Piccolo 算法的差分故障分析

赵光耀[1] 李瑞林[2] 孙 兵[3),4)] 李 超[1),3)]

[1)](国防科学技术大学计算机学院网络技术与信息安全研究所 长沙 410073)

[2)](国防科学技术大学电子科学与工程学院 长沙 410073)

[3)](国防科学技术大学理学院数学与系统科学系 长沙 410073)

[4)](中国科学院软件研究所信息安全国家重点实验室 北京 100190)

摘 要 Piccolo 算法是 CHES 2011 上提出的一个轻量级分组密码算法,它的分组长度为 64-bit,密钥长度为 80/128-bit,对应迭代轮数为 25/31 轮. Piccolo 算法采用一种广义 Feistel 结构的变种,轮变换包括轮函数 S-P-S 和轮置换 RP,能够较好地抵抗差分分析、线性分析等传统密码攻击方法. 该文将 Piccolo 算法的 S-P-S 函数视为超级 S 盒(Super Sbox),采用面向半字节的随机故障模型,提出了一种针对 Piccolo-80 算法的差分故障分析方法. 理论分析和实验结果表明:通过在算法第 24 轮输入的第 1 个和第 3 个寄存器各诱导 1 次随机半字节故障,能够将 Piccolo-80 算法的密钥空间缩小至约 22-bit. 因此,为安全使用 Piccolo 算法,在其实现时必须做一定的防护措施.

关键词 差分故障分析;超级 S 盒;轻量级分组密码;Piccolo 算法

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2012.01918

Differential Fault Analysis on Piccolo

ZHAO Guang-Yao[1] LI Rui-Lin[2] SUN Bing[3),4)] LI Chao[1),3)]

[1)](*Institute of Network Technology and Information Security, School of Computer, National University of Defense Technology, Changsha* 410073)

[2)](*School of Electronic Science and Engineering, National University of Defense Technology, Changsha* 410073)

[3)](*Department of Mathematics and System Science, Science College, National University of Defense Technology, Changsha* 410073)

[4)](*State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing* 100190)

Abstract Piccolo was proposed at CHES 2011 as a lightweight block cipher with block size 64-bit. The key size of Piccolo is 80-bit/128-bit, and the corresponding round number is 25/31. Piccolo adopts a variant of generalized Feistel structure, and its round transformation consists of the round function S-P-S and the round permutation PR. The designers show that Piccolo is resistant against most classical attacks, such as differential and linear cryptanalysis. This paper presents a first differential fault analysis on Piccolo-80 based on the random nibble-oriented fault model by treating the S-P-S function as a Super Sbox. Both the theoretical analysis and the experimental result demonstrate that the key space can be reduced from 80-bit to about 22-bit by injecting a fault at the first and third register in the 24th input respectively. This indicates that cryptographic devices supporting Piccolo should be carefully protected.

Keywords differential fault analysis; Super Sbox; lightweight block cipher; Piccolo

1 引 言

随着物联网技术的不断发展,数据安全问题越来越受到人们的重视. 由于物联网中许多设备的计算能力较低、存储空间小、资源有限,传统的加密算法不能得到很好的应用. 在此情况下,设计一种执行效率高、资源消耗少的密码算法来保护微型设备间

收稿日期:2012-05-17;最终修改稿收到日期:2012-07-04. 本课题得到国家自然科学基金(61103192,61070215)及信息安全国家重点实验室开放基金(01-02-5)资助.**赵光耀**,男,1982 年生,博士研究生,主要研究方向为编码密码理论及其应用. E-mail: zhaoguangyao08@gmail.com. **李瑞林**,男,1982 年生,博士,讲师,主要研究方向为编码密码理论及其应用. **孙 兵**,男,1981 年生,博士,讲师,主要研究方向为编码密码理论及其应用. **李 超**,男,1966 年生,博士,教授,主要研究领域为编码密码理论及其应用.

的信息传输安全显得越来越重要. 近年来，轻量级密码算法的设计与分析受到了人们的广泛关注，密码学者提出了许多轻量级密码算法，如 MIBS[1]、LED[2]、HIGHT[3]、LBlock[4]、PRESENT[5]、KLEIN[6]等. Piccolo[7]算法是在 CHES 2011 上提出的一种轻量级密码，由日本索尼公司的 Shibutani 等学者设计，它的分组长度为 64-bit，密钥长度可以为 80-bit 或 128-bit. 与其它的轻量级算法相比，Piccolo 算法最大的优点是其能耗极小，而且只需额外增加少量的硬件开销，便可同时支持加解密，因而尤其适用于低能耗设备.

Biham 和 Shamir 首次在文献[8]中将差分分析[9]的思想推广至差分故障分析，用来对 DES 类的密码算法进行攻击，使得现实环境中的分组密码受到了更大的威胁. 近些年来，人们利用该思想陆续对一些轻量级密码算法进行了分析，包括 Keeloq[10-11]、MIBS[12]、LED[13-14]①、LBlock[15]、HIGHT[16]等. 差分故障分析的一个关键问题是如何合理地建立故障模型，包括故障诱导的时间、位置和取值. 在实际攻击当中，需要根据加密算法的结构、轮函数的特点、算法实现的软硬件环境以及攻击所采用的设备[17-18]来确定究竟采取哪一个模型更加适合.

目前，对 Piccolo 算法的传统安全性分析主要有 Biclique 攻击[19]. 本文在对算法组件进行深入分析后，提出了一种针对 Piccolo-80 算法的差分故障攻击方法，能够以较少的故障注入次数，在较短的时间内恢复出种子密钥. 理论分析和实验验证表明，诱导 2 个故障即可将 80-bit 的种子密钥空间减少到约 22-bit.

本文第 2 节简单介绍 Piccolo 算法；第 3 节给出算法的一个等价结构，并对 Piccolo 算法的 S 盒以及 S-P-S 结构的差分特性进行描述；第 4 节给出对 Piccolo 算法的差分故障分析，包括基本思想、详细的攻击步骤和攻击的复杂度分析；第 5 节给出攻击的实验结果；第 6 节对全文进行总结；附录给出攻击的一组实验结果.

2　Piccolo 算法

首先给出本文所用记号，然后简要介绍 Piccolo 算法.

2.1　符号及术语说明

$a_{(b)}$：长度为 b-bit 的数据 a；

$a|b$：数据 a 与 b 的级联；

$a \leftarrow b$：将 b 的值赋给 a.

$\Delta OUTF^i$：第 i 轮 F 变换层的输出差分，$\Delta OUTF^i = \Delta OUTF_0^i | \Delta OUTF_1^i | \Delta OUTF_2^i | \Delta OUTF_3^i$；

ΔOUT^i：第 i 轮的输出差分，$\Delta OUT^i = \Delta OUT_0^i | \Delta OUT_1^i | \Delta OUT_2^i | \Delta OUT_3^i$；

X^L 或 X^R：X 的左(或右)半部分. 若 X 为 16 位，则 X^L 表示 X 的高 8 位；

半字节：长度为 4-bit 的向量.

2.2　Piccolo 算法

Piccolo 算法分组长度为 64-bit，密钥长度可为 80-bit 和 128-bit，对应的算法分别记为 Piccolo-80 和 Piccolo-128，迭代轮数分别为 25 和 31. 本文研究对象为 Piccolo-80. 为表述方便，以下如无特别说明，Piccolo 均指 Piccolo-80.

Piccolo 算法所采用的结构是广义 Feistel 结构的一种变体，如图 1 所示，该结构包括 4 个分支(寄

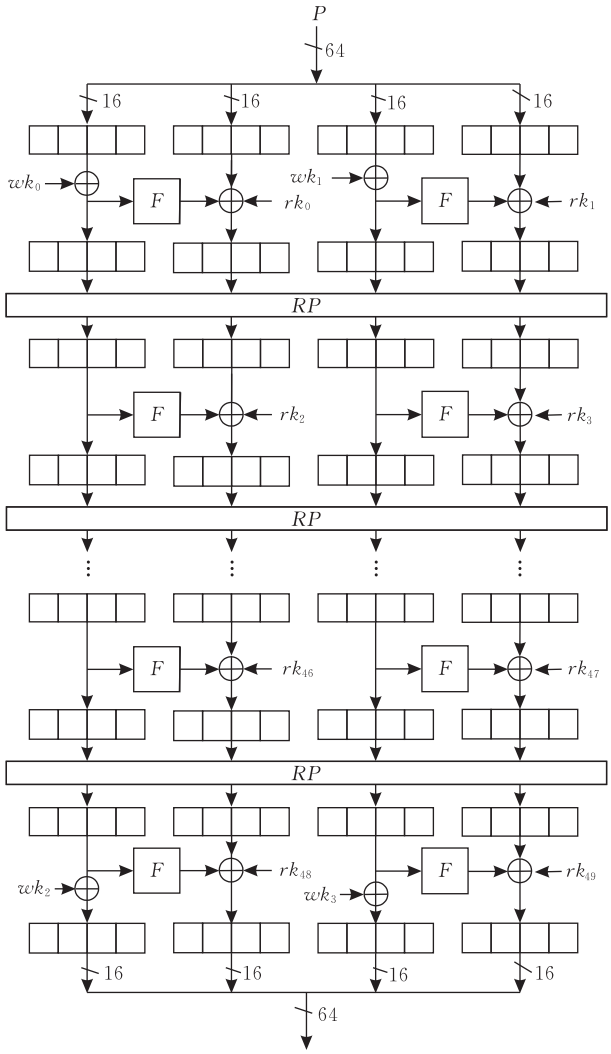

图 1　Piccolo 加密流程

① 另可参见：Zhao Xin-Jie, Guo Shi-Ze, Zhang Fan, Wang Tao, Shi Zhi-Jie, Ji Ke-Ke. Algebraic Differential Fault Attacks on LED using a Single Fault Injection. Cryptology ePrint Archive, 2012, http://eprint.iacr.org/2012/347.pdf

存器),每个分支(寄存器)包含 16-bit 数据. Piccolo 算法每轮包含两类变换:轮函数 $F:(0,1)^{16}\rightarrow(0,1)^{16}$ 和轮置换 $RP:(0,1)^{64}\rightarrow(0,1)^{64}$(最后一轮除外,仅包含轮函数 F),其中 F 函数采用 S-P-S 三层结构(见图 2),P 变换采用有限域 $GF(16)$ 上的矩阵,定义如下

$$\boldsymbol{M}=\begin{pmatrix}2&3&1&1\\1&2&3&1\\1&1&2&3\\3&1&1&2\end{pmatrix}.$$

轮置换 RP 则是基于字节的位置变换,如图 3 所示.

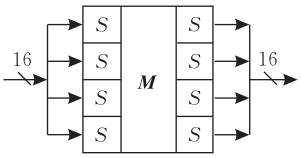

图 2 F 函数

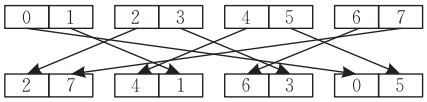

图 3 轮置换 RP

Piccolo 算法的密钥扩展算法比较简单,采用基于置换的实现方法,这在一定程度上减少了硬件开销,同时也使得轮密钥建立时间更短. 密钥扩展算法使用 80-bit 的种子密钥 $k_{(80)}$ 作为输入,输出 4 个 16-bit 的白化密钥 $wk_{i(16)}(0\leq i<4)$ 和 50 个 16-bit 的轮密钥 $rk_{j(16)}(0\leq j<50)$.

首先将 80-bit 的种子密钥 k_{80} 划分为 5 个 16-bit 的字:$k_{(80)}=k_{0(16)}\mid k_{1(16)}\mid k_{2(16)}\mid k_{3(16)}\mid k_{4(16)}$,轮密钥可按如下方式得到:

$wk_0\leftarrow k_0^L\mid k_1^R, wk_1\leftarrow k_1^L\mid k_0^R,$

$wk_2\leftarrow k_4^L\mid k_3^R, wk_3\leftarrow k_3^L\mid k_4^R;$

for $i\leftarrow 0$ to $(r-1)$ do:

$$(rk_{2i},rk_{2i+1})\leftarrow(con_{2i},con_{2i+1})\oplus\begin{cases}(k_2,k_3), & i \bmod 5=0 \text{ 或 } 2\\(k_0,k_1), & i \bmod 5=1 \text{ 或 } 4\\(k_4,k_4), & i \bmod 5=3\end{cases}$$

其中的轮常数为如下形式:

$$(con_{2i},con_{2i+1})\leftarrow$$

$$(c_{i+1}\mid c_0\mid c_{i+1}\mid\{00\}_2\mid c_{i+1}\mid c_0\mid c_{i+1})\oplus\{0f1e2d3c\}_{16},$$

这里 c_i 是将 i 表示成 5-bit 的二进制数,如 $c_{13}=\{01101\}_2$.

不难发现,白化密钥 wk_2 和 wk_3 对应于种子密钥中的 k_3、k_4,最后一轮的轮密钥 rk_{48}、rk_{49} 与种子密钥中的 k_0、k_1 则只相差一个轮常数.

3 Piccolo 算法组件性质

3.1 Piccolo 算法的一个等价结构及差分传播性质

通过分析,我们发现可以根据轮置换的逆变换,将 Piccolo 算法的第 25 轮轮密钥进行拆分重组,上移一轮后作为第 24 轮的白化密钥. 图 4 所示为算法最后两轮等价结构,其中 rk_{46},rk_{47} 用虚线表示,旨在说明对应的轮密钥也可以上移至前一轮.

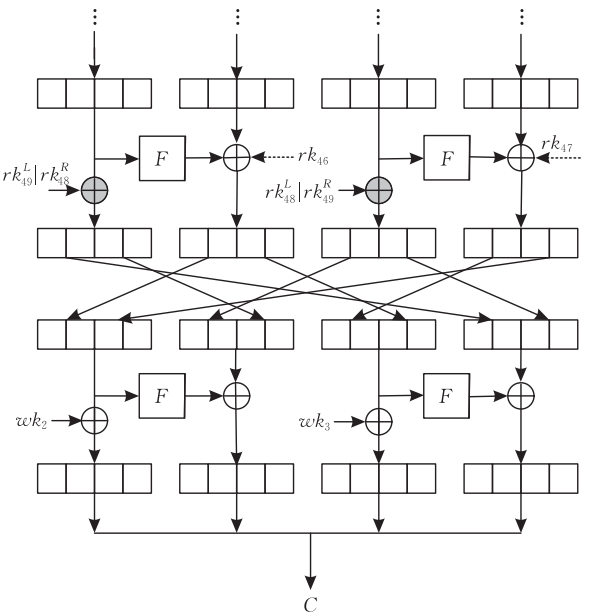

图 4 Piccolo 的一种等价结构

Piccolo 算法结构属于广义 Feistel 结构的变种,且 RP 变换是基于字节的置换,容易得到以下差分传播性质:

$$\Delta OUTF_1^i=(\Delta OUT_0^{i+1})^L\mid(\Delta OUT_2^{i+1})^R \quad (1)$$

$$\Delta OUTF_3^i=(\Delta OUT_2^{i+1})^L\mid(\Delta OUT_0^{i+1})^R \quad (2)$$

3.2 Piccolo 算法 S 盒的差分特性

本节简单描述 Piccolo 算法中 S 盒($S:\mathbb{F}_2^4\rightarrow\mathbb{F}_2^4$)的差分特性.

假设给定 $\alpha\in\mathbb{F}_2^4$,$\beta\in\mathbb{F}_2^4$,定义集合 $IN(\alpha,\beta)=\{z\in\mathbb{F}_2^4\mid S(z\oplus\alpha)\oplus S(z)=\beta\}$,$N(\alpha,\beta)=\sharp IN(\alpha,\beta)$,称 α 为 S 盒的输入差分,β 为 S 盒的输出差分.

Piccolo 算法 S 盒差分分布性质如表 1 所示.

表 1 Piccolo 算法 S 盒差分分布性质

$N(\alpha,\beta)$	出现次数	概率	$N(\alpha,\beta)\neq 0$ 时所占比重	平均值
0	159	**0.621**	—	—
2	72	0.281	0.742	1.484
4	24	0.094	0.247	0.988
16	1	0.004	0.011	0.176

表 1 说明,当给定 $\alpha\in\mathbb{F}_2^4$,$\beta\in\mathbb{F}_2^4$ 时,对于方程

$S(z\oplus\alpha)\oplus S(z)=\beta$，62.1%的情况无解，而在有解的情况下，74.2%的情况下有 2 个解，24.7%的概率有 4 个解，且解的平均个数为 2.65（=1.484+0.988+0.176）.

3.3　S-P-S 结构差分特性

Piccolo 算法中 F 函数采用 S-P-S 三层结构，与传统的 S-P 结构相比，其混淆性能更强. 由于 Piccolo 算法采用的 S 盒是有限域 $GF(16)$ 上的一个置换，P 置换采用的是 $GF(16)$ 上的矩阵 $\boldsymbol{M}$，所以将 S-P-S 结构看成一个大的 S 盒，其输入和输出均为 16-bit，可视为有限域 $GF(2^{16})$ 上的一个置换. 这类似于文献[20]中提出的超级 S 盒(Super Sbox)的概念①，只需将密钥加部分的密钥取为全零即可，如图 5 所示，其中灰色底纹表示活跃的半字节. 将 3.2 节中定义的 $IN(\alpha,\beta)$ 及 $N(\alpha,\beta)$ 推广至超级 S 盒，即 $IN(\alpha,\beta)=\{x\in\mathbb{F}_2^{16}\mid SS(x\oplus\alpha)\oplus SS(x)=\beta\}$，$N(\alpha,\beta)=\sharp IN(\alpha,\beta)$，其中 SS 表示超级 S 盒，$\alpha\in\mathbb{F}_2^{16}$，$\beta\in\mathbb{F}_2^{16}$ 分别为超级 S 盒的输入差分和输出差分.

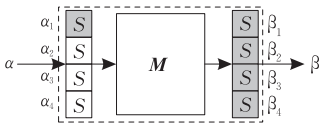

图 5　F 函数差分分析模型

下面给出几种特殊情形下超级 S 盒的差分传播特性：

(1) 输入差分仅在单个半字节上非零的情形.

这种情况下，输入差分有 $4\times(2^4-1)=60$ 个可能取值，我们考虑输出差分的分布情况，此时输入/输出差分对 (α,β) 取值共有 $60\times2^{16}=3\,932\,160$ 种，统计 $N(\alpha,\beta)$ 的取值情况，结果见表 2. 表 2 说明，当超级 S 盒的输入差分只有单个半字节非零时，在所有输入/输出差分对 (α,β) 中，平均意义下，有 15.3%的 (α,β) 对应的 $N(\alpha,\beta)\neq0$，且 $N(\alpha,\beta)$ 的平均值为 6.53.

表 2　输入差分在单个半字节上非零时超级 S 盒差分特性

$N(\alpha,\beta)$	出现次数	最大值	概率	累加值	平均值
0	3329724	0	0.847	0	0
≠0	602436	96	**0.153**	3932160	**6.53**

(2) 输入差分为 $(\alpha_1,\alpha_2,0,0)$ 或 $(0,0,\alpha_3,\alpha_4)$ (α_i 非零)的情形.

此时，输入差分共有 $2\times(2^4-1)^2=510$ 个可能取值，考虑输出差分的分布情况，输入/输出差分对共有 510×2^{16} 种取值，统计 $N(\alpha,\beta)$ 的取值情况，结果如表 3 所示. 表 3 说明，当超级 S 盒的输入差分形式为 $(\alpha_1,\alpha_2,0,0)$ 和 $(0,0,\alpha_3,\alpha_4)$，其中 α_i 非零时，平均意义下，26.3%的概率 $N(\alpha,\beta)\neq0$，且当 $N(\alpha,\beta)\neq0$ 时，其平均值为 3.8.

表 3　输入差分为 $(\boldsymbol{\alpha_1},\boldsymbol{\alpha_2},\boldsymbol{0},\boldsymbol{0})$ 和 $(\boldsymbol{0},\boldsymbol{0},\boldsymbol{\alpha_3},\boldsymbol{\alpha_4})$ 时超级 S 盒的差分特性 ($\boldsymbol{\alpha_i}$ 非零)

$N(\alpha,\beta)$	出现次数	最大值	概率	累加值	平均值
0	24626684	0	0.737	0	0
≠0	8796676	96	**0.263**	33423360	**3.80**

(3) 超级 S 盒的扰动差分传播特性.

为了确切地研究 Piccolo 算法故障攻击时超级 S 盒的差分传播性质，我们根据攻击算法所示的差分传播特点(图 9，图 10)，建立图 6 所示的差分分析模型. 仍然考虑输入差分为 $(\alpha_1,\alpha_2,0,0)$ 或 $(0,0,\alpha_3,\alpha_4)$ (α_i 非零)的情形. 假设给定输入差分 α 时，输出差分共有 n 个可能值. 图 6 中 β^i 表示 α 对应的第 i 个输出差分值；θ 表示输出差分的未知部分(扰动)，经过分析，θ 共有 32 个可能值，θ^i 表示 θ 的第 i 个可能取值.

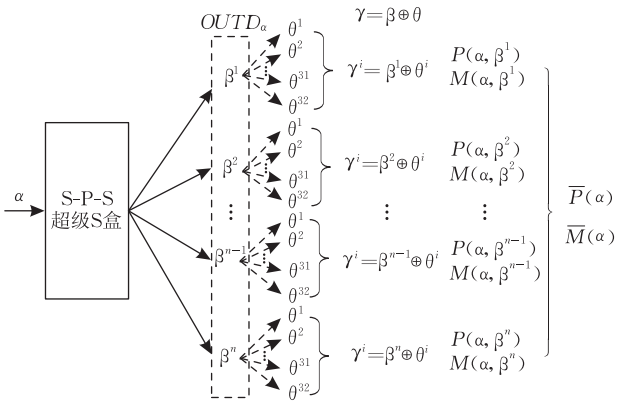

图 6　输入差分为 $(\alpha_1,\alpha_2,0,0)$ 或 $(0,0,\alpha_3,\alpha_4)$ 时扰动差分传播特性分析模型

① 输入差分 $\alpha\in\{(\alpha_1,\alpha_2,0,0)\mid\alpha_i\neq0\}$.

对随机给定的 α，首先获得其所有可能的输出差分组成的集合 $OUTD_\alpha$，因此对于任意 $\beta\in OUTD_\alpha$，必有 $N(\alpha,\beta)>0$，此时我们对 β 进行一个扰动获得 $\gamma=\beta\oplus\theta$，其中 $\theta\in\{(\theta_1,0,0,0),(0,\theta_2,0,0)\mid\theta_i\in\mathbb{F}_2^4\}$，并判断 γ 是否仍属于 $OUTD_\alpha$，即判断 $N(\alpha,\gamma)>0$ 是否成立. 对随机给定的 α 和 θ，我们可以利用如下的算法 1 得到 $N(\alpha,\gamma)>0$ 成立的平均概率 $\overline{P}$ 以及成立时方程 $SS(\alpha\oplus x)\oplus SS(x)=\gamma$ 解的平均数目 $\overline{M}$.

① 另可参见：Daemen J, Rijmen V. Two-round AES differentials. Cryptology ePrint Archive, 2006, http://eprint.iacr.org/2006/039.pdf

算法 1. 超级 S 盒的扰动差分传播特性.

输入：$Set(\alpha)=\{(\alpha_1,\alpha_2,0,0)\mid\alpha_i\neq 0\}$,

$Noise=\{(\theta_1,0,0,0),(0,\theta_2,0,0)\mid\theta_i\in\mathbb{F}_2^4\}\triangleq\{\theta^i\mid 1\leq i\leq 32\}$

输出：$\overline{P}$及$\overline{M}$

$COUNT(\alpha,\beta)=0, A_\gamma(\alpha,\beta)=0$

For $\alpha\in Set(\alpha)$

  $OUTD_\alpha\leftarrow\{\beta\mid N(\alpha,\beta)>0\}$

  For $\beta\in OUTD_\alpha$

    For $\theta\in Noise$

      $\gamma=\beta\oplus\theta$;

      If $\gamma\in OUTD_\alpha$

        $COUNT(\alpha,\beta)++$

        $A_\gamma(\alpha,\beta)=A_\gamma(\alpha,\beta)+N(\alpha,\gamma)$;

    End For

    $P(\alpha,\beta)=COUNT(\alpha,\beta)/|Noise|$

    $M(\alpha,\beta)=A_\gamma(\alpha,\beta)/COUNT(\alpha,\beta)$

  End For

  $\overline{P}(\alpha)=\left(\sum_{\beta\in OUTD_\alpha}P(\alpha,\beta)\right)/|OUTD_\alpha|$

  $\overline{M}(\alpha)=\left(\sum_{\beta\in OUTD_\alpha}M(\alpha,\beta)\right)/|OUTD_\alpha|$

End For

$\overline{P}=\left(\sum_{\alpha\in Set(\alpha)}\overline{P}(\alpha)\right)/|Set(\alpha)|$

$\overline{M}=\left(\sum_{\alpha\in Set(\alpha)}\overline{M}(\alpha)\right)/|Set(\alpha)|$

② 输入差分 $\alpha\in\{(0,0,\alpha_3,\alpha_4)\mid\alpha_i\neq 0\}$.

分析过程与①类似，区别仅为 $\theta\in\{(0,0,\theta_3,0),(0,0,0,\theta_4)\mid\theta_i\in\mathbb{F}_2^4\}$.

①②情形下，输入差分均有 $(2^4-1)^2=225$ 个可能取值. 按照图 6 所示的模型分别得到超级 S 盒对应的扰动差分传播性质，见表 4.

表 4 超级 S 盒的扰动差分传播特性(α_i非零)

α 的取值形式	$\overline{P}$	$\overline{M}$
$(\alpha_1,\alpha_2,0,0)$	**0.426**	**3.675**
$(0,0,\alpha_3,\alpha_4)$	**0.430**	**3.684**

4 对 Piccolo 算法的差分故障分析

4.1 基本记号和符号

为简单起见，给出以下基本记号和符号(见图 7)：

记明文为 $P=(X_0\mid X_1\mid X_2\mid X_3)$，密文为 $C=(C_0\mid C_1\mid C_2\mid C_3)$；

IN^i：第 i 轮的输入，$IN^i=IN_0^i\mid IN_1^i\mid IN_2^i\mid IN_3^i$，$IN^0=P$；

OUT^i：第 i 轮的输出，$OUT^i=OUT_0^i\mid OUT_1^i\mid OUT_2^i\mid OUT_3^i$，$OUT^{25}=C$；

$OUTF^i$：第 i 轮 F 变换层的输出，$OUTF^i=OUTF_0^i\mid OUTF_1^i\mid OUTF_2^i\mid OUTF_3^i$，$RP(OUTF^i)=OUT^i$；

$INSS_L^i$或$INSS_R^i$：第 i 轮左边(或右边)F 函数(超级 S 盒)的输入；

$OUTSS_L^i$或$OUTSS_R^i$：第 i 轮左边(或右边)F 函数(超级 S 盒)的输出；

$\langle X\rangle$：X 所有可能取值的集合；

$|\langle X\rangle|$：X 所有可能取值的个数；

ΔX：X 的差分值，即假设有两个 X：x_1,x_2，则 $\Delta X=x_1\oplus x_2$.

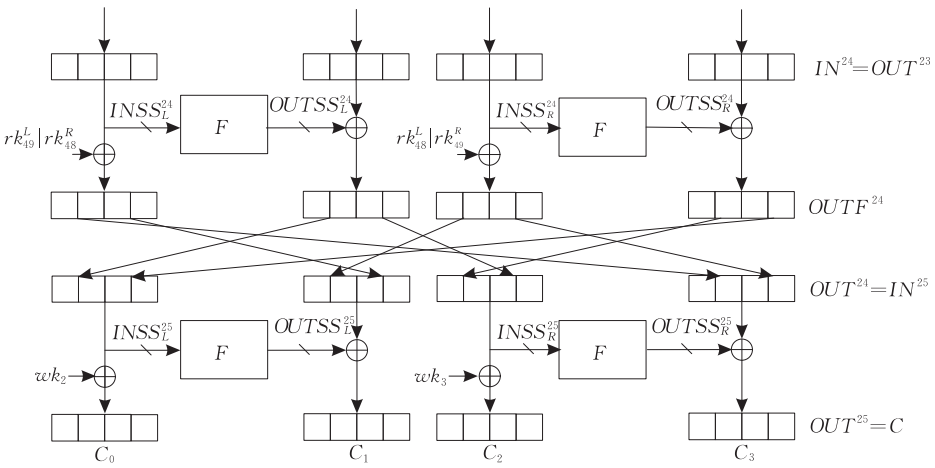

图 7 Piccolo 差分故障分析的相关记号示意图

4.2 Piccolo 算法差分故障分析的模型和原理

Piccolo 算法采用的 S 盒输入输出均为 4-bit，所以我们采用基于半字节的随机故障诱导模型. 假定攻击者可以对算法运行过程中某时刻的指定存储单元(如第 i 个寄存器)诱导随机的半字节故障，但不知道故障对应的半字节在存储单元中的位置及具体取值. 对于同一个明文 P，攻击者可以获得其在某一未知密钥 MK 下加密所得的正确密文和错误密文.

对 Piccolo 算法的差分故障分析原理如下：对任意明文 P 进行加密，获取对应的正确密文 C. 当加密过程运行到第 24 轮时，在输入的第 1 个和第 3 个寄存器中各诱导一次半字节随机故障，并记录相应的错误密文 C^A 和 C^B. 根据收集到的正确密文与错误密文，利用超级 S 盒的差分特性对白化密钥 wk_2 和 wk_3 进行筛选. 然后利用剩余的 wk_2 和 wk_3 值对密文 C 作一轮解密，同样利用超级 S 盒的差分特性确定 $rk_{49}^L|rk_{48}^R$ 以及 $rk_{48}^L|rk_{49}^R$ 的候选值，依据密钥扩展算法，得到 MK 的所有可能取值，最后利用 P 和 C 进行验证，确定唯一正确的 MK.

注意到很多采用广义 Fesitel 结构的分组密码的故障分析方法均采用了上述类似模型，而在实际攻击过程中，根据攻击者拥有的攻击设备和条件，诱导的故障可能并不在我们期望的存储单元中（如第 24 轮的第 1 个和第 3 个寄存器中），这时我们可借助于错误密文与正确密文的差分来判断故障诱导的位置是否恰好在所需的寄存器上. 如图 8 所示，若故障发生在第 24 轮输入的第 2 个寄存器上（不论发生在哪个半字节位置），则对应密文差分的活跃字节数不超过 3 个. 类似地，若故障发生在第 24 轮的第 4 个寄存器上，则对应密文差分的活跃字节数也不超过 3 个. 而由图 9 和图 10 可知，若故障发生在第 24 轮的第 1 个和第 3 个寄存器上，则对应密文差分的活跃字节数超过 4 个. 进一步，若 $(\Delta C_0)^R=0$，则故障位于第 1 个寄存器；若 $(\Delta C_0)^R\neq 0$，则故障位于第 3 个寄存器.

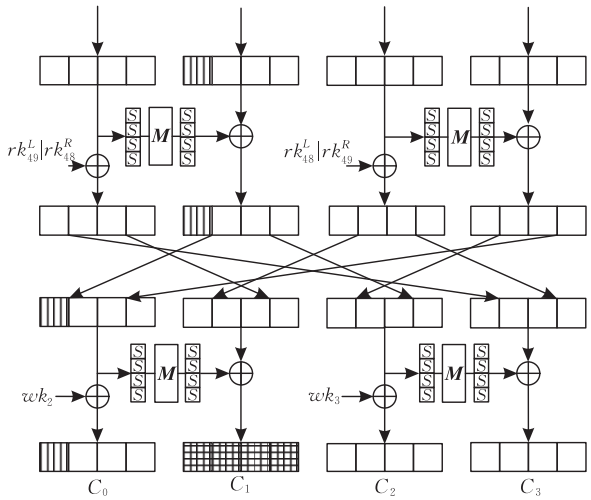

图 8　在第 24 轮输入的第 2 个寄存器处诱导随机半字节故障差分传播示意图

由以上分析可知，通过观测正确密文与对应错误密文的差分，可以有效地判断故障所在的寄存器，快速筛选出有效的错误密文进行分析，从而提高攻击的效率.

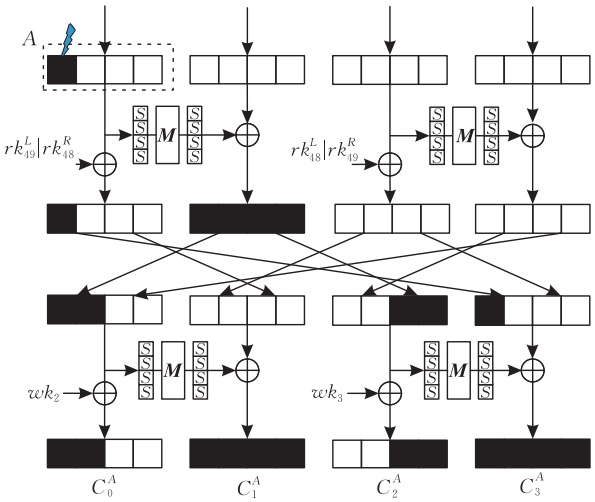

图 9　诱导的随机半字节故障在 A 处时差分传播示意图

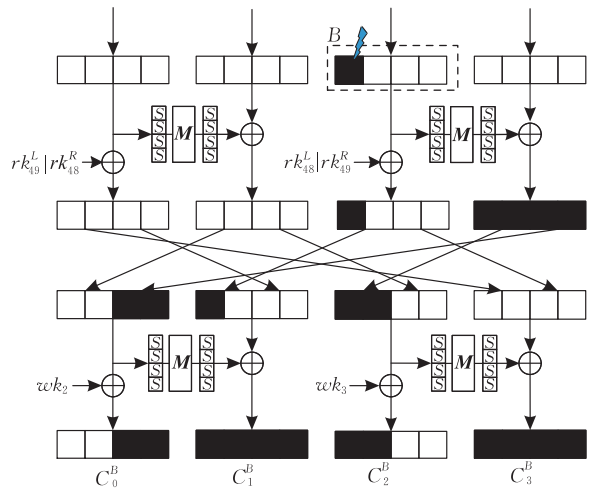

图 10　诱导的随机半字节故障在 B 处时差分传播示意图

4.3　攻击的详细步骤

攻击过程按照如下 5 个步骤进行：

1. 故障诱导和数据收集.

任意选择一个明文 P，在种子密钥 MK 的作用下加密，记录正确密文 C，当算法运行至第 24 轮时，在输入的第 1 个和第 3 个寄存器中分别诱导随机半字节故障，并记录相应的错误密文 C^A 和 C^B. 这里，C^A 表示故障位于 IN_0^{24} 处（图 9 中的 A 所示位置）时对应的错误密文，C^B 表示故障位于 IN_2^{24} 处（图 10 中的 B 所示位置）时对应的错误密文. 故障诱导后引入的差分传播如图 9 和图 10 所示.

2. 获取 wk_2，wk_3，rk_{48}，rk_{49} 的所有可能候选值.

2a. 通过正确密文 C 与错误密文 C^A，得到 F 函数亦即超级 S 盒的输入/输出差分，根据超级 S 盒的差分特性进行筛选，获得所有可能的输入值 $INSS_L^{25}$ 及 $INSS_R^{25}$，由于 $INSS_L^{25}\oplus wk_2=C_0$，$INSS_R^{25}\oplus wk_3=C_2$，可得 wk_2 的候选值集合 $\langle wk_{2A}\rangle$，wk_3 的候选值集合 $\langle wk_{3A}\rangle$. 进一步，利用 C 与错误密文 C^B 进行分析，可得到 wk_2 的候选值集合 $\langle wk_{2B}\rangle$ 及 wk_3 的

候选值集合$\langle wk_{3B}\rangle$.求$\langle wk_{2A}\rangle$与$\langle wk_{2B}\rangle$的交集,得到筛选后的wk_2候选值集合$\langle wk_2\rangle$;求$\langle wk_{3A}\rangle$与$\langle wk_{3B}\rangle$的交集,得到筛选后的wk_3候选值集合$\langle wk_3\rangle$.

2b. 利用步2a中得到的$wk_2\in\langle wk_2\rangle$,$wk_3\in\langle wk_3\rangle$,对$C$及$C^A$、$C^B$进行一轮解密,并记录对应的差分值$(\Delta OUTF^{24})^A$及$(\Delta OUTF^{24})^B$及由正确密文$C$进行一轮解密得到的$OUTF_0^{24}$及$OUTF_2^{24}$.利用超级S盒的差分特性,可获得所有可能的输入值$INSS_L^{24}$及$INSS_R^{24}$,由于$INSS_L^{24}\oplus(rk_{49}^L\,|\,rk_{48}^R)=OUTF_0^{24}$,$INSS_R^{24}\oplus(rk_{48}^L\,|\,rk_{49}^R)=OUTF_2^{24}$,可得$rk_{49}^L\,|\,rk_{48}^R$及$rk_{48}^L\,|\,rk_{49}^R$的候选值集合$\langle rk_{49}^L|rk_{48}^R\rangle$、$\langle rk_{48}^L|rk_{49}^R\rangle$.

3. 根据密钥扩展算法,得到MK中对应的k_3,k_4,k_0,k_1对应的候选值集合$\langle k_3\rangle$,$\langle k_4\rangle$,$\langle k_0\rangle$,$\langle k_1\rangle$.

4. 穷搜索k_2,得到MK的候选值集合$\langle MK\rangle$.

5. 利用P和C,通过$E_{MK}(P)=C$验证,得到唯一正确密钥MK.

4.4 复杂度分析

步2a的复杂度.通过步1中收集到的正确密文C与错误密文C^A,可以确定$\Delta INSS_L^{25}$,$\Delta INSS_R^{25}$的值,由于故障位置未知,$\Delta OUTSS_L^{25}$及$\Delta OUTSS_R^{25}$分别有$2\times2^4=32$种可能取值.按照3.3节所述分析模型,超级S盒的输入差分α值已经确定,但它对应的输出差分β未知,但我们知道输出差分候选值共有32个,在这32个可能取值中,31个可以视为对β扰动之后得到的差分γ,根据超级S盒的扰动差分传播特性(表4),平均意义下α和γ能够匹配的概率为42.6%且匹配后的平均值为3.675.由此可得,平均意义下$INSS_L^{25}$共有$3.8+31\times0.426\times3.675\approx52$个可能取值;类似地,$INSS_R^{25}$约有$3.8+31\times0.43\times3.684\approx53$种可能取值,对应可得$|\langle wk_{2A}\rangle|\approx52$,$|\langle wk_{3A}\rangle|\approx53$;同样地,利用$C$与错误密文$C^B$进行分析,可得平均意义下,$|\langle wk_{2B}\rangle|$与$|\langle wk_{3B}\rangle|$也分别为53和52.由于正确的$wk_2$和$wk_3$一定会包含在各个候选值集合中,而$2^{16}\times(52/2^{16})\times(53/2^{16})<1$,所以平均意义下,对两次的候选值集合求交集后,$|\langle wk_2\rangle|=1$,$|\langle wk_3\rangle|=1$.

步2b的复杂度.由3.2节所述差分传播性质(1)和(2)可知,$(\Delta OUTF_1^{24})^A$、$(\Delta OUTF_3^{24})^B$可直接由对应的密文差分观测到.求交集后$|\langle wk_2\rangle|=1$,$|\langle wk_3\rangle|=1$,利用wk_2和wk_3进行一轮解密后,$(\Delta OUTF_0^{24})^A$及$(\Delta OUTF_2^{24})^B$的取值也可相应确定,即超级S盒的输入/输出差分均可确定.根据超级S盒差分特性(表2),可得平均意义下$rk_{49}^L\,|\,rk_{48}^R$的候选值个数为6.53个,$rk_{48}^L\,|\,rk_{49}^R$的候选值个数也为6.53个.

步3的复杂度.根据密钥扩展算法知$|\langle k_3\rangle|=1$,$|\langle k_4\rangle|=1$,$|\langle k_0\rangle|\times|\langle k_1\rangle|=(6.53)^2\approx2^{5.4}$.

步4的复杂度.穷搜索k_2,可得到MK的候选值个数为$N=1\times1\times2^{5.4}\times2^{16}\approx2^{21.4}$个.

注意到在随机给定超级S盒输入/输出差分的情况下,要找到所有合适的输入值,需进行2^{16}次搜索.步2a需要$2\times2^{16}\times32=2^{22}$次搜索,步2b需要$2\times2^{16}$次搜索,即在得到$MK$候选值前共需要约$2^{22}$次搜索.若采用预计算模式,即事先计算并存储超级S盒输入/输出差分与输入值的对应关系,则可省去搜索时间,但需要耗费约$60\times2^{16}\times16+510\times2^{16}\times16$ bits$\approx2^{26}$ Bytes的存储空间.

分析结果表明,通过在第24轮输入状态的第1个和第3个寄存器各诱导1个随机半字节故障,利用正确密文与2个错误密文进行分析,能够将Piccolo算法80-bit的密钥空间缩小至约22-bit.

5 实验及结果

在PC机上(CPU:Pentium Dual-Core E6700 3.20GHz,RAM:2GB)使用C++语言编程(Visual C++6.0)对本文给出的攻击方法进行了200次模拟实验.对k_0,k_1,k_3,k_4共64-bit的种子密钥搜索空间分布情况进行统计,结果如图11所示,64-bit种子密钥的平均搜索空间约为6-bit,加上对k_2的搜索,对种子密钥的搜索空间平均约为22-bit.附录给出了一组实际的攻击实验数据及其结果.

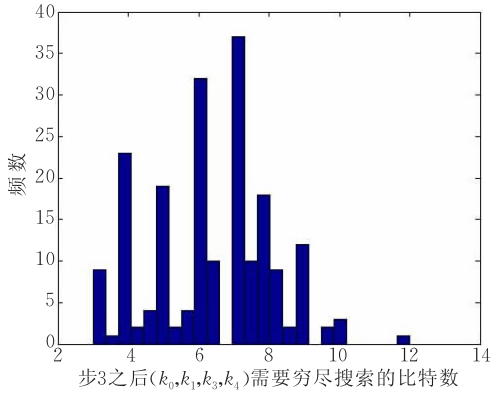

图11 对64-bit密钥(k_0,k_1,k_3,k_4)的搜索量分布图

6 结 语

本文提出了在半字节随机故障诱导模型下对Piccolo-80算法的差分故障分析方法,给出了Piccolo算法的一个等价结构,将S-P-S结构整体视为超级S盒,并根据所采用的故障模型研究了超级S盒的部分差分传播性质.理论分析和实验结果表明,在第24轮的第1个和第3个寄存器各诱导1个随机半字节故障,可将80-bit的密钥空间缩小至约22-bit.

这表明为安全使用 Piccolo 算法，在其实现时必须做一定的防护措施.

参 考 文 献

[1] Izadi M, Sadeghiyan B, Sadeghian S S, Khanooki H A. MIBS: A new lightweight block cipher//Proceedings of the CANS 2009. Kanazawa, Ishikawa, Japan, 2009: 334-348

[2] Guo J, Peyrin T, Poschmann A, Robshaw M. The LED Block Cipher//Proceedings of the CHES 2011. Nara, Japan, 2011: 326-341

[3] Hong D, Sung J, Hong S, Lim J, Lee S, Koo B, Lee C, Chang D, Lee J, Jeong K, Kim H, Kim J, Chee S. HIGHT: A new block cipher suitable for low-resource device//Proceedings of the CHES 2006. Yokohama, Japan, 2006: 46-59

[4] Wu Wen-Ling, Zhang Lei. LBlock: A lightweight block cipher//Proceedings of the ACNS 2011. Nerja (Malaga), Spain, 2011: 327-344

[5] Bogdanov A, Knudsen L, Leander G, Paar C, Poschmann A, Robshaw M J B, Seurin Y, Vikkelsoe C. PRESENT: An ultra-lightweight block cipher//Proceedings of the CHES 2007. Vienna, Austria, 2007: 450-466

[6] Gong Z, Nikova S, Law Y-W. A new family of lightweight block ciphers//Proceedings of the RFIDSec 2011. Amherst, Massachusetts, USA, 2012: 1-18

[7] Shibutani K, Isobe T, Hiwatari H, Mitsuda A, Akishita T, Shirai T. Piccolo: An ultra-lightweight blockcipher//Proceedings of the CHES 2011. Nara, Japan, 2011: 342-357

[8] Biham E, Shamir A. Differential fault analysis of secret key cryptosystems//Proceedings of the CRYPTO 1997. Santa Barbara, California, USA, 1997: 513-525

[9] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 1991, 4(1): 3-72

[10] Li Lin, Li Rui-Lin, Xie Duan-Qiang, Li Chao. Differential fault attack on KeeLoq and SHACAL-1. Journal of Wuhan University (Natural Science Edition), 2008, 54(5): 507-512 (in Chinese)
(李琳，李瑞林，谢端强，李超. KeeLoq 和 SHACAL-1 算法的差分故障攻击. 武汉大学学报理学版，2008，54(5)：507-512)

[11] You Jian-Xiong, Li Rui-Lin, Li Chao. Fault attack on light weight block cipher Keeloq. Acta Scientiarum Naturalium Universitatis Pekinensis, 2010, 46(5): 756-762(in Chinese)
(游建雄，李瑞林，李超. 轻量级分组密码 Keeloq 的故障攻击. 北京大学学报(自然科学版)，2010，46(5)：756-762)

[12] Zhao Xin-Jie, Wang Tao, Wang Su-Zhen, Wu Yang. Research on deep differential fault analysis against MIBS. Journal on Communications, 2010, 31(12): 82-89(in Chinese)
(赵新杰，王韬，王素贞，吴杨. MIBS 深度差分故障分析研究. 通信学报，2010，31(12)：82-89)

[13] Jovanovic P, Kreuzer M, Polian I. A fault attack on the LED block cipher//Proceedings of the COSADE 2012. Darmstadt, Germany, 2012: 120-134

[14] Li Wei, Gu Da-Wu, Zhao Chen, Liu Zhi-Qiang, Liu Ya. Security analysis of the LED lightweight cipher in the internet of things. Chinese Journal of Computers, 2012, 35(3): 434-445(in Chinese)
(李玮，谷大武，赵辰，刘志强，刘亚. 物联网环境下 LED 轻量级密码算法的安全性分析. 计算机学报，2012，35(3)：434-445)

[15] Zhao Liang, Nishide T, Sakurai K. Differential fault analysis of full LBlock//Proceedings of the COSADE 2012. Darmstadt, Germany, 2012: 135-150

[16] Fan Wei-Jie, Wu Wen-Ling, Zhang Lei. Differential fault analysis on HIGHT. Journal of the Graduate School of the Chinese Academy of Sciences, 2012, 29(2): 271-276(in Chinese)
(范伟杰，吴文玲，张蕾. HIGHT 算法的差分故障攻击. 中国科学院研究生院学报，2012，29(2)：271-276)

[17] Giraud C, Thiebeauld H. A survey on fault attacks//Proceedings of the CARDIS 2004. Toulouse, France, 2004: 159-176

[18] Bar-El H, Choukri H, Naccache D, Tunstall M, Whelan C. The sorcerer's apprentice guide to fault attacks. Proceedings of IEEE, 2006, 94(2): 370-386

[19] Wang Yan-Feng, Wu Wen-Ling, Yu Xiao-Li. Biclique cryptanalysis of reduced-round piccolo block cipher//Proceedings of the Information Security Practice and Experience. Hangzhou, China, 2012: 337-352

[20] Daemen J, Rijmen V. Understanding two-round differentials in AES//Proceedings of the SCN 2006. Maiori, Italy, 2006: 78-94

附录. 一组攻击实验数据及其结果.

明文 P：　7d20 7242 49e9 4dc2
加密密钥 MK：　6881 15c2 5d98 4af9 5919
正确密文 C：　6e3a c0c8 a0d2 7a1c
错误密文 C^A：　b93a 04cf a036 8e59
错误密文 C^B：　6e15 0c74 75d2 aa30

$\langle wk_{2A}\rangle$：108 个：

2226 2249 2259 226e 22be 22c6 22d0 22e0 2520 254e 255e 2569 25b9 25c0 25d6 25e6 2e22 2e55 3204 3214 323c 327b 3282 329c 32ab 32f2 350b 351b 3532 3574 358c 3592 35a4 35fc 3e4d 3ec4 490e 4ef8 5911 595e 599e 59aa 59b9 59ca 59e1 59f9 5e12 5e55 5e95 5eac 5eb7 5ecc 5ee2 5ef7 8912 8955 8995 89ac 89b7 89cc 89e2 89f7 8e11 8e5e 8e9e 8eaa 8eb9 8eca 8ee1 8ef9 99f8 9e0e e20b e21b e232 e274 e28c e292 e2a4 e2fc e504 e514 e53c e57b e582 e59c e5ab e5f2 e94d e9c4 f220 f24e f25e f269 f2b9 f2c0 f2d6 f2e6 f526 f549 f559 f56e f5be f5c6 f5d0 f5e0 f922 f955

$\langle wk_{3A}\rangle$：58 个

0556 05b2 0919 09fd 176e 178a 300c 30e8 3a0d 3ae9 4711 47f5 4a19 4afd 4d56 4db2 5118 51fc 5b15 5bf1 6109 61ed 6415 64f1 6f08 6f1d 6fec 6ff9 7e18 7efc 8611 86f5 8c52 8cb6 9b0c 9be8 9c0d 9ce9 a01c a0f8 a518 a5fc ad08 adec ae09 ae11 aeed aef5 be6e be8a cd11 cdf5 ec15 ecf1 ed56 edb2 f915 f9f1

$\langle wk_{2B}\rangle$：38 个

035e 0371 0388 03a7 25d1 25fe 2d0f 2d20 2fde 2ff1 475e 4771 59d6 59f9 6918 6937 6a59 6a76 7a90 7abf 7cc9 7ce6 9246 9269 985e 9871 9c51 9c7e ac00 ac2f d290 d2bf e3c6 e3e9 e6d1 e6fe f4d1 f4fe

$\langle wk_{3B}\rangle$：176 个

2804 2819 282a 283f 2872 2883 2899 289b 28ac 28bf 28e0 2d03 2d10 2d2c 2d37 2d7b 2d84 2d90 2d92 2daa 2db7 2de9 380c 381b 3823 3870 3883 388a 3899 38a4 38d8 38e2 38f8 3d0a 3d12 3d24 3d79 3d84 3d8c 3d90 3da3 3dd6 3deb 3df6 4a19 4a39 4a46 4a6c 4a72 4a95 4ac2 4ad3 4ae7 4af1 4b02 4b29 4b33 4b56 4b62 4b85

4ba7 4bb1 4bcc 4bd9 4e06 4e1b 4e21 4e4e 4e64 4e66 4e70 4e9f
4ed1 4eda 4eed 4ef8 4f00 4f11 4f2b 4f31 4f3a 4f5e 4f76 4f8f
4fad 4fb8 4fc4 4fc6 9a00 9a11 9a2b 9a31 9a3a 9a5e 9a76 9a8f
9aad 9ab8 9ac4 9ac6 9b06 9b1b 9b21 9b4e 9b64 9b66 9b70 9b9f
9bd1 9bda 9bed 9bf8 9e02 9e29 9e33 9e56 9e62 9e85 9ea7 9eb1
9ecc 9ed9 9f19 9f39 9f46 9f6c 9f72 9f95 9fc2 9fd3 9fe7 9ff1
e80a e812 e824 e879 e884 e88c e890 e8a3 e8d6 e8eb e8f6 ed0c
ed1b ed23 ed70 ed83 ed8a ed99 eda4 edd8 ede2 edf8 f803 f810
f82c f837 f87b f884 f890 f892 f8aa f8b7 f8e9 fd04 fd19 fd2a
fd3f fd72 fd83 fd99 fd9b fdac fdbf fde0

$\langle wk_2 \rangle$：1 个

59f9

$\langle wk_3 \rangle$：1 个

4a19

$\langle rk_{49}^{L} \mid rk_{48}^{R} \rangle$：8 个

0e74 0e7d 1836 183f 34f6 34ff 5ca4 5cad

$\langle rk_{48}^{L} \mid rk_{49}^{R} \rangle$：8 个

4b73 4f73 5be9 5fe9 abe7 afe7 eb75 ef75

恢复出的正确密钥 MK：

6881 15c2 5d98 4af9 5919

ZHAO Guang-Yao, born in 1982, Ph. D. candidate. His research interest is coding theory and crypotography.

LI Rui-Lin, born in 1982, Ph. D., lecturer. His research interest is coding theory and crypotography.

SUN Bing, born in 1981, Ph. D., lecturer. His research interest is coding theory and crypotography.

LI Chao, born in 1966, Ph. D., professor. His research interest is coding theory and crypotography.

Background

Due to the rapid and large development of low resource devices such as RFID tags and sensor nodes which need cryptographic algorithms to provide security and privacy, lightweight block ciphers received a lot of attention in recent years. There exist many lightweight block ciphers such as PRESENT, MIBS, LBlock, Piccolo, LED etc. which are usually implemented in special hardware or software environments. Hence, they may suffer from a kind of physical attacks—the so-called fault attack.

Fault attack is where the adversary could actively disturb part of the internal states, or cause calculation errors during the execution of a cryptographic algorithm. The idea of using faults to break the cryptosystems was introduced by Boneh et al. from Bellcore in 1996. They showed that in the RSA-CRT setting, a single computational mistake can completely break the scheme by factoring the public key. In 1997, Biham and Shamir extended such idea and proposed the method of differential fault analysis (DFA), and applied it to DES successfully. Since then, DFA had been applied to many other block ciphers, such as AES, Camellia, CLEFIA, IDEA, SMS4, PRESENT, Keeloq, etc. By introducing some faults to the states during a normal execution of a cryptographic algorithm, this kind of attack can derive the information about the secret key by differential analysis based on both the right and wrong outputs of the target algorithm.

At CHES 2011, a new ultra-lightweight block cipher Piccolo was proposed by Shibutani et al. Piccolo has great hardware and software performances, and its energy cost per bit is very low. It achieves both high security and extremely compact implementation. The key size of Piccolo is 80-bit/128-bit, and the corresponding round number is 25/31. Piccolo adopts a variant of generalized Feistel structure, and its round transformation consists of the round function S-P-S and the round permutation PR. The designers show that Piccolo is resistant against most classical attacks such as differential and linear cryptanalyses. At ISPEC 2012, Wang Yanfeng et al. presented a biclique cryptanalysis of the full round Piccolo-80 without postwhitening keys and 28-round Piccolo-128 without prewhitening keys by analyzing the distribution of the subkeys.

This paper presents a first differential fault analysis on Piccolo-80 based on the random nibble-oriented fault model by treating the S-P-S function as a Super Sbox. After introducing 1 fault in the first and third register of the input of the 24th round respectively, the keyspace can be reduced from 80-bit to about 22-bit. This indicates that cryptographic devices supporting Piccolo should be carefully protected.

Our work is supported by the National Natural Science Foundation of China (61103192, 61070215), and the Opening Projector of State Key Laboratory of Information Security (01-02-5). One aim of these projects is to evaluate the security of block ciphers.