 32 个 16 字节的块：$P_{j,k}$，$k=1,2,\cdots,32$. 每个 $P_{j,k}$ 对应的逻辑位置为 $i=k+32(j-1)$，令 $I=[i]_{128}$.

LRW-AES 可以看成将 AES 用于扇区加密的一种保密工作模式. LRW-AES 需要两个密钥，一个是 128(192 或 256)比特的加密密钥 K_1，另一个是 128 比特的 Tweak 密钥 K_2，对每一块 128 比特的明文 P，LRW-AES 加密过程如下：

If $I>2^{128}-1$ or $I<0$, output *INVAID*.

$T \leftarrow K_2 \otimes I$.

$PP \leftarrow P \oplus T$.

$CC \leftarrow E_{K_1}(PP)$.

$C \leftarrow CC \oplus T$.

输出 C.

3.5.2 大分组的 Tweakable 加密方案——EME-32-AES

EME-32-AES 是分组长度为 512 字节的 Tweakable 分组密码，它是 EME 模式的具体实例. 它需要一个 128(192 或 256)比特的加密密钥 K 和一个公开的 128 比特的 Tweak T(T 由扇区位置确定)，对 512 字节的消息 $P=P_1 \parallel P_2 \parallel \cdots \parallel P_{32}$，EME-32-AES 加密过程如下：

Let $L=2 \cdot E_K(0^{128})$.

For $j=1,2,\cdots,32$, do

　$PP_j \leftarrow P_j \oplus (2^{j-1} \cdot L)$

　$PPP_j \leftarrow E_K(PP_j)$

$SP \leftarrow PPP_1 \oplus PPP_2 \oplus \cdots \oplus PPP_{32}$

$MP \leftarrow PPP_1 \oplus SP \oplus T$

$MC \leftarrow E_K(MP)$

$M \leftarrow MP \oplus MC$

For $j=2,3,\cdots,32$, do

　$CCC_j \leftarrow PPP_j \oplus (2^{j-1} \cdot M)$

　$SC \leftarrow CCC_2 \oplus \cdots \oplus CCC_{32}$

　$CCC_1 \leftarrow MC \oplus SC \oplus T$

For $j=1,2,\cdots,32$, do

　$CC_j \leftarrow E_K(CCC_j)(2^{j-1} \cdot L)$

　$C_j \leftarrow CC_j \oplus 2^{j-1} \cdot L$

Return $C_1,\cdots,C_{32}$

3.6 Hash 模式

分组密码的 Hash 模式就是基于分组密码构造 Hash 函数的方案，主要是先利用分组密码构造压缩函数，然后将压缩函数迭代构成 Hash 函数. 这方面的工作最早可以追溯到 1984 年 Winternitz 的成果[85]；他证明了 Davies-Meyer 方案具有抵抗恢复原像攻击的安全性. 在 Winternitz 工作的基础上，Merkle[86]证明了三类基于分组密码的 Hash 函数具有抵抗恢复原像攻击的安全性. 利用分组密码设计 Hash 函数最早的方案是 Matyas-Meyer-Oseas(简称 MMO)[87]，MMO 被收在 ISO IEC10118-2 中，后来成为其它分组密码构造 Hash 函数的主要模块. 不过 MMO 方案的输出长度和分组长度一样，对于某些应用，这样的 Hash 函数的输出长度太短，特别是对于抗碰撞性来说，一种解决办法就是用双倍长度构造，其中最著名的方案是 MDC-2 和 MDC-4[88,89]；MDC-2 用了两个并行的 MMO 方案. NIST 没有为 AES 征集 Hash 模式，但是仍然收到了一个方案——AES-Hash，AES-Hash 仅适用于分组和密钥长度均为 256 比特的 AES，而此规模的 AES 还没有被标准化，因此，AES-Hash 不可能被采纳.

上述方案由于各种原因没有得到广泛应用. 用分组密码设计 Hash 函数的优点是明显的，它可以直接利用现存分组密码的软件和硬件实现，降低成本. 最重要的是，分组密码经过了大量的研究，我们对其安全性有了一定的了解，对 Hash 函数安全性可以建立在对分组密码的信任基础上. 特别在目前的情况下，MD5 和 SHA 等相继被发现有问题，相应的设计方法受到怀疑，因此迫切需要更安全的设计方法，这样基于分组密码设计 Hash 函数很自然再次受到关注.

Preneel[90]等人综合讨论了 64 种最基本的基于分组密码构造的 Hash 函数及其安全性，指出其中的 12 种方案是安全的. Black 和 Rogaway[22]等人证明了在黑盒子模型下，这 12 种方案以及另外 8 种方案都具有抵抗碰撞攻击的安全性；然而，在抵抗恢复原像攻击方面，这 12 种方案比起另外 8 种方案具有更好的安全性. 20 种被证明是安全的方案的速率是 1，这一点比较好，但是我们注意到每次调用分组密码都涉及到一个新的密钥，每一次迭代都要重新进行一次密钥编排，大大降低了算法的效率，特别对那些密钥编排算法慢的分组密码来说. 因此，基于分组密码的 Hash 函数的有效性不仅仅要求速率为 1 而

且应该使用一个密钥. 如果我们将速率为 1 而且仅使用一个密钥的基于分组密码的 Hash 函数称为有效的,那么如何设计?正面的研究没有进展,但是,Black[91]在 2004 年从反面给了一个结果:说明基于分组密码的 DM 型 Hash 函数不存在有效的可证安全的方案. 上述讨论的 Hash 函数,其输出长度与所采用的分组密码的分组长度相等. 对于输出长度大于分组长度的情形,也有一些研究结果[92~98];但总的来讲,这方面的工作还不成熟,值得进一步探讨.

4 结束语

分组密码工作模式是利用分组密码解决实际问题的关键一步,好的工作模式可以弥补分组密码的某些缺憾,比如,在千兆网环境中,如果不希望数据加密成为瓶颈,则需要高速度的分组密码算法,但是目前还没有软件速度达到此要求的分组密码;而利用可并行的工作模式可以解决此问题. 相反,不好的工作模式即使所用的分组密码是好的,方案也可能不安全. 比如 ECB-AES 部分泄露明文的信息;再比如因为 CBC 的 Padding 方式,导致 CBC-AES 遭受潜信道攻击[99~103];但这些安全缺陷不是 AES 的错,而是它被误用造成的. 因此,分组密码工作模式和分组密码算法同样重要;在实际应用中,任何一方的失误都会导致安全隐患. 国外对此领域的研究很重视,不断有新的成果涌现[104~108]. 和国外相比,我国学术界和产业界关注更多的是分组密码算法自身的研发,对如何利用分组密码解决实际问题的工作模式研究得并不多,通常采用国外现成的工作模式解决应用需求. 这种拿来用的现象在某些通用的应用环境是可以,但是对某些具体环境就不可能最大化地发挥我们的优势,比如在某些环境,密钥管理问题大,那么密钥的比特数应该成为一个重要的衡量指标;再比如在某些环境,头文件中有计数器,那么设计模式时就可以不考虑计数方面的开销. 希望本文能起到抛砖引玉的作用,吸引国内更多的学者参与其中,推动我们国家在这个领域的研究和标准化进程.

参 考 文 献

1 National Institute of Standards and Technology(NIST). Federal Information Processing Standards Publication 81(FIPS PUB 81): DES Modes of Operation, December 1980

2 American National Standards Institute. ANSI X3.106-1983, American National Standard for Information Systems-Data Encryption Algorithm-Modes of Operation, 1983

3 International Organization for Standardization. ISO 8372: 1987, Information Processing—Modes of Operation for a 64-bit Block Cipher Algorithm, 1987

4 International Organization for Standardization. ISO/IEC 10116: 1997, Information Technology—Security Techniques—Modes of Operation for an n-bit Block Cipher, 2nd edition, 1997

5 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

6 National Institute of Standards and Technology(NIST). NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, December 2001

7 National Institute of Standards and Technology(NIST). NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005

8 National Institute of Standards and Technology(NIST). NIST Special Publication 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004

9 International Organization for Standardization. ISO/IEC WD 19772: 2004, Information Technology—Security Techniques—Authenticated Encryption Mechanisms, 2004

10 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

11 Goldwasser S., Micali S.. Probabilistic encryption. Journal of Computer and System Science, 1984, 28(2): 270~299

12 Blum M., Micali S.. How to generate cryptographically strong sequences of pseudorandom bits. SIAM Journal on Computing, 1984, 13(4): 850~864

13 Goldreich O., Goldwasser S., Micali S.. How to construct random functions. Journal of the ACM, 1986, 33(4): 792~807

14 Goldwasser S., Micali S., Rivest R.. A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal of Computing, 1998, 17(2): 281~308

15 Bellare M., Desai A., Jokipii E., Rogaway P.. A concrete security treatment of symmetric encryption. In: Proceedings of the 38th IEEE Symposium on Foundations of Computer Science, IEEE Computer Society, Washington, DC, USA, 1997, 394~403

16 Bellare M., Namprempre C.. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In: Okamoto T. ed.. Advances in Cryptology—Asiacrypt 2000. Lecture Notes in Computer Science 1976. Berlin: Springer-Verlag, 2000, 531~545

17 Bellare M., Rogaway R.. Introduction to Modern Cryptology, 2004, Available at http://www-cse.ucsd.edu/users/mihir/

18 Goldreich O.. Foundations of Cryptography: Basic Tools. Cambridge University Press, 2001

19 Goldreich O.. Foundations of Cryptography: Basic Applications. Cambridge University Press, 2004

20 Bellare M.. Practice-oriented provable-security. In: Okamoto E., Davida G., Mambo M. eds.. In: Proceedings of the 1st International Workshop on Information Security—ISW97. Lecture Notes in Computer Science 1396. Berlin: Springer-Verlag, 1997, 131～145

21 Luby M., Rackoff C.. How to construct pseudorandom permutations from pseudorandom functions. SIAM Journal on Computing, 1988, 17(2): 373～386

22 Black J., Rogway P., Shrimpton T.. Black-box analysis of the block-cipher-based hash-function constructions from PGV. In: Yung M. ed.. Advances in Cryptology—Crypto'02. Lecture Notes in Computer Science 2442. Berlin: Springer-Verlag, 2002, 320～355

23 Bellare M., Kilian J., Rogaway P.. The security of the cipher block chaining. In: Desmedt Y. G. ed.. Advances in Cryptology—Crypto'94. Lecture Notes in Computer Science 839. Berlin: Springer-Verlag, 1994, 341～358

24 Jutla C.. Encryption modes with almost free message integrity. In: Pfitzmann B. ed.. Advances in Cryptology—Eurocrypt'01. Lecture Notes in Computer Science 2045. Berlin: Springer-Verlag, 2001, 529～544

25 Gligor V., Donescu P.. Fast encryption and authentication: XCBC encryption and XECB authentication modes. In: Matsui M. ed.. Fast Software Encryption—FSE 2001. Lecture Notes in Computer Science 2355. Berlin: Springer-Verlag, 2002, 92～108

26 Jous A., Martinet G., Valette F.. Blockwise adaptive attacks-revisting the security of some provably secure encryption modes: CBC, GEM, IACBC. In: Yung M. ed.. Advances in Cryptology—Crypto'02. Lecture Notes in Computer Science 2442. Berlin: Springer-Verlag, 2002, 17～30

27 Fouque Pierre-Alain. Practical symmetric on-line encryption. In: Johansson Th. ed.. Fast Software Encryption—FSE 2003. Lecture Notes in Computer Science 2887. Berlin: Springer-Verlag, 2003, 362～375

28 Bellare M., Boldyreva A., Knudsen L., Namprempre C.. On-line ciphers and the Hash-CBC construction. In: Kilian J. ed.. Advances in Cryptology—Crypto'01. Lecture Notes in Computer Science 2139. Berlin: Springer-Verlag, 2001, 482～499

29 Halevi S., Rogaway P.. A tweakable enciphering mode. In: Boneh D. ed.. Advances in Cryptology—Crypto'03. Lecture Notes in Computer Science 2729. Berlin: Springer-Verlag, 2003, 482～499

30 Alkassar A.. Optimized self-synchronizing mode of operation. In: Matsui M. ed.. Fast Software Encryption—FSE 2001. Lecture Notes in Computer Science 2355. Berlin: Springer-Verlag, 2001, 78～91

31 McGrew D. A., Fluhrer S.. The extended codebook(XCB) mode of operation. http://eprint.iacr.org/2004/278.pdf

32 Jung O., Ruland C.. Encryption with statistical self-synchronization in synchronous broadband networks. In: Koç Ç. K., Paar C. eds.. Cryptographic Hardware and Embedded Systems—CHES'99. Lecture Notes in Computer Science 1717. Berlin: Springer-Verlag, 1999, 340～352

33 Diffie W., Hellman M. E.. Privacy and authentication: An introduction to cryptography. Proceedings of the IEEE, 1979, 67(3): 397～427

34 Whiting D., Ferguson N., Housley R.. Counter with CBC-MAC(CCM). Submission to NIST of Operation Process. Available at http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/

35 Bellare M., Rogaway P., Wagner D.. The EAX mode of operation. In: Meier W., Roy B. eds.. Fast Software Encryption—FSE 2004. Lecture Notes in Computer Science 3017. Berlin: Springer-Verlag, 2004, 389～407

36 Kohno T., Viega J., Whiting D.. The CWC-AES dual-use mode. Submission to NIST Modes of Operation Process, 2003, Available at http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/

37 McGrew D., Viega J.. The Galois/Counter mode of operation (GCM). Submission to NIST Modes of Operation Process, 2004, Available at http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/

38 Bellare M., Kilian J., Rogaway P.. The security of the cipher block chaining message authentication code. Journal of Computer and System Sciences, 2000, 61(3): 362～399

39 Kang J. S., Shin S. U., Hong D., Yi O.. Provable security of KASUMI and 3GPP encryption mode f8. In: Boyd C. ed.. Advances in Cryptology—Asiacrypt 2001. Lecture Notes in Computer Science 2248. Berlin: Springer-Verlag, 2001, 255～271

40 Iwata T., Kurosawa K.. On the correctness of security proofs for the 3GPP confidentiality and integrity algorithms. In: Paterson K. G. ed.. Cryptography and Coding. Lecture Notes in Computer Science 2898. Berlin: Springer-Verlag, 2003, 306～318

41 Iwata T., Kohno T.. New security proofs for the 3GPP confidentiality and integrity algorithms. In: Roy B., Meier W. eds.. Fast Software Encryption—FSE 2004. Lecture Notes in Computer Science 3017. Berlin: Springer-Verlag, 2004, 427～445

42 Biham E., Dunkelman O., Keller N.. A related-key rectangle attack on the full KASUMI. In: Proceedings of the Asiacrypto 2005, Taj Coromandal, Chennai, India, 2005, 38～53

43 Bellare M., Kilian J., Rogaway P.. The security of the cipher block chaining message authentication code. In: Desmedt Y. G. ed.. Advances in Cryptology—Crypto'94. Lecture Notes in Computer Science 839. Berlin: Springer-Verlag, 1994, 341～358

44 Petrank E., Rackoff C.. CBC MAC for real-time data sources. Journal of Cryptology, 2000, 13(2): 315～338

45 Black J., Rogaway P.. CBC-MACs for arbitrary length messages: The three-key constructions. In: Bellare M. ed.. Advances in Cryptology—Crypto 2000. Lecture Notes in Computer Science 1880. Berlin: Springer-Verlag, 2000, 197～215

46 Kurosawa K., Iwata T.. TMAC: Two-key CBC MAC. In: Joye M. ed.. Topics in Cryptology—CT-RSA 2003. Lecture

Notes in Computer Science 2612. Berlin: Springer-Verlag, 2003, 33～49

47 Iwata T., Kurosawa K.. OMAC: One-key CBC MAC. In: Johansson T. ed.. Fast Software Encryption—FSE 2003. Lecture Notes in Computer Science 2887. Berlin: Springer-Verlag, 2003, 129～153

48 Iwata T., Kurosawa K.. Stronger security bounds for OMAC, TMAC and XCBC. In: Johansson T., Maitra S. eds.. Progress in Cryptology—Indocrypt 2003. Lecture Notes in Computer Science 2904. Berlin: Springer-Verlag, 2003, 402～415

49 Jaulmes E., Joux A., Valette F.. On the security of randomized CBC-MAC beyond the birthday paradox limit: A new construction. In: Daemen J., Rijmen V. eds.. Fast Software Encryption—FSE 2002. Lecture Notes in Computer Science 2365. Berlin: Springer-Verlag, 2002, 237～251

50 Knudsen L. R., Kohno T.. Analysis of RMAC. In: Johansson T. ed.. Fast Software Encryption—FSE 2003. Lecture Notes in Computer Science 2887. Berlin: Springer-Verlag, 2003, 182～191

51 Joux A., Poupard G., Stern J.. New attacks against standardized MACs. In: Johansson T. ed.. Fast Software Encryption—FSE 2003. Lecture Notes in Computer Science 2887. Berlin: Springer-Verlag, 2003, 170～181

52 Knudsen L. R., Mitchell C. J.. Partial key recovery attack against RMAC. Journal of Cryptology, 2005, 18(3): 375～389

53 Bellare M., Gueriny R., Rogaway P.. XOR MACs: New methods for message authentication using finite pseudorandom functions. In: Coppersmith D. ed.. Advances in Cryptology—Crypto'95. Lecture Notes in Computer Science 963. Berlin: Springer-Verlag, 1995, 15～28

54 Black J., Rogaway P.. A block-cipher mode-of-operation for parallelizable message authentication. In: Knudsen L. R. ed.. Advances in Cryptology—Eurocrypt 2002. Lecture Notes in Computer Science 2332. Berlin: Springer-Verlag, 2002, 384～397

55 Hong D., Kang J. S., Preneel B., Ryu H.. A concrete security analysis for 3GPP-MAC. In: Johansson T. ed.. Fast Software Encryption—FSE 2003. Lecture Notes in Computer Science 2887. Berlin: Springer-Verlag, 2003, 154～169

56 Knudsen L. R., Mitchell C. J.. Analysis of 3gpp-MAC and two-key 3gpp-MAC. Discrete Applied Mathematics, 2003, 128(1): 181～191

57 Krawczyk H.. The order of encryption and authentication for protecting communications. In: Kilian J. ed.. Advances in Cryptology—Crypto 2001. Lecture Notes in Computer Science 2139. Berlin: Springer-Verlag, 2001, 310～331

58 Jutla C. S.. Parallelizable encryption mode with almost free message integrity. Submission to NIST Modes of Operation Process, 2000, Available from http://csrc.nist.gov/encryption/modes

59 Jonsson J.. On the security of CTR+CBC-MAC. In: Nyberg K., Heys H. M. eds.. Selected Areas in Cryptography—SAC 2002. Lecture Notes in Computer Science 2595. Berlin: Springer-Verlag, 2002, 76～93

60 Rogaway P., Wagner D.. A critique of CCM. Available from http://www.cs.ucdavis.edu/～rogaway/papers/2003

61 Schaad J., Housley R.. RFC 3394, Advanced Encryption Standard(AES) Key Wrap Algorithm. Internet Engineering Task Force, September, 2002

62 Rogaway P., Bellare M., Black J., Krovetz T.. OCB: A block-cipher mode of operation for efficient authenticated encryption. In: Proceedings of the 8th ACM Conference on Computer and Communications Security(CCS-8), 2001, 196～205

63 Wegman M., Carter L.. New hash functions and their use in authentication and set equality. Journal of Computer and System Sciences, 1981, 22: 265～279

64 McGrew D., Viega J.. The security and performance of the Galois/Counter Mode(GCM) of operation. In: Johansson Th., Maitra S. eds.. Progress in Cryptology—Indocrypt 2004. Lecture Notes in Computer Science 3348. Berlin: Springer-Verlag, 2004, 218～226

65 Gligor V., Donescu P.. Infinite Garble Extension. Submission to NIST Modes of Operation Process, 2000, Available from http://csrc.nist.gov/encryption/modes

66 Bellare M., Rogaway P., Wagner D.. The EAX mode of operation. In: Meier W., Roy B. eds.. Fast Software Encryption—FSE 2004. Lecture Notes in Computer Science 3017. Berlin: Springer-Verlag, 2004, 389～407

67 Naor M., Reingold O.. On the construction of pseudorandom permutations: Luby-Racko_Revisited. Journal of Cryptology, 1999, 12(1): 78～90

68 Iwata T., Yoshino T., Yuasa T., Kurosawa K.. Round security and super-pseudorandomness of MISTY type structure. In: Matsui M. ed.. Fast Software Encryption—FSE 2001. Lecture Notes in Computer Science 2355. Berlin: Springer-Verlag, 2001, 233～247

69 Minier M., Gilbert H.. New results on the pseudorandomness of some blockcipher constructions. In: Matsui M. ed.. Fast Software Encryption—FSE 2001. Lecture Notes in Computer Science 2355. Berlin: Springer-Verlag, 2001, 248～266

70 Iwata T., Yoshino T., Kurosawa K.. Non-cryptographic primitive for pseudorandom permutation. In: Daemen J., Rijmen V. eds.. Fast Software Encryption—FSE 2002. Lecture Notes in Computer Science 2365. Berlin: Springer-Verlag, 2002, 149～163

71 Ramzan Z., Reyzin L.. On the round security of symmetric-key cryptographic primitives. In: Bellare M. ed.. Advances in Cryptology—Crypto 2000. Lecture Notes in Computer Science 1880. Berlin: Springer-Verlag, 2000, 376～393

72 Wu Wen-Ling, Feng Deng-Guo, Cheng Hua. Collision attack and pseudorandomness of reduced-round Camellia. In: Handschuh H., Hasan A. eds.. Selected Areas in Cryptography—SAC 2004. Lecture Notes in Computer Science 3357. Berlin: Springer-Verlag, 2005, 256～270

73 Wu Wen-Ling. Pseudorandomness of Camellia-like scheme. Journal of Computer Science and Technology, 2006, 12(1): 1～10

74 Wu Wen-Ling, Zhang Wen-Tao, Lin Dong-Dai. On the security of generalized Feistel scheme with SP round function. International Journal Network Security, 2006, 2(3): 296～305

75 Bellare M., Rogaway P.. On the construction of variable-input-length ciphers. In: Knudsen L. R. ed.. Fast Software Encryption — FSE'99. Lecture Notes in Computer Science 1636. Berlin: Springer-Verlag, 1999, 231～244

76 Ramzan Z., Patel S., Sundardm G.. Efficient constructions of variable-input-length block ciphers. In: Helena H., Hasan A.. Selected Areas in Cryptography — SAC 2004. Lecture Notes in Computer Science 3562. Berlin: Springer-Verlag, 2005, 353～367

77 McGrew D. A., Fluhrer S. R.. The ABL mode of operation. Available from http://grouper. ieee. org/groups/1619/email. pdf0004. pdf

78 Halevi S.,Rogaway P.. A tweakable enciphering mode. In: Boneh D. ed.. Advance in Cryptology — Crypto'03. Lecture Notes in Computer Science 2729. Berlin: Springer-Verlag, 2003, 482～499

79 Halevi S., Rogaway P.. A parallelizable enciphering mode. In: Okamoto T. ed.. Topics in Cryptology — CT-RSA 2004. Lecture Notes in Computer Science 2964. Berlin: Springer-Verlag, 2004, 292～304

80 Wang Peng, Feng Deng-Guo, Wu Wen-Ling. HCTR: A tweakable enciphering mode. In: Feng D. G., Lin D. D., Yung M. eds.. SKLOIS Conference Information Security and Cryptology — CISC 2005. Lecture Notes in Computer Science 3822. Berlin: Springer-Verlag, 2005, 156～165

81 Liskov M., Rivest R. L., Wagner D.. Tweakable block cipher. In: Yung M. ed.. Advances in Cryptology — Crypto 2002. Lecture Notes in Computer Science 2442. Berlin: Springer-Verlag, 2002, 31～46

82 Wang Peng, Feng Deng-Guo, Wu Wen-Ling. On the security of tweakable modes of operation: TBC and TAE". In: Robert Deng ed.. Information Security Conference — ISC 2005. Lecture Notes in Computer Science 3650. Berlin: Springer-Verlag, 2005, 274～287

83 Rogaway P.. Efficient instantiations of tweakable blockciphers and refinements to mode OCB and PMAC. In: Lee P. J. ed.. Advances in Cryptology — Asiacrypto 2004. Lecture Notes in Computer Science 3329. Berlin: Springer-Verlag, 2004, 16～31

84 http://www. siswg. org/docs/index. html

85 Winternitz R.. A secure one-way hash function built from DES. In: Proceedings of the IEEE Symposium on Information Security and Privacy, IEEE Computer Society, 1984, 88～90

86 Merkle R.. One way hash functions and DES. In: Brassard G. ed.. Advances in Cryptology — Crypto'89. Lecture Notes in Computer Science 435. Berlin: Springer-Verlag, 1990, 53～61

87 Matyas S. M., Meyer C. H., Oseas J.. Generating strong one-way functions with cryptographic algorithms. IBM Technical Disclosure Bulletin, 1985, 27: 5658～5659

88 Matyas S. M.. Key processing with control vectors. Journal of Cryptology, 1991, 3: 113～116

89 Meyer C. H., Schilling M.. Secure program load with manipulation detection code. In: Proceedings of the 6th Worldwide Congress on Computer and Communication Security and Protection(SECURICOM'88), Paris, France, 1988, 111～130

90 Preneel B., Govaerts R., Vandewalle J.. Hash functions based on block ciphers: A synthetic approach. In: Stinson D. R. ed.. Advances in Cryptology — Crypto'93. Lecture Notes in Computer Science 773. Berlin: Springer-Verlag, 1994, 368～378

91 Black J., Cochran M., Shrimpton T.. On the impossiblity of highly efficient blockcipher based Hash Functions. In: Cramer R. ed.. Advances in Cryptology — Eurocrypto 2005. Lecture Notes in Computer Science 3494. Berlin: Springer-Verlag, 2005, 526～541

92 Hirose S.. Secure block ciphers are not sufficient for one-way hash functions in PGV model. In: Nyberg K., Heys H. ed.. Selected Areas in Cryptography — SAC 2002. Lecture Notes in Computer Science 2595. Berlin: Springer-Verlag, 2003, 339～352

93 Damgård. A design principle for hash functions. In: Brassard G. ed.. Advances in Cryptology — Crypto'89. Lecture Notes in Computer Science 435. Berlin: Springer-Verlag, 1990, 416～427

94 Lai X., Massey J. L.. Hash functions based on block ciphers. In: Rueppel R. A. ed.. Advances in Cryptology — Eurocrypt'92. Lecture Notes in Computer Science 658. Berlin: Springer-Verlag, 1992, 55～70

95 Hohl W., Lai X., Meier T., Waldvogel C.. Security of iterated hash function based on block ciphers. In: Stinson D. R. ed.. Advances in Cryptology — Crypto'93. Lecture Notes in Computer Science 773. Berlin: Springer-Verlag, 1993, 379～390

96 Hirose S.. Provably secure double-block-lengh hash functions in a block-box model. In: Park C., Chee S. eds.. Information Security and Cryptology — ICISC 2004. Lecture Notes in Computer Science 3506. Berlin: Springer-Verlag, 2005, 330～342

97 Knudsen L., Lai X., Preneel B.. Attacks on fast double block length hash functions. Journal of Cryptology, 1998, 11(1): 56～64

98 Nandi M., Lee W., Sakurai K., Lee S.. Security analysis of a 2/3-rate double length compression function in the block-box model. In: Gilbert H., Handschuh H. eds.. Fast Software Encryption — FSE 2005. Lecture Notes in Computer Science 3557. Berlin: Springer-Verlag, 2005, 243～254

99 Vaudenay S.. Security flaws induced by CBC padding-Applications to SSL, IPSEC, WTLS. In: Knudsen L. R. ed.. Advances in Cryptology — Eurocrypt 2002. Lecture Notes in Computer Science 2332. Berlin: Springer-Verlag, 2002, 534～545

100 Black J., Urtubia H.. Side-channel attacks on symmetric encryption schemes: The case for authenticated encryption. In: Proceedings of the 11th USENIX Security Symposium, San Francisco, CA, USA, 2002, 327～338

101 Paterson K. G., Yau A.. Padding oracle attacks on the ISO CBC mode encryption standard. In: Okamoto T. ed.. Topics in Cryptology — CT-RSA 2004. Lecture Notes in Computer Science 2964. Berlin: Springer-Verlag, 2004, 305～323

102 Canvel B., Hiltgen A., Vaudenay S., Vuagnoux M.. Password interception in a SSL/TLS channel. In: Boneh D. ed.. Advances in Cryptology — Crypto 2003. Lecture Notes in Computer Science 2729. Berlin: Springer-Verlag, 2003, 583～599

103 Wen Feng-Tong, Wu Wen-Ling, Wen Qiao-Yan. Error oracle attacks on several modes of operation. In: Proceedings of Conference on Computational Intelligence and Security — CIS 2005, Xi'an, China, 2005, 390～396

104 Bellare M., Pietrzak K., Rogaway P.. Improved security analysis for CBC MAC. In: Shoup V. ed.. Advances in Cryptology — Crypto 2005. Lecture Notes in Computer Science 3621. Berlin: Springer-Verlag, 2005, 527～545

105 Mitchell C. J.. Cryptanalysis of two variants of PCBC mode when used for message integrity. In: Boyd C., Juan M. González Nieto eds.. Information Security and Privacy — ACISP 2005. Lecture Notes in Computer Science 3574. Berlin: Springer-Verlag, 2005, 560～571

106 Mister S., Zuccherato R.. An attack on CFB mode encryption as used by open PGP. In: Proceedings of the SAC 2005, Kingston, Ontario, Canada, 2005, 86～99

107 Mitchell C. J.. Partial key recovery attacks on XCBC, TMAC and OMAC. In: Proceedings of the International Conference on Cryptography and Coding — CCC 2005. Cirencester, UK, 2005, 168～181

108 Phan R. C. W., Siddiqi M. U.. Related-mode attacks on block cipher mode of operation. In: Gervasi O., Gavrilova M. L., Kumar V. eds.. Computational Science and Its Applications — ICCSA 2005. Lecture Notes in Computer Science 3482. Berlin: Springer-Verlag, 2005, 661～671

WU Wen-Ling, born in 1966, Ph.D., researcher, Ph. D. supervisor. Her research interests include cryptography and information security.

FENG Deng-Guo, professor and Ph. D. supervisor. He mainly engaged in the research and development of information and network security.

Background

In 1980 NBS(now NIST) published four modes of operation for block ciphers with the DES as a particular application. The four modes are the Electronic Code Book(ECB), the Cipher Block Chaining (CBC), the Cipher FeedBack (CFB), and the Output FeedBack(OFB). With the advent of AES, there is a need to update long-standing modes of operation and an opportunity to consider the development of new modes.

In 2000, NIST plans to develop new modes and announces request for candidate modes from the public. NIST received a number of proposed modes and made all submissions publicly available for review and comment. NIST is in the process of recommending modes in a series of special publications. In SP 800-38A, five confidentiality modes are specified for use with any approved block cipher, such as the AES algorithm. The modes in SP 800-38A are updated versions of the ECB, CBC, CFB, and OFB modes that are specified in FIPS Pub. 81; in addition, SP 800-38A specifies the CTR mode. The CMAC authentication mode is specified in SP 800-38B for use with any approved block cipher. CMAC is an essentially the One-Key CBC-MAC(OMAC) algorithm submitted by Iwata and Kurosawa. SP 800-38C specifies the CCM mode of the AES algorithm. CCM combines the counter mode for confidentiality with the cipher block chaining technique for authentication. In the near future, NIST intends to specify at least two additional authenticated encryption modes: Galois Counter Mode(GCM) restricted to large tag sizes, and the AES Key Wrap(AESKW). GCM is intended for high-throughput applications that can take advantage of its parallelizability while tolerating its tag size restrictions. AESKW is intended for the authenticated encryption of specialized data, such as cryptographic keys, without using a nonce, for distribution or storage. Except above modes published by NIST, other organizations and research communities had presented some famous modes, such as f8, f9 and OCB.

A mode of operation is an algorithm that features the use of a symmetric key block cipher algorithm to provide an information service, such as confidentiality or authentication. A good mode can remedy some weaknesses of block cipher, on the other hand, a poorly designed mode may be insecure even though the underlying block cipher is good. There were many public research results on block cipher mode of operation in the past a few years. The authors introduce the design rationales, security model, research results and the state-of-the-art of research on block cipher mode of operation in this paper, and plan to further analysis the public modes and design new modes for special purpose.