文章编号: 1001- 2486(2010) 04- 0137- 04

对特殊类型 Feistel 密码的 Square 攻击*

张 鹏[1], 孙 兵[1], 李 超[1,2]
(1. 国防科技大学 理学院, 湖南 长沙 410073; 2. 信息安全国家重点实验室, 北京 100190)

摘 要: 对轮函数为 SP 结构的两类特殊类型 Feistel 密码抗 Square 攻击的能力进行了研究。通过改变轮函数中 P 置换的位置从而给出了此类 Feistel 密码的等价结构, 以 SNAKE(2) 和 CLEFIA 为例, 给出了基于等价结构 Square 攻击的具体过程, 将 6 轮 SNAKE(2) 的 Square 攻击的时间复杂度由 2^{24} 降为 $2^{13.4}$; 将 6 轮 CLEFIA 的 Square 攻击的时间复杂度由 $2^{34.4}$ 降为 $2^{12.4}$。结果表明, 在设计轮函数为 SP 结构的 Feistel 密码时, 必须充分考虑等价结构对算法抗 Square 攻击的影响。

关键词: Feistel 密码; Square 攻击; 等价结构; SNAKE(2); CLEFIA
中图分类号: TN918 文献标识码: A

Square Attack on Some Special Feistel Ciphers

ZHANG Peng[1], SUN Bing[1], LI Chao[1,2]
(1. College of Science, National Univ. of Defense Technology, Changsha 410073, China;
2. State Key Laboratory of Information Security, Beijing 100190, China)

Abstract: Securities of two special Feistel ciphers with SP-structured round functions against Square attack were studied. By changing the position of P permutation of the round functions in an equivalent manner, some new cryptanalytic results of round-reduced SNAKE(2) and CLEFIA were presented. Time complexity of Square attack against 6-round SNAKE(2) was reduced from 2^{24} to $2^{13.4}$, and for 6-round CLEFIA, time complexity of Square attack was reduced from $2^{34.4}$ to $2^{12.4}$. The results show that, in designing Feistel ciphers with SP-structured round functions, influence of equivalent structures and Square attack should be taken into consideration.

Key words: feistel cipher; square attack; equivalent structures; SNAKE(2); CLEFIA

分析各种分组密码算法的安全性一直是密码设计中的重点问题。Square 攻击[1] 是 Daemen 等针对类 Square 密码算法提出的一种攻击方法, 在 FSE2002 上, Knudsen 和 Wagner 在总结 Square 攻击[1]、Saturation 攻击[2] 和 Multiset 攻击[3] 的基础上, 提出了积分攻击[4]。利用上述攻击思想, 人们分析了许多著名密码算法的安全性。在 SAC2005 上, Duo 等提出了基于等价结构的 Square 攻击[5], 从而改进了 Camellia 的 Square 攻击, 推广了 Square 攻击的方法, 但作者并没有对基于等价结构的 Square 攻击做系统的研究。

1 特殊类型 Feistel 密码的等价结构

1.1 PKS 型 Feistel 密码的等价结构

PKS 类 Feistel 结构的 F 函数由密钥加、S 盒和 P 置换构成, 不妨设 F 函数的具体结构为 $P \rightarrow K \rightarrow S$, 其中, P、K、S 分别表示 P 置换、密钥加和 S 盒运算, 具体流程见图 1。

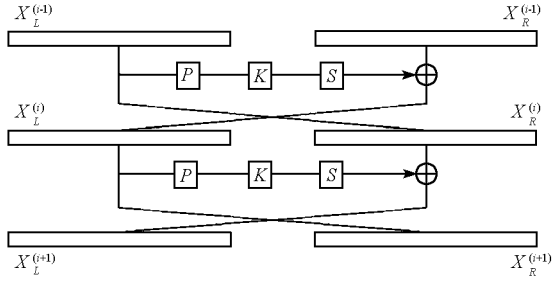

图 1 PKS 型 Feistel 密码的两轮加密示意图
Fig. 1 Two-round Encryption of PKS Feistel Cipher

等价结构Ⅰ: 若 F 函数的具体结构为 $P \rightarrow K \rightarrow S$, 设 F 函数的输入为 X, 则其输出为

$$F(X) = S(P(X) \oplus K) = S(P(X \oplus P^{-1}(K)))$$

* 收稿日期: 2009- 09- 08
基金项目: 国家自然科学基金资助项目(60803156); 信息安全国家重点实验室开放基金资助项目(01- 07)
作者简介: 张鹏(1983—), 男, 博士生。

$$= S(P(X \oplus K^*))$$

其中, $K^* = P^{-1}(K)$, 于是利用等价密钥原结构可以等价为: $K^* \rightarrow P \rightarrow S$, 为了对比的方便, 不妨将该结构记为: $K \rightarrow P \rightarrow S$($K$ 为等价密钥), 具体流程见图2(Ⅰ)。

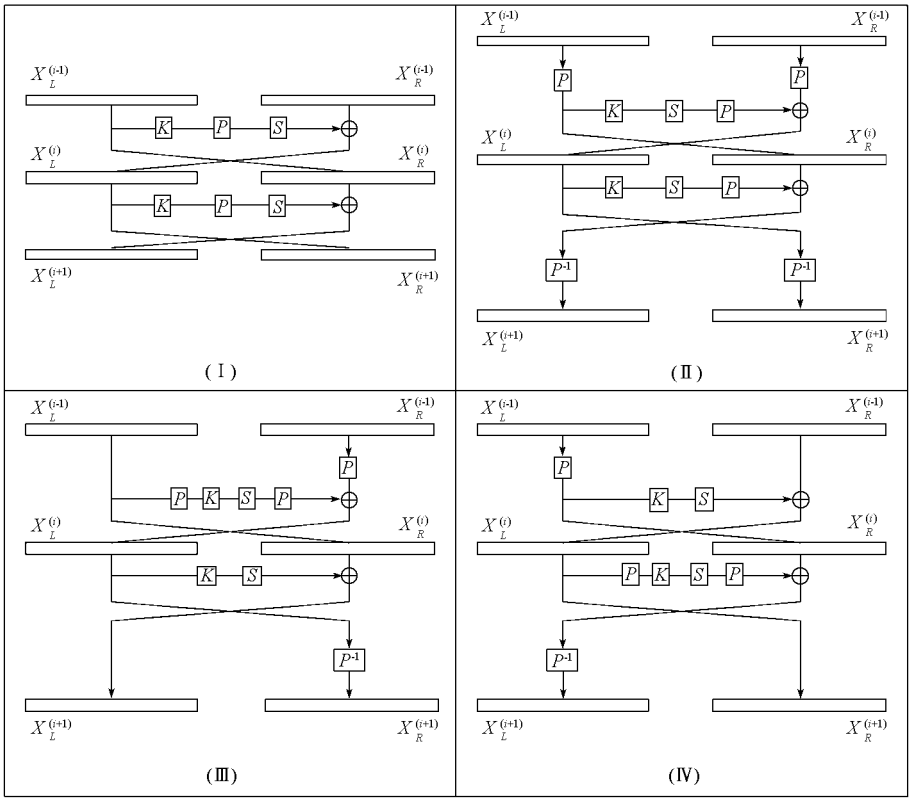

图 2 PKS 型 Feistel 密码的等价结构示意图

Fig. 2 Equivalent structures of PKS feistel cipher

等价结构Ⅱ, Ⅲ, Ⅳ: Duo 等提出了 Camellia 算法的等价结构[5], 下面将给出 PKS 型 Feistel 结构的三个等价结构, 等价结构的具体流程见图 2(Ⅱ, Ⅲ, Ⅳ)。

定理 1 原 PKS 型 Feistel 密码(图 1 所示)与其等价结构Ⅱ, Ⅲ, Ⅳ等价。

证明: 这里只给出原密码与等价结构Ⅱ等价的证明。

设 $X_L^{(i)}$、$X_R^{(i)}$ 分别表示 $P \rightarrow K \rightarrow S$ 型 Feistel 密码中第 i 轮输出的左右两部分, $X_L^{(i)*}$、$X_R^{(i)*}$ 分别表示等价结构Ⅱ中第 i 轮输出的左右两部分, $K^{(i)}$ 表示第 i 轮的密钥。

令 $X_L^{(i-1)} = X_L^{(i-1)*}$, $X_R^{(i-1)} = X_R^{(i-1)*}$, 则在原 $P \rightarrow K \rightarrow S$ 密码中, 有

$$X_L^{(i)} = X_R^{(i-1)} \oplus S(P(X_L^{(i-1)}) \oplus K^{(i)}); \quad X_R^{(i)} = X_L^{(i-1)};$$

$$X_L^{(i+1)} = X_R^{(i)} \oplus S(P(X_L^{(i)}) \oplus K^{(i+1)}) = X_L^{(i-1)} \oplus S(P(X_L^{(i)}) \oplus K^{(i+1)}); X_R^{(i+1)} = X_L^{(i)}$$

在等价结构Ⅱ中, 有

$$X_L^{(i)*} = P(X_R^{(i-1)*}) \oplus P(S(P(X_L^{(i-1)*}) \oplus K^{(i)})) = P(X_R^{(i-1)} \oplus S(P(X_L^{(i-1)}) \oplus K^{(i)})) = P(X_L^{(i)});$$

$$X_R^{(i)*} = X_L^{(i-1)*} = X_L^{(i-1)} = X_R^{(i)};$$

$$X_L^{(i+1)*} = X_R^{(i)*} \oplus S(X_L^{(i)*} \oplus K^{(i+1)}) = X_R^{(i)} \oplus S(P(X_L^{(i)}) \oplus K^{(i+1)}) = X_L^{(i+1)};$$

$$X_R^{(i+1)*} = P^{-1}(X_L^{(i)*}) = X_L^{(i)} = X_R^{(i+1)}$$

因此, 对任意相同的输入原密码与等价结构Ⅱ均能得到相同的加密结果, 即原密码与等价结构Ⅱ等价, 同理可证原密码与其它等价结构等价, 证毕。

1.2 PKS型广义 Feistel 密码的等价结构

CLEFIA[6] 密码是在 FSE 2007 上提出的一个分组密码算法。算法采用了广义 Feistel 结构。为叙述

问题的方便, 这里不考虑算法的白化密钥, 算法的具体加密流程见图 3。其中, $X_3^{(i)} \| X_2^{(i)} \| X_1^{(i)} \| X_0^{(i)}$ 表示第 i 轮的输出; K_1、K_2 表示两侧的密钥加; S_1、S_2 表示两侧的总的 S 盒运算; P_1、P_2 表示两侧的 P 置换运算。

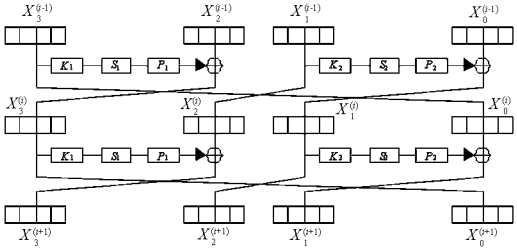

图 3　CLEFIA 第 i 和 $i+1$ 轮的加密流程图
Fig. 3　Two-round encryption of CLEFIA

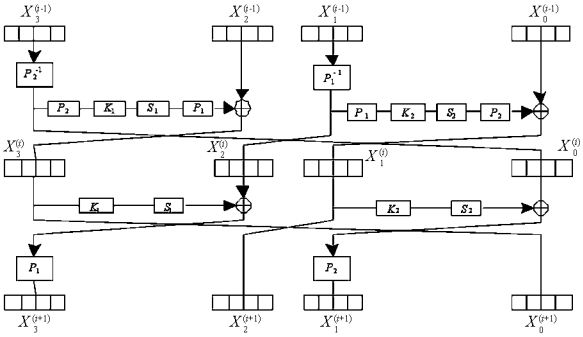

图 4　CLEFIA(Ⅱ)第 i 和 $i+1$ 轮的加密流程图
Fig. 4　Two-round encryption of CLEFIA(Ⅱ)

显然, CLEFIA 是一类特殊的 PKS 型 Feistel 密码, 利用 1.1 节中的方法, 可以得出其等价结构, 这里只给出一个能较好改进其 Square 攻击的等价结构, 不妨记为 CLEFIA(Ⅱ), 具体流程见图 4。等价的证明过程与定理 1 的证明类似, 这里不再详述。

定理 2　CLEFIA 与 CLEFIA(Ⅱ)等价。

2　基于等价结构的 Square 攻击

2.1　PKS 型 Feistel 密码的改进 Square 攻击

SNAKE 算法[7] 是 Lee 等学者在 JW-ISC' 97 上提出的一个 Feistel 型分组密码, 在提交的算法中, 设计者设计了两种版本: SNAKE(1) 和 SNAKE(2)。SNAKE(2) 采用的即是 1.1 节中所述的 $K \overrightarrow{\ } P \overrightarrow{\ } S$ 型 Feistel 结构, 其轮函数具体流程见图 5(a)。其等价的 $P \overrightarrow{\ } K \overrightarrow{\ } S$ 型结构见图 5(b), 其中 $K_3^* \| K_2^* \| K_1^* \| K_0^* = P(K_3 \| K_2 \| K_1 \| K_0)$, 即 $K_3^* \| K_2^* \| K_1^* \| K_0^*$ 为等价密钥。为了叙述方便, 以下仍用 $K_3 \| K_2 \| K_1 \| K_0$ 表示等价密钥。

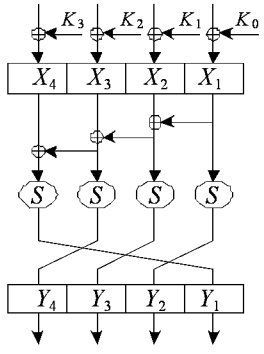

图 5(a)　SNAKE(2) 算法轮函数
Fig. 5(a)　Round Function of SNAKE(2)

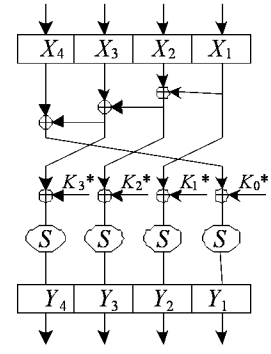

图 5(b)　SNAKE(2) 算法等价轮函数
Fig. 5(b)　Equivalent Round Function of SNAKE(2)

原结构中的轮函数为 $K \overrightarrow{\ } P \overrightarrow{\ } S$ 型结构, 验证猜测密钥时, 密钥后面有 P 置换进行扩散, 因此会使复杂度大大增加, 如果采用等价的 $P \overrightarrow{\ } K \overrightarrow{\ } S$ 型结构, 则每个字节均可单独验证相应的密钥字节, 因此攻击时将 $K \overrightarrow{\ } P \overrightarrow{\ } S$ 型结构等价成 $P \overrightarrow{\ } K \overrightarrow{\ } S$ 型结构, 会使复杂度大大降低。

此外, 在寻找 SNAKE(2) 的 Square 区分器时, 如果采用等价结构 III, 区分器输出的平衡字节会由原结构的一个增加到四个, 从而可以大大降低其 Square 攻击的复杂度, 区分器具体形式如下:

利用原结构得到的区分器(a): $(C,C,C,C,A,C,C,C) \xrightarrow{5\ round} (?,?,?,?,?,?,?,A,?)$;

基于等价结构(Ⅱ)的区分器(b): $(C,C,C,C,A,A,C,C) \xrightarrow{5\ round} (?,?,?,?,\Delta,A,A,A)$

其中, A 表示活跃字节, 且区分器(b)明文中的两个活跃字节取相同的值进行遍历; C 表示稳定字节, 即为常数; Δ 表示平衡字节; ? 表示字节的性质无法预测。

利用区分器(a)进行攻击时, 得到第 6 轮的轮密钥需要的时间复杂度为: $(2^8 \times 2^8)/(4\times 6) + 2^{24} \approx 2^{24}$; 利用区分器(b)进行攻击时, 得到第 6 轮的轮密钥需要的时间复杂度为: $4\times(2^8 \times 2^8)/(4\times 6) \approx 2^{13.4}$。可见利用基于等价结构的区分器进行攻击, 能大大降低攻击的复杂度。

2.2 PKS型广义 Feistel 密码的改进 Square 攻击

以CLEFIA 为例给出PKS 型广义Feistel 密码基于等价结构的Square 攻击, 文献[8] 对CLEFIA 进行了比较详细的安全性分析, 并给出了基于字节的5 轮Square 区分器(见图6(a)), 如果将区分器的最后两轮换成等价结构 CLEFIA(Ⅱ), 则可以得到一个新的5 轮 Square 区分器(见图6(b)); 利用区分器(a)进行攻击时, 得到第 6轮的轮密钥 K_1 需要的时间复杂度为: $[(2^8)^4\times 2^8 + (2^8)^3\times 2^8 + (2^8)^2\times 2^8 + 2^8\times 2^8]/(8\times 6) \approx 2^{34.4}$; 利用区分器(b)进行攻击时, 得到第 6 轮的轮密钥 K_1 需要的时间复杂度为: $4\times(2^8\times 2^8)/(8\times 6) \approx 2^{12.4}$, 可见利用基于等价结构的区分器进行攻击, 能大大降低攻击的复杂度。

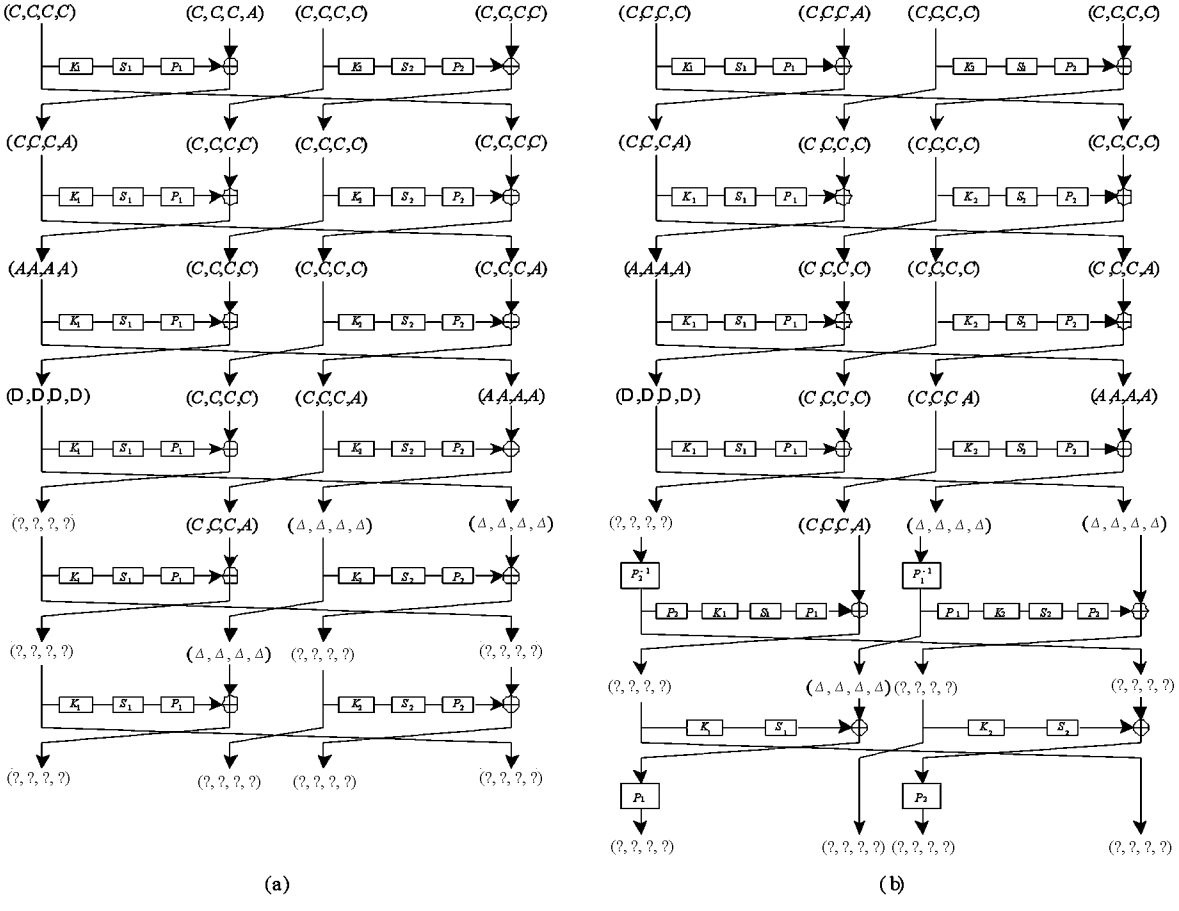

图 6 CLEFIA 及其等价结构基于字节的 5 轮 Square 区分器

Fig. 6 Five-round square distinguishers of CLEFIA and CLEFIA(Ⅱ)

此外, 在 CLEFIA 的高阶积分攻击中, 如果将区分器的最后两轮换成等价结构, 采用上述方法, 也可以大大降低攻击的时间复杂度, 具体攻击过程不再详述。

(下转第 149 页)

显然 ξ_1, ξ_2 是不饱和维, ξ_3 是饱和维, ξ_4, ξ_5 是超饱和维。用本文提到的信息维的增减技术将关联子空间各元素统一到四维, 取权重列 $\delta=(0.2, 0.3, 0.3, 0.2)$, 这里略去计算过程而直接给出结果:

$$\gamma(\xi_0, \xi_1)=0.15,\ \gamma(\xi_0, \xi_2)=0.16,\ \gamma(\xi_0, \xi_3)=0.18,\ \gamma(\xi_0, \xi_4)=0.21,\ \gamma(\xi_0, \xi_5)=0.17$$

由此得到聚焦序列: $\xi_0 \leftarrow \xi_4 \leftarrow \xi_3 \leftarrow \xi_5 \leftarrow \xi_2 \leftarrow \xi_1$。

3　讨 论

(1) 由于信息获取技术的复杂性及关联度计算的柔性环境, 由式(11)确定的接近 ξ_0 的序列 ξ_{i_1}, ξ_{i_2}, ξ_{i_3} …, ξ_{i_n} 的序关系非唯一, 它符合灰色系统"解是非唯一"的思想, 也是信息获取技术逐步深入的体现;

(2) 将本体思想引入到元数据模型中来[1], 建立基于本体的元数据模型, 提出一种面向语义内容的更为全面的信息资源描述方式, 为关联度分析的可操作和可实现提供了一种系统、完整的思路;

(3) 仙农信息熵是信息领域中广泛使用的一种度量信息的方法, 用拓扑结构来描述信息空间, 在此基础上建立基于信息熵的分层、分维的信息度量空间, 折射出这种聚焦方法的可行性和应用前景。

参 考 文 献:

[1] 黄宏斌. 基于语义关系的× × 信息资源聚焦服务方法及关键技术研究[D]. 长沙: 国防科技大学, 2007.

[2] Feng L S, Yi L. On Measure of Information Content of Grey Numbers[J]. The International Journal of Systems & Cybernetics, 2006, 35(6): 1256 – 1264.

[3] 汪小龙. 信息获取科学的若干问题研究[D]. 合肥: 中国科技大学, 2003.

[4] Papazoglou M P, Proper H A, Yang J. Landscaping the Information Space of Larg Multi-database Networks[J]. Data and Knowledge Engineering, 2001, 36(3): 251– 281.

[5] 腾书华, 周石琳, 孙即祥, 等. 基于条件熵的不完备信息系统属性约简算法[J]. 国防科技大学学报, 2010, 32(1): 90– 94.

[6] 罗党, 刘思峰. 不完备信息系统的灰色关联决策方法[J]. 应用科学学报, 2005, 23(4): 57– 60.

[7] 刘思峰, 谢乃明. 灰色系统理论及应用[M]. 北京: 科学出版社, 2008.

(上接第 140 页)

3　结 论

本文通过对两类特殊类型 Feistel 密码等价结构的详细刻画和分析, 给出了基于等价结构的改进 Square 攻击。并分别以SNAKE(2)和 CLEFIA 为例, 给出了基于等价结构 Square 攻击的具体过程。攻击结果表明, 等价结构可大大降低特殊类型Feistel 密码 Square 攻击的时间复杂度, 从而能较好地改进这两类Feistel 密码的 Square 攻击。

参 考 文 献:

[1] Daemen J, Knudsen L, Rijmen V. The Block Cipher Square[C]// FSE 1997, LNCS 1267: 149– 165.

[2] Lucks S. The Saturation Attack-a Bait for Twofish[C]// FSE 2001, LNCS 2355: 1– 15.

[3] Biryukov A, Shamir A. Structural Cryptanalysis of SASAS[C]// EUROCRYPT 2001, LNCS 2229: 394– 405.

[4] Knudsen L, Wagner D. Integral Cryptanalysis[C]// FSE 2002, LNCS 2365: 112– 127.

[5] Duo L, Li C, Feng K. New Observation on Camellia[C]// SAC 2005, LNCS 3897: 51– 64.

[6] Shirai T, Shibutani K, Akishita T, et al. The 128-Bit Blockcipher CLEFIA[C]// FSE 2007, LNCS 4593: 181– 195.

[7] Lee C, Cha Y. The Block Cipher: SNAKE with Provable Resistance Against DC and LC Attacks[C]// JW– ISC 97, 1997: 3– 17.

[8] The 128-Bit Blockcipher CLEFIA: Security and Performance Evaluation[R]. Sony Corporation, Revision 1.0, June 1, 2007.