简评欧洲密码大计划的发展现状*)

张文涛　吴文玲　卿斯汉

(中国科学院软件研究所　北京 100080)　(中国科学院信息安全技术工程研究中心　北京 100080)

On Current Development of NESSIE Block Cipher Candidates

ZHANG Wen-Tao　WU Wen-Ling　QING Si-Han

(Institute of Software, Chinese Academy of Sciences, Beijing 100080, China)

(Engineering Research Center for Information Security Technology, Chinese Academy of Sciences, Beijing 100080, China)

Abstract　At the 2nd NESSIE workshop on 12-13 September 2001, NESSIE gives the selection of 7 primitives from 17 block cipher candidates for further evaluation in Phase II. In this paper, the NESSIE evaluation criteria is introduced, the reason of each candidate for selection or not is explained, furthermore, analysis results for each block cipher candidate are listed.

Keywords　NESSIE(New European Schemes for Signatures, Integrity, and Encryption), Block cipher, Evaluation criteria

1. 引言

NESSIE (New European Schemes for Signatures, Integrity, and Encryption)是一个为时三年的密码大计划,它的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。它的整个运作过程是公开透明的,2000 年 3 月公布了征集通告,2000 年 11 月 13～14 日,召开第一次 NESSIE 会议,并公布征集到的所有算法。NESSIE 共征集 17 个分组密码算法,经过一年多的评估,在今年 9 月 12～13 日召开的第二次 NESSIE 会议上,NESSIE 公布了评选出的 7 个算法:IDEA, Khazad, MISTY1, SAFER ++, Camellia, RC6, SHACAL,它们将作为 NESSIE 计划下一阶段重点评估的对象。NEESIE 预计将在明年秋季召开第三次会议,届时将宣布最后的评选结果。本文简要介绍 NESSIE 的评估原则,阐述 NESSIE 对各个候选算法的取舍原因,同时列出算法设计者和公众对各个算法的分析情况。

2. NESSIE 的评估原则

NESSIE 在征集通告[1]中给出了评估的三条基本准则:

(1)对算法的攻击应和强力攻击一样困难。

(2)对算法安全性的评估结果要和设计者宣称的安全程度相一致。如果存在一种攻击,实施它需要的计算资源比设计者宣称的要少,这会表明设计者提交的算法不合格;

(3)算法要在各种特定的环境下进行评估。这样,算法抵抗时间攻击和能量分析的能力也要考虑在内。

在对算法进行评估及对算法做取舍时,NEESIE 重点考查以下几项:

(1)算法抵抗现有攻击的能力。算法应能很好地抵抗现有的所有攻击,如密钥穷搜索攻击、差分攻击、截断差分攻击、不可能差分攻击、高阶差分攻击、线性攻击、模 n 攻击、相关密钥攻击、插值攻击、滑行攻击、飞来去器攻击、平方攻击等。

(2)算法的设计思想和设计的透明性。在评估时,设计清楚、直接、基于充分研究过的数学和密码学原则的算法,更容易得到信任。

(3)对算法的变形进行评估。比如说,改变或删除算法的一个模块,减少迭代的轮数等。对变形的分析可以间接地推论得到关于原算法的一些结论。

(4)在相同的运行环境中对各算法的安全性加以比较。NESSIE 宣称尽力保证公平地评估每一个算法。

(5)算法的统计测试结果。分析统计测试的结果,其目的是查看算法的密码学特性有无突出的异常现象。

3. 17 个分组密码的评估结果

3.1 64 比特分组密码

64 比特的算法中被选取做为第二阶段重点评估的算法有:

IDEA、Khazad、MISTY1、SAFER ++$_{64}$。没有被选取的有:CS-Cipher、Hierocrypt-L1、Nimbus。

到目前为止,没有关于 IDEA, Khazad, MISTY1 安全性存在问题的报道。世界各地的专家学者对 IDEA 进行了 10 年的深入分析,至今没有发现它存在严重的弱点和漏洞;MISTY1 已经被公开分析了 5 年,对它最好的攻击是对 5 轮 MISTY1 的一个攻击,而设计者建议的轮数是 8 轮;Khazad 借用了 AES 的一些设计思想,这使它在 64 比特分组长度的算法中有一定的吸引力。

没有关于 CS-Cipher 安全性存在问题的报道,但是它的执行速度是所有 64 比特算法中最慢的一个;Hierocrypt-L1 速度很慢,密钥编排算法中存在弱点,3.5 轮算法可以被攻击;对于 Nimbus 算法,只需要 2^8 个明密文对和 2^{10} 的时间复杂度,就可以破译整个算法。

下面我们分别简述各个算法的分析结果。

*)本文研究得到国家自然科学基金项目(No. 60103023, 60083007)和 973 项目(No. G1999035810)支持。张文涛　在读博士生,主要研究方向为分组密码的分析与设计。

3.1.1 CS-Cipher 其用户选择密钥长度是128比特，总体结构采用SP网络，建议轮数为8轮。

设计者对算法的分析：以相互独立的随机取值替换CS算法中的常数和轮子密钥，设计者证明了[2,3]这样得到的变形算法能抵抗线性和差分攻击。设计者称该结果可以应用于实际的CS算法，16/3轮的CS算法就可抵抗线性和差分攻击。

现有攻击和弱点：我们对CS算法的变形进行了分析，结果将发表在电子学报上。

3.1.2 Hierocrypt-L1 其用户选择密钥长度为128比特，总体结构采用SP网络，建议轮数为6轮。

设计者对算法的分析：设计者称[4]6轮Hierocrypt-L1抵抗差分和线性攻击，平方攻击最多只对2.5轮算法有效，截断差分最多可攻击5轮算法。在第二届NESSIE Workshop上，设计者[5]还给出了算法最好的差分和线性包的上界，对于4轮Hierocrypt-L1，两者概率的上界均是2^{-48}。

现有攻击和弱点：对Hierocrypt-L1的平方攻击[6]可以增加到3或3.5轮。

文[7]给出了Hierocrypt系列算法的密钥扩展算法中的一个弱点：在主密钥和一些轮子密钥之间存在线性关系。

3.1.3 IDEA 其用户选择密钥长度为128比特，总体结构采用半Feistel结构，建议轮数为8.5轮。

设计者对算法的分析：IDEA自1991年提出后，对它的攻击没有超过4.5轮的。在向NESSIE提交的文件中，已知的分析结果[8~12]都得到了引用。

现有攻击和弱点：文[13]给出了对2.5轮IDEA的一个平方攻击。

3.1.4 Khazad 其用户选择密钥长度是128比特，总体结构采用SP网络，建议轮数是8轮。它的设计类似SHARK密码。

设计者对算法的分析：两轮Khazad的差分特征的概率小于2^{-45}，线性逼近的优势小于$2^{-20.7}$。设计者还称Khazad抵抗插值攻击、飞来去器攻击、截断差分攻击。

现有攻击和弱点：对最大线性逼近优势的计算上有错误，但这并不影响算法的安全性。除此之外，没有对Khazad的攻击结果公布。

3.1.5 MISTY1 其用户选择密钥长度是128比特，总体结构采用Feistel网络，在每两轮之前嵌入与密钥相关的线性函数FL，建议轮数是8轮。

设计者对算法的分析：设计者称MISTY1抵抗差分和线性分析；5轮以上的不包含FL函数的MISTY1抵抗高阶差分攻击；抵抗不可能差分攻击、相关密钥攻击；滑动攻击只对2^{16}个密钥有效[14~16]。

现有攻击和弱点：文[17]给出了对5轮不包含FL函数的MISTY1的高阶差分攻击；基于滑动攻击，文[18]给出了对不包含FL函数的MISTY1的一个相关密钥攻击，该攻击仅对2^{16}个密钥有效。文[19]给出了对4轮MISTY1的一个攻击，这是目前对不包含FL的MISTY1的最好攻击。

3.1.6 Nimbus 其用户选择密钥长度是128比特，总体结构是5轮，每一轮影响整个数据字。

设计者对算法的分析：设计者称Nimbus抵抗差分攻击、线性攻击、插值攻击、不可能差分攻击、饱和攻击(saturation attack)和相对密钥攻击。

现有攻击和弱点：存在两个对于乘法运算的概率为1/2的迭代差分，运用它们中的任何一个，都可以得到一个概率为1/2的一轮Nimbus迭代差分特征。把这个差分特征迭代5次，就得到一个概率为2^{-5}的5轮差分特征。运用它，以256个明-密文对，2^{10}的复杂度就可以破译整个Nimbus算法[20]。

3.2 128比特分组密码

分组长度为128比特或更高的算法被选中做为第二阶段重点评估的有：

Camellia、RC6。没有被选中的有：Grand Cru、Noekeon、Q、Hierocrypt-3、SC2000、Anubis。

到目前为止，没有关于Camellia，RC6安全性存在问题的报道。

Grand Cru的设计基于AES算法，但它的速度在候选算法中是很慢的一个；对于Q算法，存在比穷搜索密钥攻击更快的攻击；Noekeon的两种密钥编排算法都存在许多相关密钥；Hierocrypt-3的密钥编排算法也有弱点，并且，存在对3.5轮算法的攻击；SC2000采用了Feistel结构和SP网络相结合的设计方案，采用这种结构的优点还不是很清楚；Anubis和AES十分相似，从对它的分析，它也没有显著地比AES更好的特性。

3.2.1 Grand Cru 其用户选择密钥长度是128比特，总体结构采用SP网络，建议轮数为10轮。

设计者对算法的分析：Grand Cru以Rijndeal为基础，采用多层安全策略(strategy of multiple layered security)的设计思想。该策略在一个密码算法中使用不同安全强度的子密码，如果算法还有一个子密码没有被破译，那这个算法仍然是安全的。设计者称破译Grand Cru的方法也可以破译Rijndeal。

现有攻击和弱点：没有对Grand Cru的分析结果公布。

3.2.2 Noekeon 其用户选择密钥长度是128比特，总体结构采用SP网络，建议轮数为16轮。

设计者对算法的分析：设计者称Noekeon抵抗差分和线性攻击，4轮的线性相关系数不大于2^{-24}，4轮的差分概率不大于2^{-48}。Noekeon还抵抗截断差分和插值攻击。

现有攻击和弱点：文[21]的作者指出对于Noekeon，存在许多相关密钥，和这些密钥相对应，一些特定的明文差分以很大概率导致与密钥无关的特定密文差分。并指出，满足设计者提出的设计准则的6/7的S盒会导致相应的分组密码算法易于受差分或者线性攻击。

3.2.3 Hierocrypt-3 其用户选择密钥长度可以是128、192或256比特，总体结构采用SP网络，建议轮数为6、7或8轮(依赖于密钥大小)。

设计者对算法的分析：设计者称保守估计Hierocrypt-3是抵抗差分和线性攻击的。密钥长度是128比特时，平方攻击最多只对2轮算法有效，密钥长度是128比特时，平方攻击最多对2.5轮算法有效。截断差分最多可攻击5轮算法。在第二届NESSIE Workshop上，设计者[5]还给出了算法最好的差分和线性包的上界，对于4轮Hierocrypt-3，两者概率的上界均是2^{-96}。

现有攻击和弱点：对Hierocrypt-3的平方攻击可以增加到3.5轮[4]。

文[7]给出了Hierocrypt系列算法的密钥扩展算法中的一个弱点：在主密钥和一些轮子密钥之间存在线性关系。

文[22]利用$2^{87.5}$个明-密文对，$2^{117.5}$次3轮*Hierocrypt-3*的加密，给出了对3轮Hierocrypt-3的一个不可能差分攻击。

3.2.4 Q 其用户选择密钥长度可以是不大于256比

特的任意长度，总体结构采用 SP 网络，建议轮数为 8.5 轮。

设计者对算法的分析：设计者称算法迭代 7 轮以后没有概率大于 2^{-120}的差分，不存在对整个 Q 算法的差分攻击，对于线性攻击也有同样的结论。还称算法抵抗相关密钥攻击、滑动攻击、Davies-murphy 攻击、飞来去器攻击、逼近攻击和不可能差分攻击。

现有攻击和弱点：在 NESSIE 评测过程中，发现了 Q 的一个有较高概率的差分，这个差分被用来破译了整个 Q 算法[23]。我们在对 Q 的研究中发现，用线性密码分析攻击它比强力攻击有效[24]。同时国外同行也给出了对 Q 的一个线性攻击[25]。

3.2.5 RC6 其用户选择密钥长度可以是 128、192 或 256 比特，总体结构采用广义 Feistel 网络，建议轮数为 20 轮。

设计者对算法的分析：设计者对 RC6 做了大量分析[26~29]，称 12 轮后的 RC6 抵抗差分攻击，最多 16 轮后的 RC6 抵抗线性攻击。

现有攻击和弱点：文[30,31]描述了利用明文比特和密文比特间的相关性可以攻击 15 轮的 RC6。值得注意的是：如果把算法中的数据依赖循环用特定的非零固定循环移位替代，上述攻击的效率就会降低许多。比如，对于 w =32 的 RC 6 版本，如果循环移位取某常数 d(5<d<27)，则上述攻击就不能起作用。

把轮函数以随机函数替代，文[32]指出这样的 4 轮 RC 6 的变形不是伪随机的。

3.2.6 SC2000 其用户选择密钥长度是 128、192 或 256 比特，总体结构采用混合 Feistel 和 SP 网络，建议轮数为 6.5 或 7.5 轮。

设计者对算法的分析：设计者称 5 轮 SC2000 就可抵抗差分和线性攻击。文[33]中，设计者又给出了概率更高的差分特征。

现有攻击和弱点：文[34,35]给出了对 3.5 轮 SC2000 的攻击。文[34]给出了两个概率分别为 2^{-106}和 2^{-107}的 3.5 轮差分特征，这些差分特征的概率比在文[13]中公布的要高。利用它们，可以得到 4.5 轮 SC2000 一个变形的第一轮和最后一轮密钥的 32 个比特位。文[35]给出了对 3.5 轮 SC2000 的一个变形的攻击。

3.2.7 Anubis 其用户选择密钥长度是可变的，但最少 128 比特，总体结构采用 SP 网络，轮数与密钥长度有关(最少 12 轮)。

设计者对算法的分析：设计者称没有概率大于 2^{-125}的 4 轮差分特征存在，没有概率大于 $2^{-57.5}$的 4 轮线性逼近偏差存在。Anubis 抵抗相关密钥攻击、插值攻击和飞来去器攻击，截断差分攻击最多只对 6 轮算法有效。饱和攻击(saturation attack)也最多只对 6 轮算法有效，该饱和攻击需要 $6*2^{32}$个明密文对，2^{24}比特的存储空间(不包括明密文对的存储空间)，时间复杂度相当于 $6*2^{48}$个 S-盒查表运算。设计者还称用 Gilbert-Minier 攻击可以攻击到 7 轮 Anubis，需要 2^{32}个明密文对和 2^{140}次 S-盒查表运算。不可能差分攻击可以攻击到 5 轮 Anubis，需要 $2^{29.5}$个明密文对，时间复杂度相当于 2^{31}个 S-盒查表运算。

现有攻击和弱点：设计者在对线性逼近偏差的计算中有个小错误，但这似乎并不影响算法的安全性。除此以外，没有关于对 Anubis 的其它弱点或者攻击的报道。

3.2.8 Camellia 其用户选择密钥长度可以是 128、192 或 256 比特，总体结构采用基本的 Feistel 结构，每隔六轮再嵌入一个可逆函数 FL，建议轮数为 18 轮。

设计者对算法的分析：设计者称，Camellia 抵抗差分和线性攻击。12 轮 Camellia 的差分和线性特征的概率不高于 2^{-128}，10 轮 Camellia(无论是否嵌入 FL 函数)与一个随机置换抵抗截断差分攻击的能力相当，不包含 FL 函数的算法抵抗线性包分析。设计者还称该算法抵抗不可能差分攻击、飞来去器攻击、高阶差分攻击、相关密钥攻击和滑行攻击。

现有攻击和弱点：存在概率为 2^{-52}的 3 轮迭代差分特征，利用它，可以攻击不包含 FL 函数的 9 轮 Camellia。存在一个一轮截断差分特征，利用它，可以构造一个概率为 2^{-112}的不含 FL 函数的 8 轮截断差分，如果包含 FL 函数，则相应的概率减为 2^{-120}。

文[36]给出了对不包含 FL 函数的 10 轮 Camellia 的一个高阶差分攻击。文[37]给出了对 6 轮 Camellia 的一个平方攻击，该攻击所需时间复杂度比上面的高阶差分攻击要大，但它所需的明密文对要少。文[38]中给出了 Camellia 的两个 9 轮截断差分，利用它们，可以攻击到 11 轮不含 FL 函数的 Camellia。另外，该文作者还给出了一个 7 轮不可能差分。

3.3 160 比特分组的密码

Shacal 的分组长度是 160 比特，密钥长度可以是 512 或更少比特，但最少 128 比特，总体是 4 轮结构，每轮 20 个步骤。

设计者对算法的分析：设计者研究了该算法抵抗差分和线性分析的能力。声称对该算法的线性攻击至少需要 2^{80}个已知明密文对，对该算法的差分攻击则至少需要 2^{116}个已知明密文对。

现有攻击和弱点：没有发现大的弱点。

3.4 分组长度可变的密码

分组长度可变的密码有 NUSH 和 SAFER ++，NUSH 没有入选，而 SAFER ++入选。NUSH 的线性攻击要比穷搜索有效。SAFER $++_{64}$是 SAFER $++_{128}$经过一些改变得到的，SAFER 系列密码在对它的分析和攻击中不断得到改进，它的安全性也经过了时间的考验。到目前为止，没有关于 SAFER ++安全性存在安全问题的报道。

3.4.1 NUSH 其分组长度可以是 64、128 或 256 比特，用户选择密钥长度可以是 128、192 或 256 比特，建议轮数是 9、68 或 132 轮(对应于分组长度)。

设计者对算法的分析：设计者向 NESSIE 提交的文件中，称 NUSH 抵抗差分、线性攻击、相关密钥攻击等，没有弱密钥，没有给出其详细分析。

现有攻击和弱点：文[39]给出了对不同分组长度 NUSH 算法的线性攻击。

3.4.2 SAFER ++ 传统版本的 SAFER ++分组长度是 64 比特，密钥长度是 128 比特，总体结构采用 SP 网络，建议轮数为 8 轮。常规版本的 SAFER ++分组长度是 128 比特，密钥长度可以为 128 或 256 比特，总体结构采用 SP 网络，建议轮数是 7 轮或 8 轮(依赖于密钥长度)。

设计者对算法的分析：设计者称 6 轮 SAFER 抵抗差分攻击，2.5 轮 SAFER 抵抗线性攻击。

现有攻击和弱点：文[40]给出了对 4 轮 SAFER ++的线性攻击。我们在对 SAFER ++的研究[42]发现，5 轮 SAFER ++对非线性密码分析是不免疫的。这些攻击不影响算法的安全性，但它说明该算法抵抗线性攻击的能力没有

设计者宣称的那么高。

结束语 NESSIE 计划引起了世界范围的广泛关注，我们研究小组跟踪它的发展，并在整个计划中有针对性地开展我们的工作。本文简要介绍 NESSIE 的评估原则，阐述 NESSIE 对各个候选算法的取舍原因，同时列出算法设计者和公众对各个算法的分析情况。目的是让国内了解 NESSIE 的发展现状以及我们的工作。

参 考 文 献

1 NESSIE. http://www.cryptonessie.org

2 Stern J, Vaudenay S. CS-CIPHER, Fast Software Encryption, Springer-Verlag, 1998. 189～205

3 Vaudenay S. On the Security of CS-cipher, Fast Software Encryption. Springer-Verlag, 1999. 260～274

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

5 Ohkuma K, Shimizu H, Sano F, Kawamura S. Security assessment of Hierocrypt and Rijndael against the differential and linear cryptanalysis. In: Proc. of the 2nd NESSIE workshop, 2001

6 Barreto P S L M, Rijmen V, Nakahara J Jr, Preneel B. Improved SQUARE attacks against reduced HIEROCRYPT. Fast Software Encryption, 2001

7 Furuya S, Rijmen V. Observations on Hierocrypt-3/L1 Key Scheduling Algorithms. In: Proc. of the 2nd NESSIE workshop, 2001

8 Meier W. On the security of the IDEA block cipher. Advance in Cryptology-Eurocrypt '93, 1994. 371～385

9 Daemen J, Govaerts R, Vandewalle J. Weak keys for IDEA. Advance in Cryptology -Crypto '93, 1994. 224～231

10 Borst J, Knudsen L, Rijmen V. Two attacks on reduced IDEA (extended abstract). Advance in Cryptology-Eurocrypt '97, 1997. 1～13

11 Hawkes P. Differential-linear weak key classes of IDEA. Adv. in Cryptology -Eurocrypt '98, 1998. 112～126

12 Biham, Biruykov A, Shamir A. Miss in the middle attacks on IDEA. Khufu and Khafre, Fast Software Encryption, Springer-Verlag, 1999. 212～221

13 Nakahara Jr J, et al. Square attacks on reduced -round PES and IDEA block ciphers. In: Proceedings of the 2nd NESSIE workshop, 2001

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, Springer-Verlag, 1996. 205～217

16 Matsui M. New Block Encryption Algorithm MISTY, Fast Software Encryption, Springer-Verlag, 1997. 54～68

17 Tanaka H, Hisamatsu H, Kaneko K. Higher order differential attack of MISTY1 without FL functions. JWIS'98, 1998

18 Furuya S, Takaragi K. Slide attacks combined with known-plaintext attacks. SCIS 2000, 2000

19 Kuhn U. Cryptanalysis of reduced-round MISTY. Adv. in Cryptology -Eurocrypt 2001, LNCS 2045, 2001. 325～339

20 Furman V. Differential Cryptanalysis of Nimbus. Fast Software Encryption, 2001

21 Knudsen L R, Raddum H. On Noekeon. In: Proceedings of the 2nd NESSIE workshop, 2001

22 Cheon J H, Kim M J, Kim K. Impossible differential cryptanalysis of Hierocrypt-3 reduced to 3 rounds. In: Proceedings of the 2nd NESSIE workshop, 2001

23 Biham E, Furman V, Misztal M, Rijmen V. Differential cryptanalysis of Q. In: Proc. of the 2nd NESSIE workshop, 2001

24 吴文玲、Q 分组密码的线性分析：[中国科学院信息安全技术工程研究中心技术报告]

25 Keliher L, Merjer H, Tavares S. High probability linear hulls in Q. In: Proc. of the 2nd NESSIE workshop, 2001

26 Contini S, Rivest R L, Robshaw M J B, Yin Y L. The Security of the RC6 block cipher. www.rsa.com/rsalabs/aes/

27 Contini S. Rivest R L, Robshaw M J B, Yin Y L. Some comments on the first round AES evaluation of RC6. http://csrc.nist.gov/encryption/aes/round1/pubcmnts.htm

28 Contini S, Rivest R, Robshaw M J B, Yin Y L. Improved analysis of some simplified variants of RC6. Fast Software Encryption, 1999. 1～15

29 Rivest R L, Robshaw M J B, Sidney R, Yin Y L. the RC6 block cipher, v1. 1. www.rsa.com/rsalabs/aes/

30 Knudsen L R, Meier W. Correlations in RC6 with a reduced number of rounds. Fast Software Encryption, 2000, LNCS 1978. 94～108

31 Gilbert H, Handschuh H, Joux A, Vaudenay S. A statistical attack on RC6. Fast Software Encryption, 2000, LNCS 1978. 64～74

32 Iwata T, Kurosawa K. On the pseudorandomness of the AES finalists-RC6 and Serpent. Fast Software Encryption, 2000, LNCS 1978. 231～243

33 Shimoyama T, Yanami H, Yokoyama K, et al. The Block Cipher SC2000. In: Proc. of FSE2001, 2001

34 Knudsen L, Raddum H. A differential attack on reduced-round SC2000. In: Proc. of the 2nd NESSIE workshop, 2001

35 Dunkelman O, Keller N. Boomerang and rectangle attacks on SC2000. NES/DOC/TEC/WP3/014/1

36 Kawabata T, Kaneko T. A study on higher order differential attack of Camellia. In: Proc. of the 2nd NESSIE workshop, 2001

37 He Yeping, Qing Sihan. Square attack on reduced Camellia Cipher. ICICS01

38 Sugita M, Kobara K, Imai H. Security of reduced version of the block cipher Camellia against truncated and impossible defferential cryptanalysis. AsiaCrypt 2001, 2001

39 WU Wen-ling, FENG Deng-guo. linear cryptanalysis of NUSH block cipher. SCIENCE IN CHINA(Series F), 2001, 44(6): 1～9

40 Preneel B, Nakahara Jr J, Vandewalle J. Linear cryptanalysis of reduced-round SAFER ++. In: Proc. of the 2nd NESSIE workshop, 2001

41 吴文玲，卿斯汉．CS-CIPHER 两个变体的线性密码分析．电子学报，2002(2)

42 吴文玲，马恒太，唐柳英，卿斯汉．5 轮 SAFER++的非线性密码分析：[中国科学院信息安全技术工程研究中心技术报告]