doi:10.11959/j.issn.1000-436x.2015291

针对密码芯片频域互信息能量分析攻击

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

摘 要：在对密码芯片进行时域上互信息能量分析基础上，提出频域上最大互信息系数能量分析攻击的方法。该方法结合了密码芯片在频域上信息泄露的原理和互信息能量分析攻击的原理，引入了最大互信息系数的概念，避免了在时域上进行曲线精确对齐的操作，并针对国产密码算法 SMS4 进行了攻击测试。实验表明，频域上最大互信息系数攻击的有效性扩展了侧信道能量分析攻击的方法。
关键词：侧信道攻击；互信息量；频域；最大互信息系数
中图分类号：TP309.1 **文献标识码**：A

Mutual information power analysis attack in the frequency domain of the crypto chip

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

Abstract: Based on the mutual information power analysis attack in time domain of the crypto chip, a method for analyzing the energy of the maximum mutual information coefficient in the frequency domain was proposed. This method combined the principle of password chip information leakage in frequency domain and the principle of mutual information power analysis. The concept of maximum mutual information coefficient was introduced, which avoided the operation of accurate alignment in time domain. Experiments on the algorithm of SMS4 show that the effectiveness of the maximum mutual information coefficient attack in the frequency domain is extended to the method of the side channel energy analysis.
Key words: side-channel attack; mutual information; frequency domain; maximum mutual information coefficient

1 引言

侧信道分析攻击技术的发展已经对传统密码芯片的安全性提出了严峻的挑战，并对一些重点研究领域提出了新的要求。尤其是新型攻击方法的提出，使密码芯片的安全问题更加突出。针对密码芯片能量攻击，目前最主要的方法有差分能量分析攻击[1]、相关性分析攻击[2]、模板攻击[3]等。针对密码芯片的互信息攻击是密码芯片能量分析攻击的一种，互信息攻击是利用信息论的基本知识，同时结合密码芯片在运行密码算法时泄露的数据相关性和操作相关性进行攻击的。Gierlichs 等[4]2008 年在密码硬件与嵌入式系统国际会议上首先提出，利用平均互信息得到处理数据与泄露中间值之间以及泄露中间值与测量值之间的相互依赖关系的程度，文献[5,6]主要是对如何利用有效的方法进行计算平均互信息，文

收稿日期：2015-11-09
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 (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(13Z A0091); The Scientific Research Foundation of CUIT (CRF201301)

献[6]对互信息攻击、差分能量分析攻击和相关系数攻击 3 种攻击方法进行了分析总结。以上的这些互信息攻击都是针对时域信号进行分析，其前提是多条样本在同一时刻必须对齐，否则会出现攻击失败的结果。这一现象是在时域上进行能量分析攻击的一个缺点，针对这个缺点，在文献[7]提出，密码芯片在运行时泄露的信息在时域上的变化差异在频域上依然会体现出来，并证明了针对密码芯片频域上攻击的有效性，用实验证明了这一特性。本文根据这一特性并结合互信息能量分析攻击的理论，提出了针对密码芯片在频域上的互信息攻击的方法，即频域上互信息系数攻击。首先采集密码芯片的时域能量迹，通过快速傅里叶变换，将能量迹信号从时域变换到频域，然后在频域上利用互信息系数进行攻击，从而破解密钥。实验证明，本文提出的在频域上进行互信息攻击的方法正确、有效，扩展了针对密码芯片侧信道能量分析攻击的方法。

2 互信息分析能量分析攻击原理

2.1 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 $X=(X_1,X_2,\cdots,X_n)$、$Y=(Y_1,Y_2,\cdots,Y_n)$ 为 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。

$$H(X|Y)=-\sum_{y\in Y}p(y)\log p(y)\sum_{x\in X}p(x|y)\log p(x|y) \quad (1)$$

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

$$I(X;Y)=H(X)-H(X|Y) \quad (2)$$

2.2 互信息能量分析攻击模型

假设 K、X、Z 均是随机变量集合，K 代表密钥的集合，k^* 代表正确的密钥，X 代表目标密码算法的输入的明文，Z 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，一般认为，攻击成功时

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

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[2]在 2004 年提出了相关系数分析，Gierliehs 等[4]在 CHES 2008 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。定义互信息

$$I(l,M(x,k))=H(I)-H(I|M(x,k)) \quad (3)$$

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 $H(I|M(x,k))$ 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。

3 频域上最大互信息系数能量分析攻击

功耗信号时域上的总能量等于频域上的总能量，即如果信号经过傅立叶变换后，其总能量保持不变。采集的能量迹为离散的有限时间序列，因此可以使用离散傅里叶变换进行分析[8]。本文将频域分析和互信息系数(MIC, mutual information coefficient)分析相结合，创新地提出了频域上互信息系数分析的方法。Yanis Linge 等[8]提出了互信息系数的方法，利用有效的方法计算 2 个随机变量 A、B 之间的依赖程度。定义如下

$$\mathrm{MIC}(A,B)_{p,q}=\frac{I(A,B)_{p,q}}{\mathrm{lb}(\min_{p,q})} \quad (4)$$

其中，$\forall_{p,q}\leqslant n^{0.6}$，$n$ 代表随机变量 A、B 中元素的总个数，p 代表将随机变量 A 划分为 p 个不相交的区间，q 代表将随机变量 B 划分为 q 个不相交的区间。将此应用到能量分析攻击中有

$$\max_{k\in K}(|\mathrm{MIC}(M(x,k),l)|)=k^* \quad (5)$$

其中，l 是时域信号经过傅里叶变换后对应的频点幅度。由于 $M(x,k)$计算得出的中间值是离散的，为了计算方便，可以将 p 固定，例如，对于 SMS4 算法而言，可以将 $M(x,k)$当作 SBOX 输入或者输出的汉明重量，此时 p=9；对于 DES 而言，p=5，而对

q 进行不同的划分，其取值范围为 $[1, n^{0.6}]$。每次猜测不同的密钥，得出的互信息系数是不同的，找出互信息系数最大时对应的猜测密钥，此时的猜测密钥为正确的密钥。

4　针对 SMS4 算法频域上互信息能量分析攻击

4.1　SMS4 算法

SMS4 算法是我国自主研发的分组密码算法，分组长度为 128 bit，密钥长度为 128 bit，加密算法与密钥扩展算法都采用 32 轮非线性迭代结构。加密算法与解密算法的结构相同，只是轮密钥的使用顺序相反。SMS4 加密流程如图 1 所示。

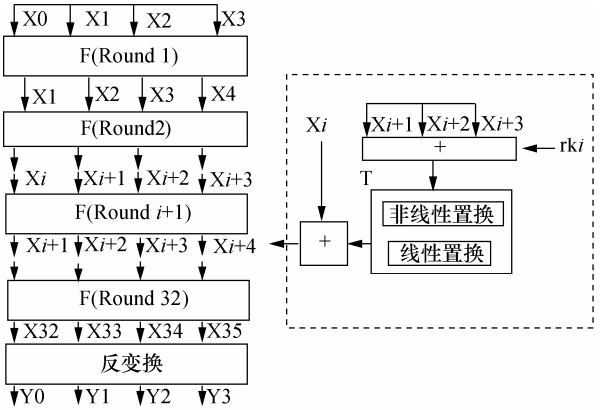

图 1　SMS4 加密算法

4.2　实验设置

令 SMS4 加密密钥

$k = 0x0123456789ABCD\ EFFEDCBA9876543210$

随机产生 10 000 组明文，在 FPGA 上对 SMS4 密码算法进行加密运算，并利用数字存储示波器采集加密运算中所产生的能量迹，如图 2 所示，选择 SMS4 前 4 轮每轮的 SBOX 输出作为攻击点[9]。

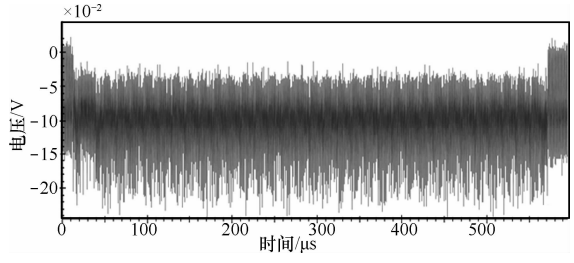

图 2　SMS4 原始能量迹

4.3　数据预处理

数字存储示波器采集到的能量曲线，前 4 轮每条样本为 20×10^3 个点，经过主成分分析提取贡献率在 80%以上的主成分[10]，每条样本为 200 个点，如图 3 所示，然后利用傅里叶变换将其变换到频域上进行分析，如图 4 所示。

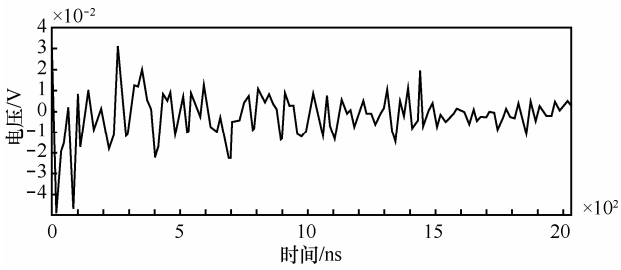

图 3　主成分分析提取后的能量迹

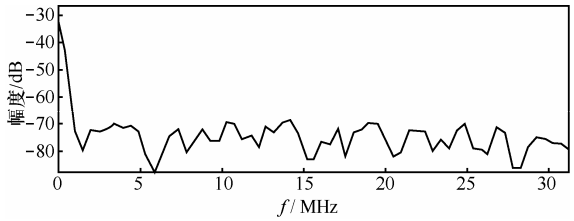

图 4　傅里叶变换后能量迹

4.4　实验结果分析

利用最大互信息系数对傅里叶变换后的数据进行互信息能量分析攻击。首先针对第一轮子密钥进行攻击，攻击结果如表 1 所示，根据攻击结果每字节得到的最大互信息系数，可以得到对应的第一轮猜测密钥是 rk0=0xF12186F9。然后运用同样的方法，对第 2 轮、第 3 轮、第 4 轮子密钥进行攻击，攻击结果如表 2~表 4 所示，得出对应的猜测密钥分别是 $rk1 = 0x41662B61$，$rk2 = 0x5A6AB19A$，$rk3 = 0x7BA92077$。

表 1　　第 1 轮结果

轮密钥字节	候选	频域最大互信息系数	猜测密钥
1	1	0.043 571 472 0	241(0xF1)
	2	0.007 938 385 0	31(0x1f)
	3	0.007 115 841 0	102(0x66)
	4	0.006 329 059 6	28(0x1c)
2	1	0.036 564 110 00	33(0x21)
	2	0.006 736 755 4	228(0xe4)
	3	0.005 486 011 5	83(0x53)
	4	0.005 437 374 0	229(0xe5)
3	1	0.044 842 243 0	134(0x86)
	2	0.008 697 510 0	67(0x43)
	3	0.007 817 268 0	36(0x24)
	4	0.007 753 372 0	182(0xb6)
4	1	0.034 046 173 0	249(0xf9)
	2	0.008 589 506 0	60(0x3c)
	3	0.006 022 691 7	78(0x4e)
	4	0.006 016 969 7	224(0xe0)

表 2　　第 2 轮结果

轮密钥字节	候选	频域最大互信息系数	猜测密钥
1	1	0.033 164 740 0	65(0x41)
	2	0.006 588 220 6	212(0xd4)
	3	0.005 852 937 7	125(0x7d)
	4	0.004 956 245 4	33(0x21)
2	1	0.048 377 990 0	102(0x66)
	2	0.006 922 722 0	55(0x37)
	3	0.006 760 597 0	79(0x4f)
	4	0.006 491 184 2	155(0x9b)
3	1	0.033 032 417 0	43(0x2b)
	2	0.005 889 415 7	185(0xb9)
	3	0.005 424 499 5	242(0xf2)
	4	0.005 342 483 5	85(0x55)
4	1	0.035 979 510 0	97(0x61)
	2	0.007 492 542 3	72(0x48)
	3	0.006 677 389 0	156(0x9c)
	4	0.006 122 350 7	140(0x8c)

表 3　　第 3 轮结果

轮密钥字节	候选	频域最大互信息系数	猜测密钥
1	1	0.042 356 968	165(0x5A)
	2	0.006 289 959	206(0xce)
	3	0.006 042 480 5	180(0xb4)
	4	0.005 656 719	130(0x82)
2	1	0.103 671 31	106(0x6a)
	2	0.070 810 32	47(0x2f)
	3	0.070 729 02	205(0xcd)
	4	0.070 331 57	175(0xaf)
3	1	0.092 463 255	177(0xb1)
	2	0.010 447 979	116(0x74)
	3	0.009 287 119	35(0x23)
	4	0.009 178 4	159(0x9f)
4	1	0.034 647 465	154(0x9a)
	2	0.008 566 856	95(0x5f)
	3	0.006 348 61	239(0xef)
	4	0.005 563 259	48(0x30)

表 4　　第 4 轮结果

轮密钥字节	候选	相关系数	猜测密钥
1	1	0.044 526 577	123(0x7b)
	2	0.007 409 572 6	149(0x95)
	3	0.006 247 520 4	236(0xec)
	4	0.005 962 372	190(0xbe)
2	1	0.043 119 907	169(0xa9)
	2	0.006 299 019	14(0xe)
	3	0.006 114 959 7	153(0x99)
	4	0.005 852 222 4	135(0x87)
3	1	0.029 844 284 0	32(0x20)
	2	0.006 619 453 4	229(0xe5)
	3	0.006 265 640 3	228(0xe4)
	4	0.005 478 859 0	9(0x09)
4	1	0.037 795 544 0	119(0x77)
	2	0.006 820 678 7	178(0xb2)
	3	0.006 348 610 0	123(0x7b)
	4	0.006 346 225 7	192(0xc0)

根据 rk0、rk1、rk2、rk3 可以利用 SMS4 密钥扩展反推出 SMS4 原始的加密密钥，可得到最终原始加密密钥为

$$k = 0\text{x}0123456789\text{ABCDEFFEDCBA}9876543210$$

5　结束语

本文以国产密码算法 SMS4 为实验对象，以 S 盒输出为攻击点进行频域上的互信息能量分析攻击，可以恢复出前 4 轮或者末 4 轮的轮密钥，根据密钥扩展算法，从而推算出 128 bit 的加密密钥攻击结果正确，并证明了该攻击方法的有效可行性。

参考文献：

[1] KOCHER P, JAFFE J, JUN B. Differential power analysis[A]. Crypto 1999[C]. Santa-Barbara, CA, USA, 1999. 398-412.

[2] BRIER E, CLAVIER C, OLIVIER F. Correlation power analysis with a leakage model[A]. Cryptographic Hardware Embedded System-CHES 2004 Lec-ture Notes in Computer Science[C]. 2004. 16-29.

[3] CHARI S, RAO J, ROHATGI P. Template attacks. cryptographic hard-ware and embedded systems-ches[A]. The 4th International Workshop, Redwood Shores[C]. 2002.

[4] GIERLICHS B, BATINA L, TUYLS P, *et al*. Mutual information analysis[A]. CHES 2008[C]. Washington DC, USA, 2008.

[5] VEYRAT-CHARVILLON N, STANDAERT F X. Mutual information analysis: how,when and why[A]. Cryptographic Hardware and Embedded Sys-tems - CHES 2009[C]. Lecture Notes in Computer Science. Springer, 2009.

[6] GIERLICHS B, BATINA L, TUYLS P. Mutual information analysis a universal differential side-channel attack[J]. Journal of Cryptology, 2010, 24(2):269-291.

[7] MATEOS E, GEBOTYS C H. A new correlation frequency analysis of the side channel[A]. Proceedings of the 5th Workshop on Embedded Systems Se-curity[C]. ACM, 2010.

[8] LINGE Y, DUMAS C. LAMBERT-LACROIX S. Maximal Information Coefficient Analysis[R]. Cryptology ePrint Archive:Report 2014/012,2014.

[9] 沈薇. SM4 算法的能量攻击及其防御研究[D]. 西安:西安电子科技大学,2009.
SHEN W. Research of Power Attack and Defense on SM4 Algorithm[D]. Xi'an: Xidian University,2009.

[10] BATINA L, HOGENBOOM J, *et al*. Getting more from PCA: first results of using principal component analysis for extensive power analysis[A]. Topics in Cryptology–CT-RSA 2012[C]. Springer Berlin Hei-delberg, 2012. 383-397.

作者简介：

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。

吴震[通信作者]（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。E-mail: wzhen@cuit.edu.cn。

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。