doi:10.11959/j.issn.1000-436x.2015066

基于差异度的密码芯片旁路攻击研究

张阳，陈开颜，李雄伟，陈军广，李艳
（军械工程学院 信息工程系，河北 石家庄 050003）

摘 要：针对旁路攻击方法存在的样本量大、分析时间长等问题，结合微控制器的系统结构，分析了旁路泄漏信号的噪声来源及其差分抑制方法；定义了信号差异度和汉明重量差异度，分析了二者间的反比映射关系；利用加密过程中差异度的变化特征，提出了基于差异度的密钥分析方法；以 DES 密码算法为验证目标，仅用 150 组功耗轨迹，分析用时 1.03 s 破解了密钥，可推广应用于以通用微控制器作为实现载体的其他分组密码系统。
关键词：密码芯片；旁路攻击；噪声分析；差异度；密钥分析
中图分类号：TN918 **文献标识码**：A

Side channel attack of cipher chips based on difference variability

ZHANG Yang, CHEN Kai-yan, LI Xiong-wei, CHEN Jun-guang, LI Yan
（Department of Information Engineering, Ordnance Engineering College, Shijiazhuang 050003, China）

Abstract: Side channel attack (SCA) has the problems of high sample quantity and long analysis time. Noise of side channel leakage and its differential reduction method are researched combined with the architecture of micro control unit (MCU). Signal difference variability and hamming weight difference variability are defined, whose inverse proportion is checked. Method of key analysis based on difference variability is proposed, which uses its change property in encrypt process. Data encryption standard (DES) is cracked in experiment, which only needs 150 power tracks and 1.03 s analysis time. The attack method can be extended to crack other block ciphers which implemented in general purpose MCU.
Key words: cipher chip; side channel attack; noise analysis; difference variability; key analysis

1 引言

随着信息时代的到来，密码芯片在信息的存储、处理和传输等环节的安全防护中发挥了至关重要的作用。旁路攻击由 Kocher[1]于 1996 年提出，利用密码芯片运行过程中泄漏的物理信号（如功耗[2]、电磁[3]、时间[1]等）破解密钥，呈现出强大的攻击能力[4]。为了提高攻击效率，研究人员提出了差分能量分析(DPA, differential power analysis)[5]、相关性能量分析(CPA, correlation power analysis)[6]、模板分析(template analysis)[7]、互信息分析(MIA, mutual information analysis)[8]等分析方法，主要聚焦于如何提取和利用旁路信号中密钥运算相关的信息。然而这些方法共同存在的问题在于对旁路信号的刻画不够细致，对旁路信号中包含的大量噪声处理不足，只能通过增大样本量以及复杂的模式识别方法来弥补缺陷。由此带来的问题是需要采集的样本数量高达几千乃至上万条，密钥分析的时间长达数小时[9]。

针对上述问题，本文从旁路信号分析的角度入手，提出改进方案，主要工作如下。

1) 以通用微控制器作为加密系统的实现载体，对其旁路信号进行了重新描述。结合微控制器系统结构分析了旁路信号的主要噪声来源及其统计分布特征，在此基础上采用差分方法进行降噪，对差分结果的电子噪声分布特征进行了分析。

收稿日期：2013-11-10；修回日期：2014-01-03
基金项目：国家自然科学基金资助项目(61271152, 51377170); 河北省自然科学基金资助项目(F2012506008)
Foundation Items: The National Natural Science Foundation of China(61271152,51377170); The National Natural Science Foundation of Hebei Province (F2012506008)

2) 定义了信号差异度和汉明重量差异度，结合总线操作特点分析了二者之间的反比映射关系。实验结果表明该映射具有较好的稳定性。

3) 提出了基于汉明重量差异度的密钥分析方法，充分利用了加密过程中差异度的变化特征，给出了基于差异度的分析实现步骤。以 DES 密码算法为分析和验证目标，仅用 150 组功耗轨迹，分析用时 1.03 s 破解了密钥，证明了该方法的有效性，大大降低了攻击所需的样本量和分析时间。

2　旁路信号分析与噪声抑制

旁路信号的采集是旁路分析的前提，旁路信号中既包含了用于密钥分析的有效信号，同时包含了大量的噪声信号。旁路信号的能否有效分析和处理将极大影响后续分析过程的效率。

理想状态下，敌手希望能够获取只与加密过程中间数据直接相关的能量泄漏，而实际获取的旁路信号中还包含以下几种。

1) 电子噪声(P_{en})：主要包括电源噪声、时钟噪声、示波器的量化噪声、测量电阻的热噪声等，这些噪声只能通过技术手段尽可能抑制，无法完全消除。同时电子噪声服从正态分布 $P_{en}\sim N(0,\sigma^2)$[10]；

2) 逻辑噪声(P_{ln})：微控制器的动态功耗主要由组合逻辑和时序部件的动态功耗组成[10]。其中组合逻辑功耗主要包括运算器、控制器等部件运算时所用的功耗；时序部件功耗主要包括寄存器、总线等进行数据读写操作时所发生的数据位翻转所用的功耗。对旁路攻击而言，有效信号为加密过程的中间数据翻转所对应的功耗信号(P_e)，除此之外所有其他部件的功耗信号均视为逻辑噪声(P_{ln})。由微控制器的基本组成结构可知，P_{ln} 是 P_e 的伴生信号，其信号强度要远大于 P_e。因此，P_{ln} 是对旁路分析影响最大的部分。

3) 恒定分量(P_{const})：主要指微控制器的静态功耗，用于保持电路工作的基本状态。

因此，可以用式(1)表示微控制器功耗旁路信号的组成。

$$P_t=P_e+P_{en}+P_{ln}+P_{const} \tag{1}$$

其中，P_t 表示某时刻的总功耗。由式(1)，旁路分析希望从 P_t 中提取出 P_e，需要尽可能排除其他部分的干扰。传统旁路分析方法通过加大样本量，同时采用复杂的统计分析方法降低其他噪声的干扰，必然造成样本量与分析时间的增加。

考虑微控制器上实现的密码算法，当 2 个不同明文在相同旁路攻击点上采集得到旁路信号 P_{t1}，P_{t2}，由于此时 2 次加密对应相同的运算指令，调用的功能部件均相同，部件中加载的指令、地址等数据也相同，仅参与操作的加密中间数据不同。因此当前条件下 2 次加密对应的 P_{ln}、P_{const} 分量相等，旁路信号差分后得到

$$DP=P_{t1}-P_{t2}=(P_{e1}-P_{e2})+(P_{en1}-P_{en2}) \tag{2}$$

其中，DP 为 2 个不同明文旁路功耗点上的中间数据翻转差异所对应的能量消耗，此时逻辑噪声 P_{ln} 与恒定噪声 P_{const} 已经被差分运算消除。

由于 $P_{en}\sim N(0,\sigma^2)$，用 P_{den} 表示式（2）中的 $P_{en1}-P_{en2}$，则其服从正态分布 $N(0,\sigma_1^2+\sigma_2^2)$。为了使 P_{den} 更趋近期望值μ=0，可以通过物理降噪，同时采用取样本均值的方法降噪。

3　基于差异度的旁路分析

旁路分析过程一般分为以下 3 个步骤。

1) 采集加密算法运行过程中的旁路信号，即实验中通过采样得到的旁路泄漏轨迹；

2) 建立密码芯片运行过程中的旁路泄漏模型，根据泄漏模型猜测不同密钥进行加密运算所对应的理论旁路泄漏值；

3) 通过统计分析方法判断在旁路泄漏模型下猜测的泄漏值与实际旁路泄漏轨迹的相关性，进而获取密钥。

本节对旁路泄漏轨迹的差异进行刻画并建立模型，在模型指导下进行旁路密码分析。

3.1　建立差异度模型

由前文分析可知，实际旁路信号包含了大量噪声信号，难以直接提取加密过程的中间数据，因此需大量样本分析才能获取密钥。根据式(2)可知，通过对 2 个不同明文相同旁路攻击点上旁路泄漏轨迹作差，可消除逻辑噪声与恒定噪声，下面探讨利用该差异进行旁路密码分析的方法。

旁路泄漏模型通常为汉明重量模型和汉明重量模型[11]。微控制器中所有操作数据必须通过总线传输，同时由于总线挂载设备多，驱动能力强，其引起的功耗变化最为明显，因此总线是微控制器中数据翻转能量体现的最集中部件。则对总线操作特征进行细致分析，能够获得较为理想的数据翻转相关信息。对于使用预充电总线的微控制器而言，部件在占据总线时先将总线数据预置为高，然后翻转

为所需传输的数据，即总线上的数据翻转为从固定值（全部为 1）跳变为目标数据。因此微控制器的数据依赖性表现为：数据翻转的能量消耗反比于该数据的汉明重量[10]，可用式(3)表示。其中，$HW(x)$为总线数据 x 的汉明重量，α为反比能量映射因子。

$$P_e=\alpha HW(x) \tag{3}$$

因此可用汉明重量模型来分析微控制器中总线上的数据变化所对应的功耗变化。为进一步刻画旁路信号的差异，给出信号差异度的定义。

定义 1 信号差异度是不同明文在相同加密过程同一时间点上的旁路信号差异，即前文 *DP*。因此信号差异度体现了该时间点上数据翻转差异对应的能量差异，可将式(2)改写为

$$DP=(P_{e1}-P_{e2})+P_{den}=\alpha(HW(x_1)-HW(x_2))+P_{den} \tag{4}$$

其中，x_1, x_2 为当前总线上传输的数据。由式(4)可将差异度的定义扩展到汉明重量，对汉明重量差异度进行定义。

定义 2 汉明重量差异度是 2 个数据的汉明重量之差，如式(5)所示。

$$D(x_1, x_2)=HW(x_1)-HW(x_2) \tag{5}$$

结合式(4)、式(5)可知，信号差异度是汉明重量差异度在旁路信号差异上的映射，实验中对应为 2 条旁路泄漏轨迹功耗点之间的差分。因此通过对旁路泄漏轨迹进行差分，并对 P_{den} 进行降噪处理，可以得到较为理想的信号差异度能量值，进而可以映射得到对应的汉明重量差异度。同时由于α为反比因子，因此信号差异度反比于对应的汉明重量差异度。需要注意的是汉明重量差异度与汉明重量并不相同。例如令 x_1=0xF0，x_2=0x0F，则汉明重量为 8，而汉明重量差异度为 0。

3.2 基于汉明重量差异度的密钥分析方法

下面以 DES 为例，阐述基于汉明重量差异度的密钥分析方法。DES 是迄今为止最具代表性的分组密码算法[12]，针对其进行的攻击方法研究，能够进一步推广应用于其他分组密码算法。

图 1 中给出了旁路功耗点的选取位置。图中左右两侧分别代表 DES 加密系统对不同明文进行的第一轮加密操作。图中仅给出了f函数的异或操作(XOR)和 S 盒操作 2 个步骤。2 次加密使用了相同的密钥 K。E_1、E_2 为参与运算的 2 个明文经过初始置换 IP 和扩展置换 E 得到的结果，则 E_1、E_2 可计算得出。选取图中 S 盒替换前后位置作为旁路功耗点，采集对应的功耗轨迹。旁路功耗点处能够体现出密钥K参与运算后给信号差异度带来的非线性变化，将其映射为汉明重量差异度，进而分析哪些密钥值能够满足汉明重量差异度的要求，从而快速破解密钥。

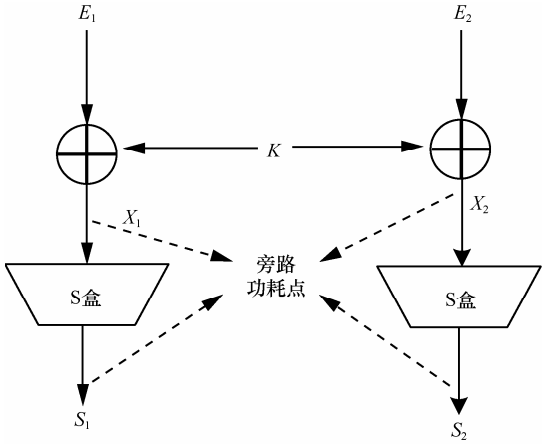


图 1 旁路功耗点选取

用 $S(x)$代表输入为 x 的 S 盒操作，则 $S_1=S(X_1)$, $S_2=S(X_2)$。由图 1 可得 $X_1=E_1\oplus K$，$X_2=E_2\oplus K$。K 为 6 bit 密钥，因此共 64 种猜测。

则

$$D(X_1,X_2)=HW(E_1\oplus K)-HW(E_2\oplus K) \tag{6}$$

$$D(S_1,S_2)=HW(S(X_1)-HW(S(X_2)) \tag{7}$$

两式中明文与密钥的 XOR 和 S 盒操作都会使汉明重量差异度发生变化，分别分析如下。

式(6)中，假设 E_1=0x38，E_2=0x07，当 $D(X_1,X_2)$=6 时，将 K={0,1,…,63}分别代入式(6)，满足条件的仅有 K=0x07。因此在确定差异度的前提下，只有部分密钥 K 能够满足要求，从而大大减小 K 的猜测空间。

式(7)中，由于 S 盒的不均匀分布特性，经过 S 盒操作得到结果 S_1、S_2 的汉明重量差异度同样会产生变化，可以进一步减小 K 的猜测空间。

2 个条件联立可以将 K 值的猜测空间限定于较小范围内，甚至可以得到唯一的密钥值。

基于差异度的旁路分析方法如图 2 所示，主要包括 3 个步骤。

步骤 1)中不是采用传统旁路攻击的随机明文，而是采用选择明文，是根据 E 的变化需要反向推导获得的明文。每个明文的加密过程中，如果 S 盒对应的明文相同，则差异度始终为 0，无法体现出变化特征，则无法减小 K 的猜测空间。为了提高攻击

效率，通过选择明文方法使每个 S 盒所对应的明文均发生变化。其中 m 组明文用于求取两两之间的信号差异度，一般取值为 3。每组采集 n 遍用于抑制电子噪声。

基于差异度的密钥分析

1）选择m组明文进行加密，每组采集n遍

2）获得各组轨迹均值两两之间的信号差异度

$Diff$=mean(P_i)−mean(P_j)

将信号差异度映射为汉明重量差异度D_f,D_b

3）for:i=0…63

$X_i=E_i \oplus i$, $X_j=E_j \oplus i$;

$S_i=S(X_i)$,$S_j=S(X_j)$;

if(D_f==$D(X_i,X_j)$且D_b==$D(S_i,S_j)$) 保留i

else丢弃i

图 2　基于差异度的密钥分析过程

步骤 2)中求得各组旁路泄漏轨迹两两之间的信号差异度，并进行信号差异度向汉明重量差异度的映射。映射的方法为：首先通过相同芯片的已知加密过程对信号差异度进行样本统计，建立每个差异度所对应的能量值，再用置信度方法将差分后的功耗值与统计值进行比较，从而得到其汉明重量差异度值。

步骤 3)用于得到满足当前 S 盒差异度变化特征的密钥值，经过该步骤能够将密钥空间压缩于很小范围内。

4　实验验证

实验平台配置如图 3 所示，在 AT89S52 单片机上实现 DES 程序，采用直流稳压电源 DH1719A 为密码系统提供稳定供电，采用 Tektronix DPO4032 示波器（带宽 350 MHz，被动探头 P6139A）采集旁路泄漏轨迹并通过 USB 数据线传输至 PC 机（I3-2310，320 GB HDD，2 GB DDR3 RAM）。由 PC 机上 LabVIEW 编写的虚拟仪器控制平台控制采集过程，并通过 RS232 将选择的明文发送给密码系统。

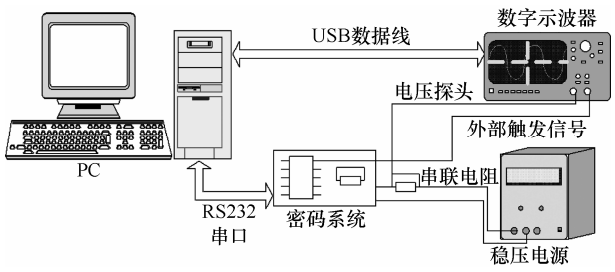


图 3　实验平台配置

4.1　差异度提取实验

采样 4 组明文的加密过程中旁路功耗点处的泄漏轨迹，明文分别为：0xFFFFFFFFFFFFFFFF、0x0000000000000000 、 0x1100000000000000 、0x1122334455667788，每组采样 50 个样本，每个样本采样 10 000 点，分别编号为 1、2、3、4 组。将各组轨迹平均化，并两两差分。整体差异结果及 S 盒之前的信号差异度（即前文中 X_1,X_2 处差异度）局部放大如图 4 所示，其中放大区间为 137~140 点。

S 盒对应的密钥为已知值 0xF0，由此可以计算得出各组两两之间的差异度如表 1 所示。将该表与差异度功耗局部放大图进行比较可以发现，汉明重量差异度与其信号差异度之间呈现出反比关系，与分析一致。同时，当汉明重量差异度值相等时，其所对应的信号差异度轨迹几乎重合，证明实验具有较好的稳定性。对 S 盒运算之后的结果进行分析，同样可以得到相同结论，证明了差异度模型对实际能量轨迹刻画和分析的准确性。

表 1　4 组明文两两之间的汉明重量差异度

差异组	差异度值
$D(X_1,X_2)$	−2
$D(X_1,X_3)$	−2
$D(X_1,X_4)$	−1
$D(X_2,X_3)$	0
$D(X_2,X_4)$	1
$D(X_3,X_4)$	1

4.2　通过选择明文的密钥破解

分析 DES 的加密过程可知，当明文由全 0 变为全 1 时，第一轮 f 函数中每个分组对应的 E 值由 0x00 变化至 0x3F。为了获得差异度变化同时减少分析所需的明文个数，选择明文时每一个使用二者之间的某一数据，组合并进行反向推导从而得到需要的明文。令 8 个 S 盒所对应 E 值均为 0x0C，反向推导可得对应的明文为 0x00FFFF0000FFFF00。

表 2 中给出了采用 3 组明文获得第一轮第一个 S 盒对应的密钥空间分析过程，其中汉明重量差异度值通过 4.1 节实验方法获得，E 值由明文经过推导获得。将 E、$D(X_1,X_2)$、$D(S_1,S_2)$值分别代入式(6)和式(7)，可以求得满足该条件的可能密钥 K 值。如表 2 所示，密钥空间中为满足条件的猜测密钥值，

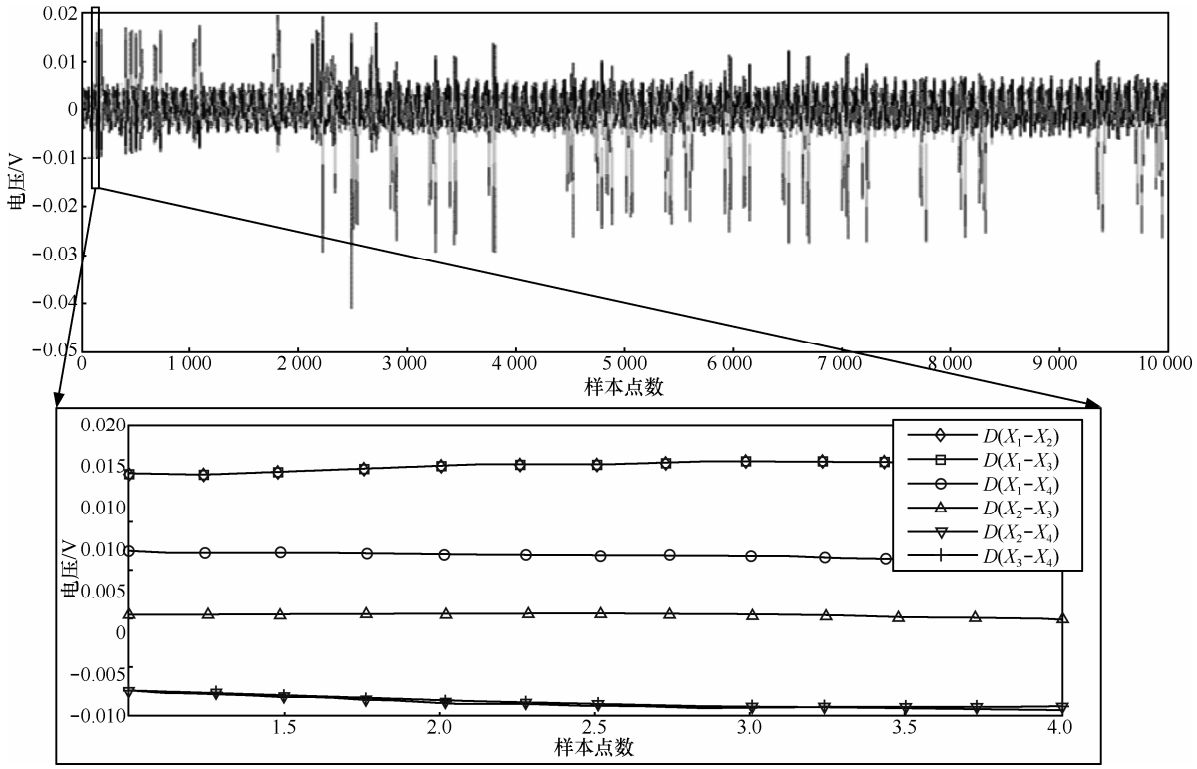


图 4 不同明文旁路泄漏轨迹差分结果及其局部放大

表 2 第一轮第一个 S 盒对应的密钥分析

组别	明文	E	$D(X_1,X_2)$	$D(S_1,S_2)$	密钥空间(0x)
1	0x0000000000000000	00	−2	1	05，12，18，21，24
	0xFFFFFFFFFFFFFFFF	3F			
2	0x0000000000000000	00	0	0	05，07，09，0B，…18，…24…
	0x00FFFF0000FFFF00	0C			
3	0x00FFFF0000FFFF00	0C	−2	1	05，18，24
	0xFFFFFFFFFFFFFFFF	3F			

均为 16 进制表示，粗体为空间重叠部分。因此通过该方法将密钥猜测范围从 64 种压缩到了 3 种。

采用类似方法计算其他 S 盒的对应密钥值，分别得到各自对应的压缩空间如表 3 所示。

表 3 第一轮各 S 盒对应密钥空间

对应 S 盒	密钥空间
1	05,18,24
2	13
3	04,08
4	08
5	05,09
6	32
7	27,2B
8	02,10

对各个 S 盒对应密钥值进行组合只能得到第一轮对应的 48 位密钥，剩余的 8 位密钥需要通过搜索 256 种可能情况来确定。将每一种可能组合值依次代入密钥反向推导过程，得到密钥后用该密钥加密明文，将其与正确加密结果比较，相同则破解成功，否则尝试下一种组合。因此当前情况下总猜测空间为 12 288=3×1×2×1×2×1×2×2×2^8，远小于 2^{56} 的密钥空间，同时不需要进行大样本量的数据采集，降低了分析时间。根据差异度分析得到的压缩密钥空间，编程进行密钥恢复，经过 1.03 s 获得了该加密密钥为 0x1122334455667788，成功破解了加密系统。

本攻击方案仅用 150 组功耗轨迹，成功完成了攻击，远小于传统旁路攻击所需的样本数量[7,9,13]。同时如果进一步改善原始信号质量，降低电子噪声的干扰，可以将所需轨迹数量降至更低。

5　结束语

本文针对传统旁路攻击方法存在的旁路泄漏轨迹采集样本量大，分析时间长等问题，提出了一种基于差异度的旁路分析方法，更为准确地刻画旁路信号与内部运算之间联系，大大降低了攻击所需的样本量和分析时间。以 AT89S52 上实现的 DES 密码算法为分析和验证目标，仅用 150 组功耗轨迹，分析用时 1.03 s 破解了密钥，获得了良好的攻击效果。

DES 加密算法是最具代表性的分组密码算法，其他分组密码算法也采用了类似的多轮加密和多个 S 盒变换等结构。本文攻击方法针对分组密码算法的特定轮展开攻击，将该轮每一个 S 盒对应的密钥空间逐个进行压缩。因此采用本文方法对 AES、3DES 等其他分组密码算法进行攻击时，只需根据其轮变换特点进行相应调整和分析，从而获取差异度并破解该分组密码算法。例如对 128 位密钥的 AES 加密算法进行攻击时，将攻击点置于第一轮加密的轮密钥加和字节替换前后，分析旁路波形数据获得差异度，从而快速得到该轮 16 个 S 盒各自所对应的压缩密钥空间，进行组合验证并反向推导后即可得到初始密钥。因此本文攻击方法能够较好的推广应用于其他分组加密算法。

本文攻击的目标芯片为 AT89S52，主要利用其总线信号变化特征展开攻击，因此该方法对于采用总线结构的微控制器具有一定的适用性，在 AT89C51 芯片上同样验证了本方法的有效性。攻击效果的主要影响因素包括芯片实现的工艺水平、采样设备的精度等。为了提高本方法的适用性，实现相同型号芯片之间的模版构建与差异度识别，下一阶段研究主要从 2 个方面展开：一是提高旁路信号质量，研究并设计专用硬件模块，对原始信号进行放大、滤波等处理，获得高质量旁路信号，从而有效提高差异度识别率；二是研究差异度分析的模式识别方法，包括基于相同型号不同芯片的模版特征选取和构建方法，以及不同芯片之间的差异度模式匹配方法。

参考文献：

[1] KOCHER P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[A]. N Koblitz, editor, CRYPTO[C]. 1996.104-113.

[2] MANGARD S, OSWALD E, POPP T. Power Analysis Attacks: Revealing the Secrets of Smart Cards[M]. Advances in Information Security. Springer, 2007.

[3] MEYNARD O, GUILLEY S, DANGER J L, *et al*. Far correlation-based EMA with a precharacterized leakage model[A]. Design, Automation & Test in Europe Conference & Exhibition (DATE) [C]. 2010. 977-980.

[4] EISENBARTH T, KASPER T, MORADI A. *et al*. On the power of power analysis in the real world: a complete break of the keeloq code hopping scheme[A]. CRYPTO 2008[C]. 2008. 203-220.

[5] KOCHER P C, JAFFE J, JUN B. Differential power analysis[A]. CRYPTO 1999[C]. 1999.388-397.

[6] BRIER E, CLAVIER C, OLIVIER F. Correlation power analysis with a leakage model[A]. M Joyeand J J Quisquater[C]. 2004. 16-29.

[7] 邓高明, 赵强, 张鹏等. 针对密码芯片的电磁频域模板分析攻击[J]. 计算机学报, 2009, 32(4): 602-610.
DENG G M, ZHAO Q, ZHANG P, *et al*. EM frequently domain template analysis on cipher chips[J]. Chinese Journal of Computers, 2009, 32(4): 602-610.

[8] BATINA L, GIERLICHS B, PROUFF E. *et al*. Mutual information analysis: a comprehensive study[J]. Journal of Cryptology, 2011,24(2): 269-291.

[9] DPA Contest[EB/OL]. http://www.dpacontest.org.

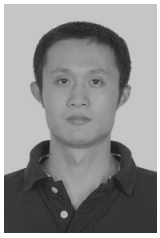
[10] HENNESSY L, PATTERSON A 著, 白跃彬译. 计算机系统结构-量化研究方法(第四版)[M]. 北京:电子工业出版社, 2007.
HENNESSY L, PATTERSON A, BAI Y B. Computer Architecture: A Quantitative Approach Fourth Edition[M]. Beijing: Publishing House of Electronics Industry, 2007.

[11] MANGARD S, OSWALD E, POPP T 著,冯登国等译. 能量分析攻击[M]. 北京:科学出版社, 2010.
MANGARD S, OSWALD E, POPP T, FENG D G. Power Analysis Attacks[M]. Beijing: Science Press, 2007.

[12] 吴文玲, 冯登国, 张文涛. 分组密码的设计与分析(第 2 版)[M]. 北京:清华大学出版社, 2009.
WU W L, FENG D G, ZHANG W T. Design and Analysis of Block Cipher[M]. Beijing: Tsinghua University Press, 2009.

[13] 张鹏, 邓高明, 陈开颜等. 针对 AES 密码芯片的远场相关性电磁分析攻击[J]. 华中科技大学学报(自然科学版), 2009, 37(8):31-34.
ZAHNG P, DENG G M, CHEN K Y, *et al*. Electromagnetic correlation analysis attacks on microcontroller implementations of AES in far field[J]. Journal of Huazhong University of Science and Technology(Natural Science Edition), 2009, 37(8):31-34.

作者简介：



张阳（1984-），男，河北南宫人，军械工程学院讲师，主要研究方向为信息安全、芯片安全。

陈开颜（1970-），女，河北秦皇岛人，军械工程学院副教授，主要研究方向为密码旁路分析、信息安全。

李雄伟（1975-），男，河北定州人，军械工程学院副教授，主要研究方向为信息安全。

陈军广（1978-），男，河北石家庄人，军械工程学院讲师，主要研究方向为计算机应用。

李艳（1981-），女，河北衡水人，军械工程学院讲师，主要研究方向为计算机应用。