欧洲21世纪数据加密标准候选算法简评*

吴文玲，贺也平，冯登国，卿斯汉

(中国科学院 软件研究所 信息安全国家重点实验室，北京 100080)；
(中国科学院 信息安全技术工程研究中心，北京 100080)
E-mail：wwl@ercist.iscas.ac.cn

摘要：简要介绍了欧洲NESSIE(new European schemes for signatures, integrity, and encryption)大计划最近公布的17个分组密码算法的基本设计思想、最新分析结果及其有效性.

关键词：AES；NESSIE；加密；解密；密钥
中图法分类号：TP393 **文献标识码**：A

继美国征集AES(advanced encryption standard)[1]结束之后，欧洲又开始进行称为NESSIE[2](new European schemes for signatures, integrity, and encryption)的密码大计划，其主要目的是为了推出一系列安全的密码模块；另一个目的是保持欧洲在密码研究领域的领先地位，并增强密码在欧洲工业中的作用.与AES相比，NESSIE涉及的范围更广，不仅征集了分组密码，而且还征集了流密码、公钥密码、数字签名、消息认证码以及杂凑函数.整个运作过程是公开的、透明的，2000年3月公布了征集通告，2000年11月13～14日召开第1次NESSIE会议，并公布了征集到的所有算法.NESSIE共收到了17个分组密码，按照分组长度分为4部分.为了让更多的国内读者了解这些分组密码，本文简要介绍这些分组密码的背景、设计思想、最新分析结果及其有效性.

1 64比特分组密码

1.1 CS-Cipher

CS-Cipher[3,4]由法国的Jacques Stern和Serge Vaudenay设计，最早公布于1998年的Fast Software Encryption会议论文集上，它的整体结构是SP(substitution-permutation)网络，轮函数中使用了快速傅里叶变换、乘法及S-盒等基本运算，看似安全，但是由于盒的非线性性和扩散层的性质不够好，所以，与SHARK相比，CS-Cipher的安全性并不理想.我们在这方面的工作将另文发表.

有效性：在Pentium (133MHz)系统下，CS-Cipher的软件加密速度可达8Mbit/s.

1.2 Hierocrypt-L1

Hierocrypt-L1[5]是日本东芝公司提交的一个64比特分组的密码算法.它采用设计者称为蜂窝状SP网络的整体结构，此结构的每一轮形如SP_1SP，S由8×8的S-盒并置而成，P_1由两个F_2^{32}上的线性变换并置而成，P是F_2^{64}上的线性变换.采用此结构的优点是，设计者可以估计算法抵抗差

* 收稿日期：2000-11-30；修改日期：2000-12-12
基金项目：国家重点基础研究发展规划资助项目(G1999035802)；国家自然科学基金资助项目(60083007)
作者简介：吴文玲(1966－)，女，陕西人，博士，副研究员，主要研究领域为分组密码的设计与分析；贺也平(1962－)，男，江西人，博士后，主要研究领域为分组密码的设计与分析；冯登国(1965－)，男，陕西人，博士，研究员，博士生导师，主要研究领域为信息安全理论与技术；卿斯汉(1939－)，男，湖南人，研究员，博士生导师，主要研究领域为信息安全理论与技术.

分和线性密码分析的能力.

Hierocrypt-L1 选用有限域 F_2^8 上的幂函数 x^{247} 作为 S-盒,它的代数次数为 7,差分和线性概率都达到了最佳状态. SP_1S 可以看成是两个 32×32 盒的并置,它的最大差分和线性特征的概率上界为 2^{-30}. 设计者称 5 轮 Hierocrypt-L1 是安全的.

有效性:在 Pentium (550MHz)系统下,Hierocrypt-L1 的软件加密速度可达 139Mbit/s,解密速度可达 67Mbit/s.

1.3 IDEA

X. J. Lai 和 J. L. Massey 提出的第 1 版 IDEA(国际数据加密算法)于 1990 年公布,当时称为 PES(建议加密标准). 1991 年,在 Biham 和 Shamir 提出差分密码分析[6]之后,设计者推出了改进算法 IPES,即改进型建议加密标准. 1992 年,设计者又将 IPES 改名为 IDEA[7]. IDEA 的分组长度为 64 比特,密钥长度是 128 比特,其设计思想是"混合使用来自不同代数群中的运算". 所用的运算有 16 比特子块的逐比特异或、16 比特整数的模 2^{16} 加和 16 比特整数的模 $2^{16}+1$ 乘(其中全零子块对应于 2^{16}).

10 年来,世界各地的专家学者对 IDEA 的安全性进行了深入的分析[8~12],主要结果有:

- 差分密码分析可以攻击 2.5 轮 IDEA.
- 截断差分密码分析可以攻击 3.5 轮 IDEA.
- 中间相遇攻击可以攻击 4.5 轮 IDEA.
- 有一些弱密钥.

有效性:在 Pentium (90MHz)系统下,IDEA 的软件加密速度可达 4.2Mbit/s;在 Pentium II (366MHz)系统下,IDEA 的软件加密速度可达 31Mbit/s;在 Pentium III(600MHz)系统下,IDEA 的软件加密速度可达 61Mbit/s.

1.4 Khazad

Khazad 分组密码由巴西的 Paulo S. L. M. Barreto 和比利时的 Vincent Rijmen 共同设计,它的分组长度为 64 比特,密钥长度为 128 比特,整体结构是 SP 网络,它的设计类似于 SHARK[13]密码,遵循宽尾巴原则(wide trail strategy). 与 SHARK 密码的不同之处在于,Khazad 的每个基本模块都是对合的,因此,Khazad 的加解密是相似的.

现有的分析结果:

- 两轮 Khazad 的差分特征的概率小于 2^{-45},线性逼近的优势小于 $2^{-29.7}$.
- 4 轮 Khazad 就可以抵抗截断差分密码分析.
- Khazad 抵抗现有所有攻击.

有效性:在 Pentium III(550MHz)系统下,Khazad 的加解密速度可达 65.7Mbit/s.

1.5 MISTY1

MISTY1 是由日本的 Mitsuru Matsui 提交的一个分组密码,它的分组长度为 64 比特,密钥长度为 128 比特,轮数是可变的,但必须是 4 的倍数. 针对差分和线性密码分析,文献[14,15]相继给出了可证明安全的理论结果,基于这些理论研究结果,Mitsuru Matsui 在文献[16]中推出了 MISTY1 和 MISTY2,MISTY1 的轮函数被称为是递归结构. 近几年一直没有 MISTY 的分析结果公布.

有效性:MISTY1 的硬件加密速度可达 450Mbit/s,在 Pentium (100MHz)系统下,软件加密速度可达 20Mbit/s.

1.6 Nimbus

Nimbus是由巴西的Alexis Warner Machado设计的,它是一个5轮的64比特分组迭代密码,其设计非常简单,仅用了3种常用的基本模块,一个是模2^{64}乘法,另一个是64比特异或运算,最后一个是比特变换.设计者称此算法是安全的(但是,在公开后不久,就被彻底攻破,攻击所需的数据复杂度仅为1024),在Pentium (166MHz)系统下加密速度可达20Mbit/s.

2 128比特分组密码

2.1 Anubis

Anubis分组密码由巴西的Paulo S. L. M. Barreto和比利时的Vincent Rijmen共同设计,他们还共同给NESSIE提交了Khazad密码,Anubis的分组长度为128比特,密钥长度为可变的$3N$比特($4\leqslant N\leqslant 10$).它的S-盒的选取和Khazad密码一样,其线性层的设计类似于Rijndeal密码,遵循宽尾巴原则(wide trail strategy).与Rijndeal密码相比,Anubis的优点是加解密相似.

现有的分析结果:

- 4轮Anubis的差分特征的概率小于2^{-128},线性逼近[17]的优势小于$2^{-57.5}$.
- 6轮Anubis就可以抵抗截断差分密码分析[18].
- Anubis抵抗已知的其他攻击.

有效性:在Pentium III(550MHz)系统下,Anubis的加解密速度随密钥长度的不同而发生变化,具体见表1.

Table 1

表1

Key length①	128	160	192	224	256	288	320
Speed②(Mbit/s)	119	112	105	100	95	90	86

①密钥长度,②速度.

2.2 Camellia

1998年,NTT公司给NIST提交了E2,2000年,NTT和Mitsubishi电子公司联合给NESSIE提交Camellia[19],Camellia最早公布于今年的SAC会议上.E2和Camellia的设计目标类似于AES的要求,即分组长度是128比特,并支持128、192及256比特这3种规模的密钥长度;比二重DES快,而且至少和三重DES一样安全.

E2和Camellia采用的都是Feistel结构,和E2相比,Camellia有如下几个特点:

(1) Camellia的轮函数采用的是1-轮SP结构,而E2的轮函数采用的是2-SP结构.E2的设计者在文献[20]中使用了大量笔墨来说明轮函数采用2-轮SP结构的优点,为什么两年之后Camellia的轮函数要采用1-轮SP结构?其中的原因是设计者有了文献[21]的研究结果,据此结果,设计者可以给出Camellia抵抗差分和线性密码分析的定量估计.

(2) Camellia每隔6轮嵌入由逻辑运算构成的函数FL和EL^{-1}.如此设计的目的是为了提供不规则的Feistel结构,抵抗未来的攻击方法;而且FL和EL^{-1}的嵌入并不影响Feistel密码加解密相似的特性.

(3) Camellia的密钥编排算法是飞弹型的,也就是说,能以任意顺序生成子密钥:其中对于128比特的密钥,所需的存储量是32字节;对于192和256比特的密钥,所需的存储量是64字节.

(4) Camellia的轮函数中的扩散层P的设计类似于E2,仅用字节⊕运算,以保证它的效率,P

的分枝数也为5,但是它在某些方面比E2的扩散层要好.

(5) Camellia采用了4个不同的S-盒,从我们的讨论可知,这一点是保证Camellia安全性的重要一环.

目前对Camellia的分析结果有:

- 没有嵌入FL和FL^{-1}的16-轮Camellia的差分和线性概率的界为2^{-132}.
- 嵌入FL和FL^{-1}的12-轮Camellia对差分和线性密码分析是安全的.
- (没有)嵌入FL和FL^{-1}的10-轮Camellia对截断差分密码分析是安全的.
- 没有嵌入FL和FL^{-1}的10-轮Camellia对截断线性密码分析是安全的.

Camellia对不可能差分密码分析、飞来去器攻击、高阶差分攻击、插值攻击、滑动攻击及相关密钥攻击都是安全的.

设计者在设计时没有考虑能量攻击,指出依靠硬件技术保护Camellia,使其免受能量攻击.

2.3 Grand Cru

Graud Cru是由比利时的Johan Borst和K. U. Leuven设计的一个分组长度为128比特的密码算法,它以Rijndeal为基础,在多层安全策略(strategy of multiply layered security)的指导下来设计.多层安全策略的思想是在一个密码算法中包含不同安全强度的子密码,每个子密码的设计侧重点不同,每个子密码使用不同的子密钥集,知道部分子密钥集不能推出其他子密钥信息.多层安全策略的设计思想值得我们注意,最近公布的几个算法均采用此方法.此设计方法可以提高算法的安全性,但是利用此方法很难构造在各种平台上都快速实现的算法.

2.4 Hierocrypt-3

Hierocrypt-3是日本东芝公司提交的一个128比特分组的密码算法,它的设计思想类似于Hierocrypt-L1.

2.5 Noekeon

Noekeon是由比利时的Joan Daemen,Michael Peeters,Gilles Van Assche和Vincent Rijmen共同设计的一个分组密码,它的分组长度和密钥长度均为128比特,其整体结构采用的是16轮SP网络,为了保证加解密相似,设计者要求每个基本模块都是对合的.另外,设计者还使用了类似于Serpent的"Bit-Slice"技术,它所用的S-盒的差分和线性概率都达到了最佳程度.目前,最好的理论分析结果是可以构造9轮的线性逼近,其优势为2^{-62}.

有效性:Noekeon可以在各种平台上安全而有效地实现,尤其适宜资源有限的智能.在Pentium II(200MHz)系统下,Noekeon的软件加密速度可达49Mbit/s.

2.6 Q

Q是由美国的Leslie-Mack' McBride设计的,它是一个可以支持任意长度密钥的128比特分组密码,其整体结构是7轮的SP网络,它的轮函数设计基于Rijndeal和Serpent;非线性层类似于Rijndeal,用一个8×8的盒并置而成;线性层类似于Serpent,用"bit-slice"S-盒.与Serpent相比,Q的雪崩特性和速度更好.与Rijndeal相比,Q的S结构能更好地抵抗未来的密码分析.另外,每一轮的非线性层由两个固定的密钥变换包围,这样,Q的S-盒就随密钥的变化而发生变化,在一定程度上提高了Q的安全性.目前,对Q最有效的攻击是差分密码分析,攻击的数据复杂度为2^{115}.

2.7 SC2000

SC2000是由日本东京科技大学的Takeshi Shimoyama等人提交的分组密码,它的分组长度为128比特,可以支持128、192或256比特这3种密钥规模.SC2000采用了Feistel结构和SP网络相

结合的技术,整体结构是SP网络,轮函数中的部分变换采用Feistel结构,使用了4×4、5×5和6×6这3种规模的S-盒,总之,SC2000的设计比较复杂,设计者既不能从理论上证明它的安全性,也不能给出估计它对差分和线性密码分析的概率上界.在分析报告中,设计者用搜索的办法说明SC2000对差分和线性密码分析是安全的.

3 160比特分组的密码

3.1 SHCAL

SHCAL是由Gemplus公司的Helena Handschuh和David Naccache设计的一个分组密码,它的分组长度为160比特,密钥长度建议为128～512比特.SHCAL的设计基于安全杂凑算法[22](SHA-1),它的安全性等价于SHA-1.

4 分组长度可变的密码

4.1 NUSH

NUSH是由俄罗斯的Anatoly N. Lebedev和Alexey A. Volchkov设计的分组密码,它的分组长度可以为64、128或256比特,密钥长度为128、192或256比特,它的整体结构采用的是SP网络.NUSH分组密码没有用S-盒,它是利用不同运算(加法、逻辑运算及移位等)的混合达到"扩散"和"混淆"的目的.NUSH的递交者同时还向NESSIE递交了以NUSH分组密码为基础的消息认证码、杂凑函数、数字签名及非对称密码体制等.我们对不同分组长度和密钥规模的NUSH进行了线性密码分析,每一种攻击的复杂度δ由它所需的数据复杂度ε和时间复杂度η组成,记为$\delta=(\varepsilon,\eta)$.对于分组长度为64比特的NUSH,当密钥为128时,3种攻击的复杂度分别为$(2^{58},2^{124})$、$(2^{60},2^{78})$和$(2^{62},2^{45})$;当密钥为192时,3种攻击的复杂度分别为$(2^{58},2^{157})$、$(2^{60},2^{96})$和$(2^{62},2^{58})$;当密钥为256时,3种攻击的复杂度分别为$(2^{58},2^{125})$、$(2^{60},2^{78})$和$(2^{62},2^{53})$;对于分组长度为128比特的NUSH,当密钥为128时,3种攻击的复杂度分别为$(2^{122},2^{95})$、$(2^{124},2^{57})$和$(2^{126},2^{52})$;当密钥为192时,3种攻击的复杂度分别为$(2^{122},2^{142})$、$(2^{124},2^{75})$和$(2^{126},2^{58})$;当密钥为256时,3种攻击的复杂度分别为$(2^{122},2^{168})$、$(2^{124},2^{81})$和$(2^{126},2^{64})$.对于分组长度为256比特的NUSH,当密钥为128时,两种攻击的复杂度分别为$(2^{252},2^{122})$和$(2^{254},2^{119})$;当密钥为192时,两种攻击的复杂度分别为$(2^{252},2^{181})$和$(2^{254},2^{177})$;当密钥为256时,两种攻击的复杂度分别为$(2^{252},2^{2401})$和$(2^{254},2^{219})$.从这些结果可以看出,NUSH对线性密码分析是不免疫的,而且密钥规模的增大不能保证安全性的提高.

4.2 RC6

RC6是进入AES最后一轮决赛的5个算法之一,它的各种性能都得到了充分的分析[23,24]与测试.这里我们限于篇幅不再详述.

4.3 SAFER++

SAFER++是SAFER[25,25]系列算法中的最新产品,它有两个版本,一个分组长度为128比特,密钥长度为128或256比特;另一个分组长度为64比特,密钥长度为128比特.与SAFER+相比,SAFER++的不同之处表现在线性层,SAFER+采用的是多维2-点变换扩散器,而SAFER++采用的是多维4-点变换扩散器.设计者称SAFER++比SAFER+更简单、更有效、密码特性更好.

5 结束语

我们首先给出17个分组密码的一览表,见表2.

Table 2
表 2

Cipher①	Country (Company)②	General structure③	Design characteristic④
CS-Cipher	France	SP	S-Box⑤
Hierocrypt-L1	Japan	SP	S-Box
IDEA	Switzerland	SP	Operations from different groups⑥
Khazad	Belgium	SP	S-Box
MISTY1	Japan	Recursive structure⑦	S-Box
Nimbus	Brazil	SP	Multiplication and exclusive-or⑧
Anubis	Brazil, Belgium	SP	S-Box
Camellia	Japan	Feistel	S-Box
Grand Cru	Belgium	SP	S-Box
Hierocrypt-3	Japan	SP	S-Box
Noekeon	Belgium	SP	Bit-Slice⑨
Q	USA	SP	S-Box
SC2000	Japan	SP	S-Box
SHACAL	Gemplus Company		Based hash function⑩
NUSH	Russia	SP	Mixing different operations⑪
RC6	USA	Generalized Feistel⑫	Data-Dependent rotation⑬
SAFER++	Switzerland	SP	S-Box

①算法名称,②国家(公司),③整体结构,④设计特点,⑤S-盒,⑥不同群中的运算,⑦递归,⑧乘法和异或,⑨逻辑运算,⑩以杂凑函数为基础,⑪各种运算混合,⑫乘法数据相依循环,⑬广义 Feistel.

从表中可以看出,日本提交了5个算法,是递交数量最多的国家,这一点显示了日本在分组密码领域的研究是非常活跃的.与AES的15个候选算法相比,NESSIE的17个候选算法的设计比较单一,没有多少新思想,受AES的影响比较大,整体结构主要采用SP网络,非线性主要靠S-盒来实现.

References:

[1] AES Candidate Algorithms. http://csrc.nist.gov/encryption/aes/aes_home.htm#candidates.

[2] NESSIE. http://www.cryptonessie.org.

[3] Stern, J., Vaudenay, S. CS-CIPHER. Fast Software Encryption, LNCS 1372, Berlin: Springer-Verlag, 1998. 189~205.

[4] Vaudenay, S. On the security of CS-Cipher. Fast Software Encryption, LNCS 1636, Berlin: Springer-Verlag, 1999. 260~274.

[5] Hierocrypt-L1 and Hierocrypt 3. http://www.toshiba.co.jp/rdc/security/hierocrypt/.

[6] Lai, Xue-jia. On the Design and Security of Block Ciphers. Konstanz: Hartung-Gorre Verlag, 1992.

[7] Biham, E., Shamir, A. Differential Cryptanalysis of Data Encryption Standard. New York: Springer-Verlag, 1993.

[8] Meier, W. On the security of the IDEA block cipher. In: Helleseth, T., ed. Advances in Cryptology-Eurocrypt'93. Berlin: Springer-Verlag, 1994. 371~385.

[9] Daemen, J., Govaerts, R., Vandewalle, J. Weak keys for IDEA. In: Stinson, D. R., ed. Advance in Cryptology-Crypto'93. New York: Springer-Verlag, 1994. 224~231.

[10] Borst, J., Knudsen, L., Rijmen V. Two attacks on reduced IDEA (extendec abstract). In: Anderson, R., ed. Advance in Cryptology-Eurocrypt'97. Berlin: Springer-Verlag, 1997. 1~13.

[11] Philip Hawkes. Differential-Linear weak key classes of IDEA. In: Preneel, B., ed. Advance in Cryptology-Eurocrypt'98. Berlin: Springer-Verlag, 1998. 112~126.

[12] Biham, A. B., Shamir, A. Miss in the middle attacks on IDEA, Khufu and Khafre. Fast Software Encryption, LNCS 1636, Berlin: Springer-Verlag, 1999. 212~221.

[13] Rijmen, V., Daemen, J. The cipher SHARK. Fast Software Encryption, LNCS 1039, Berlin: Springer-Verlag, 1996. 99

~111.

[14] Nyberg, K., Kundsen, L. Provable security against differential cryptanalysis. Journal of Cryptology, 1995,8(1):156~168.

[15] Matsui, M. New structure of block ciphers with provable security against differential and linear cryptanalysis. Fast Software Encryption, LNCS 1039, Berlin: Springer-Verlag, 1996. 205~217.

[16] Matsui, M. New block encryption algorithm MISTY. Fast Software Encryption, LNCS 1267, Berlin: Springer-Verlag, 1997. 54~68.

[17] Mitsuru, Matsui. Linear cryptanalysis method for DES Cipher. In: Helleseth, T., ed. Advances in Cryptology-Eurocrypt'93. Berlin: Springer-Verlag, 1993. 386~397.

[18] Knudsen, L.R. Truncated and higher order differentials. Fast Software Encryption, LNCS 1008, New York: Springer-Verlag, 1995. 196~211.

[19] Aoki, K., Ichikawa, T., Kanda, M., *et al*. Specification of Camellia—a 128bit Block Cipher. In: Proceedings of the 17th Annual Workshop on Selected Areas in Cryptography SAC'2000, 2000.

[20] NTT-Nippon Telegraph and Telephone Corporation. E2-Efficient Encryption algorithm. http://info.isl.ntt.co.jp/e2

[21] Kanda, M. Practical security evaluation against differential and linear attacks for Feistel ciphers with SPN round function. In: Proceedings of the 17th Annual Workshop on Selected Areas in Cryptography SAC'2000. 2000.

[22] FIPS 180-1. Secure Hash Standard, Federal Information Processing Standards Publication (FIPS PUB) 180. U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, 1993.

[23] Kaliski, B.S., Yin, Y.L. On differential and linear cryptanalysis of the RC5 encryption algorithm. In: Coppersmith, D., ed. Advances in Cryptology-Crypto'95, Lecture Notes in Computer Science 963. Berlin: Springer-Verlag, 1995. 171~184.

[24] Contini, S., Yin, Y.L. On differential properties of data-dependent rotations and their use in MARS and RC6. In: Proceedings of the 2nd Advanced Encryption Standard (AES) Candidate Conference. http://www.dice.ucl.ac.be/crypto/CAESAR/caesar.html.

[25] Massey, J. SAFER K-64: a byte-oriented block-ciphering algorithm. Fast Software Encryption, Lecture Notes in Computer Science 809, 1994. 1~17.

[26] Massey, J. On the optimality of SAFER+ diffusion. In: Proceedings of the 2nd Advanced Encryption Standard (AES) Candidate Conference. http://www.dice.ucl.ac.be/crypto/CAESAR/caesar.html.

Brief Commentary on 21st Century European Data Encryption Standard Candidate Algorithms

WU Wen-ling, HE Ye-ping, FENG Deng-guo, QING Si-han

(*State Key Laboratory of Information Security, Institute of Software, The Chinese Academy of Sciences, Beijing* 100080, *China*); (*Engineering Research Center for Information Security Technology, The Chinese Academy of Sciences, Beijing* 100080, *China*)

E mail: wwl@ercist.iscas.ac.cn

Received November 30, 2000; accepted December 12, 2000

Abstract: In this paper, the basic design ideas, recent analysis results and validity of the 17 NESSIE (new european schemes for signatures, integrity, and encryption) candidate algorithms are introduced.

Key words: AES (advanced encryption standard); NESSIE (new European schemes for signatures, integrity, and encryption); encryption; decryption; key