doi:10.11959/j.issn.1000-436x.2015270

针对 SM4 轮输出的改进型选择明文功耗分析攻击

杜之波，吴震，王敏，饶金涛
（成都信息工程大学 信息安全工程学院，四川 成都 610225）

摘 要：Wang 等通过攻击时引入固定数据，在 2013 年的 CIS 上提出了针对 SM4 密码算法选择明文功耗分析攻击，但该方法存在选择明文次数、采集功耗信号曲线次数和条数多的问题，攻击过程复杂。分析发现该固定数据和轮子密钥之间的相关性可用于恢复轮子密钥，为此提出针对 SM4 密码算法轮输出的改进型选择明文功耗分析攻击。攻击时选择特殊的明文采集功耗信号曲线，将固定数据作为攻击目标，利用攻击出的固定数据来破解轮子密钥，实验验证了该方法的有效性。使用此方法进行攻击，不仅可以降低选择明文次数、采集功耗信号曲线次数和条数，提高攻击效率，而且还可应用于针对 SM4 密码算法线性变换的选择明文攻击。
关键词：SM4 算法；能量分析攻击；选择明文；轮输出；固定数据
中图分类号：TP309.1 **文献标识码**：A

Improved chosen-plaintext power analysis attack against SM4 at the round-output

DU Zhi-bo, WU Zhen, WANG Min, RAO Jin-tao
(College of Information Security Engineering, Chengdu University of Information Technology, Chengdu 610225, China)

Abstract: The power analysis attack on SM4 using the chosen-plaintext method was proposed by Wang *et al* in 2013 CIS. The fixed data was introduced in the method when attacking the round key. However, the attack process was complex. There were many problems in the process, such as more power traces, more numbers of the chosen-plaintext and acquisition power traces. The correlation between the fixed data and the round key were presented, which could be used to decode the round key. Based on the correlation, the improved chosen-plaintext power analysis attack against SM4 at the round-output was proposed. The proposed method attacked the fixed data by analyzing the power traces of the special plaintext. And the round key was derived based on the correlation. The results show that the proposed attack algorithm is effective. The proposed method not only improves the efficiency of the attack by reducing number of power traces, number of the chosen-plaintext and number of acquisition power traces, but also can be applied to a chosen-plaintext power analysis attack against SM4 at the shift operation.
Key words: SM4 algorithm; power analysis attack; chosen-plaintext; round output; fixed data

1 引言

随着密码分析学的发展，现代密码设备的安全不再单纯停留在密码算法设计的安全上，而是关注密码设备实现的安全。密码算法在硬件设备上运行时，存在执行时间、功耗等物理信息泄露的问题，

收稿日期：2014-12-15；**修回日期**：2015-09-15
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 of China (863 Program) (2012AA01A403)；“The 12th FIVE-YEARS” National Cryptogram Development Fund (MMJJ201101022)；Sichuan Science and Technology Support Programmer (2014GZ0148); The Education Department Key Scientific Research Projects of Sichuan Province (13ZA0091); Project Supported by the Scientific Research Foundation of CUIT (CRF201301)

侧信道攻击[1]就是利用密码设备运行时泄露的物理信息，结合对密码算法的分析进行破译。功耗分析攻击[2]是侧信道攻击的一种，因其攻击能力强，实施起来相对容易，对密码设备的安全造成了严重的威胁，成为国内外侧信道攻击研究的热点方向之一[3,4]。

SM4 密码算法作为国内官方公布的第一个商用密码算法和国内无线局域网产品使用的分组密码算法[5]，对其侧信道功耗分析攻击的研究，不仅具有 SM4 密码算法防御安全方面的意义，而且对评估其实现安全性也具有十分重要的意义。目前，国内外针对 SM4 密码算法的侧信道功耗分析攻击的研究，主要集中在针对 SM4 密码算法的攻击和防御方案等方面[5~9]，文献[10]通过选择明文的方法，当绕开选择轮数输出作为攻击点时，SM4 密码算法线性变换的扩散混淆作用对攻击产生密钥搜索空间大的影响，成功实施了对 SM4 轮输出的选择明文攻击。但是如果按照该文献的攻击方法攻击完整的密钥，存在选择明文次数、采集曲线次数和处理曲线条数较多等问题。

本文通过对 SM4 密码算法轮结构特点的分析，结合文献[10]所述的攻击方法，发现固定数据 *mask* 和密钥具有一定的相关性，可为密钥破解提供有用信息。为此，本文提出了针对 SM4 密码算法轮输出的改进型选择明文攻击方法，当每次攻击时，此方法通过选择不同的攻击中间变量更换攻击目标，来获取和密钥相关的不同的 *mask* 信息，利用攻击出的所有 *mask* 信息，即可恢复出对应的轮子密钥，从而达到减少选择明文次数、采集曲线次数和处理曲线条数较多的问题，提高攻击效率，并给出针对实测功耗曲线的攻击结果，验证了该方法的有效性。此外，该方法还可扩展到针对 SM4 密码算法线性变换输出的选择明文功耗分析攻击。

2 SM4 算法

SM4 密码算法是分组长度和密钥长度均为 128 bit 的分组密码算法，其加密算法和密钥扩展算法均为 32 轮非线性迭代结构，只是轮密钥使用顺序相反，其加密算法的详细流程如图 1 所示。

在图 1 中，X 为输入明文，表示为$(X_0, X_1, X_2, X_3) \in (Z_2^{32})^4$（$X_i \in Z_2^{32}$，$Z_2^e$ 表示 e bit 的向量集），其中 $i \in [0,31]$，$rk_i \in Z_2^{32}$ 表示轮子密钥，Y 为输出密钥，表示为$(Y_0, Y_1, Y_2, Y_3) \in (Z_2^{32})^4$。SM4 密码算法的轮迭代运算的流程如图 1 中的轮迭代函数 F 所

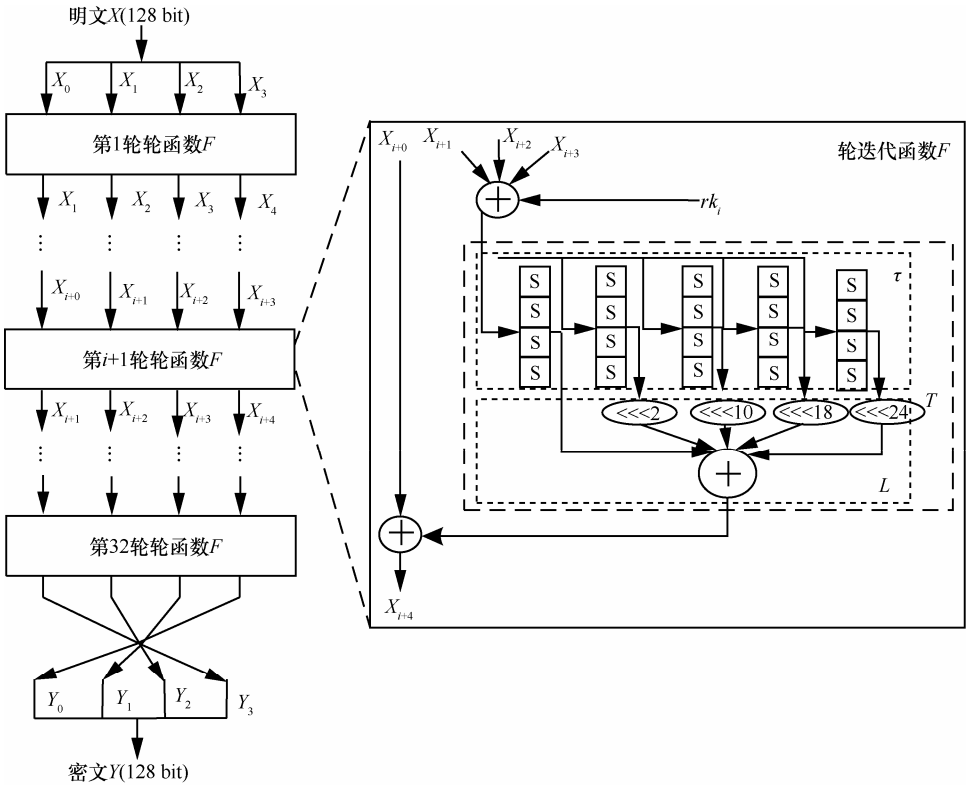

图 1 SM4 密码算法的加密算法流程

示，其运算表达式如式(1)所示，轮迭代函数 F 主要是由合成置换 T 构成，其中合成置换 T 是由非线性变换 τ 和线性变换 L 串联而成。

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

非线性变换 τ 由 4 个相同 S 盒构成，每个 S 盒为 8 入 8 出的代替表，表示为 $b_{i,k} = Sbox(a_{i,k})$，其中 $k \in \{0,1,2,3\}$，$a_{i,k}$，$b_{i,k} \in Z_2^8$，$a_{i,k}$ 为第 i 轮第 k 个 S 盒输入，$b_{i,k}$ 为第 i 轮第 k 个 S 盒输出。

L 线性变换是在 τ 变换基础上完成的循环移位异或运算，其计算表达式如式(2)所示，其中 $B_i \in Z_2^{32}$ 为 τ 变换输出，$C_i \in Z_2^{32}$ 为 L 线性变换输出，且 $C_i = c_{i,0} \| c_{i,1} \| c_{i,2} \| c_{i,3}$，$c_{i,k} \in Z_2^8$，其中||表示 2 个数据按位拼接。

$$\begin{aligned} C_i = L(B_i) = B_i \oplus (B_i <<<2) \oplus (B_i <<<10) \oplus \\ (B_i <<<18) \oplus (B_i <<<24) \end{aligned} \tag{2}$$

SM4 密钥扩展算法轮结构和加密算法轮结构基本相同，只是线性变换变为式(3)，其轮子密钥的生成过程如式(4)和式(5)所示，其中 $MK = (MK_0, MK_1, MK_2, MK_3)$ 为输入密钥（$MK_i \in Z_2^{32}$，i=0,1,2,3），$FK=(FK_0, FK_1, FK_2, FK_3)$ 和 $CK=(CK_0, CK_1, \cdots, CK_{31})$ 为已知系统参数（$FK_i, CK_i \in Z_2^{32}$，i=0,1,2,3），轮密钥为 $rk_i \in Z_2^{32}$（i=0,1,⋯,31）。

$$L'(B) = B \oplus (B <<<13) \oplus (B <<<23) \tag{3}$$

$$\begin{aligned} (K_0, K_1, K_2, K_3) = (MK_0 \oplus FK_0, MK_1 \oplus FK_1, \\ MK_2 \oplus FK_2, MK_3 \oplus FK_3) \end{aligned} \tag{4}$$

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

3　功耗分析攻击

功耗分析攻击是采集密码设备运行时泄露的功耗信号，结合对密码算法的分析，建立合适的功耗模型，利用统计学原理等，来破解和恢复密钥。目前，常用的功耗分析攻击方法有简单功耗分析（SPA, simple power analysis）攻击、差分功耗分析（DPA, differential power analysis）攻击、相关性功耗分析（CPA, correlation power analysis）攻击[11,12]和模板攻击（TA, template attack）[13]等。其中，CPA 比 SPA 具有更强的攻击性，比 DPA 具有更好的量化性，比 TA 具有攻击效率高等优点，所以实际中使用较多的是 CPA，其攻击过程如下。

1) 随机或者有选择地确定 N 组明文或者密文 $d_i=(d_i, \cdots, d_N)$，进行加解密运算，同时在运算时测量密码设备泄露的功耗泄露信号 $t_i=(t_{i,1}, \cdots, t_{i,l})$，其中，$l$ 表示信号轨迹长度，所有的功耗信号便形成功耗信号矩阵 $\boldsymbol{T}$。

2) 猜测密钥 k_j（j=1,2,⋯,k），由 d_i 和 k_j 计算密码算法在攻击点产生的中间数据 $v_{i,j}=f(d_i, k_j)$，即得到假设中间值矩阵 $\boldsymbol{V}$。

3) 将假设中间数据矩阵 $\boldsymbol{V}$ 映射成泄露矩阵 $\boldsymbol{H}$，即选择合适的功耗模型，将 $\boldsymbol{V}$ 中每一个中间数据 $v_{i,j}$ 映射成 $\boldsymbol{H}$ 中对应的假设泄露值 $h_{i,j}$。

4) 使用 Pearson 相关系数，计算 $\boldsymbol{T}$ 矩阵的列数据和 $\boldsymbol{H}$ 矩阵的数据之间的相关系数，取相关系数绝对值最大值对应的 k_j，即为攻击出的密钥。

4　针对SM4轮输出的选择明文功耗分析攻击

针对 SM4 轮输出的功耗分析攻击，其攻击的中间数据计算表达式如式(1)所示，在该式中，线性变换 L 将轮子密钥的影响扩散到轮输出的较多位中，导致轮输出的任一比特都与轮输入和密钥相关联，所以直接将轮输出作为攻击的中间数据。当实施功耗分析攻击时，需将整个轮输出的 32 bit 作为攻击的中间数据。当选择整个轮输出的 32 bit 作为攻击的中间数据时，轮子密钥的搜索空间为 $[0, 2^{32}-1]$，该搜索空间比较大，攻击时需采集和处理功耗信号曲线的条数至少为 2^{32}，这极大地增大了攻击的复杂度和数据处理难度，导致直接以轮输出作为攻击中间数据，实施功耗分析攻击不可行。为此，文献[10]提出了针对 SM4 的选择明文功耗分析攻击。

文献[10]以攻击第 1 轮子密钥的高字节为例详述了攻击过程，攻击时，选择特殊的明文（X_0, X_1, X_2, X_3) = (00000000h, 00000000h, 00000000h, XX000000h)，其中 X 表示变化数据，进行加密运算来采集功耗信号数据，则中间数据计算表达式由式(1)变为式(6)。

$$\begin{aligned} X_4 &= F(X_0, X_1, X_2, X_3, rk_0) \\ &= T(XX000000\text{h} \oplus rk_0) \end{aligned} \tag{6}$$

在式(6)中，由于 T 变换是由 τ 变换和 L 线性

变换串联而成，所以首先计算 τ 变换，计算过程如式(7)所示，其中，$b_{0,1}$、$b_{0,2}$ 和 $b_{0,3}$ 为固定常量，$b_{0,0}$ 为变化量，最后计算 L 线性变换，其计算过程如图 2 所示，在该图中 X 表示变化数据，其他字符表示固定数据。

$$\begin{aligned} B_0 &= \tau(A_0) = \tau(XX000000\text{h} \oplus rk_0) \\ &= \tau(a_{0,0} \| a_{0,1} \| a_{0,2} \| a_{0,3}) \\ &= (b_{0,0}, b_{0,1}, b_{0,2}, b_{0,3}) \end{aligned} \tag{7}$$

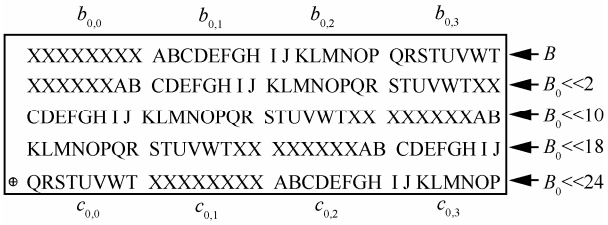

图 2 攻击左数第一个字节时线性变换运算关系

在图 2 中，$c_{0,0} = b_{0,0} \oplus (b_{0,0}<<2) \oplus (b_{0,1}>>6) \oplus (b_{0,1}<<2) \oplus (b_{0,2}>>6) \oplus (b_{0,2}<<2) \oplus (b_{0,3}>>6) \oplus b_{0,3}$，其中$((b_{0,1}>>6) \oplus (b_{0,1}<<2) \oplus (b_{0,2}>>6) \oplus (b_{0,2}<<2) \oplus (b_{0,3}>>6) \oplus b_{0,3})$为固定数据，标记为 $mask_{0,0}$（$mask_{0,i}$ 表示在 L 运算关系图中和 $c_{0,i}$ 对应的固定数据运算结果），则 $c_{0,0}$ 可表示为 $b_{0,0} \oplus (b_{0,0}<<2) \oplus mask_{0,0}$，攻击的中间数据计算表达式变为式(8)，攻击时，以 $X_{4,0}$ 的汉明重量和汉明距离建立功耗模型，根据功耗分析攻击原理，即可攻击出首轮轮子密钥的高字节 $rk_{0,0}$。

$$X_{4,0} = c_{0,0} = b_{0,0} \oplus (b_{0,0}<<2) \oplus mask_{0,0} \tag{8}$$

5 针对 SM4 轮输出的改进的选择明文功耗分析攻击的方法

如果按照文献[10]的攻击过程攻击出完整的加密密钥，那么需选择明文 16 次，采集数据 16 次，所以该攻击方法选择明文采集曲线次数多，攻击过程复杂。

此外，由式(6)和图 1 可知固定数据 $mask_{0,0}$ 是由轮子密钥 $rk_{0,0}$ 和输入经过 τ 变换和 L 线性变换计算而得，所以攻击出的 $mask_{0,0}$ 和密钥具有一定的相关性。

基于文献[10]攻击过程的复杂性和对固定数据 $mask$ 及密钥之间的相关性分析，提出了针对 SM4 轮输出的改进型选择明文攻击，攻击算法如下。

1) 首先攻击第 1 轮，此时 i=0。

2) 采集特殊的明文$(X_i, X_{i+1}, X_{i+2}, X_{i+3})$进行加密运算时泄露的功耗信号，其中 X_i 为随机数，$(X_{i+1} \oplus X_{i+2} \oplus X_{i+3})$的第 j 个字节为随机数 R，其他字节为固定数 D，其中，j=0,1,2,3。

3) 攻击 rk_i 的第 j 个字节，攻击目标为 $rk_{i,j}$ 和 $mask_{i,j}$，选择轮函数输出的 X_{i+4} 的第 j 个字节作为攻击的中间变量实施攻击，中间变量表达式如式(9)所示，其中 $b_{i,j}^{rk_{i,j},D}$ 表示输入为$(rk_{i,j} \oplus D)$时 S 盒输出，$mask_{i,j}$ 计算表达式如式(10)所示。

$$X_{i+4,j} = X_{i,j} \oplus mask_{i,j} \oplus b_{i,j}^{rk_{i,j},D} \oplus (b_{i,j}^{rk_{i,j},D}<<2) \tag{9}$$

$$\begin{aligned} mask_{i,j} = {} & b_{i,(j+3) \bmod 4}^{rk_{i,(j+3) \bmod 4},D} \oplus (b_{i,(j+3) \bmod 4}^{rk_{i,(j+3) \bmod 4},D}>>6) \oplus \\ & (b_{i,(j+2) \bmod 4}^{rk_{i,(j+2) \bmod 4},D}<<2) \oplus (b_{i,(j+2) \bmod 4}^{rk_{i,(j+2) \bmod 4},D}>>6) \oplus \\ & (b_{i,(j+1) \bmod 4}^{rk_{i,(j+1) \bmod 4},D}<<2) \oplus (b_{i,(j+1) \bmod 4}^{rk_{i,(j+1) \bmod 4},D}>>6) \end{aligned} \tag{10}$$

4) 攻击第 $(j$+1)mod4 个字节，攻击目标为 $mask_{i,(j+1) \bmod 4}$，选择轮函数输出 X_{i+4} 的第$(j$+1)mod4 个字节作为攻击的中间变量实施攻击，中间变量表达式如式(11)所示，其中 $mask_{i,(j+1) \bmod 4}$ 的计算表达式如式(12)所示。

$$\begin{aligned} X_{i+4,(j+1) \bmod 4} = {} & X_{i,(j+1) \bmod 4} \oplus mask_{i,(j+1) \bmod 4} \oplus \\ & b_{i,j}^{rk_{i,j},D} \oplus (b_{i,j}^{rk_{i,j},D}>>6) \end{aligned} \tag{11}$$

$$\begin{aligned} mask_{i,(j+1) \bmod 4} = {} & b_{i,(j+1) \bmod 4}^{rk_{i,(j+1) \bmod 4},D} \oplus (b_{i,(j+1) \bmod 4}^{rk_{i,(j+1) \bmod 4},D}<<2) \oplus \\ & (b_{i,(j+2) \bmod 4}^{rk_{i,(j+2) \bmod 4},D}<<2) \oplus (b_{i,(j+2) \bmod 4}^{rk_{i,(j+2) \bmod 4},D}>>6) \oplus \\ & (b_{i,(j+3) \bmod 4}^{rk_{i,(j+3) \bmod 4},D}<<2) \oplus (b_{i,(j+3) \bmod 4}^{rk_{i,(j+3) \bmod 4},D}>>6) \end{aligned} \tag{12}$$

5) 攻击第 $(j$+2)mod4 个字节，攻击目标为 $mask_{i,(j+2) \bmod 4}$，选择轮函数输出 X_{i+4} 的第$(j$+2)mod4 个字节作为攻击的中间变量实施攻击，中间变量表达式如式(13)所示，其中 $mask_{i,(j+2) \bmod 4}$ 的计算表达式如式(14)所示。

$$\begin{aligned} X_{i+4,(j+2) \bmod 4} = {} & X_{i,(j+2) \bmod 4} \oplus mask_{i,(j+2) \bmod 4} \oplus \\ & (b_{i,j}^{rk_{i,j},D}<<2) \oplus (b_{i,j}^{rk_{i,j},D}>>6) \end{aligned} \tag{13}$$

$$\begin{aligned} mask_{i,(j+2) \bmod 4} = {} & b_{i,(j+2) \bmod 4}^{rk_{i,(j+2) \bmod 4},D} \oplus (b_{i,(j+2) \bmod 4}^{rk_{i,(j+2) \bmod 4},D}<<2) \\ & \oplus (b_{i,(j+3) \bmod 4}^{rk_{i,(j+3) \bmod 4},D}<<2) \oplus (b_{i,(j+3) \bmod 4}^{rk_{i,(j+3) \bmod 4},D}>>6) \end{aligned}$$

$$\oplus\ b_{i,(j+1)\bmod 4}^{rk_{i,(j+1)\bmod 4},D} \oplus (b_{i,(j+1)\bmod 4}^{rk_{i,(j+1)\bmod 4},D} >>6) \tag{14}$$

6) 攻击第(*j*+3)mod4 个字节，攻击目标位 $mask_{i,(j+3)\bmod 4}$，选择轮函数输出 X_{i+4} 的第(*j*+3)mod4 个字节作为攻击的中间变量实施攻击，中间变量表达式如式(15)所示，其中 $mask_{i,(j+3)\bmod 4}$ 计算表达式如式(16)所示。

$$X_{i+4,(j+3)\bmod 4} = X_{i,(j+3)\bmod 4} \oplus mask_{i,(j+3)\bmod 4} \oplus (b_{i,j}^{rk_{i,j},D} <<2) \oplus (b_{i,j}^{rk_{i,j},D} >>6) \tag{15}$$

$$mask_{i,(j+3)\bmod 4} = b_{i,(j+3)\bmod 4}^{rk_{i,(j+3)\bmod 4},D} \oplus (b_{i,(j+3)\bmod 4}^{rk_{i,(j+3)\bmod 4},D} <<2) \oplus (b_{i,(j+1)\bmod 4}^{rk_{i,(j+1)\bmod 4},D} <<2) \oplus (b_{i,(j+1)\bmod 4}^{rk_{i,(j+1)\bmod 4},D} >>6) \oplus b_{i,(j+2)\bmod 4}^{rk_{i,(j+2)\bmod 4},D} \oplus (b_{i,(j+2)\bmod 4}^{rk_{i,(j+2)\bmod 4},D} >>6) \tag{16}$$

7) 将式（12）、式（14）和式（16）等号两边分别进行异或运算，得式(17)，由该式可计算出 $b_{i,(j+3)\bmod 4}^{rk_{i,(j+3)\bmod 4},D}$，根据 S 盒的逆运算，即可得 $rk_{i,(j+3)\bmod 4}$ 的值。

$$b_{i,(j+3)\bmod 4}^{rk_{i,(j+3)\bmod 4},D} \oplus (b_{i,(j+3)\bmod 4}^{rk_{i,(j+3)\bmod 4},D} <<2) = mask_{i,(j+1)\bmod 4} \oplus mask_{i,(j+2)\bmod 4} \oplus mask_{i,(j+3)\bmod 4} \tag{17}$$

8) 式（10）和式（12）等号两边分别进行异或运算，得式(18)，由该式可计算出 $b_{i,(j+1)\bmod 4}^{rk_{i,(j+1)\bmod 4},D}$，根据 S 盒的逆运算，即可得 $rk_{i,(j+1)\bmod 4}$ 的值。

$$b_{i,(j+1)\bmod 4}^{rk_{i,(j+1)\bmod 4},D} \oplus (b_{i,(j+1)\bmod 4}^{rk_{i,(j+1)\bmod 4},D} <<2) = mask_{i,j} \oplus mask_{i,(j+1)\bmod 4} \oplus b_{i,(j+3)\bmod 4}^{rk_{i,(j+3)\bmod 4},D} \oplus (b_{i,(j+3)\bmod 4}^{rk_{i,(j+3)\bmod 4},D} <<2) \tag{18}$$

9) 根据式（10）、式（12）、式（14）和式（16）中任何一个子式，可计算出 $b_{i,(j+2)\bmod 4}^{rk_{i,(j+2)\bmod 4},D}$，由 S 盒的逆运算，即可得 $rk_{i,(j+2)\bmod 4}$ 的值。

10) 攻击出 rk_i 的所有字节 $rk_{i,j}$、$rk_{i,(j+1)\bmod 4}$、$rk_{i,(j+2)\bmod 4}$ 和 $rk_{i,(j+3)\bmod 4}$。

11) ++*i*，返回到步骤 2)继续攻击，直到攻击出前 4 轮的轮子密钥，再根据密钥扩展算法的逆运算即可逆推出系统输入密钥 MK[9]。

6　针对 SM4 改进的选择明文功耗分析攻击实验

实验选择的攻击对象为 SM4 算法软实现的智能卡，被攻击的密钥 *K* 为 0x0123456789abcdeffedcba9876543210，对应的第 1 轮轮子密钥为 0xF12186F9。实验软硬件环境：Inspector 软件、功耗曲线采集平台、示波器。按照第 5 节所述的攻击算法，采集功耗信号曲线 1 000 条，其中选择 *D*=0，对曲线采取的预处理为 Inspector 软件所带的低通滤波，滤波参数为 20，低通滤波后的单条功耗信号曲线如图 3 所示。

6.1　攻击过程

按照第 5 节所述的攻击方法，攻击 $rk_{0,0}$ 和 $mask_{0,0}$，攻击结果如图 4 所示，即 $rk_{0,0}$=0xF1，$mask_{0,0}$=0x04。

```
Best correlation:
0,sub key:  61 700(0xF104),value:   0.209 7at position:11 364
1,sub key: 61 947(0xF1FB),value: -0.209 7,at position:11 364
2,sub key:  61 716(0xF114),value:   0.195 1,at position:11 369
3,sub key: 61 931(0xF1FB),value: -0.195 1,at position:11 369
The Best Key:0xF1
The Best Mask:0x04
```

图 4　攻击 $rk_{0,0}$ 和 $mask_{0,0}$ 的结果

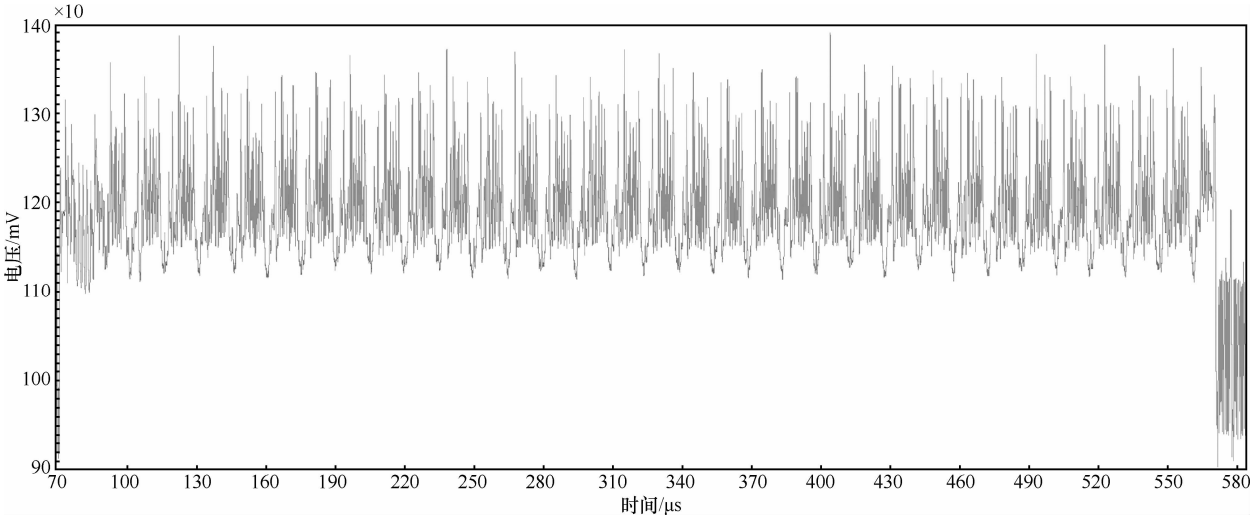

图 3　低通滤波后的功耗信号曲线

在已经攻击出 $rk_{0,0}$ 和 $mask_{0,0}$ 的基础上，按照第 5 节所述的攻击方法，攻击 $mask_{0,1}$、$mask_{0,2}$ 和 $mask_{0,3}$，攻击结果分别如图 5~图 7 所示，即 $mask_{0,1}$ = 0x11，$mask_{0,2}$ =0x20，$mask_{0,3}$=0x67。

```
Best correlation:
0,sub key:     17(0x11),value:    0.229 4,at position:11 360
1,sub key:    238(0xEE),value:   -0.229 4,at position:11 360
2,sub key:     81(0x51),value:    0.218 2,at position:11 348
3,sub key:    174(0xAE),value:   -0.218 2,at position:11 348
The Best Mask:0x11
```

图 5 攻击 $mask_{0,1}$ 的结果

```
Best correlation:
0,sub key:     32(0x20),value:    0.243 0,at position:11 340
1,sub key:    223(0xDF),value:   -0.243 0,at position:11 340
2,sub key:    160(0xA0),value:    0.215 9,at position:11 344
3,sub key:     95(0x5F),value:   -0.215 9,at position:11 344
The Best Mask:0x20
```

图 6 攻击 $mask_{0,2}$ 的结果

```
Best correlation:
0,sub key:    103(0x67),value:    0.332 4,at position:11 365
1,sub key:    152(0x98),value:   -0.332 4,at position:11 365
2,sub key:    111(0x6F),value:    0.292 4,at position:11 365
3,sub key:    144(0x90),value:   -0.292 4,at position:11 365
The Best Mask:0x67
```

图 7 攻击 $mask_{0,3}$ 的结果

由式(17)可得 $b_{0,3}^{0,rk_{0,3}} \oplus (b_{0,3}^{0,rk_{0,3}} <<2)$=0x56，即 $b_{0,3}^{0,rk_{0,3}}$ =0xEE，根据 S 盒子的反变换，可得 $rk_{0,3}$ = 0xF9。

在已经计算出 $b_{0,3}^{0,rk_{0,3}}$ 的基础上，由式(18)可得 $(b_{0,1}^{0,rk_{0,1}} >>6) \oplus b_{0,1}^{0,rk_{0,1}}$ =0x43，即 $b_{0,1}^{0,rk_{0,1}}$ =0x42，根据 S 盒的反变换，可得 $rk_{0,1}$ =0x21。

在已经计算出 $b_{0,1}^{0,rk_{0,1}}$ 和 $b_{0,3}^{0,rk_{0,3}}$ 的基础上，由式(9)，可推导出 $b_{0,2}^{0,rk_{0,2}}$ =0x38，根据 S 盒的反变换，可得 $rk_{0,2}$ =0x86。

攻击出的完整轮子密钥为 F12186F9，该值和真实的第 1 轮轮子密钥相同，攻击成功。

6.2 攻击性能对比

如果文献[10]攻击轮子密钥的高字节所需曲线条数为 N，则攻击完整的轮子密钥所需曲线条数应该为 $4N$。在相同实验环境条件下，本文所述的攻击方法只需文献[10]攻击轮子密钥的高字节时采集的 N 条功耗信号曲线，即可完成轮子密钥的攻击。攻击加解密密钥，文献[10]所述的攻击方法和改进型选择明文功耗分析攻击的攻击性能对比如表 1 所示。

表 1 2 种攻击方法的性能对比

攻击方法	选择明文次数	采集曲线次数	单轮攻击曲线条数
针对 SM4 选择明文功耗分析攻击	16	16	$4N$
针对 SM4 轮输出的改进型选择明文功耗分析攻击	4	4	N

由表 1 中的数据对比可知，本文所述的攻击方法相比文献[10]的攻击方法，减少了攻击选择明文采集曲线的次数和条数，提高了攻击效率。

7 结束语

本文简述和分析了针对 SM4 选择明文功耗分析攻击[10]，如果按照该方法攻击加解密密钥，那么存在选择明文次数、采集功耗信号曲线次数和条数多问题，攻击过程复杂。

基于文献[10]方法的复杂性，本文研究了固定数据 *mask* 和密钥之间的相关性，攻击时通过将 *mask* 作为攻击对象和利用 *mask* 恢复轮子密钥的方法，不仅实现对轮子密钥的攻击，而且相比文献[10]降低了选择明文采集功耗信号曲线的次数和条数，提高了攻击效率，此外，该方法还可用于对 SM4 线性变换的选择明文攻击。

参考文献：

[1] PAUL K, JOSHUA J, BENJAMIN J. Differential power analysis[A]. Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology[C]. 1999. 388- 397.

[2] ERIC B, CHRISTOPHE C, FRANCIS O. Correlation power analysis with a leakage model[A]. Proceeding of 6th International Workshop Cambridge[C]. MA, USA, 2004.16-29.

[3] CHEN A D, XU S, CHEN Y, *et al*. Collision-based chosen-message simple power clustering attack algorithm[J]. China Communications, 2013,10(5):114-119.

[4] 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.

[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/2006210164231979 90.pdf, 2006.
Office of State Commercial Cipher Administration. Block cipher for WLAN products-SMS4[EB/OL]. http://www. oscca. gov. cn/UpFile/

200621016423197990.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. Investigation of Power Analysis Attacks and Its Counter-Measures 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]. 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.

[10] WANG S T, GU D W, LIU J R, *et al*. A power analysis on SMS4 using the chosen plaintext method[A]. 2013 Ninth International Conference on Computational Intelligence and Security[C]. Springer, 2013. 748-752.

[11] SURESH C, JOSYULA R R, PANKAJ R. Template attacks[A]. Proceedings of 4th International Workshop Redwood Shores[C]. CA, USA, 2003.13-28.

[12] 王敏, 杜之波, 吴震, 等. 针对 SMS4 轮输出的选择明文能量分析攻击[J]. 通信学报, 2015, 36(1): 2015016.
WANG M, DU Z B, WU Z, *et al*. Chosen-plaintext power analysis attack against SMS4 with the round-output as the intermediate data[J]. Journal on Communications, 2015, 36(1): 2015016.

[13] BRIER E, CLAVIER C, OLIVIER F. Correlation power analysis with a leakage module[A]. Proceedings of 6th International Workshop Cambridge[C]. MA, USA, 2004. 125-134.

作者简介：

杜之波（1982-），男，山东冠县人，成都信息工程大学讲师，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，成都信息工程大学副教授，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。

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

饶金涛（1985-），男，湖北黄冈人，成都信息工程大学助教，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。