doi:10.11959/j.issn.1000-436x.2016248

针对基于 SM3 的 HMAC 的互信息能量分析攻击

吴震[1]，王敏[1]，饶金涛[1]，杜之波[1]，王胜[2]，张凌浩[2]
（1. 成都信息工程大学 信息安全工程学院，四川 成都 610225；
2. 国网四川省电力公司电力科学研究院，四川 成都 610072）

摘 要：提出了对应的互信息能量分析攻击，该方法结合了能量分析的基本原理和信息论的基础，利用能量泄露的中间值和能量迹计算两者的互信息大小，从而达到提取密钥的目的。利用该方法针对基于 SM3 的 HMAC 算法进行了实测攻击，实验表明，该方法可以成功恢复出 SM3 算法初始状态从而提取出正确的密钥，扩展了侧信道攻击的方法。
关键词：HAMC 算法；SM3 算法；能量分析攻击；互信息能量分析攻击；初始状态
中图分类号：TP309.1 **文献标识码**：A

Mutual information power analysis attack of HMAC based on SM3

WU Zhen[1], WANG Min[1], RAO Jin-tao[1], DU Zhi-bo[1], WANG Sheng[2], ZHANG Ling-hao[2]
(1. College of Information Security Engineering, Chengdu University of Information Technology, Chengdu 610225, China;
2. State Grid Sichuan Electric Power Research Institute, Chengdu 610072, China)

Abstract: A novel method of mutual information power analysis attack was proposed. The method was built on the basis of the basic principle of power analysis and the basic theory of information. For the purpose of attacking the key, the mutual information values was computed using two values between the mediate variable with the power traces. An experiment was implemented on the algorithm of HMAC based on SM3 using this method. The experimental results show the proposed attack method is effective because the initial value of state variable can be successfully retrieved to compute the real true key.
Key words: HAMC algorithm, SM3 algorithm, power analysis attack, mutual information power analysis attack, initial state

1 引言

侧信道攻击通过研究密码设备在运行过程中泄露的能量、电磁辐射或者时间等旁路信息[1]，进而分析和破解密钥一种方法。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)，Brier 等[3]提出了相关性能量分析攻击(CPA, correlation power analysis)，Chari 等[4]提出了模板攻击(TA, template attack)，Gierlichs 等[5]2008 年在密码硬件与嵌入式系统国际会议(CHES08)上提出了互信息能量分析攻击。由于能量分析攻击与其他攻击方法相比，起成本较低，攻击效率比较高，因此成为了目前研究的热点。

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[6]，对消息的完整性和信源的身份进行认证。而 HAMC 的安全性主要是取决于散列函数的选择，目前，散列函数主要有 SHA1、SHA2 和 MD5 等。而 SM3 是我国自主研发的散列算法[7]，主要用于计算消息摘要，从而实现数字签名认证。目前，针对 HMAC 的侧信道能量分析攻击，主要是针对 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

收稿日期：2016-09-08
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）；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）
Foundation Items: The National Science and Technology Major Project (No.2014ZX01032401-001), The National High Technology Research and Development Program of China (863 Program) (No.2012AA01A403), Sichuan Science and Technology Support Program (No.2014GZ0148), Sichuan Provincial Education Department Key Scientific Research Projects (No.13ZA0091)

析攻击的研究较少[9,10]，而且攻击主要是利用线性相关皮尔逊相关系数或者差分的方法进行分析攻击。所以研究其他攻击方法对 SM3 的侧信道攻击防御具有极其深远的意义。

本文通过对基于 SM3 的 HMAC 算法进行了分析，针对该算法能量信息泄露点进行定位，结合互信息能量分析攻击原理，提出了针对基于 SM3 的 HMAC 互信息能量分析攻击方法。经过 10 次互信息能量分析攻击，可以完全恢复出被攻击的中间状态。最后经过在真实环境下进行实测攻击，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 算法是 Krawazyk 等于 1996 年提出的一种基于散列函数和密钥进行消息认证的方法，可以对消息的完整性和信源的身份进行认证，具体是利用一个已知的散列函数，同时引入密钥和任意长度的消息，最终计算出消息摘要，具体计算如式(1)所示。

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

其中，H 代表使用的散列函数，K 代表密钥，*opad* 和 *ipad* 是常量。

对于基于 SM3 的 HMAC 算法，式(1)中的 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，IV 表示初始状态预设的常量，下同，*opad*=0x5A，*ipad*=0x36，HMAC 算法的实现如图 1 所示。

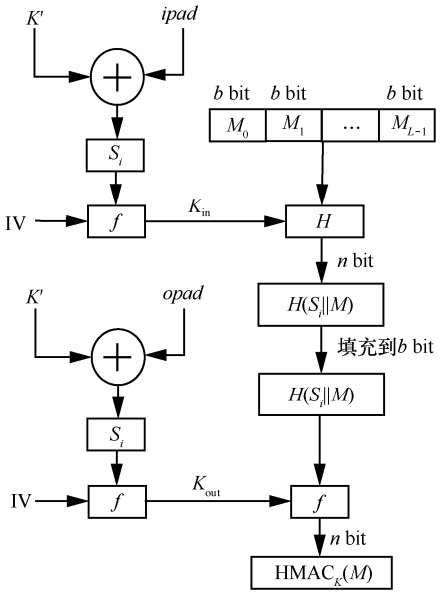


图 1 HMAC 算法

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，具体运算过程分为填充消息、扩展消息、迭代压缩 3 步。

1) 填充消息

假设消息 m 的长度为 l bit。首先将比特“1”添加到消息的末尾，再添加 k 个“0”，k 是满足 $l+1+k=448 \bmod 512$ 的最小的非负整数。然后再添加一个 64 bit 比特串，该比特串是长度 1 的二进制表示。填充后的消息 m' 的比特长度为 512 的倍数。将填充后的消息 m' 按 512 bit 进行分组为

$$m' = B^{(0)}B^{(1)}\cdots B^{(n)} \quad (2)$$

其中，$n=\dfrac{l+k+65}{512}$。

2) 扩展消息

将消息分组 $B^{(i)}$ 按照以下方式扩展生成 132 个字 $W_0,W_1,\cdots,W_{67}$，$W_0',W_1',\cdots,W_{63}'$，用于压缩函数。

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

② for j=16 to 67

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

end for

③ for j=0 to 16

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

end for

其中，$P_1(X)= X\oplus (X<<<9)\oplus (X<<<17)$

3)迭代压缩

迭代压缩的压缩函数 $V^{i+1}=CF(V^{(i)},B^{(i)})$ $(0\leqslant i\leqslant n-1)$描述如下

①$ABCDEFGH \leftarrow V^{(i)}$

②for j=0 to 63

③$SS_1\leftarrow((A<<<12))+E+(T_j<<<j)<<<7$

④$SS_2\leftarrow SS1\oplus (A<<<12)$

⑤$TT_1\leftarrow FF_j(A,B,C)+D+SS_2+W_j'$

⑥$TT_2\leftarrow GG_j(E,F,G)+H+SS_1+W_j$

⑦$D\leftarrow C$

⑧$C\leftarrow B<<<9$

⑨$B\leftarrow A$

⑩$A\leftarrow TT_1$

⑪$H\leftarrow G$

⑫$G \leftarrow F<<<19$

⑬$F \leftarrow E$

⑭$E \leftarrow P_0(TT_2)$

⑮end for

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

在压缩函数中，A、B、C、D、E、F、G 和 H 代表 32 bit 寄存器，SS_1、SS_2、TT_1 和 TT_2 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，$P_0(X)$为置换函数，T_j 为固定常量。

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

$$GG_j(X,Y,Z)=\begin{cases}X\oplus Y\oplus Z, 0\leqslant j\leqslant 15\\ (X\wedge Y)\vee(\neg X\wedge Z), 16\leqslant j\leqslant 63\end{cases} \tag{4}$$

$$P_0(\mathrm{X})= X\oplus(X<<<9)\oplus(X<<<17) \tag{5}$$

3　互信息能量分析攻击原理

3.1　互信息

熵和互信息是信息论中最基本的度量，本节主要介绍熵和互信息的基本知识，设 $X=(X_1,X_2,\cdots,X_n)$ 为一组有限随机离散变量集合，则 X 的信息熵为 $H(X)=\sum_{x\in X}-p(x)\mathrm{lb}p(x)$，其中，$p(x)$ 为所有变量可能出现的取值组合的概率分布。

类似地，设 $X=(X_1,X_2,\cdots,X_n)$，$Y=(Y_1,Y_2,\cdots,Y_n)$ 这 2 个有限的离散随机变量集合，X 的条件熵是在 Y 给定的前提下 X 的不确定度。

$$H(X\mid Y)=-\sum_{y\in Y}p(y)\mathrm{lb}p(y)\sum_{x\in X}p(x\mid y)\mathrm{lb}p(x\mid y)$$

互信息是 2 个随机变量的统计相关度的一种度量，2 个变量集之间的互信息定义为

$$I(X;Y)=H(X)-H(X\mid Y)$$

3.2　互信息能量分析攻击

假设 K 是随机变量集合，代表密钥的集合；k^* 代表正确的密钥；X 是随机变量，代表目标密码算法的输入的明文；Z 是随机变量，代表密码算法中间状态的输出（中间值）。定义一个泄露函数 $L(Z)=f(X,K)$，泄露函数是依赖于设备，$L(Z)$ 是连续的。

对于侧信道能量分析攻击而言，假设存在 n 次测量，$l_i=f(x_i,k^*)(i=1,\cdots,n)$,在给定一个密钥 k 的情况下，可以通过 $M=(X,k)$ (代表计算中间值的函数)计算出中间值，M 是离散的。因此，对于每一个假定的 k，通过 $M=(x_i,k)(x_i\in X)$ 可以得到 n 个中间值。侧信道攻击就是利用这些中间值和测量值进行建模[11,12]，一般认为，攻击成功时，有

$$\max_{k\in K}(|D(M(x,k),l)|)=k^*$$

其中，D 代表区分器。具有代表性的区分器有相关系数分析、互信息分析。Brier 等在 2004 年提出了相关系数分析，Gierliehs 等在 CHES08 会议上提出互信息分析(MIA, mutual information analysis)，利用互信息的基本理论与能量分析攻击相结合，提出了一种区分器[5]。互信息如式(6)所示。

$$I(l,M(x,k))=H(I)-H(I\mid M(x,k)) \tag{6}$$

当假定的密钥不同时，得到的平均互信息也不同。得到平均互信息的值与条件熵 $H(I\mid M(x,k))$ 有关，当条件熵达到最小的时候，平均互信息量达到最大，此时说明测量值 l 和 $M(x,k)$ 存在的相关度越大，此时密钥猜测正确。同时这种区分器也可以检测非线性的关系。

4　针对基于SM3的HMAC互信息能量攻击分析

本节主要针对 SM3 的 HAMC 互信息能量分析攻击，攻击的目标不是密钥 K，而是攻击 SM3 密码杂凑函数的秘密的 2 个中间状态 K_{in} 和 K_{out}，当攻击者得到这 2 个中间状态，就可以进行消息伪造和假冒信源身份认证。

4.1　针对基于SM3的HMAC互信息能量攻击原理

由图 1 可以得知，K_{in} 和 K_{out} 为 2 个秘密的中间状态，而且只有在密钥 K 发生改变的时候 K_{in} 和 K_{out} 才会发生改变，K_{in}=f(IV, ($K\oplus ipad$))，K_{in}=f(IV, ($K\oplus ipad$))，f 代表 SM3 杂凑运算。K_{in} 为第 1 次 SM3 杂凑运算的中间结果，用 H^0 表示 K_{in}。由 2.2 节的 3)迭代压缩的第①步可知，攻击的目标 H^0 可表示为 $A_0||B_0||C_0||D_0||E_0||F_0||G_0||H_0$。

HMAC 算法的第 2 次杂凑运算表示为 $V^1=CF(H^0,B^{(0)})$，在该表达式中，H^0 参与运算，在运算过程中，将产生和 H^0 直接相关的中间变量。所以针对基于 SM3 的 HMAC 互信息能量分析攻击，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。

4.2 针对基于SM3的HMAC互信息能量攻击过程

由第2.2节的3)迭代压缩的第③~⑭步可知，当$0 \leqslant j \leqslant 15$时，假设所有32位寄存器的初始值均为0，此时有$A_0B_0C_0D_0E_0F_0G_0 = V^{(0)}$，被攻击的可以如下描述。

① $SS_{1j} \leftarrow ((A_j <<<12)) + E_j + (T_j <<< j) <<<7$

② $SS_{2j} \leftarrow SS_{1j} \oplus (A_j <<<12)$

③ $TT_{1j} \leftarrow FF_j(A_j, B_j, C_j) + D_j + SS_{2j} + W_j'$

④ $TT_{2j} \leftarrow GG_j(E_j, F_j, G_j) + H_j + SS_{1j} + W_j$

⑤ $D_{j+1} \leftarrow C_j$

⑥ $C_{j+1} \leftarrow B_j <<<9$

⑦ $B_{j+1} \leftarrow A_j$

⑧ $A_{j+1} \leftarrow TT_{1j}$

⑨ $H_{j+1} \leftarrow G_j$

⑩ $G_{j+1} \leftarrow F_j <<<19$

⑪ $F_{j+1} \leftarrow E_j$

⑫ $E_{j+1} \leftarrow P_0(TT_{2j})$

基于SM3的HMAC能量分析攻击方法详细分析如下。

1) 攻击压缩函数的第1轮，即j=0时，令$X_0 = A_0 \oplus B_0 \oplus C_0 + D_0 + SS_{20}$，$Y_0 = E_0 \oplus F_0 \oplus G_0 + H_0 + SS_{10}$，则被攻击者第③、④步变为式(6)和式(7)。

$$TT_{10} \leftarrow X_0 + W_j' \tag{6}$$

$$TT_{20} \leftarrow Y_0 + W_j \tag{7}$$

在式(6)和式(7)中，X_0和Y_0是由攻击目标H^0计算所得，是固定的秘密信息，W_0'和W_0是由消息扩展得到的，即变化的已知数据，所以根据互信息能量分析攻击原理，首先计算采集到的所有能量迹在该时刻的概率分布，接着计算在猜测密钥下，中间变量$TT1_0$和$TT2_0$汉明距离或者汉明重量的概率分布，以及在该汉明重量概率分布的条件下重新计算采集到的能量迹在该时刻的概率分布，从而得出互信息的大小，分析攻击出和H^0相关的X_0和Y_0的真实值。

2) 攻击压缩函数的第1轮，即j=0时，根据1)可得，TT_{10}和TT_{20}此时已经为已知值，并且是变化的值，在第⑧步和第⑫步，利用1)中的方法，根据汉明距离$HD(A_0, A_1)$和汉明距离$HD(E_0, E_1)$和曲线上的能量迹分别计算猜测密钥下的互信息的大小，分析攻击出A_0、E_0的真实值。经过此次攻击后得到B_1=A_0, $F_1 = E_0$。

3) 攻击压缩函数的第2轮，即j=1时，此时$B_1 = A_0$, $A_1 = TT_{10}$, $C_1 = B_0 <<<9$, A_1、B_1此时为已知值，C_1为未知值，在式$FF_1(A_1, B_1, C_1)$=$A_1 \oplus B_1 \oplus C_1$中，利用汉明重量$HW(FF_1(A_1$、$B_1$、$C_1))$和曲线上的能量迹计算猜测值下的互信息大小，分析攻击出C_1，进而反推出B_0。

4) 攻击压缩函数的第1轮，即j=0时，此时在式$FF_0(A_0, B_0, C_0)$=$A_0 \oplus B_0 \oplus C_0$中$A_0$、$B_0$为已知值，$C_0$为未知的值，利用$HW(FF_1(A_0$，$B_0$，$C_0))$和曲线上的能量迹计算对应猜测值下的互信息的大小，分析攻击出C_0，此时A_0、B_0、C_0均为已知值，同时可以利用第③步，根据中间变量TT_{10}的汉明重量$HW(TT_{10})$分布和曲线上的能量迹计算对应猜测值下的互信息的大小，分析攻击得出D_0。

5) 攻击压缩函数的第2轮，即j=1时，此时，A_0、E_0、B_0、C_0、D_0、B_1、A_1、F_1、E_1、C_1、SS_{10}、SS_{20}均为已知值，在式$GG_1(E_1, F_1, G_1) = E_1 \oplus F_1 \oplus G_1$中，利用汉明重量$HW(GG_1(E_1, F_1, G_1))$和曲线上的能量迹计算对应猜测值下的互信息的大小，分析攻击得出G_1，进而反推出F_1。

6) 攻击压缩函数的第2轮，即j=1时，此时，在第④步，只有H_1是未知，根据中间变量TT_{21}的汉明重量$HW(TT_{21})$和曲线上的能量迹计算对应猜测值下的互信息的大小，分析攻击得出H_1，进而反推出G_0。

7) 攻击压缩函数的第1轮，即j=0时，此时，在第④步，只有H_0是未知，根据中间变量TT_{20}的汉明重量$HW(TT_{20})$和曲线上的能量迹计算对应猜测值下的互信息的大小，分析攻击得出H_0。此时已完全恢复出目标H^0。

5 针对基于SM3的HMAC互信息能量分析攻击实验

5.1 实验设置

由于针对基于SM3的HMAC能量分析攻击，攻击目标为第2次进行SM3算法运算的初始状态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。

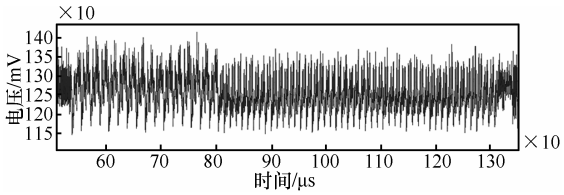


图 2　一次 SM3 杂凑算法的能量迹

5.2　实验结果分析

以攻击 X_0 和 Y_0 为例说明,攻击结果如表 1 和表 2 所示。

表 1　　X_0 攻击的结果

X_0 字节数	候选	猜测密钥	互信息
1	1	171(0xAB)	0.149 700 88
	2	175(0xAF)	0.091 114 76
	3	179(0xB3)	0.083 942 41
	4	173(0xAD)	0.080 647 47
2	1	93(0x5D)	0.057 168 96
	2	221(0xDD)	0.036 893 606
	3	97(0x61)	0.028 832 912
	4	29(0x1D)	0.028 556 347
3	1	139(0x8b)	0.045 111 18
	2	11(0xb)	0.032 523 155
	3	155(0x9b)	0.019 926 000
	4	171(0xab)	0.019 926 071
4	1	88(0x58)	0.039 939 165
	2	216(0xd8)	0.028 746 128
	3	232(0xe8)	0.026 728 153
	4	24(0x18)	0.023 374 557

表 2　　Y_0 攻击的结果

Y_0 字节数	候选	猜测密钥	互信息
1	1	59(0x3b)	0.059 343 815
	2	27(0x1b)	0.051 928 997
	3	43(0x2b)	0.047 966 957
	4	51(0x33)	0.039 445 877
2	1	123(0x7b)	0.054 609 776
	2	124(0x7c)	0.028 824 568
	3	125(0x7d)	0.027 479 887
	4	139(0x8b)	0.027 244 806
3	1	5(0x5)	0.035 793 543
	2	7(0x7)	0.019 990 921
	3	21(0x15)	0.017 910 957
	4	9(0x9)	0.017 578 125
4	1	95(0x5f)	0.058 778 763
	2	159(0x9f)	0.035 902 26
	3	223(0xdf)	0.035 723 21
	4	96(0x60)	0.033 185 96

在以上的攻击基础上，根据 4.2 节的步骤 2)可以攻击出 E_0=0xA96F30BC，根据步骤 3)可攻击出 B_0=0x4914b2b9，同理得出 C_0=0x172442D7，最终得出 H^0=0x7380166F4914B2B9172442D7DA8A0600A96F30BC163138AAE38DEE4DB0FB0E4E。

6　结束语

利用互信息能量分析攻击方法对基于 SM3 的 HMAC 算法进行实测攻击，证明了该攻击方法的有效可行性。

参考文献：

[1] KOCHER P. Timing attacks on implementAtions of diffie-hellmAn, RSA, DSS, and other systems[C]//CRYPTO 1996. 1996：104-113.

[2] KOCHER P, JAFFE J, JUN B A. Differential power analysis[C]// Proceedings of the 19th AnnuAl InternAtionAl Cryptology Conference on AdvAnces in Cryptology Lecture Notes In Computer Science. 1999: 388-397.

[3] BRIER E, CLAVIER C, OLIVIER F. Correlation power analysis with a leakage model[C]//CryptogrAphic HArdwAre And Embedded Systems. 2004: 16-29.

[4] SURESH C, JOSYULA R R, PANKAJ R. Template attacks[C]// CryptogrAphic Hardware and Embedded Systems – CHES 2002. 2003: 13-28.

[5] GIERLICHS B, BATINA L, TUYLS P, et al. Mutual information analysis[J]. In CHES 2008, LNCS, 2008: 426-442.

[6] BELLARE M, CANETTI R, KRAWCZYK H. Keying hash functions for message authentication[C]//CRYPTO. 1996: 1-15.

[7] China's office of security commercial code administration: sepecification of sm3 cryptographic hash function (2010) [EB/OL]. http://www.oscca.gov.cn/UpFile/20101222141857786.pdf.

[8] MCEVOY R, TUNSTALL M, COLIN C, et al. Differential power analysis of HMAC based on SHA-2, and countermeasures[J]. Information Security ApplicAtions, 2007: 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 Electronic Technology (ISET 2015). 2015: 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). 2015: 94-97.

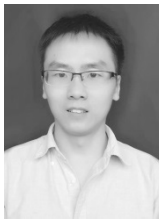
[11] 吴震, 陈运, 陈俊, 等. 真实硬件环境下幂剩余功耗轨迹指数信息提取[J]. 通信学报, 2010, 31(2): 17-21.
WU Z, CHEN Y, CHEN J, et al. Exponential information's extraction from power traces of modulo exponentiation implemented on FPGA[J]. Journal on Communications, 2010, 31(2): 17-21.

[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：

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。

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。

王胜（1987-)），男，四川达州人，国网四川省电力公司电力科学研究院工程师，主要研究方向为网络安全、电力信息安全。

张凌浩（1985-），男，山东文登人，博士，国网四川省电力公司电力科学研究院工程师，主要研究方向为网络安全、大数据技术等。