SMS4算法的不可能差分攻击研究

孙翠玲 卫宏儒

(北京科技大学数理学院 北京 100083)

摘 要 为研究分组加密算法SMS4抵抗不可能差分攻击的能力,使用了14轮不可能差分路径,给出了相关攻击结果。基于1条14轮不可能差分路径,对16轮和18轮的SMS4算法进行了攻击,改进了关于17轮的SMS4的不可能差分攻击的结果,将数据复杂度降低到$O(2^{69.47})$。计算结果表明:攻击16轮SMS4算法所需的数据复杂度为$O(2^{103})$,时间复杂度为$O(2^{92})$;攻击18轮的SMS4算法所需的数据复杂度为$O(2^{104})$,时间复杂度为$O(2^{123.84})$。

关键词 分组密码,SMS4,不可能差分攻击,Early-abort技术

中图法分类号 TN918.1 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.7.042

Research on Impossible Differential Attack of Cipher SMS4

SUN Cui-ling WEI Hong-ru

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

Abstract To analyze impossible differential cryptanalysis on the block cipher SMS4, the results were presented based on one 14-round impossible differential route. One impossible differential attack was applied to 16-round and 18-round reduced SMS4, and improved result on 17 round CLEFFIA-256 was given with the number of chosen plaintexts being reduced to $O(2^{69.47})$. Computing result shows that the attack of 16-round SMS4 needs $O(2^{103})$ choosing plaintext operations, and $O(2^{92})$ encrypting computations, and the attack of 18-round SMS4 needs $O(2^{104})$ choosing plaintext operations and $O(2^{123.84})$ encrypting computations.

Keywords Block cipher, SMS4, Impossible differential attack, Early-abort technique

1 前言

随着计算机和通信网络的广泛应用,信息的安全性已受到人们的普遍重视。信息安全已不仅仅局限于政治、军事以及外交等领域,而且现在也与人们的日常生活息息相关。在社会信息化的进程中,信息已经成为社会发展的重要资源,信息安全也成为21世纪国际竞争的重要战场。在无线局域网应用中,安全问题高居第一位。无线局域网鉴别与保密基础结构是我国自主研发的、拥有自主知识产权的无线局域网安全技术标准,也是一种安全协议。它采用的是国家密码管理委员会办公室批准的椭圆曲线密码算法和分组密码算法SMS4,其中SMS4算法是我国官方公布的第一个商用分组密码算法[1]。

SMS4算法是一个分组密码算法,其分组长度为128bit,密钥长度为128bit。加密算法与密钥扩展算法都采用32轮非线性迭代结果。解密算法与加密算法的结构相同,只是轮密钥的使用顺序相反,解密轮密钥是加密轮密钥的逆序。目前对算法的攻击方法有边信道攻击[2]、不可能差分攻击[3,4]、矩形攻击[5,6]和差分分析[7,8]等。

不可能差分分析是由Biham E在文献[9]中提出的,它作为差分分析的一种变形,以简单的分析过程和高效的攻击能力引起了人们的广泛关注。本文基于文献[4]提出的14轮不可能差分路径,利用Early-abort技术以及算法本身的特点攻击了16轮的SMS4算法和18轮的SMS4算法,并对攻击17轮的SMS4算法进行了改进,在恢复相同密钥长度的情况下,数据复杂度降低到$O(2^{69.47})$。本文第2节介绍SMS4算法;第3—5节是对16、17、18轮的攻击过程;最后对全文进行总结。

2 SMS4算法

SMS4算法是一个32轮Feistel结构的算法,分组长度及密钥长度均为128bit。明文输入表示为4个32比特字节$(X_0,X_1,X_2,X_3)\in(Z_2^{32})^4$,其对应的密文输出为$(Y_0,Y_1,Y_2,Y_3)\in(Z_2^{32})^4$。其中轮密钥表示为$rk_i\in Z_2^{32}$,$i=0,1,2,\cdots31$,轮密钥由初始密钥根据密钥扩展算法生成。

2.1 轮函数

算法采用非线性迭代结构,以字为单位进行加密运算,称一次迭代运算为一轮变换。每一轮只有32bit需要运算。

轮函数F为:

$$F(X_0,X_1,X_2,X_3,k_r)=X_0\oplus T(X_0\oplus X_1\oplus X_2\oplus X_3\oplus k_r)$$

其中,T为$z_2^{32}\rightarrow z_2^{32}$的一个可逆变换,由非线性变换$\tau$和线性

到稿日期:2014-07-14 返修日期:2014-09-20 本文受2013年国家自然科学基金(61272476),内蒙古自治区科技创新引导奖励资金(2012)项目资助。

孙翠玲(1990—),女,硕士生,主要研究方向为密码学;卫宏儒(1963—),男,副教授,硕士生导师,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,E-mail:weihr@ustb.edu.cn(通信作者)。

变化 L 复合而成。

非线性变换 τ：它是由 4 个并行的 S 盒构成。

设输入为 $A=(a_1,a_2,a_3,a_4)\in(Z_2^8)^4$，则输出为 $B=(b_1,b_2,b_3,b_4)\in(Z_2^8)^4$，则有：

$$(b_1,b_2,b_3,b_4)=\tau(A)$$
$$=(S_{box}(a_1),S_{box}(a_2),S_{box}(a_3),S_{box}(a_4))$$

线性变换 L：设输入为 $B\in Z_2^{32}$，则有：

$$C=L(B)=B\oplus(B\ll 2)\oplus(B\ll 10)\oplus(B\ll 18)\oplus(B\ll 24)$$

其中，$\lll i$ 为 32bit 循环左移 i 位。

2.2 加/解密算法

SMS4 算法的解密变换与加密变换结构相同，不同的仅是轮密钥的使用顺序。加密时轮密钥的使用顺序为 $(rk_0,rk_1,\cdots rk_{31})$，解密时轮密钥的使用顺序为 $(rk_{31},rk_{30},\cdots rk_0)$。

定义反序变换 R 为：$R(A_0,A_1,A_2,A_3)=(A_3,A_2,A_1,A_0)$，$A_i\in Z_2^{32}$ 其中 $i=0,1,2,3$；第 i 轮函数如图 1 所示，F 函数如图 2 所示。则算法的加密变换为：

$$X_{i+4}=F(X_i,X_{i+1},X_{i+2},X_{i+3},k_{ri})$$
$$=X_i\oplus T(X_{i+1}\oplus X_{i+2}\oplus X_{i+3}\oplus k_{ri})(Y_0,Y_1,Y_2,Y_3)$$
$$=R(X_{32},X_{33},X_{34},X_{35})$$
$$=(X_{35},X_{34},X_{33},X_{32})$$

第 i 轮的输出为 $(X_i,X_{i+1},X_{i+2},X_{i+3})$。

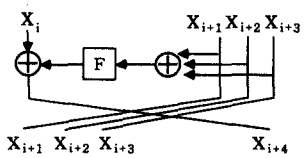

图 1 SMS4 第 i 轮的轮函数

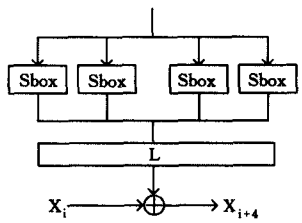

图 2 F 函数

2.3 密钥扩展算法

算法中加密算法的轮密钥由加密密钥通过密钥扩展算法生成。加密密钥为：

$$M_k=(M_{k_0},M_{k_1},M_{k_2},M_{k_3}),M_{k_i}\in Z_2^{32},i=0,1,2,3$$

若令 $K_i\in Z_2^{32}$，$i=0,1,\cdots,31$，轮密钥可以定义为 $rk_i\in Z_2^{32}$，$i=0,1,\cdots,31$，则密钥生成方法为：

首先，

$$(K_0,K_1,K_2,K_3)=(M_{K_0}\oplus F_{K_0},M_{K_1}\oplus F_{K_1},M_{K_2}\oplus F_{K_2},M_{K_3}\oplus F_{K_3})$$

然后，对 $i=0,1,2,\cdots,31$，有

$rk_i=K_{i+4}=K_i\oplus T'(K_{i+1}\oplus K_{i+2}\oplus K_{i+3}\oplus C_{K_i})$，其中 T' 变换与轮函数中的 T 变换基本相同，只将其中的线性变换 L 修改为 L'，

$$L'(B)=B\oplus(B\ll 13)\oplus(B\ll 23)$$

系统参数 F_K 的取值采用 16 进制表示为 $F_k=(F_{k_0},F_{k_1},F_{k_2},F_{k_3})$，其中：

$F_{k_0}=(A3B1BAC6)$，$F_{k_1}=(56AA3350)$

$F_{k_2}=(677D9197)$，$F_{k_3}=(B27022DC)$

固定参数 $C_K=(C_{K_0},C_{K_1},\cdots,C_{K_{31}})$ 的取值方法为：设 $C_{K_{i,j}}$ 为 C_{K_i} 的第 j 字节，其中 i 和 j 分别为 $i=0,1,2,\cdots,31$，$j=0,1,2,3$。即

$$C_{K_i}=(c_{k,0},c_{k,1},c_{k,2},c_{k,3})\in(Z_2^8)^4$$
$$c_{k_{ij}}=(4i+j)\times 7(\mathrm{mod}\ 256)$$

32 个固定参数 C_{K_i} 的具体值参见相关标准[1]。

3 16 轮 SMS4 算法的不可能差分攻击

利用文献[4]提出的 14 轮不可能差分路径：

$$(a,a,a,0)\rightarrow(a,a,a,0)$$

后加两轮对 16 轮 SMS4 进行攻击。攻击过程如下：

(1)选择明文结构

令明文 $P_0|P_1|P_2|P_3$ 满足明文差分形式为 $(\Delta P_0,\Delta P_1,\Delta P_2,\Delta P_3)=(a,a,a,0)$，该明文结构包括 2^{32} 个明文，可形成 2^{63} 个明文对。选取 2^N 个这样的结构，共有 2^{N+32} 个明文，形成 2^{N+63} 个明文对。

(2)过滤数据对

对这些明文对进行 16 轮加密，得到相应的密文对，保留满足差分形式为 $(*,*,a,a)$ 的明密文对，并将其放入一个哈希表中。由此满足条件的概率 $p=2^{-64}$，所以剩下的明密文对为 2^{N-1}。

(3)密钥恢复过程

1)猜测 32bit 密钥 rk_{15}，并且依次猜测 $rk_{15,i}$ $(i=0,1,2,3)$，恢复哈希表中所对应的明密文的第 15 轮输出，保留哈希表中第 15 轮输出差分为 $(*,a,a,a)$ 的明密文对，过滤数据对。由此满足条件的概率 $p=2^{-32}$，剩余数据对为 2^{N-33}。此步骤的复杂度为：

$$2\times\sum_{i=0}^{7}2^{N-1-8i}\times 2^{8(i+1)}=2^{N+11}$$

2)猜测满足步骤 1)的哈希表中剩下的所有明文对 (P_0,P_1,P_2,P_3) 的 32bit 密钥 rk_{14}，依次猜测 $rk_{14,i}$ $(i=0,1,2,3)$，对每个数据对密钥剩余的概率为 2^{-32}，经过 2^{N-33} 个剩余明密文对，64bit 的密钥剩余的错误密钥的个数为

$$2^{64}\times(1-2^{-32})^{2^{N-33}}<1$$

即可恢复正确密钥。经过计算可得 $N=71$。此步的复杂度为：

$$2\times 2^{32}\times 2^{32}\times[1+(1-2^{-32})+(1-2^{-32})^2+\cdots(1-2^{-32})^{2^{38}}]\approx 2^{96}$$

则由以上分析可知，攻击 16 轮 SMS4 所需明文为 2^{103}，时间复杂度为 $O(2^{92})$。

4 17 轮 SMS4 算法的改进攻击

利用文献[4]中提出的 14 轮不可能差分路径：

$$(a,a,a,0)\rightarrow(a,a,a,0)$$

后加 3 轮对 17 轮 SMS4 算法进行攻击。攻击过程如下：

(1)选择明文结构

令明文 $P_0|P_1|P_2|P_3$ 满足明文差分形式为 $(\Delta P_0,\Delta P_1,\Delta P_2,\Delta P_3)=(a,a,a,0)$，该明文结构包括 2^{32} 个明文，可形成 2^{63} 个明文对。选取 2^N 个这样的结构，共有 2^{N+32} 个明文，形成 2^{N+63} 个明文对。

(2)过滤数据对

对这些明文对进行 17 轮加密,得到相应的密文对,保留满足差分形式为(*,*,*,a)的明密文对,并将其放入一个哈希表中。由此满足条件的概率 $p=2^{96}/2^{128}=2^{-32}$,所以剩下的明密文对为 2^{N+31}。

(3)密钥恢复过程

1)首先需要猜测 32bit 密钥 rk_{16},并且依次猜测 $rk_{16,i}(i=0,1,2,3)$,恢复哈希表中所对应的明密文的第 16 轮输出,保留哈希表中第 16 轮输出差分为(*,*,a,a)的明密文对,过滤数据对。由此满足条件的概率 $p=2^{-32}$,剩余数据对为 2^{N-1}。

2)猜测满足以上哈希表中剩下所有明文对(P_0,P_1,P_2,P_3)的密钥 rk_{14},rk_{15}。并计算对应的第 14 轮和第 15 轮输出值,选取满足以上条件且第 14 轮输出差分为(a,a,a,0)、第 15 轮输出差分为(*,a,a,a)的明密文对。满足以上两轮输出差分要求的概率均为 2^{-32}。

(4)由上述分析可知,满足以上的差分是不可能差分,所以每一个通过该假设的密钥都是错误密钥。排除所有满足以上步骤的密钥,最后恢复出正确密钥。

由上面的分析可知,在分析第(1)步 2^{N-1} 明密文对之后,猜测密钥 rk_{14},rk_{15} 的 64bit 的错误率为 $2^{64}\times[(1-2^{-32})^2]^{2^{N-1}}\approx 2^{64}\times e^{-2^{N-31}}$,取 $N=37.47$,则错误率约为 2^{-120}。假设最后一轮 32 bit 密钥 rk_{16} 是正确的,对于每一个 32 bit 的密钥 rk_{16} 希望可以排除所有错误的 64 bit 密钥是 rk_{14},rk_{15},因而根据以上分析可知剩下的错误值 rk_{14},rk_{15},rk_{16} 的概率大约为 $2^{32}\times 2^{-120}=2^{-88}$。因此,当仅剩一个 rk_{14} 和 rk_{15} 的值时,可认为密钥 rk_{16} 是正确的。数据复杂度为 $O(2^{69.47})$,时间复杂度主要由步骤(1)和步骤(2)步决定。

步骤(1)的复杂度为:

$$2\times\sum_{i=0}^{7}2^{N+31-8i}\times 2^{8(i+1)}=2^{N+43}=2^{80.47}$$

步骤(2)的复杂度为:

$$2^{32}\times 2\times 2^{64}\times\{1+(1-2^{-32})^2+(1-2^{-32})^4+\cdots[(1-2^{-32})^{2^{37.47}}]\}\approx 2^{128}$$

因为分析的是 17 轮的 SMS4,所以该算法共需约复杂度为 2^{124} 的 17 轮 SMS4 加密运算。攻击的数据复杂度为 $O(2^{69.47})$,时间复杂度为 $O(2^{124})$。

5 18 轮 SMS4 算法的不可能差分攻击

利用文献[4]中提出的 14 轮不可能差分路径:

$(a,a,a,0)\rightarrow(a,a,a,0)$

前加两轮后加两轮攻击 18 轮 SMS4 算法。攻击过程如下:

(1)选择明文结构

令明文 $P_0|P_1|P_2|P_3$ 满足明文差分形式为(ΔP_0,ΔP_1,ΔP_2,ΔP_3)=(*,*,a,a),该明文结构包括 2^{64} 个明文,可形成 2^{127} 个明文对。选取 2^N 个这样的结构,共有 2^{N+64} 个明文,形成 2^{N+127} 个明文对。

(2)过滤数据对

对这些明文对进行 18 轮加密,得到相应的密文对,保留满足差分形式为(*,*,a,a)的明密文对,并将其放入一个哈希表中。由此满足条件的概率 $p=2^{-64}$,所以剩下的明密文对为 2^{N+63}。

(3)密钥恢复过程

1)首先需要猜测 32bit 密钥 rk_{17},并依次猜测 $rk_{17,i}(i=0,1,2,3)$,恢复哈希表中的对应的明密文对对应的 17 轮输出过滤数据对,保留哈希表中第 17 轮输出差分为(*,a,a,a)的明密文对。由此满足条件的概率 $p=2^{-32}$,剩余数据对为 2^{N+31}。

2)依次猜测满足步骤(1)的哈希表中所有明密文的 32bit 密钥 $rk_{0,i}(i=0,1,2,3)$,并计算对应的第一轮输出值,选取满足以上条件且第 1 轮输出差分为(*,a,a,a)的过滤数据对。由此,满足条件的概率为 $p=2^{-32}$,剩余数据对为 2^{N-1}。

3)依次猜测满足以上步骤的哈希表中剩下的所有的明文对 $P_0|P_1|P_2|P_3$ 的 32bit 密钥 $rk_{1,i}(i=0,1,2,3)$,并计算对应的第二轮输出值,选择满足以上条件且第二轮输出差分为(*,a,a,a),每个数据对密钥剩余的概率为 2^{-32},则经过 2^{N-1} 个剩余明密文对,96bit 的密钥剩余的错误密钥的个数为 $2^{96}\times(1-2^{-32})^{2^{N-1}}<1$,即可恢复正确密钥。经过计算可得 $N=40$。

攻击的复杂度计算如下:

步骤 1):

$$2\times\sum_{i=0}^{7}2^{N+63-8i}\times 2^{8(i+1)}=2^{N+75}=2^{114}$$

步骤 2):

$$2\times 2^{32}\times\sum_{i=0}^{1}2^{N+31-8i}\times 2^{8(i+1)}=2^{N+73}=2^{111}$$

步骤 3):

$$2\times 2^{96}\times[1+(1-2^{-32})+\cdots+(1-2^{-32})^{2^{39}}]=2^{128}$$

则攻击所需要的时间复杂度主要集中在步骤 3),因此时间复杂度为 $2^{128}/18\approx 2^{123.84}$,数据复杂度为 $O(2^{104})$。分析结果与相关参考文献的比较结果如表 1 所列。

表 1 几种攻击结果比较

攻击方法	轮数	数据复杂度	时间复杂度	文献
不可能差分	16	$2^{117.06}$	$2^{121.82}$	[3]
矩形攻击	16	2^{125}	2^{121}	[5]
不可能差分	16	2^{103}	2^{92}	本文
不可能差分	17	2^{103}	2^{124}	[4]
不可能差分	17	$2^{69.47}$	2^{124}	本文
矩形攻击	18	2^{124}	2^{124}	[6]
飞来器攻击	18	2^{120}	2^{119}	[6]
不可能差分	18	2^{104}	$2^{123.84}$	本文

结束语 本文对 SMS4 密码算法采用了前后分别增加轮数和同时增加轮数的方法,利用不可能差分方法和 Early-abort 技术进行分析,结果表明数据复杂度和时间复杂度都有降低,证明了攻击的可行性。另外也可以寻找更长的不可能差分路径或者不同的差分路径来攻击更长轮数的 SMS4 算法。

参 考 文 献

[1] Office of State Commercial Cipher Administration. Block Cipher for WLAN products-SMS4[EB/OL]. 2006-12-23. http://www.oscca.gov.File/2006021016423197990

[2] 张蕾,吴文玲. SMS4 密码算法的差分故障攻击[J]. 计算机学报,2006,29(9):1594-1600
Zhang Lei, Wu Wen-ling. Differential Fault Analysis on SMS4 [J]. Chinese Journal of Computers, 2006, 29(9): 1594-1600

[3] Toz D, Dunkelman O. Analysis of Two Attacks on Reduced-Round Versions of the SMS4[C]// Proceedings of ICICS 2008, Springer-verlag, 2008. LNCS: 2008, 5308: 141-156

(下转第 228 页)

重组，得到完整的 Promela 模型。在故障扩展 SysML 活动图模型中，若故障活动可达，说明行为模型不满足安全性需求，利用该模型可以迅速找到故障发生的过程和导致这个故障发生的软件行为，从而对行为模型进行修正，使系统功能模型满足安全性需求。最后，本文对一个燃气灶控制系统利用本文方法得到了带有故障信息的扩展 SysML 活动图以及与其等价的 Promela 程序，并利用 SPIN 对其进行安全性验证工作。

在下一步工作中，将考虑离散时间的转换；当前的映射表仍是人工完成，将考虑如何实现映射表的自动构建；利用模型驱动的方法，扩展 SysML 的元模型，用以包含从故障树中提取的故障信息，然后进行安全性分析验证。

参 考 文 献

[1] 黄志球，徐丙凤，阚双龙，等. 嵌入式机载软件安全性分析标准、方法及工具研究综述[J]. 软件学报，2014，25(2)：200-218
Huang Zhi-qiu, Xu Bing-feng, Kan Shuang-long, et al. Survey on Embedded Software Safety Analysis Standards, Methods and Tools for Airborne System [J]. Journal of Software, 2014, 25(2): 200-218

[2] Vesely W E, et al. Fault tree handbook[R]. Washington DC: U. S. Nuclear regulatory commission, 1981

[3] OMG. Unified Modeling Language: super structure v2.0 [EB/OL]. http://www.omg.org/docs/formal/05-07-04.pdf, 2005

[4] OMG. Systems Modeling Language. v1.2[EB/OL]. http://www.omg.org/spec/SysML/1.2, 2008

[5] 肖美华，薛锦云. 基于 SPIN/Promela 的并发系统验证[J]. 计算机科学，2004，31(8)：201-203
Xiao Mei-hua, Xue Jin-yun. Verification of Concurrent System Using SPIN/Promela[J]. Computer Science, 2004, 31(8): 201-203

[6] Walker M, Papadopoulos Y, et al. Qualitative temporal analysis: Towards a full implementation of the Fault Tree Handbook[J]. Control Engineering Practice, 2009, 17(10): 1115-1125

[7] Chu T L, Apostolakis G. Methods for probabilistic analysis of noncoherent fault trees[J]. IEEE Transactions on Reliability, 1980, 29(5): 354-360

[8] Schellhorn G, Thums A, Reif W. Formal fault tree semantics [C]// Proceedings of The Sixth World Conference on Integrated Design & Process Technology, Pasadena, CA. 2002

[9] Jarraya Y, Debbabi M, Bentahar J. On the meaning of SysML activity diagrams[C]// 16th Annual IEEE International Conference and Workshop on Engineering of Computer Based Systems (ECBS 2009). IEEE, 2009: 95-105

[10] 樊晓光，褚文奎，张凤鸣. 软件安全性研究综述[J]. 计算机科学，2011，38(5)：8-13
Fan Xiao-guang, Chu Wen-kui, Zhang Feng-ming. Surveys on Softwate safety[J]. Computer Science, 2011, 38(5): 8-13

[11] 薛克. 基于 SPIN 的 UML 活动图验证[D]. 上海：华东师范大学，2008
Xue Ke. Verification of UML ctivity chart using Spin [D]. Shanghai: East China normal university, 2008

[12] Guelfi N, Mammar A. A formal semantics of timed activity diagrams and its PROMELA translation[C]// 12th Asia-Pacific Software Engineering Conference (APSEC'05). IEEE, 2005: 8

[13] Ravn A P, Rischel H, et al. Specifying and verifying requirements of real-time systems[J]. IEEE Transactions on Software Engineering, 1993, 19(1): 41-55

[14] Lano K, Kan P, et al. Linking hazard analysis to formal specification and design in B[M]// Computer Safety, Reliability and Security. Springer Berlin Heidelberg, 1998: 60-74

[15] Ariss E O, Xu Dian-xiang, et al. Integrating safety analysis with functional modeling[J]. IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, 2011, 41(4): 610-624

[16] Sánchez M A, Felder M. A Systematic Approach to Generate Test Cases based on Faults[C]// ASSE 2003, Buenos Aires. 2003

[17] Hansen K M, Ravn A P, et al. From safety analysis to software requirements[J]. IEEE Transactions on Software Engineering, 1998, 24(7): 573-584

[18] Nazier R, Bauer T. Automated Risk-Based Testing by Integrating Safety Analysis Information into System Behavior Models [C]// 2012 IEEE 23rd International Symposium on Software Reliability Engineering Workshops (ISSREW). IEEE, 2012: 213-218

[19] Reif W, Schellhorn G, et al. Safety analysis of a radio-based crossing control system using formal methods[C]// 9th IFAC Symposium Control in Transportation Systems. 2000

[20] Dasso A, Funes A, et al. Verification, validation and testing in software engineering[M]. IGI Global, 2007

(上接第 193 页)

[4] 陈杰，胡予濮，张跃宇. 用不可能差分法分析 17 轮 SMS4 算法[J]. 西安电子科技大学学报(自然科学版)，2008，35(3)：455-458
Chen Jie, Hu Yu-pu, Zhang Yue-yu. Impossible differential attack on the 17-round block cipher SMS4[J]. Journal of Xidian University(Natural Science), 2008, 35(3): 455-458

[5] Zhang L, Zhang W, Wu W. Cryptanalysis of Reduced-Round SMS4 Block cipher[C]// Proceedings of ACISP 2008. Springer-verlag, 2008, 5107: 216-229

[6] Kim T, Kim J, Hong S, et al. Linear and Differential Cryptanalysis of Reduced SMS4 Block Cipher[OL]. http://eprint.iacr.org/2008/281

[7] Km T, Kng J, Hong S, et al. Linear and differential cryptanalysis of reduced SMS4 block c-ipher[R]. Cryptology ePrint Archive: Report 2008/281, 2008

[8] 张美玲，刘景美，王新梅. 22-轮 SMS4 的差分分析[J]. 中山大学学报(自然科学版)，2010，49(2)：43-47
Zhang Mei-ling, Liu Jing-mei, Wang Xin-mei. Differential Attack on 22-Round SMS4 Block Cipher[J]. Acta Scientiarum Naturalium Universitatis Sunyatseni, 2010, 49(2): 43-47

[9] Biham E, Biryukov A, Shamir A. Cryptana lysis of Skipjack reduced to 31 rounds using impossible differentials[C]// Advances in Cryptology-Eurocrypt, 1999. Springer Berlin Heidelberg, 1999: 12-23