对 Rijndael-256 算法新的积分攻击

魏悦川[1],孙 兵[2],李 超[1,2,3]
(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;
3.中国科学院研究生院信息安全国家重点实验室,北京 100049)

摘 要: 本文对 Rijndael-256 密码进行分析,从比特的层面上寻找平衡性,得到了一个新的 3 轮积分区分器,该区分器仅需 32 个明文就可将 3 轮 Rijndael-256 与随机置换区分开来,并且所得密文的每一比特都是平衡的.该区分器在已知的 Rijndael-256 积分区分器中所需明文量最少.基于新的区分器,对 4 至 7 轮 Rijndael-256 密码进行了攻击.文章还从字节的角度重新刻画了基于比特的积分思想,这一方法可用于分析其他基于字节设计的 SPN 型分组密码.

关键词: 分组密码; 积分攻击; Rijndael 密码; 比特模式
中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112 (2011) 02-0476-05

New Integral Attack on Rijndael-256

WEI Yue-chuan[1], SUN Bing[2], LI Chao[1,2,3]
(1. *College of Computer, National University of Defense Technology, Changsha, Hunan* 410073, *China*;
2. *Science College, National University of Defense Technology, Changsha, Hunan* 410073, *China*;
3. *State Key Laboratory of Information Security, Chinese Academy of Sciences, Beijing* 100049, *China*)

Abstract: Rijndael-256 is analyzed in this paper. We trace the propagation of the plaintexts structure at bit-level to obtain the property, and present a new 3-round distinguisher which needs least chosen plaintexts of all the known integral distinguishers. In this distinguisher, 32 chosen plaintexts are encrypted by 3-round cipher, each bit of the cipertext is balanced. Based on the new distinguisher, reduced-round Rijndael-256 are attacked. The paper also analyzes the distinguisher from another point of view, which can also be applied to other byte-oriented ciphers with SPN structure.

Key words: block cipher; integral attack; rijndael; bit-pattern

1 引言

Rijndael 算法[1]是由比利时密码学家 Daemen 和 Rijmen 共同设计的 SPN 型迭代分组密码,2000 年 10 月被 NIST 选为美国高级加密标准(AES).Rijndael 算法的明文分组长度和密钥长度分别可以选取 128 比特、192 比特和 256 比特且相互独立,本文只讨论 256 比特明文和密钥的 Rijndael 密码.

Rijndael 密码的一个主要设计目标是具有抗差分和线性分析能力[1,2].对 Rijndael 密码最早的有效分析方法是设计者提出的 Square 攻击[3],它是一个选择明文攻击,通过对满足特定形式的明文加密,然后对密文求和,将密码与随机置换区分开来,进而恢复轮密钥.Square 攻击主要针对面向字节运算算法的安全性,与后来的多重集合攻击[13]和饱和攻击[12]一起,在 FSE 2002 中被 Knudsen 纳入了积分攻击的范畴[4].积分攻击在分析基于字节设计的密码时非常有效[6~8],它是对 CLEFIA、Camellia、FOX 等著名算法的安全性最有效的分析方法之一[9,14~15].

目前对 Rijndael 的一系列积分攻击均是基于 Rijndael 的 Square 特性[5,7,11],即明文的一个字节是遍历的,3 轮加密后所得密文的各个字节是平衡的.其中对 Rijndael-256 最有效的攻击是由 Galice 和 Minier 在 2008 年给出的积分攻击[5],它对 7 轮、8 轮和 9 轮的 Rijndael-256 进行了攻击.基于 Square 特性,构造 Rijndael 密码的 3 轮区分器需要 2^8 个选择明文.如何利用更少的明文构造 Rijndael 新的区分器一直是密码界关注的焦点.

传统的积分攻击无法分析基于比特设计的密码,这是因为线性层破坏了输入字节的性质.Z'aba 等学者在 FSE 2008 中提出了基于比特的积分思想[10],它从比特的层面寻找平衡性,以往选择明文只是遍历一个字节,而基于比特的积分思想是从几个字节中分别提取出一个比特,将这些比特放到一起进行遍历,然后利用计数的技术来寻找平衡性并验证轮密钥,该思想以较少的明

收稿日期:2009-07-10;修回日期:2010-11-23
基金项目:国家自然科学基金(No.60803156,61070215);信息安全国家重点实验室开放基金(No.01-07)

文量分析了 5 至 7 轮的 Noekeon、Present 和 Serpent 等基于比特设计的密码.

本文利用基于比特的积分思想对 Rijndael-256 密码的迭代过程从微观上进行分析,找到了一个新的 3 轮区分器,只需选取 32 个明文即可将 3 轮 Rijndael-256 与随机置换区分,并且相应密文的每一个比特都是平衡的.这表明,基于比特的积分思想可以用来分析基于字节设计的算法.利用 3 轮区分器对 4 轮、5 轮、6 轮和 7 轮的 Rijndael-256 密码进行了成功的攻击.本文从字节的角度重新刻画了基于比特的积分思想,给出了新的寻找积分区分器的方法.

2　Rijndael 分组密码简介

Rijndael 密码[1]中明文分组长度和密钥长度分别可以为 128、192 和 256 比特三种长度,其变换都是面向字节的运算.本文只讨论了 256 比特明文分组长度和密钥长度的 Rijndael 密码——Rijndael-256,它共有 14 轮变换,在第一轮变换前有一个密钥加,在最后一轮变换中无列混合.

Rijndael-256 的明文数据分组可表示为 2 维字节数组,它有 4 行 8 列.数据块按 $p_0p_1\cdots p_{31}$ 的顺序映射为状态字节矩阵 $A=(a_{i,j})_{4\times 8}$:

$$a_{i,j}=p_{4i+j},0\leqslant i\leqslant 3,0\leqslant j\leqslant 7$$

Rijndael-256 算法的轮函数由以下函数复合而成.

(1)字节代替变换(SB):它是作用在状态矩阵中每个字节上的非线性变换,也是密码中唯一的非线性变换:

$$(a_{i,j})_{4\times 8}\xrightarrow{S}(S(a_{i,j}))$$

(2)行移位变换(SR):状态矩阵的 1、2、3 和 4 行分别循环左移 0、1、3、4 个字节:

$$(a_{i,j})\xrightarrow{SR}(a_{i,(j+T_i)\ mod 8})$$

其中$(T_0,T_1,T_2,T_3)=(0,1,3,4)$.

(3)列混合运算(MC):将状态矩阵左乘一个列混合矩阵,元素之间的乘法运算是有限域 $F_2{}^8$ 上的乘法运算:

$$A\xrightarrow{MC}MA$$

(4)密钥加变换(ARK):将轮密钥用异或运算作用在状态上,

$$(a_{i,j})_{4\times 8}\rightarrow(a_{i,j}\oplus k_{i,j})_{4\times 8}$$

于是一轮算法可定义为 $round(X)=ARK\circ MC\circ SR\circ SB(X)$.

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[1].

3　Rijndael-256 密码新的 3 轮区分器

Rijndael-256 密码的 Square 区分器是指:选择只有一个字节位置互不相同的 256 组明文,3 轮加密后这种取值的不同扩散到所有密文的 32 个字节上且对应字节互不相同.将 256 组密文按字节异或加,和序列为全零序列.

在以上的区分器中,我们将字节作为基本单位,而基于比特的积分攻击将单位划分的更细,它考察每一比特位置的性质.在介绍新的 Rijndael-256 的区分器之前,我们先来介绍基于比特的积分攻击中的符号与性质[10].

3.1　符号说明

在这种攻击方法中,每一个比特位置都赋予一个 N 比特的序列,根据序列中"0"和"1"的重复方式为每个位置定义一个模式,所有比特位置和相应的模式构成了一个结构.

定义 1　N 比特序列可以定义为以下 4 种模式:

(1)常量模式 c:序列只包含"0"或者只包含"1",例如 8 比特序列 00000000 和 11111111.

(2)活跃模式 a_i:序列中 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:序列中 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.

定义 2　模式 p 称为平衡的是指该模式的所有比特的异或加为 0,即 $\sum p^{(j)}=0$.

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,$a_0a_1a_2\cdots a_{n-1}$ 的横向排列值可以遍历 n 比特序列的 2^n 个状态.例如:$a_0a_1a_2a_3$ 可以表示为十六进制的集合{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15}.

性质 1　模式之间的运算遵从以下规律:

(1)$c\oplus p=p,p\in\{c,a,b\}$;　　(2)$a_i\oplus a_i=c$;

(3)$p_j\oplus q_i=b_i$,其中 $j>i,p,q\in\{a,b\}$.如果 $i=0$,则等号右侧为 b_0^*;

(4)$p\oplus b_0^*=b_0^*,p\neq b_0$.

性质 2　当 S 盒的输入模式为 $b_{i_1}b_{i_2}b_{i_3}\cdots b_{i_n},i_1,i_2,\cdots,i_n$ 不同时为 0,所有的输出比特位置都为 b_j 模式,其中 j 是 $i_1,i_2,\cdots,i_n$ 中的最小值.

3.2　Rijndael-256 新的 3 轮区分器

Rijndael-256 中有 32 个 S 盒,每个 S 盒都是 8 进 8 出的,我们将 S 盒的第 i 个输入位置上所有的值记为 p_i $(0\leqslant i\leqslant 7)$.于是可以选择 256 比特的明文 $P_{(256)}=(p_0,$

$p_1, p_2, \cdots, p_7) = (p_0, p_1, p_2, \cdots, x \parallel c_7)$,选取规则为:

(1)$p_0, p_1, \cdots, p_6$ 是任意的 32 比特常量,c_7 是任意的 27 比特常量,所有常量的比特位置上均为常量模式 c. c 的长度 $N = 32$ 比特.

(2)$x \in \{0,1\}^5$,x 的 5 个比特位置上各取一个活跃模式,将 x 表示为 $a_0a_1a_2a_3a_4$. 于是 x 遍历 0 至 32 之间所有值. 这相当于在 32 个 S 盒的 5 个当中各取出 1 比特构成 5 比特,令这 5 比特值遍历 $\{0,1\}^5$.

定理 1 3 轮 Rijndael-256 可以被 32 个选择明文与随机置换区分开来. 按一定方式选取明文,3 轮加密后所得密文的每一个比特位置都是平衡的.

按照以上所述方法选取明文,我们考察明文的迭代规律以给出定理 1 的证明.

我们令前 5 个 S 盒的最低比特遍历 $\{0,1\}^5$,每个比特位置上的序列长 $N = 32$. 前 5 个 S 盒的输入模式为 $ccccccca_i (0 \leqslant i \leqslant 4)$,其他 S 盒的输入模式均为 $cccccccc$. 迭代过程中我们用到以下规则:

(1)$ccccccca_i$ 经过 S 盒后的模式为 $d_id_id_id_id_id_id_id_ia_i$($a_i$ 也可能位于其他比特位置),这是因为 $ccccccca_i$ 表示两个值的轮流出现,且 S 盒是双射.

(2)行移位变换只改变 S 盒和相应模式的位置,对于各比特位置的平衡性没有任何影响.

(3)列混和运算是线性变换,若状态矩阵的每一列中 4 个字节均是平衡字节,则变换后的模式为这列模式中下标最小者. 且这一列中的模式为 $b_ib_ib_ib_ib_ib_ib_ib_i$. 也就是说,列混合运算不改变各比特位置的平衡性质.

(4)S 盒是唯一可破坏平衡性的部件,根据性质 2,当 S 盒的输入模式为 $b_{i_1}b_{i_2}b_{i_3}\cdots b_{i_n}$,$i_1, i_2, \cdots, i_n$ 同时不为 0,输出比特仍然是平衡的. 若输入模式为平衡模式 $b_0^* b_0^* b_0^* \cdots b_0^*$,输出模式很可能被 S 盒破坏. 若 $b_0^* b_0^* b_0^* \cdots b_0^*$ 的 N 个横向排列值中,每一个值重复偶数次,则经 S 盒映射后依然重复偶数次,所得模式依然是平衡模式 $b_0^* b_0^* b_0^* \cdots b_0^*$. 若每一个横向排列值只出现 1 次,则经过 S 盒之后平衡模式被破坏,得到 $b_0b_0b_0\cdots b_0$.

例如当明文输入第 1 个 S 盒后,前 5 个 S 盒的输出中有两个不同值,而其余 S 盒的输出只有 1 个值,所以 $b_0^* b_0^* b_0^* \cdots b_0^*$ 在经过第 2 个 S 盒前都表示两个值,每个值重复 16 次,因而在经过 S 盒后仍是平衡的.

(5)密钥加变换相当于在每个比特位置加上一个常量,不影响模式的平衡性.

按照以上规则,可以发现平衡性在第 4 轮中被 S 盒破坏,于是得到定理 1 中所描述的 3 轮区分器. 新的区分器与 Square 区分器相比,所需明文量大大减少了.

3.3 对 4 轮、5 轮、6 轮、7 轮 Rijndael-256 的攻击

我们使用 3 轮区分器攻击 4 轮 Rijndael-256 时,需要选择两个结构,明文的数量为 $2 \times 2^5 = 2^6$,将相应的密文部分解密,逐比特验证是否有 $\sum_{i=0}^{i=64} Cipher3 = 0$ 成立,$Cipher3$ 表示第 3 轮的密文,每次猜测 8 比特密钥,为恢复轮密钥 K_4 的所有比特,需重复 32 次,所以攻击需要 $2^6 \times 2^8 \times 32 = 2^{19}$次部分解密.

在 5 轮攻击中,由于线性层的扩散作用,攻击者需要猜测 K_5 的 4 个字节和 K_4 的 1 个字节(5 个字节共 40 比特)才能得到 $Cipher3$ 的 1 个字节,需要 40/8 = 5 个结构才能唯一确定正确密钥,选择明文量为 $5 \times 2^5 = 2^{7.4}$. 为得到 256 比特轮密钥需要重复 7 次上述猜测过程和 1 次穷尽搜索过程,因此,5 轮攻击共需要 $(2^{40} + 2^{32} + \cdots + 1) \times 2^5 \times 7 + 2^{32} \approx 2^{48}$次部分解密.

在 6 轮攻击中,我们使用 4 轮区分器,即在 3 轮区分器的前面加上一轮,由于有 5 个活跃字节,为了能够逆回一轮,需要猜测 8 个字节的第 1 轮轮密钥,获得新的选择明文,从而使第 2 轮的输入模式为所需要的明文. 我们利用穷尽搜索来获得 64 比特的密钥,增加的计算复杂度为 2^{64}. 6 轮攻击相当于在 5 轮攻击的基础上在前面加一轮,选择明文量为 $2^{64} \times 2^{7.4} = 2^{71.4}$,数据复杂度为 $2^{64} \times 2^{48} = 2^{112}$.

对于 7 轮攻击,一次猜测的密钥量为 1 + 4 + 16 个字节,共 168 比特,需要 21 个结构来验证密钥,选择明文量为 $21 \times 2^{64} \times 2^5 = 2^{73.3}$,需要 $(2^{168} + 2^{160} + \cdots + 1) \times 2^5 \times 2^{64} = 2^{237.1}$次部分解密. 对于 7 轮的攻击效率仅仅好于穷尽搜索.

4 对基于比特区分器的字节刻画

在上一节,我们将文献[10]中基于比特的积分思想推广至基于字节设计的分组密码 Rijndael-256,得到了新的 3 轮区分器,在这一节中,我们从字节的角度重新刻画基于比特的积分思想,对于基于字节设计的分组密码,给出一种新的寻找积分区分器的方法.

仍然按照上一节中所描述方法选择明文,不难发现,a_i 的周期为 2^{i+1},前 5 个 S 盒的最低比特依次取值为 $ccccccca_i (0 \leqslant i \leqslant 4)$,由于只有 1 比特是“0”和“1”轮流出现的,所以明文的前 5 个字节的周期也分别为 2^{i+1},故每一明文字节上均有两个值周期出现,每个值出现 16 次. 明文输入如图 1 所示,其中括号外的数字表示该字节位置上取值的周期,括号内的数字表示这一位置上有几个不相同的值,未标识数字的字节为常数,只有 1 个值,周期为 1.

2(2)	32(2)						
4(2)							
8(2)							
16(2)							

图 1 Rijndael-256 的明文字节

性质 3　当选择明文量为 32 时,周期为 2,4,8,16 的字节是平衡的.周期为 32 的字节不一定是平衡字节,若该字节位置上每个值均出现偶数次,则该字节为平衡字节.

注:本文中周期的概念与序列中周期的严格定义稍有不同,例如,本文中周期为 2 是指相同的序列组在所有的 32 组序列中以 2 为周期重复出现,而周期为 32 是指在所有的 32 组序列中,相同的序列组只出现 1 次.

在迭代过程中,我们用到以下事实.

(1)若序列 $\{M_j\}$ 是平衡的,即 $\sum_j M_j = 0$,由于 S 盒是双射,通过 S 盒后,$\{M_j\}$ 的周期不变. S 盒不影响取值的个数和每个值出现的次数.若 $\{M_j\}$ 中每个值出现偶数次,则输出仍然是平衡的.若 $\{M_j\}$ 中每个值出现奇数次,则输出不一定平衡.

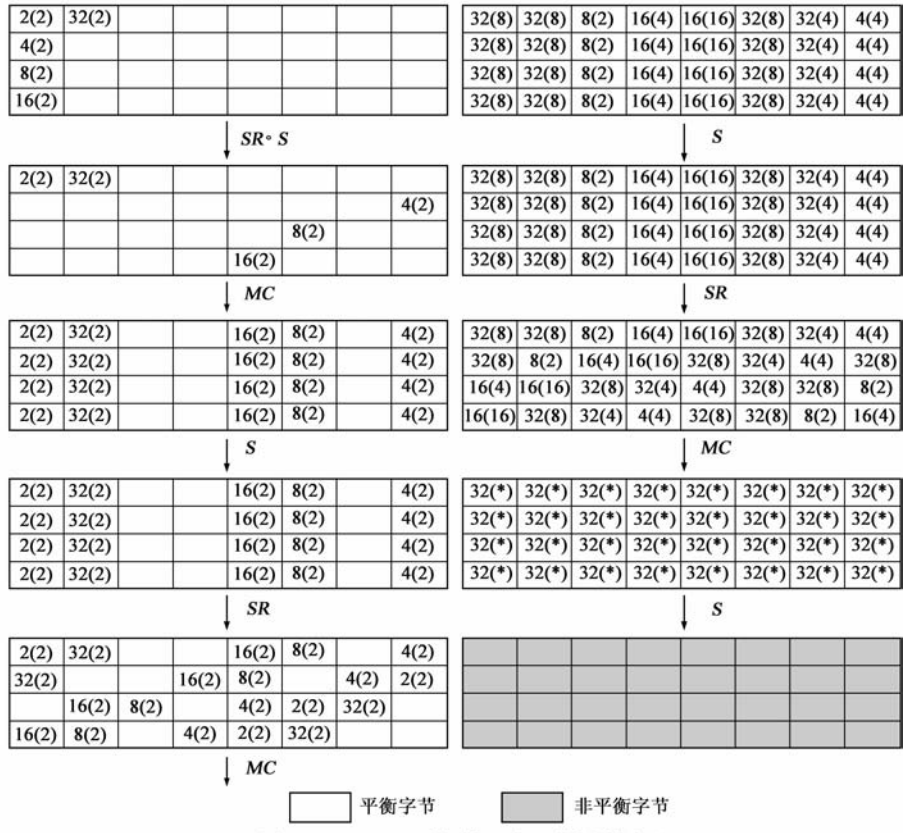


图2　Rijndael-256的3轮区分器的字节刻画

(2)行移位变换只影响字节的位置,对周期和平衡性均不影响,对取值个数也不影响.

(3) 列混合变换作用于平衡序列 $\{M_{j0}\}\cdots\{M_{j3}\}$,由于变换是线性的,所以每个字节的输出序列仍是平衡的,4 个输出字节的周期均为 $\{M_{j0}\}\cdots\{M_{j3}\}$ 中最大的周期.取值个数至多为该列中原来各字节取值个数的乘积,但是不超过全体明文个数.

(4)密钥加变换对序列周期和平衡性均不影响,对于取值个数也不影响.

以 Rijndael-256 密码为例,图 2 描述了 3 轮迭代过程中字节周期和取值数目的变化.

图 2 中,有 5 个明文字节各取两个不同值,经过 S 盒变换和行移位变换后,仍然有 5 个明文字节取两个不同值,只是位置发生了变化;经过列混合运算后扩散至 20 个字节,每个字节取两个值,周期与这一列中最大的周期相同,每个字节都是平衡字节.在第 2 轮中,S 盒变换不影响周期,周期为 32 的字节的平衡性受到质疑,但是这些字节位置上只有两个不同值,每个值重复 16 次,所以是平衡字节;经过列混合运算后,每个字节位置上至多有 16 个不同值,每个值出现偶数次,所以经过第 3 轮的 S 盒变换后仍然是平衡字节,行移位变换和列混合变换不影响平衡性,因此 3 轮变换后密文的每个字节都是平衡的.经过这一轮的列混合后,可能出现的值达到最大,用"$*$"来表示极限值 32,由于每个值出现 1 次,所以第 4 轮的 S 盒将破坏平衡性.

这种寻找积分区分器的方法可以归结为在某些字节位置上取少量值,使这些值按周期轮流出现,在迭代过程中追踪周期和取值个数的变化,以判断其平衡性.由以上分析过程不难看出,这一分析方法并没有局限于密码的具体结构,因此,该分析方法可以应用于其他基于字节设计的 SPN 型分组密码.

5　结论

本文给出了高级加密标准 Rijndael-256 的新的 3 轮区分器,区分器的可靠性在 PC 机上进行了验证,并利用这个区分器对 4 至 7 轮的 Rijndael 密码进行了攻击.本文获得的区分器是对 32 个明文进行 3 轮加密,每一比特位置上的密文之和均为零,而 Square 区分器则需要 256 个选择明文,两者相比本文中给出的区分器更强,但是如何利用这一新的积分区分器攻击更多轮的密码,如何加上类似于 Square 攻击中使用的部分和之类的技巧,还有待于进一步探究.本文还将基于比特的积分思想从字节的角度重新刻画,这对分析分组密码的积分性质提供了新的工具.

表 1 本文区分器与 Square 区分器的比较

积分区分器	所需明文量	效果
Square 区分器	256	每一密文字节平衡
本文区分器	32	每一密文字节平衡

参考文献:

[1] Daemem J, Rijmen V. AES proposal: Rijndael[A]. The First Advanced Encryption Standard Candidate Conference[C]. USA, NIST, 1998. 1 – 45.

[2] 肖国镇,白恩健,刘晓娟. AES 密码分析的若干新进展[J]. 电子学报,2003,31(10):1549 – 1554.
Xiao G Z, Bai E J, Liu X J. Some new developments on the cryptanalysis of AES[J]. Acta Electronical Sinica, 2003, 31(10):1549 – 1554. (in Chinese)

[3] Daemen J, Knudsen L R, and Rijmen V. The block cipher Square[A]. Eli Biham. Fast Software Encryption 1997[C]. Haifa: Springer-Verlag, 1997. LNCS 1267, 149 – 165.

[4] Knudsen L R, Wagner D. Integral cryptanalysis[A]. Joan Daemen, Vincent Rijmen. Fast Software Encryption 2002[C]. Belgium: Springer-Verlag, 2002. LNCS 2365, 112 – 127.

[5] Galice S, Minier M. Improving integral attacks against rijndael-256 Up to 9 rounds[A]. Serge Vaudenay. Africacrypt 2008[C]. Casablanca: Springer-Verlag 2008. LNCS 5023, 1 – 15.

[6] Yeom Y, Park S, Kim I. On the security of camellia against the square attack[A]. Joan Daemen, Vincent Rijmen. Fast Software Encryption 2002[C]. Belgium: Springer-Verlag, 2002. LNCS 2356, 89 – 99.

[7] Nakahara J, Freitas D, Phan R. New multiset attacks on rijndael with large blocks[A]. Ed Dawson, Serge Vaudenay. Advances in Cryptology-Mycrypt 2005[C]. Kuala Lumpur: Springer-Verlag, 2005. LNCS 3715, 277 – 295.

[8] 王薇,王小云. 对 CLEFIA 算法的饱和度分析. 通信学报,2008,(10):88 – 92.
Wang W, Wang X Y. Saturation cryptanalysis of CLEFIA[J]. Journal of Communication, 2008, (10):88 – 92. (in Chinese)

[9] 吴文玲,卫宏儒. 低轮 FOX 分组密码的碰撞-积分攻击[J]. 电子学报,2005,33(7):1307 – 1310.
Wu W L, Wei H R. Collision-integral attack of reduced-round Fox[J]. Acta Electronical Sinica, 2005, 33(7): 1307 – 1310. (in Chinese)

[10] Z'aba M. R, Raddum H, Henricksen M, and Dawson E. Bit-pattern based integral attack[A]. Kaisa Nyberg. Fast Software Encryption 2008[C]. Lausanne: Springer-Verlag, 2008. LNCS 5086, 363 – 381.

[11] Ferguson N, Kelsey J, Lucks S, et al. Improved cryptanalysis of Rijndael[A]. Bruce Schneier. Fast Software Encryption 2000[C]. New York: Springer-Verlag, 2001. LNCS 1978, 213 – 230.

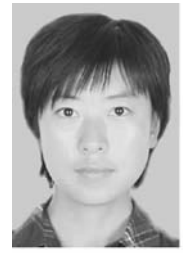
[12] Lucks S. The saturation attack—a bait for Twofish[A]. Mitsuru Matsui. Fast Software Encryption 2001[C]. Yokohama: Springer-Verlag, 2002. LNCS 2355, 1 – 15.

[13] Biryukov A. and Shamir A. Structural cryptanalysis of SASAS[A]. Birgit Pfitzmann. Eurocrypt 2001[C]. Innsbruck: Springer-Verlag, 2001. LNCS 2045, 394 – 405.

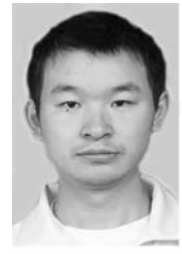
[14] Duo L, Li C, Feng K Q. New observation on Camellia[A]. Bart Preneel. Selected Areas in Cryptography 2005[C]. Kingston: Springer-Verlag, 2006. LNCS 3897, 51 – 64.

[15] Wu W L, Zhang W T, Feng D G. Integral cryptanalysis of reduced FOX block cipher[A]. Dengguo Feng, Dongdai Lin, Moti Yung. Information Security and Cryptology 2005[C]. Seoul: Springer-Verlag, 2006. LNCS 3935, 229 – 241.

作者简介:



魏悦川 女,天津蓟县人,硕士,国防科技大学计算机学院博士生,主要研究方向为编码密码理论及其应用.
E-mail: wych004@163.com



孙 兵 男,江苏南通人,博士,国防科技大学理学院讲师,主要研究方向为编码密码理论及其应用.
E-mail: happy_come@163.com

李 超 男,湖南汨罗人,博士,国防科技大学理学院教授,博士生导师,主要研究方向为编码密码理论及其应用.
E-mail: lichao_nudt@sina.com