doi:10.11959/j.issn.1000-436x.2015016

针对 SMS4 轮输出的选择明文能量分析攻击

王敏[1,2]，杜之波[2]，吴震[2]，饶金涛[2]
（1. 四川大学 电子信息学院，四川 成都 610041；2. 成都信息工程学院 信息安全工程学院，四川 成都 610225）

摘 要：提出了针对 SMS4 轮输出的选择明文能量分析攻击，攻击时以一定约束条件选择明文，先攻击出轮迭代函数的输出，再由轮迭代函数的输出反推出对应的轮子密钥，从而实现了以轮输出作为中间数据对 SMS4 的能量分析攻击，并利用该方法对无防护 SMS4 算法的能量曲线进行了能量分析攻击，实验表明该攻击方法是行之有效的。
关键词：SMS4 算法；能量分析攻击；轮输出；选择明文
中图分类号：TP309.1 **文献标识码**：A

Chosen-plaintext power analysis attack against SMS4 with the round-output as the intermediate data

WANG Min[1,2], DU Zhi-bo[2], WU Zhen[2], RAO Jin-tao[2]
(1. College of Electronics and Information Engineering, Sichuan University, Chengdu 610041, China;
2. School of Information Security Engineering, Chengdu University of Information Technology, Chengdu 610225, China)

Abstract: The method of chosen-plaintext power analysis attack against SMS4 with the round-output as the intermediate data is proposed. Firstly, this method attacks out the output of the iterative function. Then the sub key can be achieved by the output of the iterative function. And it is achieved to make the attack real and improve the efficiency, when SMS4 is attacked by taking of the method. In particular, the actual experiment of the method is done, and the results show that the attack algorithm is correct and effective.
Key words: SMS4 algorithm; power analysis attack; round output; chosen-plaintext

1 引言

能量分析攻击是通过采集加密芯片等硬件密码电子设备在进行加解密或签名等操作时产生的能量消耗，利用密码学和统计学原理等，选择合适的能量泄露模型，分析和破译密钥信息的一种攻击方式[1~4]，能量分析攻击又分为简单功耗分析攻击(SPA, simple power analysis)、差分能量分析(DPA, differential power analysis)、相关性能量分析攻击(CPA, correlation power analysis)。

国内官方公布的第一个商用密码算法—— SMS4 算法[5]，作为国内无线局域网标准的重要组成部分，对其安全性研究具有十分重要的意义。自 SMS4 算法公布起，学术界对 SMS4 的能量分析攻击展开了一系列的研究，文献[6~8]对 SMS4 算法的 S 盒子输入、S 盒子输出和循环移位成功实施了能量分析攻击，而在以轮输出作为信息泄露点进行能量分析攻击方面，尚未发现国内外有公开发表的结果，因此研究将轮输出作为中间数据对 SMS4 能量分析攻击，对提高 SMS4 算法的安全性具有重要的现实意义。

收稿日期：2013-10-18；**修回日期**：2014-01-25
基金项目：国家重大科技专项基金资助项目（2014ZX01032401-001）；国家高技术研究发展计划（863 计划）基金资助项目（2012AA01A403）；“十二五”国家密码发展基金资助项目（MMJJ201101022）；四川省科技支撑计划项目基金资助项目（2014GZ0148）；四川省教育厅重点科研基金资助项目（13ZA0091）；成都信息工程学院科研基金资助项目（CRF201301）
Foundation Items: The National Science and Technology Major Project (2014ZX01032401-001); The National High Technology Research and Development Program (863 Program) (2012AA01A403); “The 12th Five-Years” National Cryptogram Development Fund (MMJJ201101022); Sichuan Science and Technology Support Programmer (2014GZ0148); Sichuan Provincial Education Department Key Scientific Research Projects (13ZA0091); The Scientific Research Foundation of CUIT (CRF201301)

本文针对 SMS4 轮输出结构特点，具体分析了 SMS4 轮输出抗能量分析攻击的安全性，以轮输出作为中间数据直接对 SMS4 能量分析攻击出轮子密钥，存在需要采集和处理极多的能量曲线问题，导致对 SMS4 轮输出的能量分析攻击在实际数据分析和处理上不可行。为此提出了针对 SMS4 轮输出的选择明文能量分析攻击方法，以轮输出作为中间数据，先能量分析攻击出轮迭代函数的输出，再由轮迭代函数的输出反推出对应的轮子密钥，间接地实现了对 SMS4 轮输出能量分析攻击出轮子密钥的目的，给出实测的 CPA 攻击分析结果，验证了使用该方法，不仅可以成功对 SMS4 轮输出实施能量分析攻击，而且降低了采集和处理能量曲线的条数，提高了攻击效率。

2　SMS4 算法

2.1　SMS4 加解密算法

SMS4 算法中分组长度和密钥长度均为 128 bit，加密算法和解密算法均为 32 轮的非线性迭代密码算法，其加解密算法结构相同，只是运算时轮密钥使用的顺序相反，以加密算法为例，SMS4 加密算法的详细流程[6]如图 1 所示。

在图 1 中，$X_i \in Z_2^{32}$ (Z_2^e 表示 e bit 的向量集)，明文输入为$(X_0, X_1, X_2, X_3) \in (Z_2^{32})^4$，密文输出为$(Y_0, Y_1, Y_2, Y_3)$，其中，$X_i$、$X_{i+1}$、$X_{i+2}$和 X_{i+3} 为轮迭代运算函数 F 的输入，$rk_i \in Z_2^{32}$ 为每轮的轮子密钥，其中，$i \in \{0, 1, 2, \cdots, 31\}$。

从加密的流程可以看出，轮迭代函数 F 包括的运算有异或、非线性变换 τ 和线性变换 L，如式（1）所示。

$$\begin{aligned} X_{i+4} &= \mathrm{F}(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i) \\ &= X_i \oplus \mathrm{T}(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i) \end{aligned} \tag{1}$$

图 1 中，T 表示合成置换，是由非线性变换 τ 和线性变换 L 复合而成，迭代函数 F 的详细的流程[6]如图 2 所示。

在合成置换 T 中，非线性变换 τ 是由 4 个并行 S 盒子构成，每个 S 盒子为固定的 8 bit 输入 8 bit 输出的置换，记为 $b_k = Sbox(a_k)$，其中 $k \in \{0,1,2,3\}$，$b_k \in Z_2^8$，$a_k \in Z_2^8$，a_k 为 S 盒子输入，b_k 为 S 盒子输出，设 $A = a_0 \| a_1 \| a_2 \| a_3 = X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i$，$B = b_0 \| b_1 \| b_2 \| b_3$，其中，‖表示 2 个数据 bit 的拼接，则非线性变换 τ 为

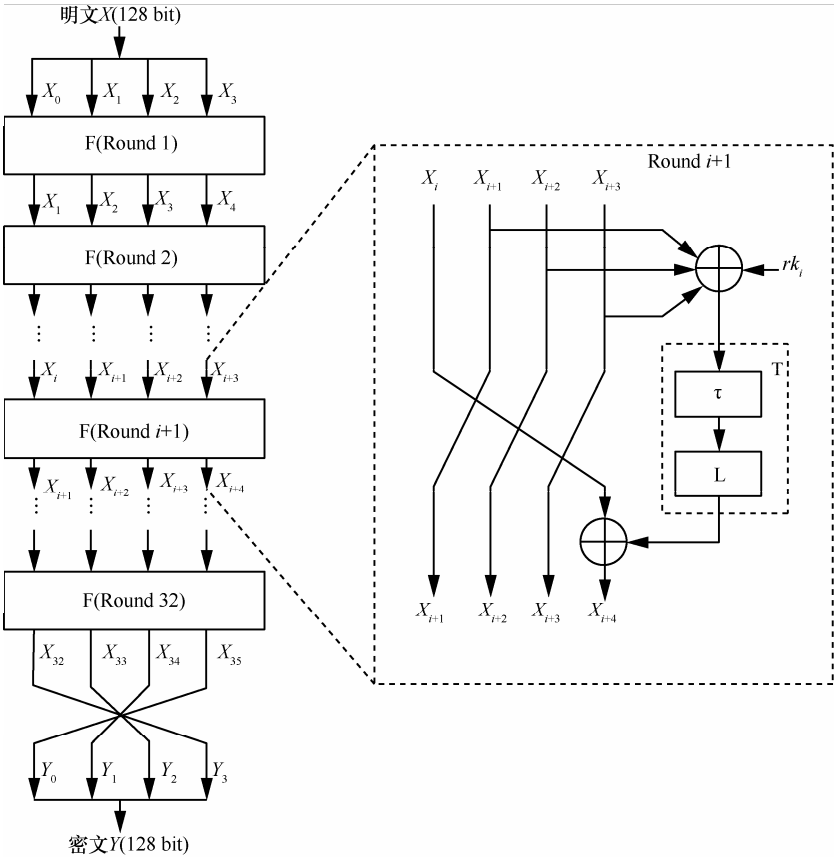

图 1　SMS4 的加密算法流程

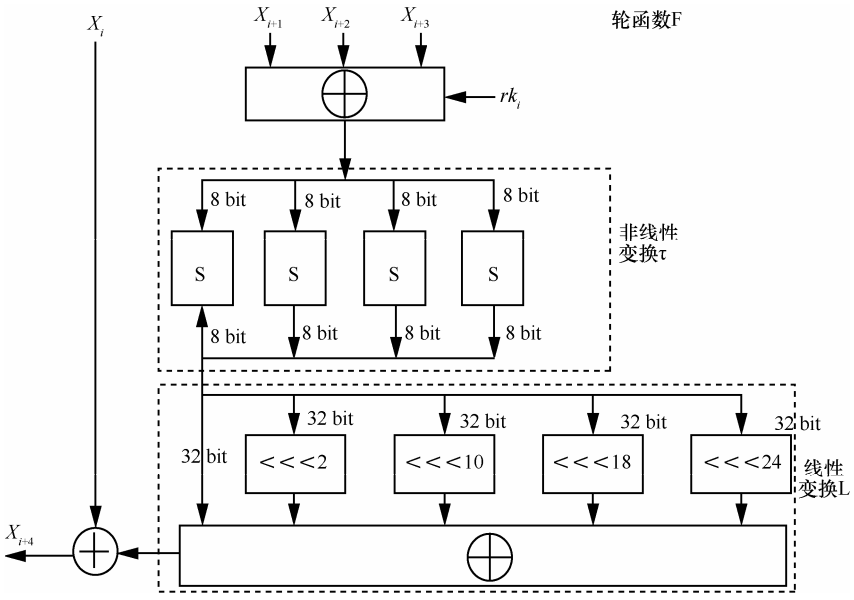

图 2 迭代函数 F 的流程

$$B=\tau(A)=Sbox(a_0)\|Sbox(a_1)\|Sbox(a_2)\|Sbox(a_3) \quad (2)$$

线性变换 L 的描述为

$$C=\mathrm{L}(B)=B\oplus(B<<<2)\oplus(B<<<10)\oplus(B<<<18)\oplus(B<<<24) \quad (3)$$

其中，$C\in Z_2^{32}$，$B\in Z_2^{32}$，C 为线性变换 L 的输出，B 为线性变换 L 的输入，同时也是非线性变换 τ 的输出。

2.2 SMS4 密钥扩展算法

SMS4 的 32 轮子密钥是由输入密钥经过 SMS4 的密钥扩展算法生成的，密钥扩展算法的流程和加密算法类似，设输入的密钥为 $MK=(MK_0, MK_1, MK_2, MK_3)$，$MK_i\in Z_2^{32}$ $(i=0,1,2,3)$；令 $K_i\in Z_2^{32}$，$i=0,1,\cdots,35$，轮密钥为 $rk_i\in Z_2^{32}$，$i=0,1,\cdots,31$，则密钥扩展方法如下

$$(K_0,K_1,K_2,K_3)=(MK_0\oplus FK_0, MK_1\oplus FK_1, MK_2\oplus FK_2, MK_3\oplus FK_3) \quad (4)$$

$$rk_i=k_{i+4}=K_i\oplus \mathrm{T}'(K_{i+1}\oplus K_{i+2}\oplus K_{i+3}\oplus CK_i) \quad (5)$$

其中，$FK=(FK_0,FK_1,FK_2,FK_3)$ 和 $CK=(CK_0, CK_1,\cdots,CK_{31})$ 为已知系统参数[4]，T′ 变换和 T 变换基本相同，不同的是线性变换 L 被修改为 L′。

$$\mathrm{L}'(B)=B\oplus(B<<<13)\oplus(B<<<23) \quad (6)$$

3 能量分析攻击

在能量分析攻击中，CPA 和 DPA 相比 SPA 具有更强的攻击性，所以能量分析攻击中比较常用的是 CPA 和 DPA，DPA 根据被攻击算法选取合适的区分函数，对功耗曲线进行差分分析来破解密钥[1]，CPA 攻击的过程如下。

1) 随机选择 N 组不相同明文 M_i $(i\in[1,N])$ 进行加密运算，采集每组明文进行加密运算时设备产生的能量曲线 T_i。

2) 猜测密钥 K_l $(l\in\Omega$，Ω 为密钥空间)，计算在 K_l 和 M_i 条件下，密码算法进行加密运算时在被攻击点产生的中间值 $D_{i,l}$。

3) 取中间值 $D_{i,l}$ 的汉明距离或者汉明重量建立功耗模型 $h_{i,l}$，根据皮尔逊相关系数计算 T_i 和 $h_{i,l}$ 相关性 ρ_l。

4) 相关性取最大值时对应的 K_l，即为实际密钥。

4 针对 SMS4 轮输出的选择明文能量分析攻击

4.1 SMS4 轮输出抗能量攻击分析

SMS4 每轮的轮输出，需要在寄存器中存储，因此数据在轮输出和保存数据的过程中，其数据的汉明重量或者汉明距离特性，将被能量曲线泄露，所以可选择轮输出作为能量分析攻击的中间数据，对 SMS4 实施能量分析攻击。选择轮输出作为中间数据，对 SMS4 进行能量分析攻击，此时要攻击分析的运算表达式(1)，在式(1)中，SMS4 移位操作将轮子密钥的影响扩散到较多轮输出位中，因此，在攻击 rk_i 的时候，不能采取一次攻击 rk_i 的若干比特，经过多次攻击的方法来攻击完整的 rk_i，而必须采取一次攻击 rk_i 完整的 32 bit 的方法来攻击

rk_i，而攻击 rk_i 的整个 32 bit 时，密钥的搜索空间为$[0, 2^{32}-1]$，该搜索空间比较大，且攻击所需采集和处理的能量条数至少为 2^{32}，因此搜索空间和所需处理曲线条数极大地增加了能量分析攻击的计算困难复杂度和处理数据的难度，使以轮输出作为中间数据，对 SMS4 轮输出能量分析攻击出轮子密钥不切实际，所以 SMS4 轮输出可以抵御能量分析攻击。

4.2　对 SMS4 轮输出的选择明文能量分析攻击原理分析

针对 4.1 节提出的针对 SMS4 轮输出能量分析攻击不可行的问题，本文提出了针对 SMS4 轮输出的选择明文能量分析攻击，令 res_i 表示为 T 置换后的结果，如下

$$res_i = \mathrm{T}(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i) \tag{7}$$

则此时被攻击的运算表达式变为

$$X_{i+4} = X_i \oplus res_i \tag{8}$$

针对 SMS4 轮输出的选择明文能量分析攻击的基本思想是：将轮输出 X_{i+4} 作为中间数据，先不直接攻击出 SMS4 的轮子密钥 rk_i，而先由式(8)攻击出 res_i。攻击时，以一定约束条件选择特殊的明文 X_0、X_1、X_2 和 X_3，使式(7)中 res_i 为固定常数，所以在攻击表达式(8)中，X_i 是输入的明文，对攻击者来讲是已知的，res_i 是攻击的目标，对攻击者来讲是未知的，X_{i+4} 对攻击者来讲虽然是未知的，但其被输出和保存到寄存器过程中，其汉明重量或者汉明距离特性通过能量曲线被泄露，所以选择合适的能量泄露模型，将轮输出作为能量分析攻击的中间数据，即可能量分析攻击出 res_i。

能量分析攻击 res_i 时，在被攻击的表达式(8)中，异或运算是线性变换，X_{i+4} 和 res_i 之间的数据影响关系是按比特一一对应的，所以，一次可攻击 res_i 为 p bit，经过 q(pq=32)次攻击，即可攻击出完整的 res_i。

由于 res_i 为线性变换 L 的输出，如式(3)所示，故可由 res_i 唯一地反推出对应的 B_i。

而 B_i 为 S 盒子的输出的拼接，如式(2)所示，由于 S 盒子为 8 输入 8 输出，且 S 盒子内容不重复，故可由 S 盒子输出唯一地反推出 S 盒子输入 A_i，又由于 $A_i = X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i$，所以可由 A_i 的反推出 rk_i。

所以，当能量分析攻击出 res_i 后，便可以唯一地反推出对应轮子密钥 rk_i，再由密钥扩展算法，即可逆推出加解密密钥[9]。

4.3　对 SMS4 轮输出的选择明文能量分析攻击方法

针对 SMS4 选择明文能量分析攻击的详细攻击方法如下。

1) 首先攻击第一轮，此时 i=0。

2) 以一定约束条件选择特殊的 X_0、X_1、X_2 和 X_3，使 X_{i+1}、X_{i+2} 和 X_{i+3} 三者的异或结果为固定数，用 D 来表示，则 X_{i+1}、X_{i+2} 和 X_{i+3} 满足的约束条件如式(9)所示，同时保证 X_i 的随机性。

$$D = X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \tag{9}$$

3) 采集大量不同的特殊明文 X_0、X_1、X_2 和 X_3 在 SMS4 密码设备上运行时的能量曲线，将 X_{i+4} 作为中间数据，对 SMS4 进行能量分析攻击，攻击出 res_i。

4) 攻击出 res_i 后，再由表达式 $res_i = \mathrm{T}(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i) = \mathrm{T}(D \oplus rk_i)$ 反推出对应的轮子密钥 rk_i。

5) i 自增，返回 2)继续攻击下一轮，直到攻击前 4 轮的轮子密钥。

当攻击出前 4 轮的扩展子密钥后，根据密钥扩展算法，即可逆向计算出初始密钥。

在攻击时，由于选择一次攻击部分比特，经过多次攻击的方式攻击完整的 res_i，所以该方法达到了降低单次攻击时密钥猜测空间的目的，通过 res_i 再反推出对应的 rk_i，使针对 SMS4 轮输出的能量分析攻击在计算和实际实现上可行，所以，由于针对 SMS4 轮输出的选择明文能量分析攻击方法的提出，使无防护 SMS4 轮输出成为了能量分析攻击的攻击点。

5　针对 SMS4 轮输出的选择明文能量分析攻击实验

5.1　能量分析攻击实验环境

实验对象为 FPGA 上实现的无防护 SMS4 算法，被攻击的密钥 K 为 0x0123456789abcdeffedcba9876543210，实验软硬件环境：Inspector 软件，功耗曲线采集平台示波器。每轮攻击所用的曲线条数为 1 000 条，曲线预处理为 Inspector 软件中的低通滤波，滤波参数为 4。

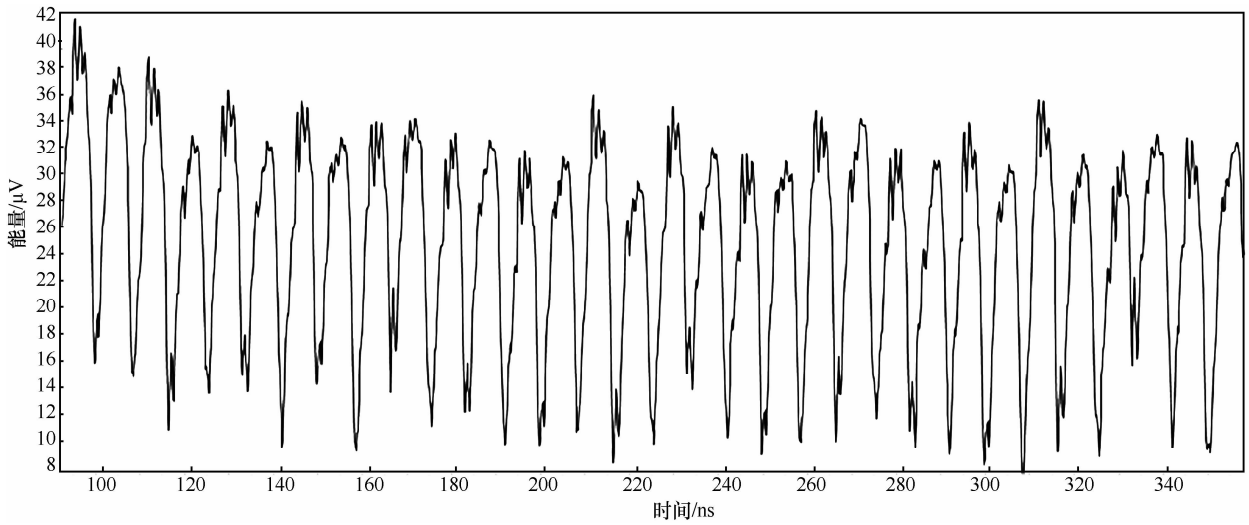

图 3 第 1 轮选择明文能量分析攻击低通后的能量曲线

5.2 对 SMS4 第 1 轮的选择明文能量分析攻击

第 1 轮的轮输入为待加密的明文，即为 X_0、X_1、X_2和 X_3，则第 1 轮的轮输出为 $X_4 = X_0 \oplus \mathrm{T}(X_1 \oplus X_2 \oplus X_3 \oplus rk_0)$，根据选择明文能量分析攻击的思想，选择特殊的明文 X_1、X_2和 X_3，约束条件为：$D = X_1 \oplus X_2 \oplus X_3 = 0$，同时保证明文的 X_0 随机性。采集到的能量曲线经低通滤波后的结果如图 3 所示。

对低通后的能量曲线实施 CPA，攻击结果如下图 4 所示，取相关性系数最大值对应的结果作为攻击结果，即第 1 轮的 res_0 =0x34E2E3A4，又由于 $res_0 = \mathrm{T}(X_1 \oplus X_2 \oplus X_3 \oplus rk_0) = \mathrm{T}(rk_0)$，所以可反推出第一轮的轮子密钥为 rk_0 =0xF12186F9。

```
Best correlation 1;
0,sub key:52(0x34),value:0.0575,at position:135
1,sub key:203(0xCB),value:-0.0575,at position:135
Best correlation 2:
0,sub key:226(0xE2),value:0.0757,at position:93
1,sub key:29(0x1D),value:-0.0757,at position:93
Best correlation 3:
0,sub key:227(0xE3),value:0.0541,at position:135
1,sub key:28(0x1C),value:-0.0541,at position:135
Best correlation 4:
0,sub key:164(0xA4),value:0.0559,at position:93
1,sub key:91(0x15B),value:-0.0559,at position:93
Round One res:34 E2 E3 A4
```

图 4 第 1 轮的攻击结果

5.3 对 SMS4 第 2 轮的选择明文能量分析攻击

在已经攻击出第 1 轮的轮密钥基础上，对第 2 轮进行选择明文能量分析攻击，第 2 轮的轮输出为 $X_5 = X_1 \oplus \mathrm{T}(X_2 \oplus X_3 \oplus X_4 \oplus rk_1)$，根据选择明文能量分析攻击的思想，选择特殊的明文 X_0、X_1、X_2和 X_3，满足 $D = X_2 \oplus X_3 \oplus X_4 = 0$，同时保证明文的 X_1 随机性，采集到的能量曲线经低通滤波后的结果如图 5 所示。

对低通后的能量曲线实施 CPA，攻击结果如下图 6 所示，取相关性系数最大值对应的结果作为攻击结果，即第 2 轮的 res_1 =0x750F11AD，又由于 $res_1 = \mathrm{T}(X_2 \oplus X_3 \oplus X_4 \oplus rk_1) = \mathrm{T}(rk_1)$，所以可反推出第 2 轮的轮子密钥为 rk_1 =0x41662b61。

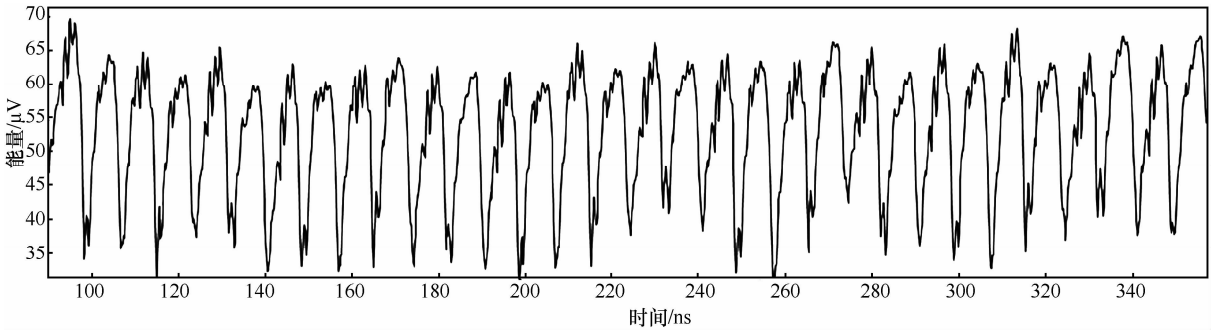

图 5 针对第 2 轮选择明文能量分析攻击低通后的能量曲线

```
Best correlation 1;
0,sub key: 117(0x75),value:-0.0784,at position:130
1,sub key:138(0x8A),value:0.0784,at position:130
Best correlation 2:
0,sub key:15(0x0F),value:-0.1037,at position:89
1,sub key: 240(0xF0),value:0.1037,at position:89
Best correlation 3:
0,sub key:17(0x11),value:-0.0899,at position:173
1,sub key:238(0xEE),value:0.0899,at position:173
Best correlation 4:
0,sub key:173(0xAD),value:-0.0634,at position:127
1,sub key:82(0x52),value:0.0634,at position:127
Round One res:75 0F 11 AD
```

图 6　第 2 轮的攻击结果

5.4　对 SMS4 第 3 轮的选择明文能量分析攻击

在已经攻击出第 1 轮和第 2 轮的轮密钥基础上，对第 3 轮进行选择明文能量分析攻击，第 3 轮的轮输出为 $X_6=X_2\oplus \mathrm{T}(X_3\oplus X_4\oplus X_5\oplus rk_2)$，根据选择明文能量分析攻击的思想，选择特殊的明文 X_0、X_1、X_2 和 X_3，约束条件为：$D=X_3\oplus X_4\oplus X_5=0$，同时保证明文的 X_2 随机性，采集到的能量曲线经低通滤波后的结果如图 7 所示。

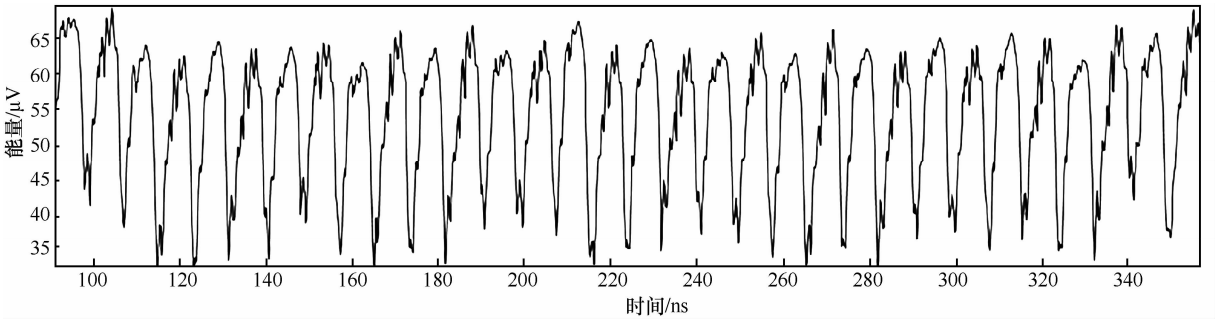

图 7　针对第 3 轮选择明文能量分析攻击低通后的能量曲线

对低通后的能量曲线实施 CPA，攻击结果如图 8 所示，取相关性系数最大值对应的结果作为攻击结果，即第 3 轮的 res_2=0x9F243EEF，又由于 $res_2=\mathrm{T}(X_3\oplus X_4\oplus X_5\oplus rk_2)=\mathrm{T}(rk_2)$，所以可反推出第 3 轮的轮子密钥为 rk_2=0x5A6AB19A。

```
Best correlation 1;
0,sub key:159(0x9F),value:-0.0828,at position:173
1,sub key:96(0x60),value:0.0828,at position:173
Best correlation 2:
1,sub key:36(0x24),value:-0.0883,at position:217
0,sub key: 219(0xDB),value:0.0883,at position:217
Best correlation 3:
1,sub key:62(0x3E),value:-0.0970,at position:217
0,sub key:193(0xC1),value:0.0970,at position:217
Best correlation 4:
0,sub key:239(0xEF),value:-0.0664,at position:173
1,sub key:16(0x10),value:0.0664,at position:173
Round One res:9F 24 3E EF
```

图 8　第 3 轮的攻击结果

5.5　对 SMS4 第 4 轮的选择明文能量分析攻击

在已经攻击出第 1 轮、第 2 轮和第 3 轮的轮密钥基础上，对第 4 轮进行选择明文能量分析攻击，第 4 轮的轮输出为 $X_7=X_3\oplus \mathrm{T}(X_4\oplus X_5\oplus X_6\oplus rk_3)$，根据选择明文能量分析攻击的思想，选择特殊的明文 X_0、X_1、X_2 和 X_3，约束条件为：$D=X_4\oplus X_5\oplus X_6=0$，同时保证明文的 X_3 随机性，采集到的能量曲线经低通后的曲线波形如图 9 所示。

对低通后的能量曲线实施 CPA，攻击结果如图 10 所示，取相关性系数最大值对应的结果作为攻击结果，即第 4 轮的 res_3=0xFE5213BF，又由于 $res_3=\mathrm{T}(X_4\oplus X_5\oplus X_6\oplus rk_3)=\mathrm{T}(rk_3)$，所以可反推出第 4 轮的轮子密钥为 rk_3=0x7ba92077。

5.6　攻击结果及性能对比

每轮子密钥的攻击过程相同，攻击从采集曲线

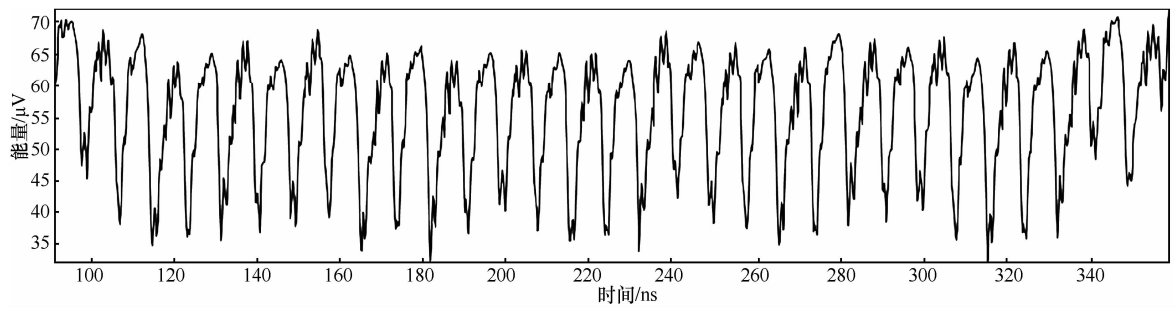

图 9　针对第 4 轮选择选择明文能量分析攻击低通后的能量曲线

到攻击完成大约 5 min，攻击出前 4 轮的轮子密钥 rk_0、rk_1、rk_2 和 rk_3 后，根据密钥扩展算法，反推出被攻击的输入密钥为：0x0123456789abcdeffedcba9876543210，该值和实际密钥 K 相同，即验证了攻击的成功性，同时也验证了对 SMS4 轮输出选择明文能量分析攻击方法的可行性。

在相同的软硬件环境条件下，对明文无任何约束条件，以轮输出作为中间数据，对 SMS4 进行能量分析攻击实验，一周尚未完成一轮的攻击。

针对 SMS4 轮输出的选择明文能量分析攻击和在对明文不做限制的条件下，采取攻击整个轮子密钥 32 bit 的方法，所需时间和曲线对比如表 1 所示。

```
Best correlation 1;
0,sub key:254(0xFE),value:-0.0825,at position:215
1,sub key:1(0x01),value:0.0825,at position:215
Best correlation 2:
0,sub key:82(0x52),value:-0.0831,at position:215
1,sub key: 173(0xAD),value:0.0831,at position:215
Best correlation 3:
0,sub key:19(0x13),value:-0.0732,at position:255
1,sub key:236(0xEC),value:0.0732,at position:255
Best correlation 4:
0,sub key:191(0xBF),value:-0.0639,at position:211
1,sub key:64(0x40),value:0.0639,at position:211
Round One res:FE 52 13 BF
```

图 10 第 4 轮的攻击结果

表 1 2 种攻击方法的性能对比

攻击方法	密钥搜索空间	完成时间	所需曲线条数
不选择明文能量分析攻击	2^{32}	>30 天	$>2^{32}$
选择明文能量分析攻击	2^8（每次攻击 8 bit）	4×5 min	4×1 000

从表 1 可以看出，基于 SMS4 轮输出信息泄露点，针对 SMS4 轮输出的选择明文能量分析攻击方法，相比对明文不做限制的条件下，采取攻击整个轮子密钥 32 bit 的方法，效率高得多，所需曲线条数也少得多，且具有实际的可行性。

6 结束语

本文对 SMS4 轮输出抵御能量分析的安全性进行了详细分析，以轮输出作为中间数据，对 SMS4 轮输出的能量分析攻击，所需的搜索密钥空间和分析处理的能量分析曲线条数，导致对 SMS4 轮输出的能量分析攻击在实际数据分析和处理上不可行。

为了实现针对 SMS4 轮输出的能量分析攻击，本文提出了针对SMS4轮输出的选择明文能量分析攻击方法，详述了该攻击方案，并通过实验验证了该攻击方法的实际可操作性以及攻击的高效性。

参考文献：

[1] KOCHER P, JAFFE J, JUN B. Differential power analysis[A]. Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology[C]. 1999.388- 397.

[2] 吴震, 陈运, 陈俊等. 真实硬件环境下幂剩余功耗轨迹指数信息提取[J]. 通信学报, 2010, 31(2):17-21.
WU Z, CHEN Y, CHEN J, *et al*. Exponential information's extraction from power traces of modulo exponentiation implemented on FPGA[J]. Journal on Communications, 2010,31(2):17-21.

[3] CHEN A D, XU S, CHEN Y. Collision-based chosen-plaintext simple power clustering attack algorithm[J]. China Communications, 2013,(5): 114-119.

[4] BRIER E, CLAVIER C, OLIVIER F. Correlation power analysis with a leakage module[A]. CHES 2004[C]. 2004.125-134.

[5] 国家商用密码管理办公室.无线局域网产品使用的 SMS4 密码算法[EB/OL].http://www.oscca.gov.cn/UpFile/200621016423197990.pdf, 2006.
Office of State Commercial Cipher Administration. Block cipher for WLAN products—SMS4[EB/OL]. http:// www.oscca.gov.cn/ UpFile/ 200622026423297990.pdf, 2006.

[6] 沈薇. SMS4 算法的能量分析攻击及其防御研究[D]. 西安: 西安电子科技大学, 2009.
SHEN W. Investigations of Power Analysis Attacks and its Countermeasures on SMS4 Cipher Algorithm[D]. Xi'an: Xidian University, 2009.

[7] BAI X F, XU Y H, GUO L. Securing SMS4 cipher against differential power analysis and its VLSI implementation[A]. Proceedings of 11th IEEE International Conference on Communication Systems[C]. Guangzhou, China, 2008.167-172.

[8] 徐艳华. 抗攻击的 SMS4 密码算法集成电路设计研究[D]. 合肥：中国科技大学, 2009.
XU Y H. Research on Attacks Resistant SMS4 Cipher VLSI Design Technology[D]. Hefei: University of Science and Technology of China, 2009.

[9] 赵新杰, 王韬, 郑媛媛. 针对 SMS4 密码算法的 Cache 计时攻击[J]. 通信学报, 2010, 31(6):89-97.
ZHAO X J, WANG T, ZHENG Y Y. Cache timing attack on SMS4[J]. Journal on Communications, 2010, 31(6):89-97.

作者简介：

王敏（1977-），女，四川资阳人，成都信息工程学院讲师，主要研究方向为网络攻防、侧信道攻击与防御。

杜之波（1982-），男，山东冠县人，成都信息工程学院讲师，主要研究方向为信息安全、侧信道攻击与防御、天线应用和物联网安全。

吴震（1975-），男，江苏苏州人，成都信息工程学院副教授，主要研究方向为信息安全、密码学、侧信道攻击与防御、信息安全设备设计与检测。

饶金涛（1985-），男，湖北黄冈人，成都信息工程学院助教，主要研究方向为信息安全、嵌入式系统安全、侧信道攻击与防御。