SNAKE(2)算法新的Square攻击

郑雅菲[1] 卫宏儒[1,2]

(北京科技大学数理学院 北京 100083)[1] (信息安全国家重点实验室 北京 100083)[2]

摘 要 重新评估了分组密码SNAKE(2)算法抵抗Square攻击的能力。指出文献[4]中给出的基于等价结构的错误5轮Square区分器。综合利用算法原结构与其等价结构,给出了一个新的6轮Square区分器。利用新的区分器,对不同轮数的SNAKE(2)算法应用了Square攻击来恢复部分等价密钥信息,7轮、8轮、9轮SNAKE(2)算法的Square攻击时间复杂度分别为$2^{12.19}$、$2^{21.59}$、$2^{30.41}$次加密运算,数据复杂度分别为2^{9}、$2^{9.59}$、2^{10}选择明文。攻击结果优于文献[4]中给出的Square攻击。

关键词 SNAKE,Square攻击,区分器,复杂度

中图法分类号 TP309 **文献标识码** A

New Square Attack on SNAKE (2)

ZHENG Ya-fei[1] WEI Hong-ru[1,2]

(School of Mathematics and Physics, University of Science and Technology Beijing, Beijing 100083, China)[1]

(State Key Laboratory of Information Security, Beijing 100083, China)[2]

Abstract The security of block cipher SNAKE (2) against Square attacks was re-evaluated. The wrong 5-round Square distinguisher based on equivalent structure given in paper [4] was pointed out. A new 6-round Square distinguisher based on both the structure of SNAKE (2) and its equivalent structures was proposed. Using the new 6-round Square distinguisher, Square attack was applied to 7,8,9-round SNAKE(2) to recover some information of the equivalent key. The time complexities are $2^{12.19}$, $2^{21.59}$, $2^{30.41}$ respectively, and the data complexities are 2^{9}, $2^{9.59}$, 2^{10} respectively. The results are better than the Square attack given by paper[4].

Keywords SNAKE, Square attack, Distinguisher, Complexity

1 引言

SNAKE(2)算法是由Lee等学者在JW-ISC1997上提出的一个Feistel型分组密码,有SNAKE(1)和SNAKE(2)两个版本。SNAKE算法对差分分析、线性分析是可证明安全的,且对高阶差分攻击和插值攻击是免疫的[1,2]。孙兵等分析了SNAKE(2)算法抵抗不可能差分攻击的能力,利用算法的9轮不可能差分,对简化轮数的SNAKE应用了不可能差分攻击[3]。张鹏等利用SNAKE(2)的等价结构构造了5轮区分器,对6轮SNAKE(2)算法应用了SQUARE攻击,攻击的时间复杂度为$2^{13.4}$[4]。2012年魏悦川等人对简化轮数的SNAKE(2)算法应用了中间相遇攻击,结果显示9轮的SNAKE(2)算法对中间相遇攻击是不抵抗的,且攻击为现实攻击[5]。

Square攻击是由Daemen等人在FSE1997上提出的针对类Square密码算法的攻击方法,是继差分密码分析与线性密码分析后公认的比较有效的密码分析方法[6];Duo等人在SAC2005上提出了基于等价结构的Square攻击,推广了Square攻击的应用[7]。2010年张鹏等人对轮函数为SP结构的两种特殊类型Feistel密码抗Square攻击的能力进行了研究,以SNAKE(2)与CLEFIA为例,介绍了其等价结构且给出了基于等价结构Square攻击的具体过程。同年,张鹏等人重新评估了Zodiac算法抵抗Square攻击的能力,通过构造基于等价结构的9轮区分器,对不同轮数的Zodiac算法实施了Square攻击,给出了完整16轮Zodiac算法不抵抗Square攻击的结论。目前Square攻击已广泛应用于分组密码,在对Camellia、CLEFIA、HIGHT、3D、Zodiac等密码的安全性分析中都得到了较好的攻击结果[8-11]。

本文重新评估SNAKE(2)算法抵抗Square攻击的能力。在等价结构的基础上构造一个新的6轮Square区分器,利用该区分器对7、8、9轮的SNAKE(2)算法应用Square攻击。本文第2节对符号表示与SNAKE(2)算法进行简单介绍;第3节介绍KPS型Feistel密码的4种等价结构;第4节改正文献[4]中给出的错误5轮Square区分器,并描述SNAKE(2)算法新的6轮Square区分器,给出基于该区分器对不同轮数SNAKE(2)算法的Square攻击;最后总结全文。

到稿日期:2013-04-22 返修日期:2013-08-10 本文受信息安全国家重点实验室2011年开放课题(02-04-3),内蒙古自治区科技创新引导奖励资金(2012)资助。

郑雅菲(1988—),女,硕士,主要研究方向为密码学,E-mail:zhengyafei111@sina.com;卫宏儒(1963—),男,副教授,主要研究方向为数学、信息安全与密码学、物联网关键技术研究。

2 SNAKE(2)算法

2.1 符号表示

本文中使用的主要符号说明如表1所列。

表1 符号说明

符号	说明
$L_i=(X_{i,1}X_{i,2}X_{i,3}X_{i,4})\in(F_2^8)^4$	第i轮输出的左半部分
$R_i=(X_{i,5}X_{i,6}X_{i,7}X_{i,8})\in(F_2^8)^4$	第i轮输出的右半部分
$K_i=(k_{i,1},k_{i,2},k_{i,3},k_{i,4})\in(F_2^8)^4$	第i轮的轮密钥
$K_i^*=(k_{i,1}^*,k_{i,2}^*,k_{i,3}^*,k_{i,4}^*)\in(F_2^8)^4$	第i轮的等价轮密钥

2.2 SNAKE(2)算法简介

SNAKE是Feistel型分组密码，算法有4个参数(m,s,w,r)，其中m为S盒的输入输出比特数，s表示轮函数中S盒的个数，w表示算法的分组长度，r表示算法的轮数。本文研究针对SANKE(2)算法，参数的具体值为：$m=8,s=4,w=64$。算法由迭代r次轮变换构成，设第i轮的输入为(L_{i-1},R_{i-1})，轮密钥为K_i，则轮变换：

$L_i=R_{i-1}\oplus F(L_{i-1}\oplus K_i);R_i=L_{i-1}$

轮函数F如图1所示，将(X_1,X_2,X_3,X_4)映射为(Y_1,Y_2,Y_3,Y_4)：

$Y_1=S(X_1\oplus X_2\oplus X_3\oplus X_4)$

$Y_2=S(X_1)$

$Y_3=S(X_1\oplus X_2)$

$Y_4=S(X_1\oplus X_2\oplus X_3)$

S为有限域上的逆函数。

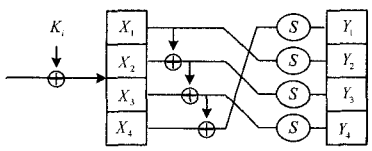

图1 SNAKE(2)算法轮函数

本文不涉及SANKE(2)算法S盒具体非线性性质与其密钥扩展的影响，故不进行介绍，其详细内容可参见文献[1,12]。

3 SNAKE(2)算法的等价结构

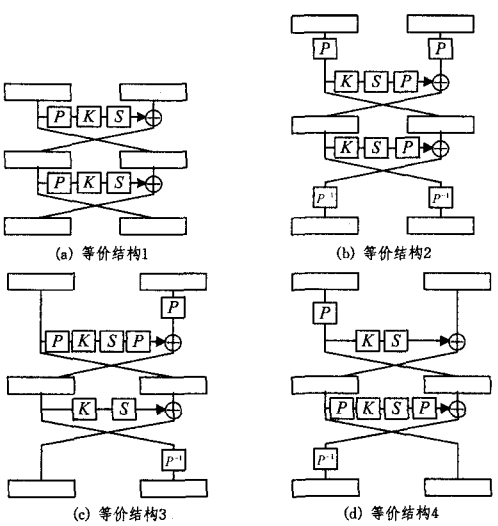

图2 SNAKE(2)算法的4种等价结构

与Zodiac算法相同，SNAKE(2)算法也属于KPS型Feistel密码，故可得到SNAKE(2)算法与Zodiac算法相同的4种等价结构，其具体流程见图2(a)、2(b)、2(c)、2(d)。文献[11]中给出了结构1和3等价的证明，同理可证结构1与2、4等价。

本文使用等价结构1和3，其中等价结构3应用于新的6轮区分器的构造，等价结构1应用于猜测密钥过程。

4 基于等价结构的新的Square攻击

文献[4]给出了SNAKE(2)算法的两个5轮区分器，即基于SNAKE(2)算法原结构得到的区分器：

$(CCCCACCC)\xrightarrow{5r}(??????A?)$

基于等价结构(3)得到的区分器：

$(CCCCAACC)\xrightarrow{5r}(????BAAA)$

其中，A表示活跃字节，C表示固定字节，B表示平衡字节，?表示字节的性质无法预测。利用上述两个区分器攻击6轮SNAKE(2)算法，得到第6轮的轮密钥的时间复杂度分别为2^{24}、$2^{13.4}$。通过推导，其中区分器$(CCCCAACC)\xrightarrow{5r}(????BAAA)$是错误的，满足形式为$(CCCCAACC)$的明文经过5轮加密后，无法在输出的第5个字节处保持平衡字节的性质，正确的5轮区分器形式应为：

$(CCCCAACC)\xrightarrow{5r}(?????AAA)$

4.1 SNAKE(2)算法新的6轮区分器

本文构造一个新的基于等价结构(3)与原结构两种形式的6轮区分器：

$(CCCCCCCCAA)\xrightarrow{6r}(?????B??)$

利用该区分器对7、8、9轮的SNAKE(2)算法实施Square攻击，结果表明本文构造的6轮区分器优于改正后文献[4]中给出的5轮区分器。

SNAKE(2)算法新的6轮Square区分器的具体形式见表2。当区分器的输入形式为$(CCCC,CCAA)$时，采用等价结构3，可得一轮加密后的输出形式$(CCCA,CCCC)$、两轮加密后的输出形式$(CCCA,CCCA)$、三轮加密后的输出形式$(AAAB,CCCA)$、四轮加密后的输出形式$(AAA?,ABBB)$；接着采用算法原结构，则五轮加密后的输出形式为$(?B??,AAA?)$，六轮加密后的输出形式为$(????,?B??)$。即当用表2所列的结构来表示等价的6轮SNAKE(2)算法时，则可得到表2中SNAKE(2)算法的一个新的6轮区分器：$(CCCCCCAA)\xrightarrow{6r}(?????B??)$。

表2 SNAKE(2)算法新的6轮区分器

$(L\|R)$	CCCC	轮函数	$CCCA\xrightarrow{P^{-1}}CCAA$
$(L_0\|R_0)$	CCCC	$P\to K_1^*\to S\to P$	CCCA
$(L_1\|R_1)$	CCCA	$K_2^*\to S$	CCCC
$(L_2\|R_2)$	CCCA	$P\to K_3^*\to S\to P$	CCCA
$(L_3\|R_3)$	AAAB	$K_4^*\to S$	CCCA
$(L_4\|R_4)$	AAA?	$K_5\to P\to S$	$AAAB\xrightarrow{P^{-1}}ABBB$
$(L_5\|R_5)$	?B??	$K_6\to P\to S$	AAA?
$(L_6\|R_6)$	????		?B??

4.2 不同轮数SNAKE(2)算法的Square攻击

利用新的6轮Square区分器$(CCCCCCAA)\xrightarrow{6r}(?????B??)$攻击7(或8)轮SNAKE(2)算法，需在等价结构后加1(或2)轮，选取满足形式为$(c_1,c_2,c_3,c_4,c_5,c_6,x,x)$的明文，其中$c_i,i=1,2,\cdots8$为任意常数，$x$表示遍历$F_2^8$，且满足$x\oplus$

$c_7=x\oplus c_8$。对选择明文加密得到7(或8)轮后的密文,猜测轮密钥并解密密文得到 $X_{6,6}$,通过验证 $X_{6,6}$ 的平衡性来排除错误密钥。不同轮数 Square 攻击需猜测的密钥字节见表3。

表3 不同轮数 Square 攻击需猜测的密钥

轮数		需猜测密钥
7	后加1轮(等价结构1)	$k^*_{7,2}$
8	后加2轮(等价结构1)	$k^*_{7,2}$,$k^*_{8,1}$
9	前加1轮,后加2轮(等价结构1)	$k^*_{1,1}$,$k^*_{8,2}$,$k^*_{9,1}$

下面,以基于上述6轮 Square 区分器的8轮 Square 攻击为例,详细介绍 Square 攻击的具体步骤及其复杂度的计算。

1)首先选取满足形式为$(c_1,c_2,c_3,c_4,c_5,c_6,x,x)$的明文组,并对其进行8轮加密,得到相应密文。由6轮区分器可知,第6轮输出的 $X_{6,6}$ 应为平衡字节。

2)猜测等价轮密钥 $k^*_{7,2}$,$k^*_{8,1}$,利用得到的相应密文和猜测密钥计算得第6轮输出:

$$X_{6,6}=X_{7,2}\oplus S(X_{7,5}\oplus k^*_{7,2})=X_{8,6}\oplus S(X_{8,1}\oplus S(X_{8,5}\oplus X_{8,6}\oplus X_{8,7}\oplus X_{8,8}\oplus k^*_{8,1})\oplus k^*_{7,2})$$

3)验证 $X_{6,6}$ 的平衡性,若满足,猜测密钥 $k^*_{7,2}$,$k^*_{8,1}$ 为正确密钥候选值,否则排除错误密钥。

4)重复上述步骤,直到得到唯一正确密钥。

Square 攻击分析8轮 SNAKE(2)算法需猜测 $k^*_{7,2}$,$k^*_{8,1}$ 2个字节共16比特密钥,错误密钥满足 $X_{6,6}$ 的平衡性的概率为 2^{-8},因此经过一次筛选后剩余错误密钥数为$(2^{16}-1)\times 2^{-8}\approx 2^8$,故3个明文组即可淘汰所有的错误密钥,攻击的数据复杂度即为 $3\times 2^8=2^{9.59}$ 选择明文。

对每个密钥猜测值,计算 $X_{6,6}$ 需要2次 S 盒求逆运算,故攻击共需 $2^{16}\times 2^{9.59}\times 2=2^{26}$ 次 S 盒逆运算,8轮 SNAKE(2)加密共有 $8\times 4=32$ 次 S 盒运算,因此8轮 SNAKE(2)算法 Square 攻击的时间复杂度为:

$$2^{16}\times 2^{9.59}\times\frac{2}{32}=2^{21.59}$$

同理可对7轮 SNAKE(2)算法应用基于6轮区分器的 Square 攻击,需猜测等价密钥 $k^*_{7,2}$,共一个字节8比特密钥,错误密钥满足 $X_{6,6}$ 的平衡性的概率为 2^{-8},因此经过一次筛选后剩余错误密钥数为$(2^8-1)\times 2^{-8}<1$,故2个明文组即可淘汰所有的错误密钥,攻击的数据复杂度即为 $2\times 2^8=2^9$ 选择明文。

对每个密钥 $k^*_{7,2}$ 的猜测值,计算 $X_{6,6}$ 需要1次 S 盒求逆运算,故攻击共需 $2^8\times 2^9\times 1=2^{17}$ 次 S 盒逆运算,7轮 SNAKE(2)加密共有 $7\times 4=28$ 次 S 盒运算,因此7轮 SNAKE(2)算法 Square 攻击的时间复杂度为:

$$2^8\times 2^9\times\frac{1}{28}=2^{12.19}$$

同理,Square 攻击分析9轮 SNAKE(2)算法,首先在6轮区分器前端加1轮,猜测第一轮等价密钥 $k^*_{1,4}$,并计算明文组的形式为:

$$(c_1',c_2',x,x,c_5',c_6',c_7',S(x\oplus c_8'\oplus k^*_{1,4}))$$

其中,c_i' 为常数,若 $k^*_{1,4}$ 的猜测值正确,则区分器的输入应满足6轮区分器的输入形式:

$$(c_1,c_2,c_3,c_4,c_5,c_6,x,x)$$

则第7轮相应的输出字节 $X_{7,6}$ 为平衡字节。对满足条件的明文组进行9轮加密,得到第9轮相应的密文,猜测密钥 $k^*_{8,2}$,$k^*_{9,1}$,对得到的密文进行部分解密,求得第7轮的输出字节 $X_{7,6}$:

$$X_{7,6}=X_{8,2}\oplus S(X_{8,5}\oplus k^*_{8,2})=X_{9,6}\oplus S(X_{9,1}\oplus S(X_{9,5}\oplus X_{9,6}\oplus X_{9,7}\oplus X_{9,8}\oplus k^*_{9,1})\oplus k^*_{8,2})$$

Square 攻击9轮 SNAKE(2)的过程如图3所示。

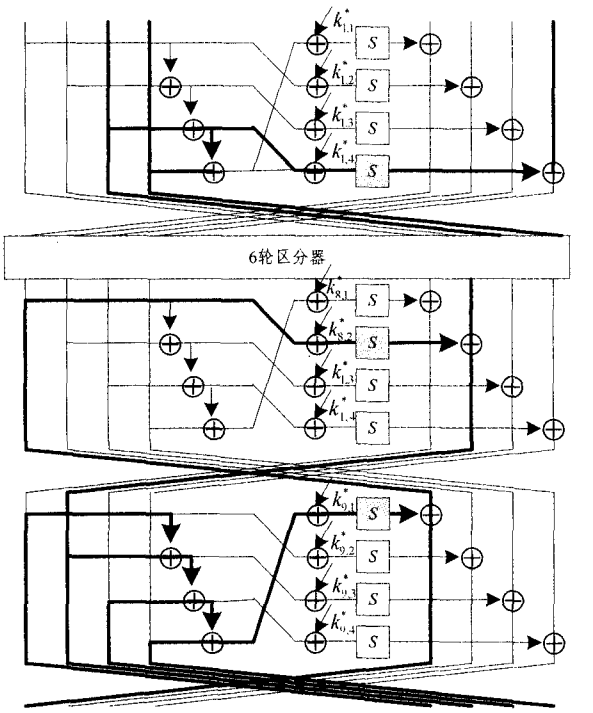

图3 对不同轮数 SNAKE(2)算法的 Square 攻击

检验 $X_{7,6}$ 是否满足平衡性,若满足,则猜测的 $k^*_{1,4}$,$k^*_{8,2}$,$k^*_{9,1}$ 为正确密钥值,若不满足,舍弃错误密钥。重复上述过程,直到得到唯一正确密钥。

Square 攻击分析9轮 SNAKE(2)算法需猜测3个字节共24比特密钥,错误密钥满足 $X_{7,6}$ 的平衡性的概率为 2^{-8},因此经过一次筛选后剩余的错误密钥数为$(2^{24}-1)\times 2^{-8}\approx 2^{16}$,故4个明文组即可淘汰所有的错误密钥,攻击的数据复杂度即为 $4\times 2^8=2^{10}$ 选择明文。

对每个密钥猜测值,计算 $X_{7,6}$ 需要3次 S 盒求逆运算,则攻击共需 $2^{24}\times 2^{10}\times 3=2^{35.58}$ 次 S 盒逆运算,9轮 SNAKE(2)加密共有 $9\times 4=36$ 次 S 盒运算,因此9轮 SNAKE(2)算法 Square 攻击的时间复杂度为:

$$2^{24}\times 2^{10}\times\frac{3}{36}=2^{30.41}$$

总结 SNAKE(2)算法7、8、9轮 Square 攻击的复杂度,如表4所列。观察表4可发现,与文献[5]的攻击结果相比,本文攻击不需要预计算复杂度,且计算复杂度优于其预计算复杂度。

表4 SNAKE(2)算法不同轮数 Square 攻击的复杂度

轮数	时间复杂度	数据复杂度	预计算复杂度	
6	$2^{13.4}$	—	—	文献[4]
7	$2^{12.19}$	2^9	—	本文
7	2^6	7	2^{32}	文献[5]
8	$2^{21.59}$	$2^{9.59}$	—	本文
8	2^{14}	8	2^{32}	文献[5]
9	$2^{30.41}$	2^{10}	—	本文
9	2^{22}	$2^{11.2}$	2^{32}	文献[5]

结束语 本文对 SNAKE(2)算法抵抗 Square 攻击的能

(下转第180页)

Kalman 滤波的方法来检测流量矩阵的异常，然后检测路由器端口是否受到 DDoS 攻击。实验结果表明该方法不仅具有较高的检测率、较低的漏报率，还在检测延迟上具有较大优势。该方法易于获取流量矩阵，也减轻了路由器的流量采集负担，因此具有一定的实用价值。目前该方法仅在仿真实验数据上进行了实验，对于真实网络环境中的流量数据是否具有同样效果是今后的研究内容。由于 P-P flow 可直接从路由器中的 Netflow 记录中统计得到，而不需要考虑多个路由器之间的数据包路由，因此它比 OD flow 更易于实时采集，也易于将该方法推广到大规模网络环境，针对多个关键路由器进行分布式检测，这也是今后的研究重点。

参 考 文 献

[1] Peng T, Leckie C, Rramaohanarao K. Protection from distributed denial of service attacks using history-based IP filtering[C]// Proceedings of the International Conference on Communication (ICC). Anchorage: IEEE, 2003: 482-486

[2] Pu S. Choosing parameters for detecting DDoS attack[C]// Proceedings of the International Conference on Wavelet Active Media Technology and Information Processing. Chengdu: IEEE Computer Society, 2012: 239-242

[3] Chen Y H, Wang K, Ku W S. Collaborative detection of DDoS attacks over multiple network domains[J]. IEEE transactions on parallel and distributed systems, 2007, 18(12): 1649-1662

[4] 莫家庆，胡忠望，林瑜华. 非参数 PCUSUM 算法 DDoS 攻击检测[J]. 计算机工程与应用，2011，47(22)：96-98

[5] 任勋益，王汝传，王海艳. 基于自相似检测 DDoS 攻击的小波分析方法[J]. 通信学报，2006，27(5)：6-11

[6] Thapngam T, Yu S, Zhou W L. DDoS discrimination by linear discriminant analysis (LDA)[C]// Proceedings of the 2012 International Conference on Computing, Networking and Communications (ICNC). Maui: IEEE Computer Society, 2012: 532-536

[7] Xia Z M, Lu S N, Li J H. DDoS flood attack detection based on fractal parameters[C]// Proceedings of the 8th International Conference on Wireless Communications, Networking and Mobile Computing. Shanghai, IEEE, 2012: 1-5

[8] Lakhina A, Papagiannaki K, Crovella M, et al. Structural analysis of network traffic flow[C]// Proceedings of the SIGMETRICS/Performance. New York: ACM, 2004: 61-72

[9] Lakhina A, Crovella M, Diot C. Diagnosing network-wide traffic anomalies[C]// Proceedings of the SIGCOMM'04. Portland: ACM, 2004: 219-230

[10] Ringberg H, Soule A, Rexford J P, et al. Sensitivity of PCA for traffic anomaly detection[C]// Proceedings of the SIGMETRICS'07. San Diego: ACM, 2007: 109-120

[11] Soule A, Salamatian K, Taft N. Combining filtering and statistical methods for anomaly detection[C]// Proceedings of the USENIX Internet Measurement Conference. Philadelphia: ACM, 2005: 331-344

[12] Cisco IOS NetFlow White Papers [EB/OL]. http://www.cisco.com/en/US/products/ps6601/prod_white_papers_list.html, 2006-08-21

[13] Cisco NetFlow Performance Analysis White Papers [EB/OL]. http://www.cisco.com/en/US/technologies/tk543/tk812/tech-nologies_white_paper0900aecd802a0eb9_ps6601_Products_White_Paper.html, 2007-06-15

[14] Hawkinds D M, Qin P H, Kang C W. The changepoint model for statistical process control [J]. Journal of Quality Technology, 2003, 35(4): 355-366

[15] Moore D, Voelker G M, Savge S. Inferring internet Denial-of-Service activity [J]. ACM Transactions on Computer Systems, 2006, 24(2): 115-139

(上接第 171 页)

力进行了重新评估。改正了文献[4]中给出的基于等价结构的错误 5 轮区分器，并综合利用 SNAKE(2)算法原结构与等价结构，构造了一个新的 6 轮 Square 区分器，基于该区分器对 7、8、9 轮的 SNAKE(2)算法应用了 Square 攻击。文献[4]中的 5 轮 Square 区分器采用一种等价结构，本文通过混合采用两种等价结构获得了新的更好的 6 轮 Square 区分器，基于新的 6 轮区分器的攻击结果好于改正后文献[4]中基于 5 轮区分器的攻击结果。在构造 Square 区分器的过程中灵活应用等价结构可期望得到更好的 Square 等价结构区分器以及更好的分析结果。

参 考 文 献

[1] Lee C, Cha Y. The Block Cipher: SNAKE with Provable Resistance against DC and LC attacks 1997[C]// Proceedings of 1997 Korea-Japan Joint Workshop on Information Security and Cryptology (JWISC'97). 1997: 3-17

[2] Moriai S, Shimoyama T, Kaneko T. Interpolation attacks of the block cipher: SNAKE 1999[J]. Lecture Notes in Computer Science, Fast Software Encryption, 1999, 1636: 275-289

[3] Sun B, Qu L, Li C. Impossible Differential Cryptanalysis of SNAKE-2 2009[C]// International Conference on IEEE Networks Security, Wireless Communications and Trusted Computing, 2009. 2009, 2: 63-66

[4] 张鹏，孙兵，李超. 对特殊类型 Feistel 密码的 Square 攻击[J]. 国防科技大学学报，2010，32(4)：137-140

[5] 魏悦川，孙兵，李超. 对简化轮数的 SNAKE(2)算法的中间相遇攻击[J]. 计算机工程与科学，2012，34(6)：28-31

[6] Daemen J, Knudsen L R, Rijmen V. The block cipher SQUARE [J]// Lecture Notes in Computer Science, Fast Software Encryption, 1997, 1267: 149-165

[7] Lei D, Chao L, Feng K. New observation on Camellia [J]. Lecture Notes in Computer Science, Selected Areas in Cryptography, 2006, 3897: 51-64

[8] 唐学海，李超，谢端强. CLEFIA 密码的 Square 攻击[J]. 电子与信息学报，2009，31(9)：2260-2263

[9] 王美一，唐学海，李超，等. 3D 密码的 Square 攻击[J]. 电子与信息学报，2010，32(1)：157-161

[10] Zhang P, Sun B, Li C. Saturation attack on the block cipher HIGHT[C]// Proceeding of the 8th International Conference on Crytology and Network Security. 2009: 76-86

[11] 张鹏，李瑞林，李超. Zodiac 算法新的 Square 攻击[J]. 电子与信息学报，2010，32(11)：2790-2794

[12] 陈华，吴文玲，冯登国. 提高 S 盒非线性度的有效算法[J]. 计算机科学，2005，32(10)：68-70