文章编号: 1001- 2486(2010) 03- 0139- 05

一种 PUFFIN 类 SPN 型分组密码的积分攻击*

魏悦川[1], 孙 兵[2], 李 超[1,2]
(1. 国防科技大学 计算机学院, 湖南 长沙 410073; 2. 国防科技大学 理学院, 湖南 长沙 410073;

摘 要: PUFFIN 是一个具有 64bit 分组长度、128bit 密钥的 SPN 型分组密码, 为评估其安全性, 从比特的层面分析其平衡性, 构造了 PUFFIN 的 5 轮积分区分器, 并利用高阶积分的思想将 5 轮区分器扩展为 6 轮, 然后对 8 轮 PUFFIN 密码进行攻击。8 轮攻击的数据复杂度为 2^{21}, 时间复杂度为 2^{34}, 空间复杂度为 2^{20}。结果表明, 8 轮 PUFFIN 密码对于给出的攻击是不免疫的。对于线性层为置换的 PUFFIN 类 SPN 型分组密码, 证明了至少存在 3 轮积分区分器, 并给出了寻找该区分器的方法。

关键词: 分组密码; 积分攻击; PUFFIN 密码; 攻击复杂度
中图分类号: TN918 文献标识码: A

An Integral Attack on PUFFIN and PUFFIN-like SPN Cipher

WEI Yue-chuan[1], SUN Bing[2], LI Chao[1,2,3]
(1. College of Computer, National Univ. of Defense Technology, Changsha 410073, China;
2. College of Science, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: PUFFIN is a block cipher with 64-bit block size and 128-bit key size. For evaluating its security, the balance at bit-level was analyzed. A 5-round integral distinguisher was constructed and then extended to a 6-round one based on the theory of higher order integral. By using the 6-round distinguisher, 8-round attack was performed. For 8-round attack, the data complexity, time complexity and space complexity were, and respectively. The result shows that PUFFIN reduced to 8 rounds is not immune to the integral attack. Besides, the cipher with SPN-structure and permutation-linear layer which at least has 3-round integral distinguisher is proved. The result also indicates the method for finding the distinguisher.

Key words: block cipher; integral attack; PUFFIN; attack complexity

分组密码 Rijndael-128 以其高效、安全被确立为美国加密标准(AES)并在应用领域中广泛应用, 然而在一些资源受限领域中, AES 的执行开销相对较大, 故不再适用。近几年, 针对资源受限环境, 密码学者设计了一系列分组密码, 如 TEA[1], mCrypton[2], SEA[3], CGEN[4], HIGHT[5] 等, PUFFIN 密码[6] 也是其中之一, 它主要适用于嵌入式系统, 具有高效率、低消耗的特点。PUFFIN 密码为 SPN 型结构, 分组长度为 64bit, 密钥长度为 128bit, 非线性层由 4×4 的 S 盒并置构成, 线性层为 64bit 置换。设计者称 5 轮 PUFFIN 密码可以扩散完全。

Knudsen 在 FSE2002 中给出了积分攻击的一般原理和方法[7]。积分攻击在分析基于字节设计的密码时非常有效, 它是对 Rijndael、Camellia、CLEFIA 等著名算法的安全性最有效的分析方法之一[8-10]。积分攻击的最主要环节是分析密文的平衡性进而寻找区分器, 通常只需确定算法的变换是满射, 因此传统的积分攻击对于基于比特设计的密码不再有效。针对基于比特设计的密码, Z'aba 等学者提出了基于比特的积分攻击, 通过判断比特位置上的平衡性来寻找区分器[11]。

本文利用基于比特的积分思想, 对 PUFFIN 密码进行分析, 构造了 PUFFIN 密码的 5 轮积分区分器, 并利用高阶积分的思想将其扩展为 6 轮, 利用该区分器对 8 轮 PUFFIN 密码进行了攻击。当 SPN 型分组密码的线性层只有 P 置换时, 即具有 PUFFIN 类结构时, 本文证明了该密码至少存在 3 轮的积分区分器。

* 收稿日期: 2009- 09- 07
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: 魏悦川(1982—), 女, 博士生。

1 符号说明

1.1 PUFFIN分组密码简介

PUFFIN分组密码具有64bit分组长度和128bit密钥长度,由32次轮函数迭代构成。PUFFIN的明文可表示为2维比特数组,有4行16列,64bit向量$p_0, p_1, \cdots, p_{63}$按$a_{0,0}, a_{1,0}, a_{2,0}, a_{3,0}, a_{0,1}, a_{1,1}, a_{2,1}, a_{3,1}$…的顺序映射为16个向量:$\boldsymbol{A}=(a_0, a_1, \cdots, a_{15})$,每个向量为4bit字,$a_j=(a_{0,j}, a_{1,j}, a_{2,j}, a_{3,j})^{\mathrm{T}}(0\leqslant j\leqslant 15)$。轮函数由以下三个变换复合而成。

非线性层γ:由16个4×4的S盒并置而成。S盒的映射取值见表1。

表1 S盒映射(十六进制)

Tab.1 S-box mapping (in Hexadecimal)

输入	0	1	2	3	4	5	6	7	输入	8	9	A	B	C	D	E	F
输出	D	7	3	2	9	A	C	1	输出	F	4	5	E	6	0	B	8

密钥加变换层σ:将64bit的轮密钥K_i用异或运算作用在64bit的状态上。

置换层P64:将64bit的数据进行置换,且置换是自逆的,即P64(P64(i))=i。P64的映射取值见表2。

表2 P64(输入=行×8+列+1)置换表

Tab.2 P64(input=row×8+column+1)

	0	1	2	3	4	5	6	7
0	13	2	60	50	51	27	10	36
1	25	7	32	61	1	49	47	19
2	34	53	16	22	57	20	48	41
3	9	52	6	31	62	30	28	11
4	37	17	58	8	33	44	46	59
5	24	55	63	38	56	39	15	23
6	14	4	5	26	18	54	42	45
7	21	35	40	3	12	29	43	64

一轮迭代过程可以表示为round=P64$\circ\gamma\circ\sigma_{K_r}$。

在PUFFIN的加密过程中,在轮函数迭代之前,首先进行密钥白化,即将明文异或上64bit密钥,然后经过一次P64置换,最后迭代32次轮函数。故加密过程可以表示为:

$$\alpha_{32}[K_0, K_1, \cdots, K_{31}] = \prod_{r=1}^{32}(\mathrm{P64}\circ\gamma\circ\sigma_{K_r})\circ\mathrm{P64}\circ\sigma_{K_0}$$

其中"$\prod$"表示轮函数的复合。由于本文不考虑密钥扩展算法的影响,因此我们不详细介绍密钥扩展算法,相关细节参见文献[6]。

1.2 基于比特的积分思想

Žaba基于比特的积分攻击[11],实际上是一种特殊的计数方法,即通过确定不同元素出现的奇偶次数来确定平衡性。

定义1 N bit序列可以定义为以下5种模式:

(1)常量模式c:序列($q_0q_1\cdots q_{2^n-1}$)中对任意$0\leqslant i\leqslant 2^n-1$,均有$q_i=q_0$。例如8bit序列00000000和11111111。

(2)活跃模式a_i:存在$0\leqslant i\leqslant n-1$,使得在序列($q_0q_1\cdots q_{2^n-1}$)中,$2^i$个"0"和$2^i$个"1"轮流出现,例如$a_1$:11001100。

(3)活跃模式b_i:存在$0\leqslant i\leqslant n-1$,使得在序列($q_0q_1\cdots q_{2^n-1}$)中,$2^i$个"0"或$2^i$个"1"连接着出现,但不一定轮流出现。例如$b_1$:11000011,$b_0$:10000000。

(4)兼容模式d_i:如果一个模式要么是c要么是a_i,我们将其统称为d_i模式。

(5) 平衡模式: 序列($q_0 q_1 \cdots q_{2^n-1}$) 满足$\sum q_i = 0$。

注: 根据定义可知, 若一条序列为 a_i 模式, 则一定为 b_i 模式。在以上描述中除了 b_0 不确定之外, 所有模式都是平衡的。为了容易区分, b_0^* 表示平衡的模式, 不平衡的模式记为 b_0。

容易看出, $a_0 a_1 a_2 \cdots a_{n-1}$的横向排列值可以遍历 $n$bit 序列的2^n 个状态。

性质 1 当 S 盒的输入模式为 $b_{i_0} b_{i_1} \cdots b_{i_{n-1}}$, $i_0, i_1, \cdots i_{n-1}$不同时为 0, 所有的输出比特位置都为 b_j 模式, 其中$j = \min\{i_0, i_1, \cdots i_{n-1}\}$。

2 PUFFIN 密码的 5 轮积分区分器

定理 1 2^4 个选择明文可以将 5 轮PUFFIN 密码与随机置换区分开来。

证明 设输入明文为 $P = (p_{i,j})_{4\times 16} = (p_0, p_1, \cdots, p_{15})$, 将 $p_{12,1}, p_{8,3}, p_{15,0}, p_{4,2}$比特位置分别设置为 a_0 模式, a_1 模式, a_2 模式和 a_3 模式。其他比特位置为常量模式 c。于是$p_{12,1} \| p_{8,3} \| p_{15,0} \| p_{4,2}$的横向排列值可以遍历$\{0,1\}^4$($\|$ 为级联运算) 。按这种方式选择的明文可以表示为:

															2
												0			
				3											
								1							

所有图中标有数字 i 的浅色阴影部分表示a_i 模式, 标有数字 i 的深色阴影部分表示 b_i 模式, 未标注的部分为常量模式。

将选择好的明文经过密钥白化和置换 P64, 由于密钥加运算不影响比特的模式, 故只有 P64 将比特的位置改变。使得第 i 个字的最后一个比特位置上 0 和 1 交替出现 2^i 次, 其中 $0 \leqslant i \leqslant 3$。即前 4 个字的最后一个比特的级联值遍历$\{0,1\}^4$。64 个状态可以表示为:

0	1	2	3												

64 个状态经过非线性层 γ, 当 S 盒的输入为 $ccca_i$ 模式时, 输入共有两个值, 每个值重复 8 次。由于 S 盒是双射, 故输出值的个数仍为 2 个, 并且每个值重复 8 次。但是每个比特位置的值可能交替出现也可能连接出现, 所以可能为模式 c, 也可能为模式 a_i。因此, 输出的形式为 $d_i d_i d_i a_i$ (a_i 也可能位于前 3 个位置) 。由于 a_i 模式和 c 模式均为 b_i 模式, 故输出直接表示为 $b_i b_i b_i b_i$; 当 S 盒的输入为 ccc 模式时, 输出仍然为 ccc 模式。64 个状态可以表示为以下形式, 其中第 0 个字为 $b_0^* b_0^* b_0^* b_0^*$, 第 1~ 3 个字为 $b_i b_i b_i b_i$ 模式, 其他为 ccc 模式。

0	1	2	3												
0	1	2	3												
0	1	2	3												
0	1	2	3												

经过下一个 P64, 每个比特的位置改变, 得到的形式为:

3			0			2						3			2
0		1										0			
	2			3		1					3	1			
							2	1						0	

以上 64 个状态经过第 2 轮的非线性层 γ, 由性质 1 可以得到如下的状态模式:

0	2	1	0	3		1	2	1			3	0		0	2
0	2	1	0	3		1	2	1			3	0		0	2
0	2	1	0	3		1	2	1			3	0		0	2
0	2	1	0	3		1	2	1			3	0		0	2

第 2 轮的 P64 将比特位置改变, 得到第 2 轮的输出。依次进行下去, 可以得到, 第 5 轮 γ 层的输出中有 2 个 4bit 字为平衡的:

?	?	?	?	?	?	?	?	?	?	0	?	?	?	?	0
?	?	?	?	?	?	?	?	?	?	0	?	?	?	?	0
?	?	?	?	?	?	?	?	?	?	0	?	?	?	?	0
?	?	?	?	?	?	?	?	?	?	0	?	?	?	?	0

当 $b_0^* \ b_0^* \ b_0^* \ b_0^*$ 模式经过 S 盒后, 不能判断值的个数时, 无法判断平衡性, 将输出表示为????, 其中“?”表示不平衡的模式或不能确定的模式。此时, 认为平衡性被破坏。以上状态经过第 5 轮 P64 变换后, 8 个平衡比特改变位置。

综上, 选择 2^4 个明文, 5 轮加密后, 所得密文中有 8 个比特位置是平衡的。该区分器可以将 5 轮 PUFFIN 密码与随机置换区分开来。

3 PUFFIN 密码的 6 轮高阶积分区分器

利用高阶积分的思想, 在第一轮之前加上一轮, 将 5 轮积分区分器扩展为 6 轮, 由于置换 P64 不影响平衡性, 故 6 轮区分器等价于 5. 5 轮区分器。

定理 2 设明文为 $P=(p_{i,j})_{4\times 16}=(p_0, p_1, \cdots, p_{15})$, 其中 $p_{0,3} \| p_{1,3} \| p_{2,3} \| p_{3,3} \| p_{1,0} \| p_{3,1} \| p_{4,0} \| p_{5,1} \| p_{6,1} \| p_{7,0} \| p_{8,1} \| p_{9,0} \| p_{10,2} \| p_{13,0} \| p_{14,1} \| p_{15,3}$遍历$\{0,1\}^{16}$, 则 6 轮加密后密文中的平衡比特与 5 轮区分器中的相同。

证明 明文经过密钥白化和线性层后, 第 4、8、12、15 个字的级联遍历$\{0,1\}^{16}$, 设经过第一轮得到的密文为 $c^{(1)}=(c_0^{(1)}, \cdots, c_{15}^{(1)})$, 明文的合理排布可以使得 $c_{0,3}^{(1)} \| c_{1,3}^{(1)} \| c_{2,3}^{(1)} \| c_{3,3}^{(1)}$遍历$\{0,1\}^4$, 由于和运算与变量顺序无关, 故对密文求和有如下关系:

$$\sum_{\{x_0,\cdots,x_{15}\}} E^{(6)} = \sum_{\{y_0,\cdots,y_{15}\}} \mathrm{round}^{(5)} = \sum_{y_4}\cdots\sum_{y_{16}}\Big(\sum_{\{y_0,y_1,y_2,y_3\}} \mathrm{round}^{(5)}\Big)$$

其中 $E^{(6)}$ 和 $\mathrm{round}^{(5)}$ 分别表示 6 轮加密运算和 5 轮轮函数运算。$\{x_0, \cdots, x_{15}\}$表示明文中的活跃比特, $\{y_0, \cdots, y_{15}\}$表示 $c^{(1)}$ 中的活跃比特。由定理 1 可知, 在 5 轮区分器中的平衡位置有 $\sum_{\{y_0,y_1,y_2,y_3\}} \mathrm{round}^{(5)} = 0$, 进而 $\sum_{\{x_0,\cdots,x_{15}\}} E^{(6)} = 0$。定理 2 得证。

4 对 8 轮 PUFFIN 密码的积分攻击

这一节中, 我们应用 6 轮区分器对 8 轮的 PUFFIN 密码进行攻击。实际上, 为简便起见, 我们利用的是5.5 轮积分区分器, 即不考虑最后一个 P64 置换。

5.5 轮积分区分器: 按照上节的方式选择明文, 5.5 轮 PUFFIN 加密后, 密文的第 10、15 个字是平衡的, 即 $\sum \text{cipher}10 = 0$, $\sum \text{cipher}15 = 0$。

8 轮积分攻击采取以下步骤:

Step 1 选择一组明文$\{P_i\}$, 使得其中的 16 个比特 $p_{0,3} \| p_{1,3} \| p_{2,3} \| p_{3,3} \| p_{1,0} \| p_{3,1} \| p_{4,0} \| p_{5,1} \| p_{6,1} \| p_{7,0} \| p_{8,1} \| p_{9,0} \| p_{10,2} \| p_{13,0} \| p_{14,1} \| p_{15,3}$遍历$\{0,1\}^{16}$, 其他比特均为固定。对其进行 8 轮加密, 不妨设密文为 $C_0, \cdots, C_{2^{16}}$。

Step 2 猜测第 8 轮的 4 个密钥字 $K_4^{(8)}, K_{10}^{(8)}, K_{11}^{(8)}, K_{14}^{(8)}$, 计算

$$Q_j^{(i)} = \gamma^{-1}(\text{P64}^{-1}(C_i) \oplus K_j^{(8)}), \quad j \in \{4, 10, 11, 14\}$$

并对$\{4, 10, 11, 14\}$4 个字的 16 个位置上的取值进行计数, 不妨设在某一个位置上, "t" 出现了 N_t 次($t = 0, 1$)。

Step 3 猜测 $K_5^{(7)}$ 的值并计算 $s = \gamma^{-1}(t \oplus K_5^{(7)})$ 和 $s^* = \sum_{N_t \bmod 2 = 1} s_0$, 其中 s_0 为 s 的第 0 比特值。

Step 4 检验 $s^* = 0$ 是否成立, 若成立, 则相应的 $K_4^{(8)}, K_{10}^{(8)}, K_{11}^{(8)}, K_{14}^{(8)}$ 和 $K_5^{(7)}$ 为正确值; 否则淘汰。

Step 5 重新选取一组明文, 重复上述步骤, 直到 $K_4^{(8)}, K_{10}^{(8)}, K_{11}^{(8)}, K_{14}^{(8)}$ 和 $K_5^{(7)}$ 唯一确定。

上述 8 轮攻击需要确定 5 个密钥字, 即需要检测 2^{20} 个密钥值, 对于一组明文, 错误密钥留下的概率为 2^{-1}, 对 32 组明文进行分析, 错误密钥留下个数的期望值为 $(2^{20} - 1) \times (2^{-1})^{32} \approx 2^{-12} < 1$, 可以认为正确密钥被唯一确定。因此数据复杂度为 $2^{16} \times 32 \approx 2^{21}$。攻击过程中, 由于需要猜测 5 个密钥字, 时间复杂度为 $2^{21} \times 2^{4\times5} = 2^{41}$ 次查表, 这相当于 $2^{41}/(8 \times 16) = 2^{34}$ 次加密。另外, 为存储密钥, 攻击还需要 2^{20} 的存储空间用于存储密钥。

5 PUFFIN 类 SPN 型分组密码的区分器

本节中, 我们首先定义 PUFFIN 类分组密码, 然后再对这一类的密码进行分析。

PUFFIN 类 SPN 型分组密码是指密码的轮函数具有非线性层 γ, 密钥加运算层 σ 和线性层 P, 其中线性层 P 为置换。轮函数定义为 round$= P \circ \gamma \circ \sigma$。进一步假设该类密码的分组长度为 n bit, 非线性层为 $b \times b$ 的S 盒的并置, 并且 $n \geqslant b(2b+1)$。

定理 3 PUFFIN 类 SPN 型分组密码至少存在 3 轮积分区分器。

证明 为证明定理 3, 我们只需给出这一类密码的 3 轮积分区分器即可。

为选择明文, 将第 0 至 $2b$ 个 S 盒的输入各取出一个比特, $m_0, m_1, \cdots, m_{2b}$, 使 i 位置上的明文按 2^i 个"0"和 2^i 个"1"交错出现($0 \leqslant i \leqslant 2b$)。即令 $m_0 \| m_1 \| \cdots \| m_{2b}$遍历$\{0,1\}^{2b+1}$, 其他位置设置为固定。

由第 3 节寻找区分器的方法可知, 第 1 轮中前 $2n+1$ 个S 盒的输入中一共有两个不同值, 每个值重复 2^{2b} 次, 经过线性层后第 2 轮 γ 层的输入要么为常量, 要么为 2 至 2^b 个不同的偶数值, 每个值重复 2^{b+1}到2^{2b+1}次, 经过线性层后每个不同的值仍旧重复偶数次(至少为 2), 这使得第 2 轮的输出平衡, 并且第3 轮 γ 层的输入为偶数, 进而仍保持平衡性, 第 3 轮的 P 置换只改变比特位置, 不改变平衡性。综上, PUFFIN 类 SPN 型分组密码至少存在 3 轮积分区分器。

(下转第 148 页)

的总数共有$(p^k+1)N_k/2$个。综合前面(1)和(2)两部分讨论,并且加上$u=0$的情况,可知使式(1)没有根的u共有$(p^k+1)(p^k-3)/2+1=(p^k-1)^2/2-1$个。 □

参考文献:

[1] Dembowski P, Ostrom T G. Planes of Order n with Collineation Groups of Order n^2[J]. Math. Z., 1968, 193: 239-258.

[2] Hughes D R, Piper F C. Projective Planes[M]. Springer-verlag, New York, Graduate Texts in Mathematics, 1973, 6.

[3] Biham E, Shamir A. Differential Cryptanalysis of DES-like Cryptosystems[J]. Journal of Cryptology, 1991, 4: 3-72.

[4] Nyberg K. Perfect Nonlinear S-boxes[C]. Advances in Cryptology-EUROCRYPT'91, LNCS 547, Springer-verlag, 1992: 378-386.

[5] Nyberg K. Differentially Uniform Mappings for Cryptography[C]. Advances in Cryptology-EUROCRYPT'93, LNCS 765, Springer-verlag, 1994: 55-64.

[6] Coulter R S, Matthews R W. Planar Functions and Planes of Lenz-barlotti Class Ⅱ[J]. Design, Coding and Cryptography, 1997, 10: 167-184.

[7] Carlet A, Charpin P, Zinoviev V. Codes, Bent Functions and Permutations Suitable for DESlike Cryptosystems[J]. Designs, Codes and Cryptography, 1998, 15(2): 125-156.

[8] Ding C, Yuan J. A Family of Skew Hadamard Difference sets[J]. Comb. Theory, Series A, 2006, 113: 1526-1535.

[9] Zha Z, Kyureghyan G M, Wang X. Perfect Nonlinear Binomials and Their Semifields[J]. Finite Fields and Their Applications, 2009, 15: 125-133.

[10] Budaghyan L, Helleseth T. New Perfect Nolinear Multinomials over $F_{p^{2k}}$ for Any Odd Prime p[C]. SETA 2008, LNCS 5203, 2008, 403-414.

[11] Coulter R S, Henderson M. Commutative Presemifields and Semifields[C]. Advances in Mathematics, 2008, 217: 282-304.

[12] Kyureghyan G M, Pott A. Some Theorems on Planar Mappings[C]. WAIFI 2008, LNCS 5130, 2008, 117-122.

[13] Helleseth T, Kyureghyan G, Ness G J, et al. On a Family of Perfect Nonlinear Binomials[J]. Boolean Functions in Cryptology and Information Security, B. Preenel and O. A. Logacher(Eds.) IOS Press 2008, 126-139.

[14] Budaghyan L, Carlet C, Leander G. On Inequivalence Between Known Power APN Functions[C]// Proceedings of the conference BFCA 2008, Copenhagen.

[15] Lidl R, Niederreiter H. Finite Fields[M]. Encyclopedia of Mathematics and Its Application, US: Addison-wesley, 1983.

(上接第143页)

6 结论

传统的积分攻击对于基于比特设计的密码不再有效,采用基于比特的分析方法能够取得较好的效果。本文从比特的层面寻找平衡性,分析了PUFFIN密码抵抗积分攻击的能力,给出了一个5轮积分区分器并利用高阶积分的思想将其扩展为6轮,在PC机上验证了PUFFIN区分器的存在性。利用6轮区分器,对8轮的PUFFIN进行了攻击。对于PUFFIN类的分组密码,通过统计活跃模式不同值重复的次数,证明了其至少存在3轮积分区分器,证明的过程同时也提供了寻找这类密码积分区分器的方法。

参考文献:

[1] Wheeler D, Needham R. TEA, a Tiny Encryption Algorithm[C]// FSE 1995, LNCS 1008: 363-366.

[2] Lim C, Korkishko T. mCrypto —A Lightweight Block Cipher for Security of Low-cost RFID Tags and Sensors[C]// WISA 2005, LNCS, 2005, 3786: 243-258.

[3] Standaert F, Piret G, Gershenfeld N, et al. SEA: A Scalable Encryption Algorithm for Small Embedded Applications[C]// CARDIS 2006, LNCS, 2006, 3928: 222-236.

[4] Robshaw M. Searching for Compact Algorithms: CGEN[C]// VIETCRYPT 2006, LNCS, 2006, 4341: 37-49.

[5] Hong D, Sung J, Hong S, et al. HIGHT: A New Block Cipher Suitable for Low-resource Device[C]// CHES 2006, LNCS, 2006, 4249: 46-59.

[6] Cheng H, Heys H, Wang C. PUFFIN: A Novel Compact Block Cipher Targeted to Embedded Digital Systems[C]// 11th Euromicro Conference on Digital System Design: Architectures, Methods and Tools. DSD, 2008: 383-390.

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

[8] Galice S, Minier M. Improving Integral Attacks Against Rijndael-256 Up to 9 Rounds[C]// AFRICACRYPT 2008, LNCS, 2008, 5023: 1-15.

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

[10] 王薇,王小云. 对CLEFIA算法的饱和度分析[J]. 通信学报, 2008(10): 88-92.

[11] Zaba M R, Raddum H, Henricksen M, et al. Bit-pattern Based Integral Attack[C]// FSE 2008, LNCS, 2008, 5086: 363-381.