分组密码算法认证运算模式的注记及可证安全性

罗 岚，秦志光，万国根，魏正耀

(电子科技大学计算机科学与技术学院 成都 610054)

【摘要】对分组密码算法CCM、CMAC加密模式进行描述，用可证安全性理论对它们进行相关研究和证明，并对各种证明情况在不同通信环境下的使用作出说明。针对认证工作模式用流程图的方式进行描述，同时证明了所有标准化的运算模式对于不同的使用环境是安全的。所研究内容对于2007年7月公布的GCM模式仍然适用，而且对于新的运算模式设计，可证安全性仍然是一个必要的环节。

关 键 词 分组密码； 运算环境； 运算模式； 可证安全性； 流密码

中图分类号 TN918.1 **文献标识码** A doi:10.3969/j.issn.1001-0548.2009.04.029

Note to the Authentication Operate Modes of Block Cipher and Provable Security

LUO Lan, QIN Zhi-Guang, WAN Guo-Gen, and WEI Zheng-yao

(School of Computer Science and Engineering，University of Electronic Science and Technology of China Chengdu 610054)

Abstract The validity of the provable security of counter with cipher block chaining message authentication code (CCM) mode and cipher-based message authentication code (CMAC) mode was studied and proved. The illustrations of different communications' encryption have been developed. The security of the novel authentication operation mode is demonstrated with flowing chart. The standardized operation modes of block cipher are proved to be safe in various environments. The proposed procedure is also applicable to Galois/counter mode (GCM) operation mode published in July, 2007. The provable security is a necessary process for a new mode of block cipher.

Key words block cipher; operation environments; operation mode; provable security; stream cipher

可证安全性(provable security，PS)理论是对安全协议框架证明而采取的一种方法，最早被应用于公开密码体制及单向散列函数。可证安全的第一次理论进展是1979年Rabin密码体制利用大素数分解数学难题而证明了可证安全性。之后文献[1]又对可证安全给出了两种更严格的定义：(1) 可证安全的概念是基于语义安全的，也就是选择密文攻击的前身；(2) 普遍的安全性证明包括文献[2]的选择密文攻击的思想。这两种可证明安全的概念有很强的相关性。可证安全第二次的理论进展是1980年数字签名的安全性证明，把选择密文攻击发展成为选择消息攻击，用存在伪造的观点代替语义安全性和普遍性。这一时期的安全性概念还包括了运算时间、能量消耗、电磁泄露、逻辑错误[3]、消息错误[4]等。20世纪90年代，可证安全两个最大的贡献在于文献[5]的“随机预言机制”和“面向应用的可证安全性”理论。因为上述工作，可证安全性理论在极大范围得到认可与发展。

可以看出：对于非对称密码体制中以数学难题为基础的公钥体制和单向散列函数，在可证安全性领域进行了很多工作；但是就对称密码体制而言，这方面的工作几乎没有进行。

随着互联网的普及，网络密码学应用的趋势更加明显。目前的网络密码因为使用环境的特殊性，主要采用的是商业化、标准化的公开分组密码算法。因此，对分组密码算法进行可证安全性研究是必要的。工作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，国际上许多密码学家讨论了多种模式。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制定[6]。文献[7]对分组密码的ECB、OFB、CBC、CFB运算模式进行了可证安全性的工作。但是，国内除了少数对NIST标准的执行模式的讨论之外，对可证安全性方面的研究与实际应用还没有自主公开的研究结

收稿日期：2008－05－26；修回日期：2009－05－23
基金项目：国家863计划(2006AA01Z428)；国家自然科学基金(60673075)
作者简介：罗 岚(1969－)，女，博士，副研究员，主要从事信息安全方面的研究.

论。伴随AES又有CTR、CCM、CMAC[8]3个新模式提出并正式列入标准。文献[9]提出的密钥延迟运算模式，对eSTREAM活动的获胜算法TRIVIUM的线性信息泄漏可以进行弥补。文献[10]和文献[11]分别对CMAC模式和CTR模式进行了安全性证明。

本文首先对分组密码CCM、CMAC加密模式进行描述，然后用可证安全性理论对它们进行相关研究，最后对之前的一些证明在不同通信环境下的使用作一些说明。对于2007年7月公布的可并行认证模式GCM[12]运算模式，可以使用类似的方式进行证明。与前3个新标准运算模式不同的是，NIST给出了GCM的图形。但本文与文献[13-14]提出的可证明安全性的方法没有必然联系。

1　基本原理与符号规定

设M为一集合，C为该集合上的密码体制，F为作用在该集合上的密码函数，D为一可能发生的事件。令标准值$d\in D$，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，使用穷尽方法寻找F，与其线性逼近(或其他)构造的完全随机仿真的函数F^*的偏差(或距离)定义为：

$$\mathrm{Adv}F^{\mathrm{ATC}(d)}=\max_D\{\mathrm{Adv}_d^{\mathrm{ATC}(d)}(F,F^*)\} \quad (1)$$

使用穷尽方法寻找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：

$$\mathrm{Adv}C^{\mathrm{ATC}(d)}=\max_D\{\mathrm{Adv}_d^{\mathrm{ATC}(d)}(C,C^*)\} \quad (2)$$

通常以约束式(1)和式(2)的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：

$$\mathrm{Adv}^{\mathrm{ATC}(d|\mathrm{mess})}(\mathrm{Mode}(C))$$

满足条件A的最佳随机预言优势为：

$$\mathrm{Adv}^{\mathrm{ATC}(d|q)}(\mathrm{Mode}(C)|A)$$

2　分组密码算法的认证运算模式的可证安全

分组密码算法运算模式在DES时期的标准有ECB、CBC、DFB、OFB等4种。2001年的SP800-38A中确定了AES的ECB、CBC、CFB、OFB和CTR等5种工作模式；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，因此在不同的使用环境选择恰当的运算方式能够使密码算法的安全功能达到最佳效果。由于ECB、CBC、DFB、OFB等4种保密模式已经在多种场合进行过流程描述与深入的研究，本文不再赘述。以下叙述AES标准中新增加的认证CCM、CMAC模式。2007年7月30日公布了新的可并行身份认证的GCM运算模式，对于这个标准的描述包括了运算草图与相关公式。

2.1　认证保密模式及可证安全性

认证保密模式(CCM)即在SP800-38C中采用的分组密码算法运算模式，也即IEEE 802.11的无线局域网的运算模式，已通过RFC 3610进行标准化，如图1所示。

尽管对CCM存在一些争论，但是FIP和RFC两大标准对其的认可，说明该运算方式具备优势。

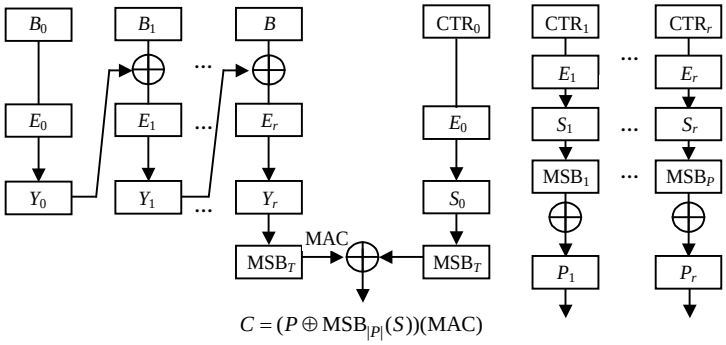

图1　分组密码算法的*CCM*运算模式

图1中，令分组密码算法为E、密钥为K、记数Counter的生成函数和格式函数分别为g和f，MAC的长度为r。输入随机数N、消息P和相关数据A，如果预先处理过程为：

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

可以看出CCM运算模式是CTR运算模式加上CMAC验证码，是CTR和CMAC两种运算模式调用加密函数次数的和。

定理 1　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文攻击与已知

明文攻击，d、mess是整数(mess≤d)，则：

$$\mathrm{Adv}C^{\mathrm{ATC}(d|\mathrm{mess})}(\mathrm{CCM}[F^*])\leqslant d^2/|2M|$$

证明　设C_1:=CCM[F^*]，C_2=C^*。假设攻击者已明，密文对为 $X_j=x_{j_1}x_{j_2},x_{j_2}x_{j_3},\mathrm{L},x_{j(n-1)},x_{j_n}$ 和 $Y_j=y_{j_1}y_{j_2}$，$y_{j_2}y_{j_3},\mathrm{L},y_{j(n-1)},y_{j_n}$，并且1≤$j$≤$q$，$n_j$是分组数，因此 $n_1+n_2+\mathrm{L}+n_q=d$。

对所有 y_{j_l}，1≤j≤q，0≤l<n_k，定义y_k为序列的第K个元素，$y_k=y_{a_b}$。

设α是使下列等式成立的最大整数，则：

$$\sum_{j=1}^{\alpha-1}n_j\leqslant k,b=k-\sum_{j=1}^{\alpha}n_j$$

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

$u,v<k,u\neq v$:$y_u\oplus x_{u+1}\oplus\mathrm{MAC}_u\neq y_v\oplus x_{v+1}\oplus\mathrm{MAC}$

$u\neq v,y_u\oplus x_{u+1}\oplus\mathrm{MAC}_u\oplus k_i\neq y_v\oplus x_{v+1}\oplus\mathrm{MAC}$

函数F^*的输入明文不同，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：

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

如果发生碰撞的元为 y_{a_0}，上述表达式为：

$$\Pr[\overline{D}_k\mid D_{k-1}]=\Pr[\exists u<k:y_{a_0}=$$
$$y_u\oplus x_{u+1}\oplus x_{k-1}]=\frac{k}{|M|}$$

则：

$$\mathrm{Adv}C^{\mathrm{ATC}(d|\mathrm{mess})}(\mathrm{CCM}[F^*])=\Pr[\overline{D}]=$$
$$\Pr[\overline{D}_{d-1}]\leqslant\sum_{k=0}^{d-1}\Pr[\overline{D_k}\mid D_{k-1}]=$$
$$\sum_{k=0}^{d-1}\frac{k}{|M|}=\frac{d^2}{2|M|}$$

定理 2　设F^*是集合M上的完全随机函数，CPA、mess、d(d≥mess)如前所定义，则有：

$$\mathrm{Adv}^{\mathrm{CPA}(d|\mathrm{mess})}(\mathrm{CCM}[F^*])\geqslant\left(1-\frac{1}{e}\right)\left(1-\frac{1}{|M|}\right)\frac{\mathrm{mess}\times d}{|M|}$$

证明　参考定理1。

2.2　认证模式及可证安全性

认证模式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2所示。

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：(1) 如果消息分组正好满足整块，使用密钥K_1来进行运算；(2) 如果消息分组有剩余，则使用填充码填成一组后再使用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。

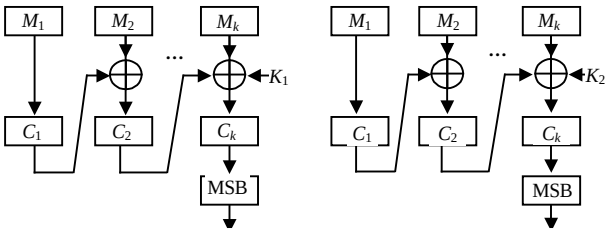

图2　分组密码算法的CMAC运算模式

定理 3　设F^*是一个M上的完美函数，ATC　　,攻[illegible]是传统意义的选择明文攻击和已知明文攻击，d、mess是整数(mess≤d)，则：

$$\mathrm{Adv}C^{\mathrm{ATC}(d|\mathrm{mess})}(\mathrm{CMAC}[F^*])\leqslant\frac{d^2}{2|M|}$$

证明　设C_1:=CMAC[F^*]，C_2=C^*。假设攻击者已知明文 $X_j=x_{j_1}x_{j_2},\mathrm{L},x_{j_n}$ 和密文 $Y_j=y_{j_0},y_{j_1}$，$y_{j_2},\mathrm{L},y_{j_n}$，并且1≤$j$≤$q$，$n_j$是分组数，因此$n_1+n_2+\mathrm{L}+n_d=d$。

对所有 y_{j_l}，1≤j≤q，0≤l<n_n，定义y_k为序列的第K个元素，$y_k=y_{a_b}$。

设α是使下列等式成立的最大整数，则：

$$\sum_{j=1}^{\alpha-1}n_j\leqslant k,b=k-\sum_{j=1}^{\alpha}n_j$$

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

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

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

函数F^*的输入明文不同，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_{a_b} 是完全随机的。因此，使用分别攻击的方法对于CMAC[F^*]和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：

$$\Pr[\overline{D}_k \mid D_{k-1}] = \Pr[\exists u < k : y_{a_0} = y_u \oplus x_{u+1} \oplus x_{k-1}] = \frac{k}{|M|}$$

则：

$$\text{Adv}C^{\text{ATC}(d|\text{mess})}(\text{CMAC}[F^*]) = \Pr[\overline{D}] = \Pr[\overline{D}_{d-1}] \leqslant \sum_{k=0}^{d-1} \Pr[\overline{D}_k \mid D_{k-1}] = \sum_{k=0}^{d-1} \frac{k}{|M|} = \frac{d^2}{2|M|}$$

定理 4　设C^*是M上的完善密码体制，ATC 是{CPA,ACPA}任意的选择明文攻击和已知明文攻击，d、mess是整数(mess≤d)，则：

$$\text{Adv}C^{\text{ATC}(d|\text{mess})}(\text{CMAC} \mid C^*) \leqslant \frac{d^2}{|M|}$$

证明　显然。

定理 5　设F^*是一个M上的完美函数，$d < \sqrt{2M}$，mess(mess≤d)是一个整数，则：

$$\text{Adv}^{\text{CPA}(d|\text{mess})}(\text{CMAC}[F^*]) \geqslant \left(1 - \frac{1}{e} - \frac{1}{|M|}\right) \frac{d^2}{2|M|}$$

证明　类似于定理3。

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

$$\text{Adv}C^{\text{CPA}(d|\text{mess})}(\text{MCAC}[F^*]) \geqslant \left(1 - \frac{1}{e}\right)\left(\frac{d^2}{2|M|}\right)^2 = \frac{1}{4}\left(1 - \frac{1}{e}\right)$$

3　结　论

分组密码算法运算模式最简单的方法就是把消息分成块后直接加密。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很出色地保证了消息的完整性和安全性。FIP与RFC两大标准均认可和采用这种运算模式。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。通过对上述认证模式可证安全性的研究可知，传统的攻击为已知消息攻击和选择消息攻击，它们都有上界和下界。如果攻击者能够在界限之内发现合适的消息与密文对，构造出碰撞的条件，说明分组密码系统存在安全问题。设计者缩小上界与下界的标准是对分组密码系统的安全改进。就密码系统而言，安全性与完整性、效率与速度是相互矛盾的，但又必须兼顾每一方面。所以，分组密码的不同运算模式更像是从不同角度对算法各种特性的展示。最近，NIST对GCM的设计和证明从形式上弥补了前几种新的运算模式在图形表示上的不足，进行了更详细的描述，其可证安全性工作与文中CCM和CMAC是类似的。

参　考　文　献

[1] GOLDWASSER S, MICALI S, RACKOFF C. The knowledge complexity of interactive proof systems[J]. SIAM Journal on Computing , 1989, 18(1): 186-208.

[2] FRANKEL Y, YUNG M. Cryptanalysis of the immunized public key systems[C]//Advances in Cryptology-Eurocrypt '95. [S.l.]: Springer-Verlag, 2004: 287-296.

[3] BELLARE M, ROGAWAY P. Random oracles are practical: a paradigm for designing efficient protocols[C]//ACM Conference on Computer and Communications Security. [S.l.]: ACM, 2007: 62-73.

[4] BONEH D, DEMILLO R, LIPTON R. On the importance of checking cryptographic protocols for faults[C]//Advances in Cryptology-Eurocrypt '97. Konstanz, Germany: Springer-Verlag, 1997: 37-51.

[5] MANGER J. A chosen ciphertext attack on RSA optimal asymmetric encryption padding(OAEP) as standardized in PKCS[C]//Advances in Cryptology-Crypto 2001. Santa Barbara: Springer-Verloag, 2001: 230-238.

[6] National Institute of Standards and Technology (NI ST). NI-ST special publication 800-38A[S]. Recommendation for Block Cipher Modes of Operation: Methods and Techniques, 2001.

[7] FIBIKOVA L. Provable secure scalable block ciphers[D]. Duisburg: University Duisburg-Essen, 2003.

[8] National Institute of Standards and Technology(NIST). NIST special publication 800-38B[S]. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005.

[9] 罗　岚, 瞿泽辉, 张凤荔, 等. 带延迟的分组密码算法密钥结合模式设计[J]. 电子科技大学学报，2007, 36(3): 649-651.
LUO Lan, QU Ze-hui, ZHANG Feng-li, et al. A key delay design on block cipher algorithm[J]. Journal of University of Electronic Science and Technology of China, 2007, 36(3): 649-651.

[10] 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[C]//第十届保密通信年会. 桂林: 信息安全与通信保密杂志社, 2007: 40-42.
LUO Lan, WEI Zheng-Yao, QIN Zhi-Guang. Provable security to one kind of hash function constructed by block cipher's CMAC mode[C]//The 10th Security Communication Conference. Guilin: Information Security and Communications Privacy, 2007: 40-42.

[11] 罗　岚. 分组密码算法设计与评估应用研究[D]. 成都: 电子科技大学, 2009.
LUO Lan. The application research of design and evaluation on block cipher[D]. Chengdu: University of

Electronic Science and Technology of China, 2009.
[12] National Institute of Standards and Technology(NIST). NIST special publication 800-38C[S]. Recommendation for Block Cipher Modes of Operation: The GCM Mode for Authentication and Confidentiality, 2007.
[13] KOBLITZ N. Another look at provable security[J]. Journal of Cryptology, 2007, 20(1): 3-37.
[14] GOLDWASSER S, BELLARE M. Lecture notes on cryptography[M/CD]. [2008-05-11]. www.cs.ucsd.edu/ users/ mihir/papers /gb. pdf.

编 辑 熊思亮

(上接第512页)

图3表示采用不同方法时的收敛情况，从中可以看出，在低信噪比下，本文所述方法具有最快的收敛速度，而对于 $A_k = A_{\min}$ 时，即便在高信噪比下，EKF也会出现发散现象。

4 结 论

本文算法本质上是具有可变增益的幅度锁定环(ALL)和相位锁定环(PLL)的联合估计，推导了二者的闭环传输函数，得出了稳态时等效噪声带宽解析表达式。数值仿真表明，与传统算法中固定幅度估计方法和包络估计幅度方法相比，该算法在高低信噪比下，均具有较高的稳态估计精度和较短的收敛时间。

参 考 文 献

[1] ZHANG H G, LI L P, CHEN T Q. An approach to blind synchronization of DS/SS signals[J]. Journal of University of Electronic Science and Technology of China, 2007, 36(2): 207-209.
[2] BUREL G. Detection of spread spectrum transmissions using fluctuations of correlation estimators[C]// ISPlACS'2000. IEEE Int Symp on Intelligent Signal Processing and Communication Systems. Kitami: Kitami Institute of Technology, 2000.
[3] DOUGLAS A H, JOHN B B. Carrier detection of PSK signals[J]. IEEE Trans on Communications, 2001, 49(3): 487-496.
[4] BARBARA F, LA S, ROBERT R, et al. An extended kalman filter frequency tracker for high-noise environments[J]. IEEE Trans on Signal Porcessing, 1996, 44(2): 431-434.
[5] YU T S, RU C W. Frequency acquisition and tracking in high dynamic environments[J]. IEEE Trans on Vehicular Tech, 2000, 49(6): 2419-2429.
[6] AGUIRRE S, HINEDI S. Two novel automatic frequency tracking loops[J]. IEEE Trans on Aerospace and Electronic Systems, 1989, 25(5): 749-760.
[7] SEGIO B, SEGIO M S. On the parameterization and design of an extended kalman filter frequency tracker[J]. IEEE Trans on Automatic Control, 2000, 45(9): 1718-1724.
[8] WEIBIN L, SHANGJIAN L, CHUNHUI Z, et al. High dynamic carrier tracking using kalman filter aided phase-locked loop[C]//International Conference on Wireless Communications, Networking and Mobile Computing. Shanghai: IEEE Press, 2007: 673-676.
[9] NESREEN I Z. GNSS receivers for weak signals[M]. Boston: Artech House Incorporate, 2006: 160-180.
[10] DON T. Principles of spread-spectrum communication systems[M]. Boston: Springer Science + Business Media Inc, 2005: 55-75.
[11] JUAN A B, GONZALO D M, ANDRES S, et al. Tracking filters using kinematic measurements[C]//10th International Conference on Information Fusion. Quebec: IEEE Press, 2007: 1-8.
[12] STEVEN M K. Fundamentals of statistical signal processing[M]. Beijing: Publishing House of Electronics Industry, 2003: 338-364.
[13] THRASYVOULOS P, ALAN J L, NILS R S, et al. On the numerical solution of the discrete-time algebraic riccati equation[J]. IEEE Trans on Automatic Contorl, 1980, 25(4): 631-641.

编 辑 漆 蓉