doi:10.11959/j.issn.1000-436x.2017066

基于 SM3 的动态令牌的能量分析攻击方法

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：提出一种针对基于 SM3 的动态令牌实施的能量分析攻击新方法，首次提出选择置换函数的输出作为能量分析攻击的目标，并将攻击结果联立得到方程组。根据给出的逆置换函数求解方程组，即可破解最终的密钥。通过实测攻击实验，验证了该攻击方法的有效性，这就很好地解决了直接选择密钥作为能量分析攻击目标所产生的问题，同时，引入中间变量作为能量分析攻击目标破解密钥方法，还可以应用于针对其他密码算法的能量分析攻击中。

关键词：动态令牌；SM3 算法；能量分析攻击；置换函数的输出；逆置换函数
中图分类号：TP309.1 **文献标识码**：A

Power analysis attack of dynamic password token based on SM3

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

Abstract: A novel method of the power analysis attack of dynamic password token based on SM3 was first proposed to choose the permutation function output as the power analysis attack target，and the simultaneous equations about the key were composed of the attack results. According to the given inverse permutation function, the key was derived by solving the simultaneous equations based on the inverse permutation function. Measured results are presented to validate the proposed method was effective. The proposed method solved the problems of permutation function keys for direct selection of target as an energy analysis attack target. And the proposed method can also be applied to the power analysis attack of the other cryptographic algorithms.

Key words: dynamic password token, SM3 algorithm, power analysis attack, permutation function output, inverse permutation function

1 引言

自 Kocher 等[1]首次提出侧信道攻击技术，并成功破解 RSA 密钥以来，侧信道攻击成为当今研究的热点，并逐渐成为硬件安全研究的一个重要分支。侧信道攻击利用密码电子设备运行时泄露的错误数据、能量和电磁等信息来破解密钥，相比传统的密码分析技术，侧信道攻击具有攻击效率高和易实施等优点。随着侧信道技术的发展，其攻击分析方法越来越成熟，包括计时分析攻击（timing attack）、能量分析攻击（power analysis attack）[2]、电磁分析攻击[3]和故障注入分析攻击（fault analysis

收稿日期：2016-08-25；**修回日期**：2017-01-16
基金项目：国家重大科技专项基金资助项目（No.2014ZX01032401-001）；国家高技术研究发展计划（“863”计划）基金资助项目（No.2012AA01A403）；“十二五”国家密码发展基金资助项目（No.MMJJ201101022）；四川省科技计划基金资助项目（No.2017GZ0313）；四川省教育厅科研基金资助项目（No.17ZB0082）；成都信息工程大学科研人才基金资助项目（No.XAKYXM008, No.XAKYXM009, No.XAKYXM010, No.XAKYXM011）
Foundation Items: The National Science and Technology Major Project (No.2014ZX01032401-001), The National High Technology Research and Development Program (863 Program) (No.2012AA01A403), “The 12th Five-Years” National Cryptogram Development Fund (No.MMJJ201101022), Sichuan Province Science and Technology Program (No.2017GZ0313), Sichuan Provincial Education Department Scientific Research Projects (No.17ZB0082), The Scientific Research Talent Fund of CUIT (No.XAKYXM008, No.XAKYXM009, No.XAKYXM010, No.XAKYXM011)

attack）[4]等攻击分析方法。

SM3 密码算法作为国内官方公布的商用密码杂凑算法，广泛应用于数字签名和验证、消息认证码的生成与验证以及随机数的生成。目前，国内外针对 SM3 密码算法的侧信道能量分析攻击的研究较少。根据攻击目标的不同，针对 SM3 的能量分析攻击主要分为针对基于 SM3 的 HAMC 的能量分析攻击和针对基于 SM3 密码算法动态令牌的能量分析攻击。文献[5~8]完成了针对基于 SM3 密码算法 HMAC 的能量分析攻击研究。在基于 SM3 密码算法动态令牌的能量分析攻击的研究中，文献[9]选择消息扩展 W_j' 的计算和迭代压缩作为攻击点，实现了针对基于 SM3 密码算法动态令牌的差分能量分析攻击。而在选择 SM3 密码算法消息扩展 $W_j(j \geqslant 16)$作为攻击点进行能量分析攻击的研究，在国内外公开发表的文献中，尚未发现有相同或类似的成果。因此，将消息扩展的 W_j 计算结果作为能量分析攻击的中间变量，对 SM3 进行能量分析攻击的研究，不仅对 SM3 密码算法防御能量分析攻击方面的研究具有重要意义，而且对评估金融等领域的 SM3 密码算法产品的安全性，以及对 SM3 密码算法产品的安全等级制定和检测也具有十分重要的科学意义及应用价值。

本文根据动态令牌原理和 SM3 密码算法的结构特点，分析了 SM3 密码算法的消息扩展在计算 W_j 时抵御能量分析攻击的安全性。由于置换函数 $P_1(X)$的扩散混淆作用，以 W_j 作为中间数据直接对 SM3 密码算法进行能量分析攻击破解密钥，存在密钥搜索空间大和攻击时间长的问题，导致对 SM3 的能量分析攻击直接攻击密钥在实际操作上不可行。为解决以上难题和实现针对 SM3 密码算法消息扩展 W_j 的能量分析攻击，提出了一种针对基于 SM3 的动态令牌的间接能量分析攻击新方法，该方法不仅首次探索了扩展消息 $W_{16} \sim W_{19}$ 与 $W_0 \sim W_3$ 之间关系，即 $W_{16} \sim W_{19}$ 都可以表示成一个未知固定信息与已知信息的异或，通过猜测该固定信息 $W_0 \sim W_3$ 就能得到 $W_{16} \sim W_{19}$，而且首次提出选择置换函数 $P_1(X)$的运算结果作为能量分析攻击目标，实现了针对基于 SM3 的动态令牌的间接能量分析攻击。首先能量分析攻击出置换函数 $P_1(X)$的运算结果后，将所有的攻击结果联立方程组，根据给出的置换函数 $P_1(X)$的逆置换函数，对方程组求解，即破解动态令牌中的密钥。通过针对 SM3 密码算法智能卡的实测攻击实验，验证了本文攻击方法的有效性，同时，该新型攻击方法相比直接选择密钥作为攻击目标进行能量分析攻击，降低了数据搜索空间和减少能量分析攻击样本数，提高能量分析的实际操作可行性和效率。同时，该方法给出置换函数 $P_1(X)$的逆置换函数，对 SM3 密码算法的其他科学研究具有重要参考意义。

2 基于 SM3 的动态令牌

2.1 动态令牌

动态令牌是动态口令系统的重要组成部分，是一种一定周期内生成一个动态口令的设备，每个口令各不相同，为用户提供身份认证。

动态令牌使用杂凑算法或分组算法，结合截位函数，根据用户密钥和时间产生动态口令，基于 SM3 密码算法的动态令牌实现过程如下所示。

1) $S = F(K, ID)$，其中，F 为 SM3 杂凑密码算法，S 为 SM3 杂凑密码算法的输出，K 是长度不小于 128 bit 的运算密钥，ID 是长度不小于 128 bit 变化的信息。

2) OD = Truncate(S)，其中，Truncate()是截位函数，OD 为截位函数的输出。

3) $P = OD$ % (10^N)，N 是令牌或其他终端显示口令的位数，P 为最终显示的动态口令。

2.2 SM3 密码杂凑算法

SM3 密码杂凑算法是杂凑值为 256 bit 的国产商用密码算法，运算过程包括消息填充、消息扩展和迭代压缩。

消息扩展是将 512 bit 的消息分组 B 按以下方法扩展生成 132 个字 $W_0, W_1, \cdots, W_{67}, W_0', W_1', \cdots, W_{63}'$，消息扩展过程描述如下。

1) 将消息分组划分为 16 个字 $W_0, W_1, \cdots, W_{15}$。

2) for j=16 to 67

$$W_j \leftarrow P_1(W_{j-16} \oplus W_{j-9} \oplus (W_{j-3} <<< 15)) \oplus (W_{j-13} <<< 7) \oplus W_{j-6} \quad (1)$$

end for

3) for j=0 to 63

$$W_j' = W_j \oplus W_{j+4}$$

end for

其中，P_1 为置换函数，如式(2)所示。

$$P_1(X) = X \oplus (X <<< 15) \oplus (X <<< 23) \quad (2)$$

迭代压缩是利用压缩函数生成 256 bit 杂凑值，压缩函数 $V^{i+1}=CF(V^{(i)},B^{(i)})(0\leqslant i\leqslant n-1)$ 的计算过程描述如下。

$$ABCDEFGH\leftarrow V^{(i)} \tag{3}$$

for j=0 to 63

$$SS_1\leftarrow((A<<<12))+E+(T_j<<<j)<<<7 \tag{4}$$

$$SS_2\leftarrow SS_1\oplus(A<<<12) \tag{5}$$

$$TT_1\leftarrow FF_j(A,B,C)+D+SS_2+W_j' \tag{6}$$

$$TT_2\leftarrow GG_j(E,F,G)+H+SS_1+W_j \tag{7}$$

$$D\leftarrow C \tag{8}$$

$$C\leftarrow B<<<9 \tag{9}$$

$$B\leftarrow A \tag{10}$$

$$A\leftarrow TT_1 \tag{11}$$

$$H\leftarrow G \tag{12}$$

$$G\leftarrow F<<<19 \tag{13}$$

$$F\leftarrow E \tag{14}$$

$$E\leftarrow P_0(TT_2) \tag{15}$$

end for

$$V^{(i+1)}\leftarrow ABCDEFGH\oplus V^{(i)}$$

在压缩函数中，$FF_j(X,Y,Z)$ 和 $GG_j(X,Y,Z)$ 为布尔函数，$P_0(X)$ 为置换函数，T_j 为固定常量，详见文献[5]。

3　能量分析攻击原理

相关性能量分析攻击[10](CPA，correlation power analysis attack)是能量分析攻击的一种，CPA 通过计算被攻击中间数据的假设值和真实能量信号曲线之间的相关性来破解密钥。CPA 具有实现简单、易实施等优点，成为能量分析攻击常用的攻击方法。CPA 详细的攻击过程[11~14]如下所述。

1) 采集密码设备运行时的能量信号曲线 T_i，$i\in[1,N]$，曲线条数为 N，并记录每条曲线对应的明文或密文 M_i。

2) 确定和密钥相关的中间变量 V，以及对应的被攻击计算表达式 $V=F(K,M)$，其中，K 为密钥。

3) 确定猜测密钥的数据长度、对应的密钥空间 ϕ 和在 ϕ 中遍历所有可能值 K_j，计算密码算法实现中和密钥等敏感数据相关的中间变量 $V_{j,k}=F(K_j,M_i)$，根据 $V_{j,k}$ 的汉明重量或汉明距离，将 $V_{j,k}$ 映射为对应的假设能耗值。

4) 根据皮尔逊相关系数式(16)，计算能量信号曲线和假设能耗值之间的相关性，取相关系数最大时，假设能耗值对应的猜测密钥 K_j 为破解出的密钥。

$$\rho(T,V)=\frac{\mathrm{E}(T,V)-\mathrm{E}(T)\mathrm{E}(V)}{\sqrt{\mathrm{Var}(T)\mathrm{Var}(V)}} \tag{16}$$

4　能量分析攻击方法

根据文献[9]提出能量分析攻击方法，针对基于 SM3 的动态令牌的能量分析攻击的场景为：密钥 K 和 ID 的长度均为 128 bit，密钥 $K=W_0\|W_1\|W_2\|W_3$。$W_4\sim W_{15}$ 为 ID 和填充后的消息，对攻击者来说是已知和变化的数据。

4.1　直接能量攻击分析

SM3 密码杂凑算法在进行消息扩展式(1)运算时，密钥 K 以字节的形式参与运算，运算结果 $W_j(j\geqslant 16)$ 需在寄存器中存储。W_j 在保存和在总线上传输过程中，其汉明重量或汉明距离和被攻击设备消耗能量之间存在一定的相关性。所以，可以选择 W_j 作为能量分析攻击的中间变量，针对基于 SM3 的动态令牌实施能量分析攻击。

根据能量分析攻击原理，最直接的攻击方法为：直接选择密钥 K 作为能量分析的攻击目标进行攻击。如当 j=16 时，被攻击的计算表达式(1)可变换为

$$\begin{aligned}&W_{16}\leftarrow P_1(W_0\oplus W_7\oplus(W_{13}<<<15))\oplus\\&(W_3<<<7)\oplus W_{10}\leftarrow P_1(W_0)\oplus(W_3<<<7)\oplus\\&P_1(W_7)\oplus P_1(W_{13}<<<15)\oplus W_{10}\end{aligned} \tag{17}$$

其中，被攻击的目标 W_0 和 W_3 为密钥 K 的最高和最低字节，是固定数据，W_7、W_{10} 和 W_{13} 是攻击者已知，且变化的数据，令 $W=P_1(W_7)\oplus P_1(W_{13}<<<15)\oplus W_{10}$，则被攻击的计算表达式(17)变为

$$\begin{aligned}&W_{16}\leftarrow P_1(W_0)\oplus(W_3<<<7)\oplus\\&W\leftarrow W_0\oplus(W_0<<<15)\oplus(W_0<<<23)\oplus\\&(W_3<<<7)\oplus W\end{aligned} \tag{18}$$

由式(18)可得，置换函数 $P_1(X)$ 将 W_0 扩散混淆到了 W_{16} 较多位中，结合被攻击目标 W_3 参与运算，单比特的 W_0 将影响 W_{16} 的多比特的汉明重量或汉明距离，所以选择 W_{16} 作为能量分析攻击的中间变量，直接攻击 W_0 和 W_3 时，需采取一次攻击 W_0 和 W_3 的所有比特方式来破解密钥，即根据第 3 节的步骤 3)，所确定的猜测密钥的数据长度为 32 bit，由于 W_0 和 W_3 均为 32 bit，且需同时攻击 W_0 和 W_3，所以该方式的密钥搜

索空间为$[0,2^{64}-1]$，该穷举空间增大了能量分析攻击的难度和数据计算复杂度，降低了攻击效率。

根据第3节步骤2)，在计算假设能耗值时，对每条曲线和每个猜测密钥都要计算假设能耗值，则能量攻击的时间复杂度为如式(19)所示。

$$\mathrm{Time}(N,\phi)=O(N\phi) \tag{19}$$

所以直接攻击W_0和W_3的时间复杂度为$O(2^{64}N)$，该时间复杂度较大，导致攻击执行效率较低，所以该攻击方式在实际攻击时不可行。

4.2 间接能量分析攻击原理

虽然置换函数$P_1(X)$将密钥K的影响扩散到W_j的较多位中，但是当置换函数$P_1(X)$对密钥K的字节进行运算时，其输出为固定信息。如当j=16时，在被攻击运算表达式(式(18))中，W_0为密钥K的高字节，$P_1(W_0)$是由W_0计算所得的固定数据，W_3为密钥K的低字节，所以可选择$K_1=P_1(W_0)\oplus(W_3<<<7)$作为密钥进行能量分析攻击。被攻击的计算表达式由式(18)变为

$$W_{16}\leftarrow K_1\oplus W \tag{20}$$

其中，被攻击的中间变量W_{16}和密钥K_1之间是比特一一对应的线性关系，K_1的单比特只能影响W_{16}对应单比特的汉明重量或汉明距离。所以能量分析攻击时，可以根据实际计算能力，选择单次攻击K_1的l bit，经过多次攻击的方法来实施，此时的密钥搜索空间为$[0,2^l-1]$，l最小可以选择1 bit，相比直接能量分析攻击数据长度32 bit，搜索空间$[0,2^{64}-1]$，则间接能量分析攻击指数级地降低了密钥的搜索空间。根据式(19)，此时的$\mathrm{Time}(N,\phi)=O(N\phi)=O(N2^l)$，时间复杂度相比直接能量分析攻击的时间复杂度，也呈指数级下降。攻击密钥K的其他字节的原理和该攻击原理相同。所以选择置换函数的输出作为能量分析攻击目标，解决了直接能量分析攻击搜索空间大、攻击时间长导致实际攻击不可行的技术难题。

所以针对SM3密码算法消息扩展W_j的能量分析攻击时，可选择置换函数的输出作为攻击目标，首先能量分析攻击出置换函数的输出，再根据逆置换函数，反推出最终的密钥，间接能量分析攻击出SM3密码算法的密钥K。

4.3 间接能量分析攻击方法

选择SM3密码算法的消息扩展W_{16}、W_{17}、W_{18}和W_{19}运算作为能量分析攻击的中间变量，攻击出W_0、W_1、W_2和W_3。主要攻击过程的流程如图1所示。

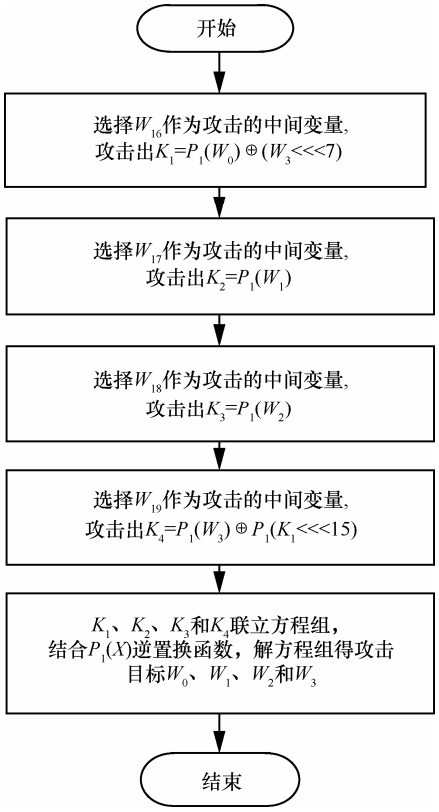

图1 攻击过程的流程

针对基于SM3的动态令牌的能量分析攻击方法详细攻击过程如下所示。

1) 选择W_{16}作为攻击的中间变量，能量分析攻击出$K_1=P_1(W_0)\oplus(W_3<<<7)$。

此时j=16，在式(17)中，W_0和W_3为密钥的第1个字节和第4个字节，令$K_1=P_1(W_0)\oplus(W_3<<<7)$，则式(17)变换为

$$W_{16}\leftarrow K_1\oplus P_1(W_7)\oplus P_1(W_{13}<<<15)\oplus W_{10} \tag{21}$$

其中，K_1是和密钥相关的固定数据，W_7、W_{10}和W_{13}是攻击者已知且变化的数据，所以根据能量分析攻击原理，选择W_{16}作为能量分析攻击的中间变量，能量分析攻击出攻击的目标K_1。

2) 选择W_{17}作为攻击的中间变量，能量分析攻击出$K_2=P_1(W_1)$。

此时j=17，被攻击表达式(1)变换为

$$W_{17}\leftarrow P_1(W_1\oplus W_8\oplus(W_{14}<<<15))\oplus$$
$$(W_4<<<7)\oplus W_{11}\leftarrow P_1(W_1)\oplus P_1(W_8)\oplus$$

$$P_1\ (W_{14} <<<15)\oplus (W_4 <<<7)\oplus W_{11} \tag{22}$$

其中，W_1为密钥第 2 个字节，令 $K_2=P_1(W_1)$，则式(22)变换为

$$W_{17}\leftarrow K_2\oplus P_1\ (W_8)\oplus P_1\ (W_{14} <<<15)\oplus (W_4 <<<7)\oplus W_{11} \tag{23}$$

其中，K_2是和密钥相关的固定数据，W_4、W_8、W_{11}和W_{14}是攻击者已知且变化的数据，所以根据能量分析攻击原理，选择W_{17}作为能量分析攻击的中间变量，能量分析攻击出攻击的目标K_2。

3) 选择W_{18}作为攻击的中间变量，能量分析攻击出 $K_3=P_1(W_2)$。

此时 j=18，此时被攻击表达式(1)变换为

$$W_{18}\leftarrow P_1(W_2\oplus W_9\oplus (W_{15} <<<15))\oplus (W_5 <<<7)\oplus W_{12}\leftarrow P_1\ (W_2)\oplus P_1\ (W_9)\oplus P_1(W_{15} <<<15)\oplus (W_5 <<<7)\oplus W_{12} \tag{24}$$

其中，W_2为密钥的第 3 个字节，令 $K_3=P_1\ (W_2)$，则式(24)变换为

$$W_{18}\leftarrow K_3\oplus P_1(W_9)\oplus P_1(W_{15} <<<15)\oplus (W_5 <<<7)\oplus W_{12} \tag{25}$$

其中，K_3是和密钥相关的固定数据，W_5、W_9、W_{12}和W_{15}是攻击者已知且变化的数据，所以根据能量分析攻击原理，选择W_{18}作为能量分析攻击的中间变量，能量分析攻击出攻击的目标K_3。

4) 选择W_{19}作为攻击的中间变量，能量分析攻击出 $K_4=P_1(W_3)\oplus P_1(K_1 <<<15)$。

此时 j=19，被攻击表达式(1)可变换为

$$W_{19}\leftarrow P_1(W_3\oplus W_{10}\oplus (W_{16} <<<15))\oplus (W_6 <<<7)\oplus W_{13}\leftarrow P_1\ (W_3)\oplus P_1(K_1 <<<15)\oplus P_1\ (W_{10})\oplus P_1((P_1(W_7)\oplus P_1\ (W_{13} <<<15)\oplus W_{10}) <<<15)\oplus (W_6 <<<7)\oplus W_{13} \tag{26}$$

其中，W_3为密钥的第 4 个字节，令 $K_4=P_1\ (W_3)\oplus P_1(K_1 <<<15)$，则式(25)变换为

$$W_{19}\leftarrow K_4\oplus P_1\ (W_{10})\oplus P_1((P_1\ (W_7)\oplus P_1\ (W_{13} <<<15)\oplus W_{10}) <<<15)\oplus (W_6 <<<7)\oplus W_{13} \tag{27}$$

其中，K_4是和密钥相关的固定数据，W_6、W_7、W_{10}和W_{13}是攻击者已知且变化的数据，所以根据能量分析攻击原理，选择W_{19}作为能量分析攻击的中间变量，能量分析攻击出攻击的目标K_4。

5) 推导出置换函数$P_1(X)$的逆置换函数。

令 $Y=P_1(X)$，$X,Y\in GF(2^{32})$，则$P_1(X)$置换函数的仿射变换如式(28)所示，对应的循环矩阵 $\boldsymbol{T}$如图 2 所示。

$$Y=X\boldsymbol{T} \tag{28}$$

$\boldsymbol{T}=$

```
10000000010000000100000000000000
01000000001000000010000000000000
00100000000100000001000000000000
00010000000010000000100000000000
00001000000001000000010000000000
00000100000000100000001000000000
00000010000000010000000100000000
00000001000000001000000010000000
00000000100000000100000001000000
00000000010000000010000000100000
00000000001000000001000000010000
00000000000100000000100000001000
00000000000010000000010000000100
00000000000001000000001000000010
00000000000000100000000100000001
10000000000000010000000010000000
01000000000000001000000001000000
00100000000000000100000000100000
00010000000000000010000000010000
00001000000000000001000000001000
00000100000000000000100000000100
00000010000000000000010000000010
00000001000000000000001000000001
10000000100000000000000100000000
01000000010000000000000010000000
00100000001000000000000001000000
00010000000100000000000000100000
00001000000010000000000000010000
00000100000001000000000000001000
00000010000000100000000000000100
00000001000000010000000000000010
00000000100000001000000000000001
```

图 2　矩阵 $\boldsymbol{T}$

由式(27)得置换函数$P_1(X)$的逆置换函数$P_1^{-1}(Y)$，如式(29)所示，对应的循环矩阵 $\boldsymbol{T}^{-1}$如图 3 所示。

$$X=P_1^{-1}(Y)=Y\boldsymbol{T}^{-1} \tag{29}$$

6) 联立方程组，解方程破解最终密钥。

由 K_1、K_2、K_3和 K_4的表达式联立的方程组如式(30)所示。由式(30)解该方程组，得密钥 K 的各个字节如式(31)所示。

$$\begin{cases} K_1=P_1(W_0)\oplus (W_3 <<<7)\\ K_2=P_1(W_1)\\ K_3=P_1(W_2)\\ K_4=P_1(W_3)\oplus P_1(K_1 <<<15)\end{cases} \tag{30}$$

$$\begin{cases} W_0=P_1^{-1}(K_1\oplus ((P_1^{-1}(K_4)\oplus (K_1 <<<15)) <<<7))\\ W_1=P_1^{-1}(K_2)\\ W_2=P_1^{-1}(K_3)\\ W_3=P_1^{-1}(K_4)\oplus (K_1 <<<15)\end{cases} \tag{31}$$

$$\boldsymbol{T}^{-1}=\begin{bmatrix}
10110000010100000111000000010000\\
01011000001010000011100000001000\\
00101100000101000001110000000100\\
00010110000010100000111000000010\\
00001011000001010000011100000001\\
10000101100000101000001110000000\\
01000010110000010100000111000000\\
00100001011000001010000011100000\\
00010000101100000101000001110000\\
00001000010110000010100000111000\\
00000100001011000001010000011100\\
00000010000101100000101000001110\\
00000001000010110000010100000111\\
10000000100001011000001010000011\\
11000000010000101100000101000001\\
11100000001000010110000010100000\\
01110000000100001011000001010000\\
00111000000010000101100000101000\\
00011100000001000010110000010100\\
00001110000000100001011000001010\\
00000111000000010000101100000101\\
10000011100000001000010110000010\\
01000001110000000100001011000001\\
10100000111000000010000101100000\\
01010000011100000001000010110000\\
00101000001110000000100001011000\\
00010100000111000000010000101100\\
00001010000011100000001000010110\\
00000101000001110000000100001011\\
10000010100000111000000010000101\\
11000001010000011100000001000010\\
01100000101000001110000000100001
\end{bmatrix}$$

图 3　矩阵 $\boldsymbol{T}^{-1}$

4.4　攻击方法性能分析

1) 密钥搜索空间分析

由式(21)、式(23)、式(24)和式(27)可知，被攻击的中间变量和攻击目标之间都是单比特一一对应的线性关系，攻击目标的 1 bit 数据，只能影响中间变量的 1 bit 的汉明重量或汉明距离。因此，在实际猜测密钥进行能量分析攻击时，可根据实际的实验条件，选择中间变量的任意比特的能量模型进行攻击，对应的猜测密钥空间可为任意 l bit，最小仅为 1 bit，最大为 32 bit，而直接攻击则为 64 bit 和 32 bit。所以本文攻击方法相比直接攻击方法，显著地减少了密钥的搜索空间，降低了攻击时的计算复杂度。

2) 时间复杂度分析

本文攻击方法在实际攻击时，可根据实际的攻击条件，选择合适长度的猜测密钥空间进行攻击。根据式(19)，其时间复杂度为 $\mathrm{Time}(N,\phi)=O(N\phi)=O(N2^{l})$，最小为 $O(2N)$，最大为 $O(2^{32}N)$，具体数值可由攻击者根据实际的计算能力来选择。相比直接攻击的 $O(2^{64}N)$和 $O(2^{32}N)$，本攻击方法显著地降低了攻击的时间复杂度。

5　实测能量分析攻击过程

为验证该攻击方法的有效性，本文在 32 bit 智能卡上实现了基于 SM3 的动态令牌的杂凑运算，被攻击密钥 K 为 0x36903BBC9EAF97ACE2E1283A1CF61BE7。实验所用的能量曲线采集设备为 Power Tracer 和示波器，分析软件为 Inspector。实验采集和分析的能量曲线样本数为 2 000，采集到的能量信号波形如图 4 所示。

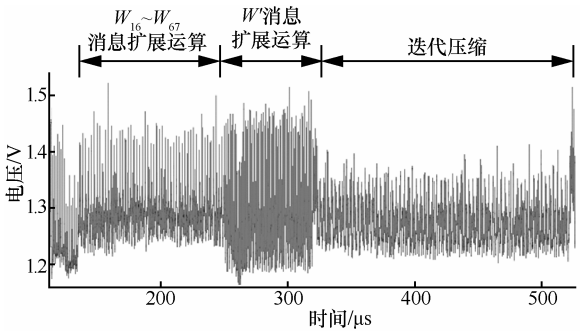

图 4　能量信号曲线

5.1　间接能量分析攻击实验

根据式(20)攻击 K_1，其中，高字节攻击结果的相关性曲线如图 5 所示，从图 5 中可以看出，相关性绝对值最大对应猜测密钥为 0x8E 和 0x71。如图 4 所示，从扩展运算的起始位置开始选择 450 个采样点，1 000 条曲线进行攻击，攻击结果如图 6 所示，攻击出的 K_1 为 0x8E589B67，攻击 10 次，平均所用时间为 11 s。

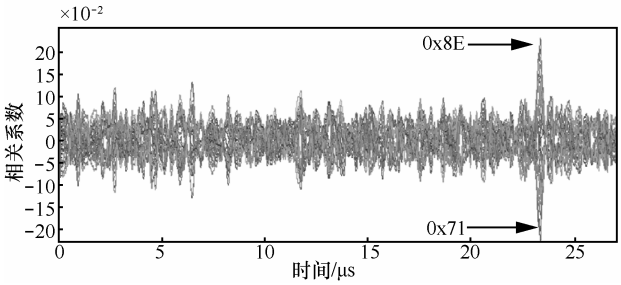

图 5　攻击结果相关性曲线

```
The start time: 12:09:23
Best correlation S-Box 1:
0, sub key: 142 (0x8E), value:    0.2236, at position: 5820
1, sub key: 113 (0x71), value: -0.2236, at position: 5820
2, sub key: 134 (0x86), value:    0.1977, at position: 5821
3, sub key: 121 (0x79), value: -0.1977, at position: 5821
Best correlation S-Box 2:
0, sub key:    88 (0x58), value:    0.3014, at position: 5789
1, sub key: 167 (0xA7), value: -0.3014, at position: 5789
2, sub key:    89 (0x59), value:    0.2881, at position: 5789
3, sub key: 166 (0xA6), value: -0.2881, at position: 5789
Best correlation S-Box 3:
0, sub key: 155 (0x9B), value:    0.2334, at position: 5825
1, sub key: 100 (0x64), value: -0.2334, at position: 5825
2, sub key: 187 (0xBB), value:    0.2236, at position: 5799
3, sub key:    68 (0x44), value: -0.2236, at position: 5799
Best correlation S-Box 4:
0, sub key: 103 (0x67), value:    0.4555, at position: 5825
1, sub key: 152 (0x98), value: -0.4555, at position: 5825
2, sub key: 119 (0x77), value:    0.4329, at position: 5825
3, sub key: 136 (0x88), value: -0.4329, at position: 5825
Round key: 8E 58 9B 67
The end time: 12:09:35
```

图 6　K_1 攻击结果

同理，根据式(22)、式(24)和式(26)攻击 K_2、K_3 和 K_4，攻击出的 K_2 为 0x83368F30，攻击出的 K_3 为 0x6B8D29DE，攻击出的 K_4 为 0xDA88D687。

将 K_1、K_2、K_3 和 K_4 代入到式(28)中，可解得被攻击密钥的各个字节 W_0 为 0x36903BBC，W_1 为 0x9EAF97AC，W_2 为 0xE2E1283A，W_3 为 0x1CF61BE7。该被攻击的密钥和实际密钥相同，验证了本文攻击方法的有效性。

5.2　直接能量分析攻击实验

在与间接能量分析攻击相同的实验条件下，根据 4.1 节攻击 W_0 和 W_3，当密钥搜索空间 ϕ 设置为[0, $2^{22}-1$]，由于计算相关系数需要较多使用长度为 ϕ 和 450ϕ 的数组，所以导致攻击分析软件 Inspector 报内存不足异常错误，不能继续进行攻击，如图 7 所示。

```
Not enough memory to analyze, got 825Mb, need 14464Mb
```

图 7　内存异常错误

为了测试直接能量分析攻击 W_0 和 W_3 所需时间，实验采取了部分密钥搜索空间测试。单次攻击搜索空间为[0, $2^{16}-1$]，攻击 10 次，平均攻击所需时间 817 s，如图 8 所示。根据第 3 节步骤 2)~步骤 4)，攻击时对每条曲线对应的明文都要计算所有猜测密钥对应的假设能耗值，所以当攻击搜索空间为[0, $2^{32}-1$]，则预计所需时间 $\frac{817\times 2^{32}}{2^{16}}\approx 620$ 天。当攻击搜索空间为[0, $2^{64}-1$]时，预计所需时间 $\frac{817\times 2^{64}}{2^{16}}\approx 2^{32}\times 620$ 天。

```
The start time: 14:33:43
Best correlation:
0, sub key: 25752 (0x6498), value: -0.3639, at position: 5823
1, sub key: 17560 (0x4498), value: -0.3592, at position: 5823
2, sub key: 25736 (0x6488), value: -0.3546, at position: 5820
3, sub key: 17544 (0x4488), value: -0.3492, at position: 5821
Round key: 64 98
The end time: 14:46:30
```

图 8　攻击时间结果

5.3　攻击结果分析

本文所述间接攻击方法和选择以 W_j 为中间变量，直接攻击 W_0、W_1、W_2 和 W_3 的攻击方法的实验攻击性能对比如表 1 所述，其中，实验攻击的曲线条数为 1 000 条，选择的采样点数为 450 个采样点。由于直接攻击在实际实验中，24 h 未完成攻击，预计所需时间较长，所以攻击实验并没有在有限的时间内完成攻击。

从表 1 可以看出，在同样的实验条件下，间接攻击方法相比直接攻击方法，从实践上实现了针对基于 SM3 的动态令牌的能量分析攻击，而且降低了能量分析攻击时的密钥搜索空间，减少了攻击时间，提高了攻击效率。

6　结束语

本文以 SM3 密码算法在动态令牌中的应用为攻击场景，通过对 SM3 密码算法的消息扩展和压缩函数的分析，结合能量分析攻击原理，提出一种针对基于 SM3 密码算法动态令牌的能量分析攻击新方法。该方法在进行能量分析攻击时，选择置换函数的输出作为攻击目标，解决了传统能量分析攻击直接选择密钥作为攻击目标所产生的搜索空间大、攻击时间长和攻击效率低等难题。实现了以消息扩展的 W_j ($j\geqslant 16$)作为中间变量，针对基于 SM3 的动态令牌的能量分析攻击。

本文攻击方法不仅对 SM3 密码算法产品的安全检测具有实际的应用意义，对 SM3 密码算法的安全防御具有指导意义，而且该方法通过引入中间变量作为能量分析攻击目标，根据该中间变量再反推出密钥的攻击思想，还可应用到针对其他密码算法的能量分析攻击中。

表 1　　**2 种攻击方法的性能对比**

攻击方法	攻击对象	密钥搜索空间	时间复杂度	攻击时间	是否成功
直接攻击	W_0 和 W_3	2^{64}	$O(1\,000\times 2^{64})$	2^{32} ×620 天	未完成攻击
	W_1	2^{32}	$O(1\,000\times 2^{32})$	620 天	未完成攻击
	W_2	2^{32}	$O(1\,000\times 2^{32})$	620 天	未完成攻击
间接攻击	W_0、W_1、W_2 和 W_3	2^8	$O(1\,000\times 2^{32})$	11 s	是

参考文献：

[1] KOCHER P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[C]//The 16th Annual International Cryptology Conference. Santa Barbara, United States, 1996: 104-113.

[2] KOCHER P, JAFFE J, JUN B. Differential power analysis[C]//The

19th Annual International Cryptology Conference Santa Barbara. 1999: 388-397.

[3] JEAN-JACQUES Q. A new tool for non-intrusive analysis of smart cards based on electromagnetic emissions, the SEMA and DEMA methods. Presented at the rump session of EUROCRYPT 2000[C]// Rump Session. 2000.

[4] DAN B, RICHARD A D, RICHARD J L. On the importance of checking cryptographic protocols for faults[C]//Springer. 1997:37-51.

[5] 杜之波, 吴震, 王敏, 等. 针对基于 SM3 的 HMAC 的能量分析攻击方法[J]. 通信学报, 2016, 37(5): 38-43.
DU Z B, WU Z, WANG M, et al. Power analysis attack of HMAC based on SM3[J]. Journal on Communications, 2016, 37(5):38-43.

[6] XIE J, SUN W, GU D, et al. Research on differential power analysis of HMAC- SM3[C]//2015 International Conference on Computer Science and Intelligent Communication. 2015:103-106.

[7] GUO L, WANG L, LIU D, et al. A chosen-plaintext differential power analysis attack on HMAC-SM3[C]//The 11th International Conference on Computational Intelligence and Security. 2015: 350-353.

[8] GUO L, WANG L, LI Q, et al. A first-order differential power analysis attack on HMAC-SM3[C]//The First International Conference on Information Science and Electronic Technology. 2015: 94-97.

[9] GUO L, WANG L, LI Q, et al. Differential power analysis on dynamic password token based on SM3 algorithm, and countermeasures[C]// The 11th International Conference on Computational Intelligence and Security. 2015: 354-357.

[10] STEFAN M, ELISABETH O, THOMAS P. Power analysis attacks: revealing the secrets of smart cards[M]. Springer Science & Business Media, 2008.

[11] 杜之波, 吴震, 王敏, 等. 针对 SM4 轮输出的改进型选择明文功耗分析攻击[J]. 通信学报, 2015, 36(10): 85-91.
DU Z B, WU Z, WANG M, et al. Improved chosen-plaintext power analysis attack against SM4 at the round-output[J]. Journal on Communications, 2015, 36(10): 85-91.

[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] HYUNJIN A, NEIL H, MAIRE O, et al. An improved second-order power analysis attack based on a new refined expecter[C]//Springer. 2015:174-186.

[14] WANG S, GU D W, LIU J R, et al. A power analysis on SMS4 using the chosen plaintext method[C]//International Conference on Computational Intelligence & Security. 2013:748-752.

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。