doi:10.11959/j.issn.1000-436x.2016090

针对基于 SM3 的 HMAC 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：现有基于 SM3 的 HMAC 的能量攻击方法，仅适用于同时存在汉明重量和汉明距离信息泄露的攻击对象，如果被攻击对象存在单一模型的信息泄露，则这些方法均不适用。针对该局限性，提出了一种针对 SM3 的 HMAC 的能量分析新型攻击方法，该新型攻击方法每次攻击时选择不同的攻击目标和其相关的中间变量，根据该中间变量的汉明距离模型或者汉明重量模型实施能量分析攻击，经过对 SM3 密码算法的前 4 轮多次实施能量分析攻击，将攻击出的所有结果联立方程组，对该方程组求解，即可推出最终的攻击目标。通过实验验证了该攻击方法的有效性。由于所提方法不仅可以对同时存在汉明重量和汉明距离信息泄露的对象进行攻击，而且还可以对仅存在单一信息泄露模型的对象进行攻击，所以该方法应用的攻击对象比现有的攻击方法应用更广。

关键词：HAMC 算法；SM3 算法；能量分析攻击；相关性能量分析攻击；初始状态
中图分类号：TP309.1 **文献标识码**：A

Power analysis attack of HMAC 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: The current power analysis attack of HMAC based on SM3 applies only to the object, on which there is the Hamming weight and Hamming distance information leakage at the same time. there is only a single information leakage mode on the attack object, then the attack methods don't work. To solve the limitations of the current attack methods, a novel method of the power analysis attack of HMAC based on SM3 was proposed. The different attack object and their related variables were selected in each power analysis attack. The attacks were implemented according to the Hamming distance model or Hamming weight model of the intermediate variables. After several power analysis attacked on the first four rounds of SM3, the equations that consists of the results proposed of all the power analysis attacks were obtained. The ultimate attack object is derived by getting the solution of the equations. The experimental results show that the oposed attack method was effective. The method can be used universally because its being available for both the situation of co-exist of hamming weight with Hamming distance, and that of either the Hamming weight or choosing the Hamming distance model existence.

Key words: HAMC algorithm, SM3 algorithm, power analysis attack, correlation power analysis attack, initial state

1 引言

侧信道攻击[1]通过研究密码设备在进行加密、解密或者签名时泄露的能量、电磁或者时间等信息，分析和破解密钥。能量分析攻击是侧信道攻击的一种，Kocher 等[2]于 1999 年首次提出了差分能量分析攻击(DPA, differential power analysis)，之后关于能量分析攻击的研究，Brier 等[3]提出了相关性

收稿日期：2015-06-10；修回日期：2015-10-07
基金项目：国家重大科技专项基金资助项目（No.2014ZX01032401）；国家高技术研究发展计划（“863”计划）（No.2012AA01A403）“十二五”国家密码发展基金资助项目（No.MMJJ201101022）；四川省科技支撑计划基金资助项目（No.2014GZ0148）；四川省教育厅重点科研基金资助项目（No.13ZA0091）；成都信息工程学院科研基金资助项目（No. CRF201301）
Foundation Items: The National Science and Technology Major Project (No.2014ZX01032401), The National High Technology Research and Development Program of China (863 Program) (No.2012AA01A403), “The 12th Five-Years” National Cryptogram Development Fund（No.MMJJ201101022), Sichuan Science and Technology Support Programmer(No.2014GZ0148), Sichuan Provincial Education Department Key Scientific Research Projects (No.13ZA0091), The Scientific Research Foundation of CUIT (No.CRF201301)

能量分析攻击(CPA, correlation power analysis)，Chari 等[4]提出了模板攻击(TA, template attacks)。由于能量分析攻击成功率高，代价相对较低，成为侧信道攻击研究热点方向之一。

散列消息鉴别码(HMAC, hash-based message authentication code)作为一种基于散列函数和密钥进行消息认证的方法，广泛应用于因特网、电子商务等领域，以保证信息的安全性、完整性和可靠性[5]。对于 HMAC 的安全性，关键在于散列算法的选择，随着散列函数 MD5 和 SHA1 被破解，国内外对新的杂凑函数展开了征集评估活动，我国于 2010 年公布了国内商用密码杂凑算法——SM3 密码杂凑算法[6]，SM3 主要用于数字签名和验证、消息认证码的生成与验证及随机数的生成。目前，国内外针对HMAC 的侧信道能量分析攻击，主要基于 SHA1、SHA2 等杂凑函数的 HMAC 能量分析攻击[7,8]，针对基于 SM3 的 HMAC 能量分析攻击的研究较少[9,10]，且攻击方法仅适用于同时存在汉明距离模型和汉明重量模型信息泄露的对象，如果被攻击对象存在单一模型的信息泄露，则这些攻击方法均不适用。所以研究既适合汉明重量模型，又适合汉明距离模型的针对基于 SM3 的 HMAC 能量分析攻击方法，不仅可以解决现有攻击方法的局限性问题，而且对 SM3 密码杂凑算法防御安全方面的研究和设计具有重要意义。

本文通过对 HMAC 算法的分析，确定针对 HMAC 算法侧信道能量分析攻击的目标和攻击位置，结合能量分析攻击原理和对 SM3 密码算法轮结构特点的分析，提出针对基于 SM3 的 HMAC 能量分析新型攻击方法。攻击时选择算法中和密钥相关的中间变量，根据该中间变量的汉明重量或者汉明距离建立能耗模型，实施能量分析攻击。每次能量分析攻击出和密钥相关的中间变量，经过多次攻击，将所有攻击的中间变量联立方程组，解方程即可恢复出被攻击的密钥。最后，经过对实测能量曲线进行攻击测试，结果验证了该攻击方法的有效性。

2　基于 SM3 的 HMAC 算法

2.1　HMAC 算法

HMAC 利用散列函数，以一个密钥和一个消息作为输入，计算出一个消息摘要。HMAC 主要功能是对信源身份正确性和消息完整性进行认证，具体算法的输出如式(1)所示。

$$\mathrm{HMAC}(K, m)=H((K \oplus opad)\|H((K \oplus ipad)\|m)) \quad (1)$$

其中，H 表示 SM3 密码杂凑算法，K^+ 表示认证密码 K 填充后的数据，m 表示消息输入，$opad$=0x5A，$ipad$=0x36，基于 SM3 的 HMAC 算法的实现如图 1 所示。

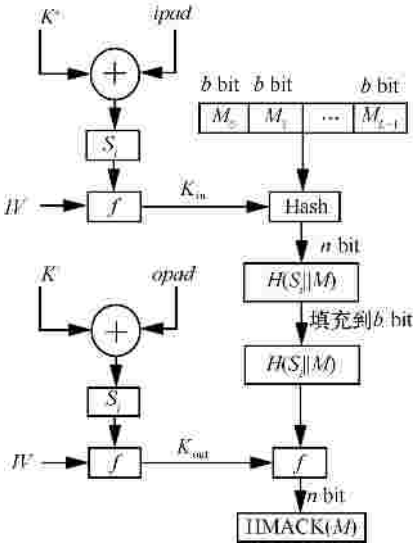

图 1　HMAC 算法

2.2　SM3 密码杂凑算法

SM3 是杂凑值长度为 256 bit 的密码杂凑算法，具体运算过程分为消息填充和迭代压缩 2 步[6]，其中，迭代压缩的压缩函数 $V^{i+1}=\mathrm{CF}(V^{(i)}, B^{(i)})$ $(0 \le i \le n-1)$描述如下。

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

2) FOR j=0 TO 63

3) $SS1$?　$((A<<<12))+E+(T_j<<<j)<<<7$

4) $SS2$?　$SS1 \oplus (A<<<12)$

5) $TT1$?　$FF_j(A,B,C)+D+SS2+W_j'$

6) $TT2$?　$GG_j(E,F,G)+H+SS1+W_j$

7) D?　C

8) C?　$B<<<9$

9) B?　A

10) A?　$TT1$

11) H?　G

12) G?　$F<<<19$

13) F?　E

14) E?　P_0　$(TT2)$

15) ENDFOR

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

在压缩函数中，A、B、C、D、E、F、G 和 H

代表 32 bit 寄存器，$SS1$、$SS2$、$TT1$ 和 $TT2$ 为中间变量，$V^{(i+1)}$ 代表压缩的结果，$B^{(i)}$ 为填充后的消息分组，$W_j^{'}$ 和 W_j 为 $B^{(i)}$ 经过消息扩展后的 32 bit 数据。$FF_j(X,Y,Z)$ 和 $GG_j(X,Y,Z)$ 为布尔函数，描述如式(2)和式(3)所示，$P_0(X)$为置换函数，描述如式(4)所示，T_j 为固定常量，详见文献[6]。

$$FF_j(X,Y,Z)=\begin{cases}X\oplus Y\oplus Z, 0\le j\le 15\\ (X\wedge Y)\vee(X\wedge Z)\vee(Y\wedge Z), 16\le j\le 63\end{cases} \tag{2}$$

$$GG_j(X,Y,Z)=\begin{cases}X\oplus Y\oplus Z, 0\le j\le 15\\ (X\wedge Y)\vee(\neg X\wedge Z), 16\le j\le 63\end{cases} \tag{3}$$

$$P_0(X)= X\oplus(X<<<9)\oplus(X<<<17) \tag{4}$$

3 能量分析攻击原理

针对密码算法的能量分析攻击，关键在于攻击点的选择，即确定算法实现中和密钥等敏感数据相关的中间变量，根据该中间变量的能量模型，进行能量分析攻击[11, 12]，其中，相关性能量分析攻击[3]的详细攻击过程如下。

1) 数据采集。采集密码设备对 N 组明文 M_n 进行加解密运算时泄露的能量信号。

2) 计算和密钥等敏感数据相关的中间变量的假设能耗值。选择算法实现中和密钥等敏感数据相关的中间变量 v，猜测密钥 k_j ($k_j\in[k_1,\cdots,k_K]$)，根据密码算法有明文 M_n 和密钥 k_j，计算对应的中间变量 $v_{n,j}$，根据 $v_{n,j}$ 的能量模型，即汉明重量模型或者汉明距离模型，将中间变量 $v_{i,j}$ 映射成对应的假设能耗值。

3) 攻击密钥。根据皮尔逊相关系数，计算假设能耗值和真实能量值之间的相关系数，相关系数绝对值最大时对应的 k_j，即为要攻击的密钥。

4 针对基于 SM3 的 HMAC 能量分析攻击

4.1 针对基于 SM3 的 HMAC 能量分析攻击原理

在认证密钥和初始向量不变的情况下，HMAC 算法进行第一次杂凑运算的 $K_{in}=f(IV,\ (K\oplus ipad))$和 $K_{out}=f(IV,\ (K\oplus opad))$为固定值，这 2 个变量只在密钥被更改时，才会发生相应的变化，所以对攻击者来讲，可以在不攻击认证密钥的情况下，通过破解 K_{in} 和 K_{out} 即可实现对信源身份进行假冒和对消息进行伪造。所以，针对基于 SM3 的 HMAC 能量攻击，其攻击的目标为 K_{in} 和 K_{out}，二者用 KV 来表示。

HMAC 算法的第 2 次杂凑运算表示为 $V^1=CF(KV, B^{(0)})$，在该表达式中，敏感信息 KV 参与计算，在计算过程中，将产生和 KV 直接相关的中间变量。所以，针对基于 SM3 的 HMAC 能量分析攻击，其攻击的运算过程为第 2 次杂凑运算，攻击的目标为第 2 次杂凑运算的初始状态。

用符号 reg_j 表示 SM3 压缩函数进行第 j 轮运算时中间变量的值，则由 2.2 节算法描述的 1）可知，攻击的目标 KV 可表示为 $A_0\|B_0\|C_0\|D_0\|E_0\|F_0\|G_0\|H_0$。由 5）和 6）可知，其运算结果 $TT1$、$TT2$ 和 KV 存在一定的相关性，且运算结果在保存和读取的过程中，其汉明重量或者汉明距离和能量曲线之间存在一定的相关性，所以可选择压缩函数的 5）和 6）作为被攻击的表达式，$TT1$ 和 $TT2$ 作为能量分析攻击的中间变量，能量分析攻击 KV。

4.2 针对基于 SM3 的 HMAC 能量分析攻击算法

由式(2)和式(3)可知，当 $0\le j\le 15$ 时，2.2 节算法描述的 5）和 6）表示为

$$TT1_j?\quad A_j\oplus B_j\oplus C_j+D_j+SS2_j+W_j^{'} \tag{5}$$

$$TT2_j?\quad E_j\oplus F_j\oplus G_j+H_j+SS1_j+W_j \tag{6}$$

针对基于 SM3 的 HMAC 能量分析攻击算法如下。

1) 攻击压缩函数的第 1 轮，j=0。令 $X_0=A_0\oplus B_0\oplus C_0+D_0+SS2_0$，$Y_0=E_0\oplus F_0\oplus G_0+H_0+SS1_0$，则式(5)和式(6)变为式(7)和式(8)。

$$TT1_0?\quad X_0+W_j^{'} \tag{7}$$

$$TT2_0?\quad Y_0+W_j \tag{8}$$

在式(7)和式(8)中，X_0 和 Y_0 是由攻击目标 KV 计算所得，是固定的敏感信息，$W_0^{'}$ 和 W_0 是由消息扩展得到的，即变化的已知数据，所以根据能量分析攻击原理，可根据中间变量 $TT1_0$ 和 $TT2_0$ 的汉明重量或汉明距离，能量分析攻击出和 KV 相关的 X_0 和 Y_0。

2) 攻击压缩函数的第 2 轮，j=1。由 2.2 节算法描述的 1）和 4）可得式(5)和式(6)中的 $A_1=TT1_0$，$E_1=P_0(TT2_0)$，由于攻击压缩函数的第一轮中已经攻击出 X_0 和 Y_0，所以根据式(7)和式(8)可计算出 $TT1_0$ 和 $TT2_0$，也即 A_1 和 E_1 是经过计算成为攻击者已知数据；进一步经过算法描述的 4）的计算，式(5)和式(6)中的 $SS2_1$ 和 $SS1_1$ 成为攻击者已知数据；经过

第 1 轮的计算，$B_1 = A_0$，$C_1 = B_0 <<< 9$，$D_1 = C_0$，$H_1 = G_0$，$G_1 = F_0 <<< 19$，$F_1 = E_0$，所以，攻击猜测的数据为 B_1、C_1、D_1、F_1、G_1 和 H_1。

令 $X_1 = B_1 \oplus C_1$，$Y_1 = F_1 \oplus G_1$，$A_1 = (a_{31} \perp a_i \perp a_0)_2$，其中，$a_i \in \{0,1\}$，则 $X_1 = (x_{31} \perp x_i \perp x_0)_2$，$Y_1 = (y_{31} \perp y_i \perp y_0)_2$，$D_1 = (d_{31} \perp d_i \perp d_0)_2$，$H_1 = (h_{31} \perp h_i \perp h_0)_2$，$E_1 = (e_{31} \perp e_i \perp e_0)_2$，被攻击表达式可表示为

$$TT1_1 ? \ 2^{32} \ (a_{31} \oplus x_{31} \oplus d_{31}) + (a_{30} \perp a_i \perp a_0) \oplus (x_{30} \perp x_i \perp x_0) + (d_{30} \perp d_i \perp d_0) + SS2_1 + W_1' \quad (9)$$

$$TT2_1 ? \ 2^{32} \ (e_{31} \oplus y_{31} \oplus h_{31}) + (e_{30} \perp e_i \perp e_0) \oplus (y_{30} \perp y_i \perp y_0) + (h_{30} \perp h_i \perp h_0) + SS1_1 + W_1 \quad (10)$$

在式(9)和式(10)中，X_1、Y_1、D_1 和 H_1 未知，A_1、E_1、$SS2_1$ 和 $SS1_1$ 为已知可计算数据，W_1' 和 W_1 是由消息扩展得到的，即是变化的已知数据，所以，根据能量分析攻击原理，可根据中间变量 $TT1_1$ 和 $TT2_1$ 的汉明重量或汉明距离，能量分析攻击 $(d_{31} \oplus x_{31})$、$(x_{30} \perp x_i \perp x_0)$、$(d_{30} \perp d_i \perp d_0)$、$(h_{31} \oplus y_{31})$、$(h_{30} \perp h_i \perp h_0)$ 和 $(y_{30} \perp y_i \perp y_0)$。

3) 攻击压缩函数的第 3 轮，j=2。经过压缩函数第 2 轮的计算，此时式(5)和式(6)中的 $A_2 = TT1_1$，$E_2 = P_0(TT2_1)$，$B_2 ? \ A_1 = TT1_0$，$F_2 ? \ E_1 = P_0(TT2_0)$，由于攻击压缩函数的第 2 轮中已经攻击 $(d_{31} \oplus x_{31})$、$(x_{30} \perp x_i \perp x_0)$、$(d_{30} \perp d_i \perp d_0)$、$(h_{31} \oplus y_{31})$、$(h_{30} \perp h_i \perp h_0)$ 和 $(y_{30} \perp y_i \perp y_0)$，所以根据式(9)和式(10)可计算出 $TT1_1$ 和 $TT2_1$，即 A_2 和 E_2 是经过计算成为攻击者已知数据，而经过第一轮的攻击，攻击者可计算出 $TT1_0$ 和 $TT2_0$，所以 B_2 和 F_2 变为已知数据；进一步经过计算，式(5)和式(6)中的 $SS2_2$ 和 $SS1_2$ 成为攻击者已知数据，所以攻击猜测的数据为 C_2、D_2、G_2 和 H_2，此时的攻击表达式为

$$TT1_2 ? \ 2^{32}(a_{31} \oplus b_{31} \oplus c_{31} \oplus d_{31}) + (a_{30} \perp a_i \perp a_0) \oplus (b_{30} \perp b_i \perp b_0) \oplus (c_{30} \perp c_i \perp c_0) + (d_{30} \perp d_i \perp d_0) + SS2_2 + W_2' \quad (11)$$

$$TT2_2 ? \ 2^{32} \ (e_{31} \oplus f_{31} \oplus g_{31} \oplus h_{31}) + (e_{30} \perp e_i \perp e_0) \oplus (f_{30} \perp f_i \perp f_0) \oplus (g_{30} \perp g_i \perp g_0) + (h_{30} \perp h_i \perp h_0) + SS1_2 + W_2 \quad (12)$$

在式(9)和式(10)中，C_2、D_2、G_2 和 H_2 未知，A_2、B_2、E_2、F_2、$SS2_2$ 和 $SS1_2$ 为已知可计算数据，W_2' 和 W_2 是由消息扩展得到的，即是变化的已知数据，所以，可根据中间变量 $TT1_2$ 和 $TT2_2$ 的汉明重量或汉明距离进行能量分析攻击，攻击 $(d_{31} \oplus c_{31})$、$(c_{30} \perp c_i \perp c_0)$、$(d_{30} \perp d_i \perp d_0)$、$(h_{31} \oplus g_{31})$、$(h_{30} \perp h_i \perp h_0)$ 和 $(g_{30} \perp g_i \perp g_0)$。

4) 攻击压缩函数的第 4 轮，j=3。经过压缩函数第 1 轮、第 2 轮和第 3 轮计算，此时式(5)和式(6)中的 $A_3 = TT1_2$，$E_3 = P_0(TT2_2)$，$B_3 ? \ A_2 = TT1_1$，$F_3 ? \ E_2 = P_0(TT2_1)$，$C_3 ? \ B_2 <<< 9 = A_1 <<< 9 = TT1_0 <<< 9$，$G_3 ? \ F_2 <<< 19 = E_1 <<< 19 = P_0(TT2_0) <<< 19$，由于经过前 3 轮的攻击，可计算出 $TT1_0$、$TT2_0$、$TT1_1$、$TT2_1$、$TT1_2$ 和 $TT2_2$，所以在式(5)和式(6)中，A_3、B_3、C_3、E_3、F_3 和 G_3 为已知可计算数据；进一步经过计算，式(5)和式(6)中的 $SS2_3$ 和 $SS1_3$ 成为攻击者已知数据，由于 W_3' 和 W_3 是由消息扩展产生，所以，攻击猜测数据为 D_3 和 H_3，此时的攻击表达式如下

$$TT1_3 ? \ A_3 \oplus B_3 \oplus C_3 + D_3 + SS2_3 + W_3' \quad (13)$$

$$TT2_3 ? \ E_3 \oplus F_3 \oplus G_3 + H_3 + SS1_3 + W_3 \quad (14)$$

其中，D_3 和 H_3 未知，A_3、B_3、C_3、E_3、F_3、G_3、$SS2_3$ 和 $SS1_3$ 为已知可计算数据，W_2' 和 W_2 是由消息扩展得到的，即是变化的已知数据，所以可根据中间变量 $TT1_3$ 和 $TT2_3$ 的汉明重量或汉明距离进行能量分析攻击，攻击 D_3 和 H_3。

5) 将 4 轮的攻击结果联立方程组，推导出攻击目标 KV。根据第 4 轮的攻击结果及 2.2 节算法描述的 7）和 8）可推导出 $C_2 = D_3$，$G_2 = H_3$，由于第 3 轮攻击已经攻击出 $(d_{31} \oplus c_{31})$、$(c_{30} \perp c_i \perp c_0)$、$(d_{30} \perp d_i \perp d_0)$、$(h_{31} \oplus g_{31})$、$(h_{30} \perp h_i \perp h_0)$ 和 $(g_{30} \perp g_i \perp g_0)$，所以，可推导出 D_2 和 H_2。

由于 $C_2 ? \ B_1 <<< 9 = A_0 <<< 9$，所以被攻击的目标 $A_0 = B_1 = C_2 >>> 9$。

由于 $D_2 ? \ C_1 = B_0 <<< 9$，所以被攻击的目标 $B_0 = D_2 >>> 9$，$C_1 = D_2$。

由于 $G_2 ? \ F_1 <<< 19 = E_0 <<< 19$，所以被攻击的目标 $E_0 = G_2 >>> 19$。

由于 $H_2 ? \ G_1 = F_0 <<< 19$，所以被攻击的目标 $F_0 = H_2 >>> 19$。

由 B_1、C_1、F_1 和 G_1 可计算出在攻击第 2 轮时的 $X_1 = B_1 \oplus C_1$ 和 $Y_1 = F_1 \oplus G_1$，再根据第 2 轮的攻击结果，可推导出 D_1 和 H_1，进一步可得 $C_0 = D_1$ 和 $G_0 = H_1$。

在计算出 A_0、B_0、C_0、E_0、F_0 和 G_0 的情况下，根据第一轮的攻击结果 X_0 和 Y_0，可计算出 D_0 和 X_0，最终得到攻击目标 KV 的值。

5 针对基于 SM3 的 HMAC 能量分析攻击实验

由于针对基于 SM3 的 HMAC 能量分析攻击，攻击目标为 SM3 算法的初始状态 IV，所以为验证攻击算法的正确性，实验直接对 SM3 算法的安全性进行了测试。攻击目标为 SM3 密码算法的初始状态 IV，攻击对象为 32 位智能卡上软实现 SM3 算法，实验环境为 Inspector SCA 平台，采集到的能量曲线为 5 000 条，波形如图 2 所示。

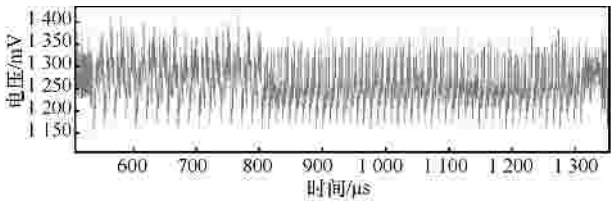

图 2 SM3 能量信号曲线

5.1 实测能量分析攻击过程

以攻击第 2 轮的式(9)为例，在已经完成对第 1 轮攻击的基础上，即完成对式(7)和式(8)的攻击，得到 X_0 =0x588B5DAB 和 Y_0 =0x5F057B3B 基础上进行攻击，从低到高按字节进行攻击的攻击结果如图 3~图 6 所示。

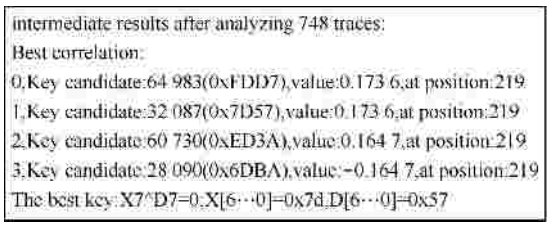

图 3 针对第 1 个字节的攻击结果

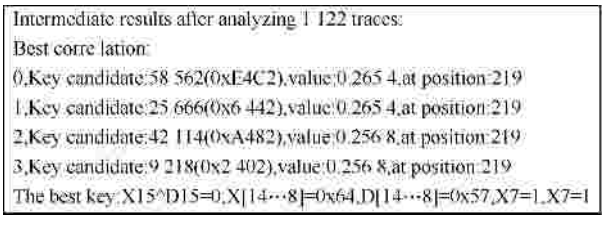

图 4 针对第 2 个字节的攻击结果

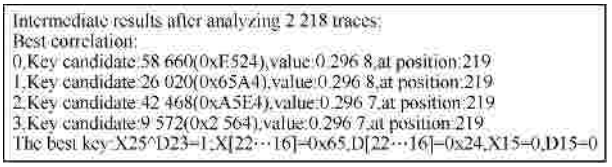

图 5 针对第 3 个字节的攻击结果

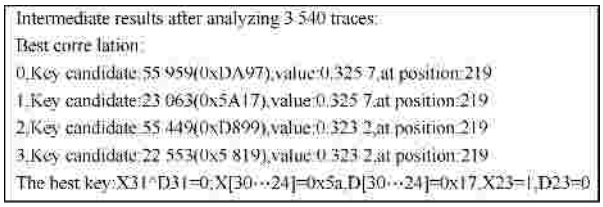

图 6 针对第 4 个字节的攻击结果

最终对式(9)的攻击结果为 $(d_{31} \oplus x_{31})=0$，$(x_{30} \perp x_i \perp x_0) = 0x5AE564FD$，$(d_{30} \perp d_i \perp d_0) =0x1724\ 42D7$，同理按照 4.2 节攻击算法的步骤 2)，对式(10)进行实测攻击，最终的攻击结果为：$(h_{31} \oplus y_{31})=1$、$(h_{30} \perp h_i \perp h_0) = 0x638DEE4D$ 和 $(y_{30} \perp y_i \perp y_0) = 0x6C3F8135$。

按照 4.2 节攻击算法的步骤 3)进行实测攻击，实测的攻击结果为：$(d_{31} \oplus c_{31})=0$，$(c_{30} \perp c_i \perp c_0) =0x2CDEE7$，$(d_{30} \perp d_i \perp d_0) = 0x29657292$，$(h_{31} \oplus g_{31}) = 0$，$(h_{30} \perp h_i \perp h_0) = 0x4550b189$ 和 $(g_{30} \perp g_i \perp g_0) = 0x05E54\ B79$。

按照 4.2 节攻击算法的步骤 4)进行实测攻击，实测的攻击结果为：D_3 =0x2CDEE7 和 $H_3 = (g_{30} \perp g_i \perp g_0) = 0x85E54B79$。

按照 4.2 节攻击算法的步骤 5)所述方法，将所有实测攻击结果联立方程组，最终得到攻击目标 IV=0x7380166f4914b2b9172442d7da8a0600a96f30bc163138aae38dee4db0fb0e4e。由于基于该 IV 对消息进行 SM3 杂凑运算的结果和被攻击智能卡杂凑运算的结果相同，所以验证了该攻击结果 IV 的正确性，同时也验证了本文所述攻击方法的可行性。

5.2 实验结果分析

在能量分析攻击中，常用的能量模型为汉明距离模型或者汉明重量模型，和现有的可参考的攻击方法[10]相比，本文方法适合的攻击模型如表 1 所示，从表 1 分析可知，本文所述攻击方法优点是：应用的攻击对象更广，适用的攻击模型更多。

表 1 攻击方法的性能对比

攻击方法	汉明重量模型	汉明距离模型	二者混合模型
本文攻击方法	适用	适用	适用
文献[10]攻击方法	不适用	不适用	适用

6　结束语

本文通过对 SM3 密码杂凑算法的结构特点分析，给出针对基于 SM3 的 HMAC 的能量分析攻击的目标和攻击方法。攻击时，选择算法中的 *TT*1 和 *TT*2 作为攻击的中间变量实施能量分析攻击，将前 4 轮的攻击结果联立方程组，并由该方程组推导出攻击目标。该攻击方法不仅适用于同时存在汉明重量和汉明距离信息泄露的对象，而且还适用于存在单一信息泄露的对象，解决了现有攻击方法仅适用于同时存在汉明距离和汉明重量信息泄露对象的局限性。

此外，虽然本文方法攻击目标选择的是 SM3 密码杂凑算法的初始状态，但是攻击选择的是针对 SM3 密码杂凑算法进行的能量分析攻击，所以本攻击方法还可以应用到基于 SM3 密码杂凑算法的其他应用场景中，对应用场景中的敏感信息实施能量分析攻击。

参考文献：

[1] PAUL K. Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems[C]//CRYPTO 1996. Berlin, c1996: 104-113.

[2] PAUL K, JOSHUA J, BENJAMIN J. Differential power analysis[C]// The 19th Annual International Cryptology Conference on Advances in Cryptology. c1999: 388-397.

[3] ERIC B, CHRISTOPHE C, FRANCIS O. Correlation power analysis with a leakage model[C]//Cryptographic Hardware and Embedded Systems – CHES 2004. c2004:16-29.

[4] SURESH C, JOSYULA R R, PANKAJ R. Template attacks[C]// Cryptographic Hardware and Embedded Systems-CHES 2002. c2003: 13-28.

[5] MIHIR B, RAN C, HUGO K. Keying hash functions for message authentication[C]//Neal Koblitz, CRYPTO. c1996: 1-15.

[6] China's Office of security commercial code administration: sepecification of SM3 cryptographic hash function[EB/OL]. http://www. oscca.gov.cn/UpFile/20101222141857786.pdf. 2010.

[7] KATSUYUKI O. Side channel attacks against HMACs based on lock-cipher based hash functions[C]//Information Security and Privacy (ACISP 2006). c2006: 432-443.

[8] ROBERT M, MICHAEL T, COLIN C M, et al. Differential power analysis of HMAC based on SHA-2, and countermeasures [J]. Information Security Applications, 2007, 4867: 317-332.

[9] GUO L M, LI Q, WANG L H, et al. A differential power analysis attack on dynamic password token based on SM3 algorithm[C]//First International Conference on Information Science and El nic Technology (ISET 2015). c2015.107-110.

[10] GUO L M, LI Q, WANG L H, et al. A first-order differential power analysis attack on HMAC-SM3[C]//First International Conference on Information Science and Electronic Technology (ISET 2015), c2015: 94-97.

[11] 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.

[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.

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。