侧信道分析技术概览与实例

葛景全[1,2,3]　屠晨阳[1,2]　高　能[1,2]

[1](中国科学院数据与通信保护研究教育中心　北京　100093)

[2](信息安全国家重点实验室(中国科学院信息工程研究所)　北京　100093)

[3](中国科学院大学网络空间安全学院　北京　100049)

(gejingquan@iie.ac.cn)

Technology Overview of Side Channel Analysis

Ge Jingquan[1,2,3], Tu Chenyang[1,2], and Gao Neng[1,2]

[1](*Data Assurance and Communication Security Research Center*, *Chinese Academy of Sciences*, *Beijing* 100093)

[2](*State Key Laboratory of Information Security* (*Institute of Information Engineering*, *Chinese Academy of Sciences*), *Beijing* 100093)

[3](*School of Cyber Security*, *University of Chinese Academy of Sciences*, *Beijing* 100049)

Abstract　Along with more and more different kinds of cipher devices are suffered from the physical security threat of side channel analysis, the side channel analysis has been paid more attention. Based on the difference of the side channel information used, this paper classifies and introduces the side channel analysis technology, including the power/electromagnetic(EM) analysis and timing analysis. In recent years, due to the widespread use of cache in modern CPUs, cache attacks have become a hot topic of side channel research. Since cache attacks require time data collection, we classify cache attacks as a type of timing analysis attack. At last, we introduce some important examples of side channel analysis in recent years, and analyze the attacking methods and degree of implementation difficulties.

Key words　side channel analysis; cipher device; power analysis; electromagnetic analysis; timing analysis; analysis example

摘　要　随着越来越多不同种类的密码设备受到侧信道分析的物理安全威胁,侧信道分析技术逐步受到人们的关注和重视.依据所利用侧信息的差异,对现有经典侧信道分析技术进行分类介绍,并重点介绍能量/电磁辐射分析和计时分析.近年来,由于现代 CPU 中 cache 的大量应用,针对 cache 的攻击越来越成为研究的热点.由于此类攻击需要采集时间数据,因此把 cache 攻击归为计时攻击的一类.最后,对近年来出现的一些重要的侧信道分析实例进行介绍,并对其攻击方法、实施难度等进行分析.

关键词　侧信道分析;密码设备;能量分析;电磁分析;计时分析;分析实例

中图法分类号　TP309.1

收稿日期:2018-11-15

通信作者:屠晨阳(tuchenyang@iie.ac.cn)

密码算法的安全性一直是密码学领域研究的核心问题，目前密码算法的安全性主要包括密码算法的设计安全以及密码算法的实现安全2个方面. 传统的密码系统假设密码算法中的秘密信息在一个可控、可靠的计算环境中进行处理. 因此，在过去的几十年里，密码分析人员通常只专注于对算法本身的理论缺陷进行研究. 然而，密码系统的实际运行环境却与设计时的理想环境不一致. 在实际应用中，密码算法一般通过某个物理设备所采用的软件或硬件方式进行实现，而物理设备会与其所处的环境发生物理交互. 分析人员可以主动策划并检测这种物理交互作用，以获得有助于密码分析的信息. 这种利用物理的手段分析、破译密码系统的方法被称为侧信道分析. 侧信道分析利用这样一个事实：计算过程中所获得的物理测量指标（能量消耗、计算时间、电磁辐射等）与计算设备的内部状态之间存在相关性. 比如在密码芯片进行密码运算时，通过靠近芯片耦合电容处的电磁探头，可以获得密码芯片的电磁辐射信息.

依据所利用侧信道信息的类型不同，侧信道分析可以分为多种不同的分析方法. 能量分析利用密码芯片在实际运行中产生的能量消耗信息；电磁分析采集密码芯片运行期间的电磁辐射信息；计时攻击利用密码芯片执行密码算法的运行时间信息；声音攻击收集密码芯片计算时的声波信息. 其中，能量分析是10余年来发展最快、研究最为深入的一个领域，我们将以能量分析为例，对侧信道分析的原理进行分析和阐述.

随着侧信道分析的攻击能力越来越强、实施成本越来越小，各种密码设备被侧信道分析成功攻击的事例越来越多. 我们将对近年来发表在学术会议以及黑客大会上的侧信道攻击实例进行介绍.

本文首先将介绍侧信道分析原理，对一些基本概念和方法进行简要阐述；然后依照不同类别阐述近年来的新攻击案例；最后对本文进行总结.

1 侧信道分析原理

1.1 侧信道分析的基本模型

密码算法是现代密码学的重要基础，整个信息系统的安全模块核心都是由以密码算法为基础的协议、应用系统搭建起来的. 对密码算法的安全性研究一直是密码学领域研究的核心问题. 传统密码分析主要利用密码算法的明密文信息，采用线性分析和差分分析等方法进行攻击，并获得密钥. 在这种分析方式下，分析人员通常将密码算法看作一个黑盒，借助密码算法的数学性质，仅利用密码算法的输入、输出信息恢复密码算法所使用密钥. 图1展示了传统密码分析学所使用的密码分析模型. 但随着密码算法的发展，密钥长度不断增长，这类攻击所要获取和处理的数据量不断激增，在现实中并不总是可行的. 比如在分组密码算法中，早期的DES算法密钥长度仅为56 b，现在常用的AES算法密钥长度可选为128 b、192 b、256 b；而在公钥密码算法中，RSA算法起初使用1 024 b的密钥，现在则推荐使用2 048 b甚至是4 096 b的密钥.

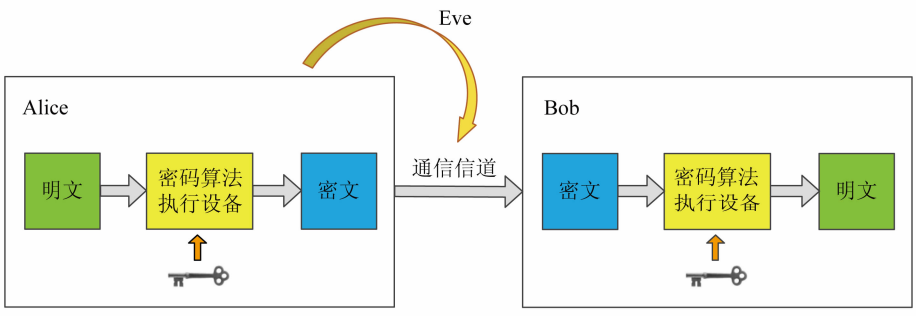


图1 传统密码分析模型

而在实际应用中，随着集成电路技术、半导体技术的不断发展，密码算法以硬件电路实现或软件程序实现的方式出现在密码设备中. 典型的密码设备包括基于ASIC平台或FPGA平台的各类智能卡、微处理器以及芯片. 这些密码设备内嵌于多种智能设备，使之具有安全功能. 因此，密码设

备是否能够保证所执行的密码算法达到其理论上的安全性成为一个重要的问题. 在实际应用中,执行密码算法的密码设备不能被视为一个无懈可击的黑盒,而是一个会泄露多种类型信息的漏风盒子. 这些泄露信息被称为侧信道信息,其中有可能含有敏感安全参数的信息. 图 2 展示了常见的侧信道信息种类. 利用密码设备实际工作时所释放的侧信道信息,恢复敏感安全参数或者密钥信息的过程被称为侧信道分析.

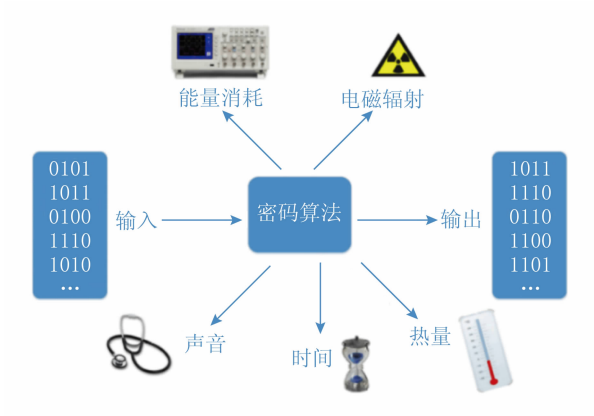


图 2　常见的侧信道信息种类

侧信道分析的概念最早是 Kocher[1] 在 Crypto96 上提出,当时他对无防护的多种密码算法智能卡实现实施了成功的计时分析. 经过近 20 年的发展,多种侧信道分析形式被提出,其中典型的分析形式包括:计时分析(包括 cache 攻击)[1-6]、能量分析[7-8]、电磁辐射分析[9-11]、故障分析[12-14]、碰撞分析[15-22]、代数侧信道分析[23-25]、声音分析[26] 等. 图 3 展示了侧信息分析模型. 研究实践发现,侧信道分析对密码设备中的密码算法操作产生严重的物理安全威胁.

在上述典型侧信道分析形式中,能量分析以易于实施、代价较小的特点,对多种运行在密码设备中的密码算法带来尤为严重的物理安全威胁. 由于侧信道信息(能量消耗、电磁辐射、运算或访问时间、声波等)的产生,均与密码芯片在实际运行中所执行的操作有关,不同的侧信道信息之间存在相互对应的关联关系. 由于能量消耗与电磁辐射 2 类侧信道信息的产生原理、分析方法等几乎完全相同,其差异仅体现在侧信道信息的表现形式上,故我们将分别介绍能量分析和计时分析的原理.

1.2　能量消耗的产生、组成与模型

密码设备在运行密码算法时执行不同的操作会引起能量消耗的变化,这是由密码设备的电路特性所决定的. 密码设备是由 CMOS 元件搭建而成,而 CMOS 元件的电气特性与纯电阻并不相同. 当 CMOS 元件的输入发生变化时,CMOS 元件的导通方向会随之改变,进而导致 CMOS 元件的电容发生充放电操作.

从物理学角度看,密码设备能量消耗是由 CMOS 元件能量消耗变化所引起的. 每一个 CMOS 元件的能量消耗总和,即所有电容充放电效果的累加导致了密码设备的能量消耗. 更进一步,CMOS 元件的输入(0 或 1,即低电平或高电平)发生变化时所引发的充放电现象,导致了明显的能量消耗. 对于触发器、寄存器等逻辑元件,01 翻转(0→1 或 1→0)导致明显的能量消耗;对于总线,01 值(高低电平)驱动总线电容进行充放电,导致明显的能量消耗.

从密码学角度看,密码设备中的 01 不均衡导致了能量消耗的差异. 不论是 01 翻转不均衡还是 01 值不均衡(不同状态发生变化时,所产生的 01 翻转数或 1 的个数不同),均会导致能量消耗的变化. 而这种不均衡所导致的能量消耗变化,使得我们能够想办法从密码设备的能量消耗信息中获取一些密码算法计算过程中的中间值,而这些中间值有助于恢复密钥信息.

电磁消耗的产生原理与能量消耗完全一致,唯一的区别在于 CMOS 元件在进行 01 翻转时在产生能量变化的同时,还会以电磁波的形式向周围空间散佚. 因此,电磁消耗的组成和模型与能量消耗完全一致,不再赘述.

能量分析利用的一个基本事实是:密码设备的能量消耗依赖于该设备执行的操作和处理的数据. 一般而言,密码设备的能量消耗由操作依赖分量、数据依赖分量、电子噪声分量、常量分量 4 部分组成. 其中操作依赖分量指的是由特定操作指令所引发的能量消耗,如 mov 指令、分支语句等;数据依赖分量指的是由操作数所引发的能量消耗,如操作数为 0 和 1 时引发不同的能量消耗;电子噪声分量指的是在采集能量消耗时电路中所引入的电子噪声;常量分量指的是由漏电流以及与操作和数据无关的晶体管转换活动造成的能量消

耗. 把任意时刻上述 4 部分分量累加起来，即可获得该时刻密码设备的能量消耗总量. 而所采集的能量曲线上的每一个点的幅值即为该时刻对应的能量消耗总量.

能量消耗模型是对实际能量消耗的一种模拟，模拟精度越高则攻击者恢复出密码设备所使用的敏感安全参数或密钥信息的能力越强. 常见的能量泄露刻画方法包括单比特模型、多比特模型、汉明重量(Hamming weight，HW)模型、汉明距离(Hamming distance，HD)模型、零值模型以及随机模型等. 其中最为常用、应用最为广泛的是汉明重量模型和汉明距离模型，下面将简要介绍这 2 类能量消耗模型.

汉明重量(HW)模型的基本思想是计算目标逻辑元件在某个特定时间段内，所处理的中间值(即比特串)中“1”的个数，并以此作为目标逻辑元件能量消耗的指标. 它通过量化中间值所引发的能量变化，来构造一个用于预测密码设备能量消耗的假设模型(即 HW 模型). HW 模型适用于那些攻击者对密码设备一无所知，或者密码设备没有连续存储目标中间值的情形. 例如，当能量分析攻击点是一个寄存器，并且该寄存器在存储每个有效中间值之前，都要重复地把寄存器置为“0”，这种情形就适用于 HW 模型. 我们可以这样理解：在使用 HW 模型对密码设备进行能量泄露刻画时，单个或 1 组逻辑元件的能量消耗应与这些逻辑元件所处理“1”的数目成正比例或反比例关系.

汉明距离(HD)模型的基本思想是计算目标逻辑元件在某个特定时间段内，所处理的中间值(即比特串)中 0→1 转换和 1→0 转换的总数，并以此作为目标逻辑元件能量泄露的指标. 也就是说 HD 方法通过量化 2 个或 2 组比特串的差异，来构造用于预测密码设备能量泄露的假设模型(即 HD 模型). HD 模型适用于那些了解目标中间值在相邻 2 个状态变化数目的情形. 在使用 HD 模型对密码设备进行能量泄露刻画时，需要目标逻辑元件的能量消耗特性满足：所有的 0→1 转换和 1→0 转换所引发的能量消耗相同，所有的 0→0 转换和 1→1 转换对能量消耗有相同的影响. 在某些情形下，上述 2 类模型可以相互转换. 比如当 HD 模型的中间值 2 个相邻状态中任意 1 个状态为固定值时，HW 模型和 HD 模型可以认为是等价的.

除了上述 2 类应用最为广泛的通用能量消耗模型之外，其他能量模型多是通过扩展这 2 类能量模型得到，或者是由于对密码设备中某些元件有更为深刻的了解，提出用于刻画特定逻辑元件的新模型. 比如，在 HD 模型中给不同的比特赋予不同的权重(例如，赋予中间值的最高有效比特位 2 倍于其他比特位的权重)，或者给不同类型的转换赋予不同的权重(例如，赋予 0→1 转换 2 倍于 1→0 转换的权重). 再比如，利用乘法器完成乘法运算时，一个操作数为 0 的乘法所需的能量消耗远小于其他情况，则可以采用零值模型对能量泄露进行刻画；零值模型的定义如下：如果一个操作数为 0，其能量消耗为 0，反之，则能量消耗为 1.

1.3 能量消耗采集与分析系统

能量分析可分为如下 2 个阶段：

1) 能量消耗采集阶段

主要用于获得实施能量分析所需要的能量消耗，采集的能量消耗曲线可通过密码实现时的被动泄露和主动诱导产生，采集的精度取决于测试计量仪器或测试方法的精度.

在采集能量消耗时只需要对密码设备的供电电源稍作改动，即在供电电源的 GND 端放置一个与密码设备串联的小电阻，再用示波器采集小电阻两端的电压变化，如图 3 所示. 这种对密码设备电路的修改相对简单易行，因为小电阻是串联在密码设备外部，并不更改密码设备内部的电路结构. 而示波器则同时充当了能量消耗的采集和存储设备.

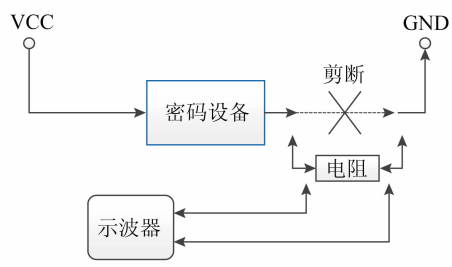


图 3 能量消耗采集示意图

2) 能量分析阶段

利用上一阶段获取的能量消耗曲线，使用一定的分析方法，结合密码算法的输入、输出和设计细节恢复出部分密钥片段，然后结合密钥扩展算法恢复主密钥.

考虑到对密码设备的实时控制(给定密码算法的输入、输出),以及对示波器所采集的能量消耗曲线进行分析处理,需要一台高性能计算机完成中控和数据处理分析等工作. 因此,整个能量消耗采集与分析系统将由计算机、带有密码设备的外部电路控制板、示波器、电源等组成.

电磁消耗系统与能量消耗系统在分析方面完全一致,主要的区别在于采集时不需要改动密码设备,只需要通过靠近芯片耦合电容处的电磁探头就可以获得密码芯片的电磁辐射信息.

1.4 能量分析方法

能量分析方法重点研究运用何种数学工具、统计手段可以更加有效地恢复出密码设备所使用的敏感安全参数或密钥信息. 现有的能量分析方法已经比较成熟,能量分析的方法主要包括简单能量分析(simple power analysis, SPA)、差分能量分析(differential power analysis, DPA)、相关能量分析(correlation power analysis, CPA)、模板攻击(template attacks, TA)以及高阶差分能量分析(high-order DPA, HoDPA). 这些方法从简单的获取一条能量曲线看图读数,到获取大量能量曲线分析其中的统计特性;从根据 1 b 信息作为分类函数,到计算猜测值和能量曲线的相关系数,再到通过预计算建立模板增强攻击效果;从对没有防护措施的密码算法实现进行一阶攻击,到对有防御措施的实现进行高阶攻击,随着 20 多年的发展,能量分析逐步建立起一套完整的方法体系,分析方法已经比较成熟.

下面,我们将对常见的能量分析方法进行简单介绍. 而电磁分析方法与能量分析方法所使用的数学工具、统计手段完全一致,故不再单独赘述.

简单能量分析(SPA):SPA 是一种能够对密码算法执行过程中所采集到的能量消耗信息进行直接分析的技术. 通常而言,攻击者采用 SPA,可以只根据 1 条或几条给定的能量曲线就恢复密码设备中的敏感安全参数或密钥信息. 这意味着被攻击密码设备中的密钥信息必须对其能量消耗有明显的影响. 一般而言,密码设备在执行密码算法操作时,不同的操作指令会导致其能量消耗产生较大变化(比如形状、幅度等). 因此,SPA 多用于那些密钥直接影响操作指令的情况.

公钥密码算法在实现时会根据密钥的取值产生条件分支,故未受保护的公钥密码算法实现是一种常见的 SPA 攻击目标. 比如未受保护的椭圆曲线算法实现,在计算点乘 $Q=P+P+\cdots+P=kP$ 时,会利用基础的倍加算法完成. 其中当乘数为 1 时,需要额外进行一次加法操作,反映在能量曲线上即为当密钥取 0 和 1 时,对应的能量消耗形状不同. 因此,攻击者可以直接通过能量曲线上的能量消耗形状读出密钥信息.

模板分析(TA):TA 主要利用能量消耗的数据依赖分量. 模板攻击首先需要构建 1 组针对目标密码设备的能量消耗模板,然后利用所采集的能量曲线与能量消耗模板进行匹配,与所采集能量曲线最匹配的模板所对应的敏感安全参数或密钥值即为所求. 在构建模板时可以采用多种策略,包括构建数据和密钥对模板、中间值模板、基于能量模型的模板等. 其中数据和密钥对模板指的是每一个数据和密钥对(d_i,k_j)构建模板;中间值模板为利用适当的函数 $f(d_i,k_j)$构建模板,比如以 S 盒输出 $S(d_i,k_j)$作为构建模板的依据;而基于能量模型的模板则充分利用了能量模型的信息,有效减少了模板数量,比如以 S 盒输出的 HW 值 $HW(S(d_i,k_j))$构建模板. 例如,对一个 8 b 的 S 盒操作构建模板,构建数据和密钥对模板共$(2^8)^2=256^2$ 个,构建中间值模板共 256 个,而构建基于 HW 模型的模板共 9 个. 构建模板完成后可以进行模板匹配. 在模板匹配时,一般采用最小二乘法通过计算所采集的能量曲线与模板之间的相似程度来判定所匹配的模板.

差分能量分析(DPA):DPA 是一种最为流行的能量分析攻击技术,由于其不需要了解目标密码设备的详细知识. 与 SPA 相比,DPA 利用能量消耗数据依赖分量,并需要大量的能量曲线来分析固定时刻密码设备的能量消耗.

标准 DPA 技术采用单比特能量消耗作为能量泄露模型. 其攻击思路如下:首先采集 1 组已知明文的能量曲线;然后,假设密钥为 Ks,以某个中间值最高有效位 b 作为区分函数,根据每条能量曲线对应明文计算该曲线的 b 值为 0 或 1,把相应的能量曲线分成 2 个集合;接下来,对 2 组能量曲线的每一个采样点求均值差,可以得到 1 条关于 Ks 均值差曲线. 如果假设密钥 Ks 猜测错误,则均

值差曲线上不应出现相对明显的尖峰，而当假设密钥 Ks 猜测正确时，则在正确时刻 t 会出现一个相对明显的尖峰.

对于多比特情形，由多比特 DPA 技术衍生出了相关能量分析（CPA）技术. 与 DPA 相比，CPA 利用协方差或相关系数来替代均值差作为区分函数. 协方差或相关函数用于刻画 2 组数据之间的线性关系. 因此，CPA 的任务就是根据实际测量的能量曲线和估算的假设能量消耗计算出相应的相关系数值. 最高的相关系数峰值揭示了与实测能量消耗最为线性相关的假设能量消耗，而对应的假设密钥值在理论上即为正确子密钥值.

随着研究的不断深入，各种防御技术不断提出，DPA 技术也不断发展，攻击能力不断增强. 在一阶 DPA 方法被提出后不久，针对一阶 DPA 方法的防御措施就被提出. 随后，二阶 DPA 分析技术被提出，用于攻击抵抗一阶 DPA 的密码系统，通过对能量曲线上的 2 部分进行预处理操作，把二阶 DPA 分析方法归约成一阶 DPA 方法.

1.5 已被分析的密码算法

针对能量分析的研究不仅在攻击方法上取得了巨大的进展，还对绝大多数密码算法进行了多种多样易于实现的攻击. 通过我们的研究发现：在目前已知的多种能量分析实现中，绝大部分能量分析需要结合目标算法的构件特性，利用其中带来能量泄露的构件，因此这些方法可以用于具有同类构件的其他算法. 密码算法的基本构件主要包括算法固有的结构，如 Sbox、线性反馈移位寄存器（linear feedback shift registers，LFSR），操作，如分支判断、密钥扩展等，以及实现所需的硬件，如寄存器、RAM、LUT. 下面分别对几类主要密码算法的能量分析成果进行简要的介绍.

公钥密码算法：公钥密码算法主要产生能量分析问题的是算法中的分支结构. 对于大部分公钥密码算法的简单实现而言，采用能量分析即可以获得较好的攻击效果，如针对 RSA/ECC 中的条件分支语句的 SPA 攻击. 在此之后，研究人员深入研究了公钥密码算法的抵抗能量分析防御措施，如选用特殊形式的曲线、改变基点、随机化密钥等方法.

分组密码算法：能量分析主要针对分组密码算法中的非线性结构，例如 Sbox 的输出，对此类分析方法可以采用掩码、DPL 等技术进行防御，而针对添加防御措施的实现需要高阶 DPA 才能实现攻击. 针对 DES/AES 等主流分组密码算法的能量分析成果非常多，如针对非线性模块的 DPA 攻击、对 AES 混合列变换的 DPA 攻击、对 AES 密钥编排的 SPA 攻击、对数据总线的攻击等.

流密码算法：针对流密码算法的能量分析，主要利用了流密码中常见的重同步机制，即每过一段时间，流密码加解密两端的 IV 值更新 1 次. 这使得攻击者可以仿照对分组密码算法的选择明文能量分析，对流密码进行选择 IV 能量分析. 2006 年以来，Fischer 等人[27] 对 eSTREAM 的候选流密码算法 Grain 和 Trivium 进行 DPA 攻击，并且于 2008 年完成对全部 eSTREAM 候选算法的抗侧信道分析评测.

轻量级密码算法：因为轻量级密码算法的主要构件均来自于已有的标准密码算法，很多在现有密码算法中使用的能量分析技术在轻量级密码算法中仍然适用. 研究人员分别对近年提出的多种轻量级密码算法如 PRINT，PRESENT 进行了能量分析研究.

1.6 计时分析（包括 cache 攻击）原理与方法

利用加密算法的加密或数据访问时间进行分析的侧信道分析方法被称为计时分析. 根据目标对象的不同，可分为普通计时分析和 cache 攻击. 普通计时分析针对智能卡系统，利用密码运算中间值输入比特位和密码运算时间的相关性来恢复密钥信息. cache 攻击则是利用 CPU 中 cache 机制的时间特性来恢复密钥信息. 近年来，cache 攻击已经成为了计时分析的一个研究热点. 因此，本文重点讲述一下 cache 攻击的原理.

在 CPU 和主存之间有一个小容量的、快速的存储区域，被称为 cache. 为了减小访问主存的延迟时间，CPU 利用 cache 存储那些最频繁被访问的内存数据. CPU 在运行程序的过程中，在主存中查找到需要的值之后会把这个数值存储进 cache 里，然后再按照一定的替换策略，将不常用到的值从 cache 中逐出. 之后，再一次访问相同内存地址可以从 cache 中直接得到数据，从而大大缩短访问时间，这个过程被称为“cache 命中”. 由于 cache 和主存访问时间上的差异，密钥可以通过一定数量的加密时间数据破解出来.

目前常用的 cache 攻击基本上可以分为五大类：统计平均方法[28]、Evict + Time[3]、Prime + Probe[3]、Flush+Reload[4-5]以及 Flush+Flush[6]. 下面将对上述方法进行介绍：

统计平均方法. 首先要收集一定数量的随机明文加密时间数据，然后通过先聚类后平均的方法，找到时间最小的聚类（说明此聚类发生了 cache 碰撞），从而得到部分甚至全部密钥. 在统计平均方法中，根据聚类的不同，可以分为第 1 轮 cache 攻击和最后一轮 cache 攻击[28].

Evict+Time 方法. 首先进行一次选择明文查找表 T 加密，然后间谍进程访问对应于查找表 T 中某个特定元素的地址（映射在同一个 cache 行），最后再进行第 2 次同样明文的加密，并采集加密时间. 如果第 2 次加密的时间显著增加，则说明其 cache 内加载了查找表 T 的对应元素[3].

Prime+Probe 方法. 首先把对应于查找表 T 的攻击者数据全部填充进 cache；然后进行一次选择明文的加密；最后，重新访问攻击者数据，采集访问时间. 通过访问时间的长短检测出哪些元素已经被逐出 cache，从而判断出加密过程用了查找表 T 中的哪几个元素. 这里攻击者仅仅对自己的简单操作进行计时，这大大降低了采集时间数据的噪声[3].

Flush+Reload 方法. Flush+Reload 技术是由 Prime+Probe 方法发展而来，攻击间谍进程和目标进程的共享页. 首先，从 cache 中剔除被监控的内存映射；然后，间谍进程允许目标访问内存；最后，间谍进程重新载入内存行，测量重新载入的时间. 如果在等待的阶段目标进程访问了指定的内存空间，那么这个内存的空间就在 cache 中有记录，重载就只需要很短的时间. 另一方面，如果目标没有访问指定的内存空间，则这个空间就需要从内存中提取，重载花费更长的时间[5].

Flush+Flush 方法. 该方法基于对缓存和未缓存的地址行进行 clflush 操作的时间差别. 当地址行在 cache 中时，由于额外执行一个数据逐出的过程，会增加 flush 的时间. 因此，地址行不在 cache 中的 clflush 操作会快于地址行在 cache 中的 clflush 操作. 攻击者只需要在共享内存的地址行上循环执行一个 clflush 操作，然后测量 clflush 操作的执行时间，以此确定哪个地址行被缓存了. 同时，clflush 操作逐出了缓存 cache 行，正好为下一轮循环攻击作好了准备[6].

2 侧信道分析实例

随着侧信道分析的能力越来越强、实施成本越来越小，各种密码设备被侧信道分析成功的事例越来越多. 比如，Eisenbarth 等人[29]在 Crypto2008 上发表了利用能量分析技术破解 KeeLoq remote keyless entry systems，其典型应用之一是遥控汽车锁；自 2009 年起，通过能量分析方式，已经成功攻破了中国地区所使用多款 Mifare 卡中的密码芯片，如广州发行的羊城通①、台湾发行的 EasyCard②等；Zhou 等人[30]在 FC2013 上发表了对手机卡中的 COMP128-1 算法成功实施了能量分析的工作；Genkin 等人[31]在 CHES2014 上提出了对 PC 上执行的 RSA 算法成功实施 Far end of cable 攻击以及 Human touch 攻击的方法；在 2015 年黑帽大会上，上海交通大学郁昱教授现场演示如何利用能量分析技术破解 3G/4G 的 SIM 卡③. 下面，我们将对近年来涌现出的侧信道分析实例进行简要介绍和分析.

2.1 专用/通用设备偷取计算机密钥

以色列特拉维夫大学的研究团队在 2015 年的 CHES 上展示了一种使用圆面包大小的专用设备来快速且低成本地盗取计算机密钥的方法[32]. 研究人员把这个收集设备戏称为“皮塔饼”（PITA，一种可撕开填馅的圆面包）. 该设备能够收集计算机发出的电磁信号，收集范围可达 50 m. 它包括一个非屏蔽铜环天线、一个拾取 1.7 Hz 的电容，这个频段泄露了密钥信息. 收集到的信号储存在一个 microSD 卡中，然后通过分析可以在几秒中内推断出密钥. 从实践中的效果来看，研究人员已经

① 唐韶华. 对“羊城通”地铁卡的实际攻击，2010（http://www.cacmct.org.cnJupload/fckeditor/芯片论坛 PPT.rar）

② 中国智能卡网. 台湾悠游卡首次遭破解，2011（http://www.smartcard.org.cn/date1/page11906.html）

③ 黑客与极客. 中国教授在 BlackHat 现场演示破解 SIM 卡 AES-128 加密，2015（http://www.freebuf.com/news/74383.html）

证实可以从运行 GnuPG 1.4.18 的笔记本电脑上捕获密钥，GnuPG 是一种开源的加密程序，使用 RSA 和 ElGamal 加密算法. 作为攻击的一部分，皮塔饼还可以给计算机发送出精心构造的密文. 当内容被解密时它就会释放出可观测到的电磁信号. 皮塔饼的设计细节如图 4 所示：

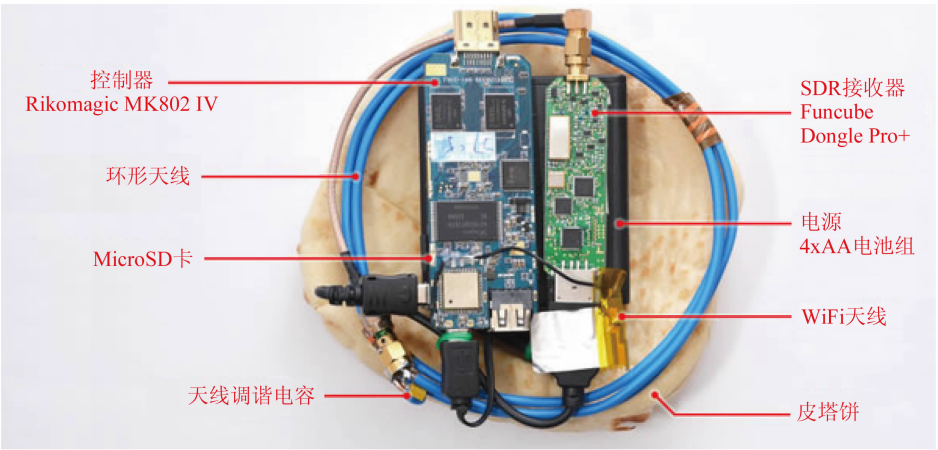


图 4　皮塔饼构造图

本分析实例主要针对 GnuPG 中使用的无保护 RSA 与 ElGamal 方案来进行. 尽管针对无保护方案的侧信道分析在目前已经不足为奇，但 GnuPG 中的密码算法实现采用了优化的实现方案，从而提高了传统侧信道分析的难度. 从侧信道信息的采集角度来看，该方案主要采用了非接触式的简易低频无线信号接收装置来进行电磁信道采集. 优化性能方面，本分析实例采用选择明文的方式大大降低了实际需要的电磁曲线数量，并使得分析所需要的时间大幅下降.

该团队在皮塔饼的基础上，结合计算机解密过程中会产生 CPU 噪声的研究结论，提出了通过廉价的消费级通用设备分析计算机所发出的无线电波窃取加密密钥[32]的理论. 为了证明这一理论，研究人员对系统在解密指定密文时所产生的电磁信号进行了分析. 结果证明，研究人员在极短的时间内就成功地提取到了笔记本上的 GnuPG 软件私有解密密钥. 在这次实验过程中，研究人员使用 Funcube Dongle Pro＋收音机测量了在 1.6～1.75 MHz 频率之间的电磁信号，并与一个安装了 Android 系统的嵌入式计算机 Rikomagic MK802 IV 相连接，由嵌入式计算机对所采集的电磁曲线数据进行存储和分析，如图 5 所示.

本分析实例从分析对象、采集的能量泄露类型到实际的分析方案均与皮塔饼分析实例相似，

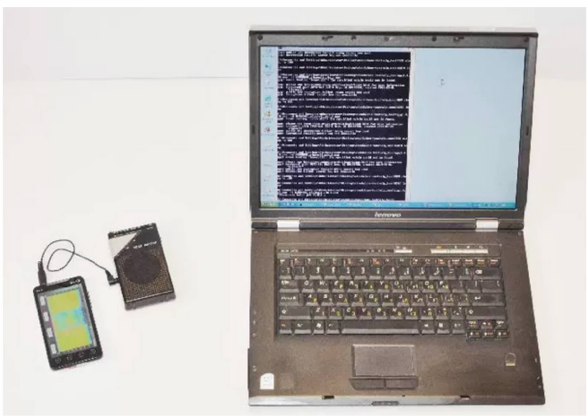


图 5　无线电窃取加密密钥实验图

唯一的区别是本实例中使用的采集装置是一个消费级别的收音机（无线电接收机），并将收集到的信号输入到嵌入式计算机中进行实际的密钥破解过程.

2.2　破解 NFC 近场通信

在 2013 年的 CT-RSA 会议上，奥地利格拉茨技术大学的研究人员汇报了其最新的研究成果，即通过使用自制的环形天线、宽带放大器以及示波器等设备对运行在 13.56 MHz 的 NFC 标签进行了实际的远程电磁分析（具体的分析方法为差分电磁分析）. 研究结果显示，即使将采集设配放在 1 m 之外也能够利用电磁信息破解近场通信设备中的秘密信息[33].

研究人员的分析目标主要是 NFC 标签中用于进行身份认证的计算电路模块，该模块采用标准的无保护 AES 算法对读卡器段发送来的身份认证挑战响应码进行加密并回传响应. 本分析实例能够在较远的 1 m 之外的距离完成实际的攻击，突破了传统上认为的近场通信信号在远距离传输中会产生较大衰减无法被有效采集的困难性，因此对于 NFC 所应用的领域如门禁、公交、手机支付等将带来很大的威胁. 由此，在 NFC 标签中添加侧信道分析的防护方案是势在必行的.

2.3 破解 3G/4G SIM 卡的加密

2016 年，上海交通大学的郁昱教授和团队组装使用了一个用于跟踪能量水平的示波器、用于监控数据流量的 MP300-SC2 协议分析仪、一个自制 SIM 卡读卡器和一个标准电脑在 10～80 min 的时间内分别破解了来自 8 家厂商的 SIM 卡. 郁昱教授现场展示了如何成功复制 SIM 卡，他同时还展示了一张克隆卡如何变更了支付宝的密码并潜在盗取账户资金[34].

3G/4G SIM 卡采用了双向认证算法协议称为 MILENAGE，这是基于 AES-128 密码算法的在 UMTS/LTE 网络中进行身份认证和密钥协商的密码算法协议，是被 NIST 认证为一个数学上的安全分组密码标准. 而从实际的实现角度来看，该协议的核心算法 AES 仍然采用了无保护的方式进行实现，再加之各个 SIM 卡制造商对原始协议的定制修改，使得标准的差分能量分析方法即可完成实际的 SIM 破解工作. 从该实验结果能够看出，尽管侧信道分析技术早已成为学术领域的研究热点，其在实际的芯片制造商特别是低成本芯片的研制厂商中仍然未能引起足够的重视，而本分析实例也将影响一大批已经发行并在市面上大量流通的 SIM 卡.

2.4 针对 CPU 的声音攻击

2014 年的 Crypto 会议上，Genkin 研究团队[26]提出了一种新型的声音攻击方案. 他们通过侦听用户计算机产生的高音调声音来解密数据，并已经成功破译了密钥长度为 4 096 b 的 RSA 密码算法，他们用一个麦克风接入到计算机侦听破解了一些被秘密数据.

首先，研究人员需要确切地知道所要侦听的频段，从而可以使用低通和高通滤波器来截获计算机中 CPU 正在解密数据时所发出的声音（实际上，声信号由 CPU 电压调节器产生，它需要在多样和丛发性负载中保持恒定电压）. 研究人员利用一个高品质的抛物面麦克风，在距离 4 m 的地方成功提取了解密密钥. 更有趣的是，他们还设法将这种攻击实验用在了远离目标的笔记本电脑，而工具则是利用了一部 30 cm 外的智能手机. 研究人员对不同的笔记本和台式机进行了攻击测试，结果都获得了不同程度的成功.

该研究是利用声音信息对秘密信息进行恢复的首次成功实例. 攻击的对象是笔记本上运行的 GPG 软件的解密密钥，主要利用该软件在旧版本中的实现漏洞进行分析. 从性能优化的角度来看，研究人员使用自适应的选择明文方案来构造攻击时所需的待解密密文消息，目的是要使得 GPG 软件在实行过程中产生大量的特定中间值循环操作，从而产生可以被声音接收器感知到的可区分秘密信息的低频声波指纹. 该研究使得针对那些使用严密防护外壳来屏蔽电磁辐射（如法拉第笼）的密码设备的攻击再次成为可能.

2.5 针对 ARM 处理器的攻击

鲁汶大学的研究团队在 2015 年对运行在 1 GHz的 ARM Cortex-A8 处理器进行了实际的攻击. 该款处理器常被用在智能手机上（如苹果 A4 处理器）. 在该项研究中，处理器被嵌入在单板计算机上并实际运行了一个完整的 Linux 操作系统[35].

作为实际攻击目标的 AES 算法采用位片化的方式进行实现（即将其中的所有运算转化为异或操作进行实现）. 实验表明在软件层面上，尽管研究人员是在一个共享资源的、多任务的、存在中断或者是竞争进程的操作系统中进行的侧信道攻击，只需要几千条能量曲线就能够恢复出 AES 的全部主密钥. 攻击的实际难点还是在于能量曲线探测的位置定位，触发信号的选择和识别以及能量曲线的对齐.

上述攻击方案主要针对 ARM 处理器中未保护的 AES 实现，由于 ARM 中的 AES 利用了位片化实现方式，与常规的 AES 不同，故其侧信道攻击点也与常规的 AES 有所不同，但并不影响整体的侧信道攻击流程以及所使用的侧信道攻击方法. 从实际攻击的角度看，由于 ARM 处理器上加

载的是一个共享资源的、多任务的、存在中断或者竞争进程的操作系统，对 ARM 处理器进行攻击所面临的最主要困难在于能量曲线探测的位置定位、触发信号的选择和识别以及能量曲线的对齐. 如果克服了上述采集阶段和预处理过程中的问题，只需要用经典的能量分析方法（比如相关能量分析）即可获得 AES 的密钥信息.

2.6 利用电磁分析破解 FPGA 代码的加密机制

FPGA 是一种在常见的密码算法硬件实现平台. 为了保证硬件设计不被恶意用户通过反向工程非法获取，FPGA 厂商通过 bitstream encryption 机制对硬件设计文件进行加密，加密算法依据具体的 FPGA 型号略有不同，大部分是 AES-128 或 AES-256，少部分比较老的 FPGA 型号采用的是 3DES. 当用户将加密后的硬件设计文件烧写入 FPGA 时，FPGA 芯片中的解密模块会自动将硬件设计文件解密，并依据硬件设计文件配置整个 FPGA 电路.

德国波鸿大学的 Moradi 团队自 2012 年起，针对 FPGA 的 bitstream encryption 机制进行了研究，并于 2016 年发布了对 Xilinx 公司的多款目前主流的 FPGA 芯片的 bitstream encryption 破解[36-39]，如图 6 所示. Moradi 团队的破解手段主要利用 FPGA 芯片在对加密的硬件设计文件执行解密时所产生的能量消耗/电磁辐射变化，并通过多比特差分能量/电磁分析技术，成功恢复出解密操作中所使用的密钥，进而可以通过反向工程将所烧写的硬件设计文件恢复出来.

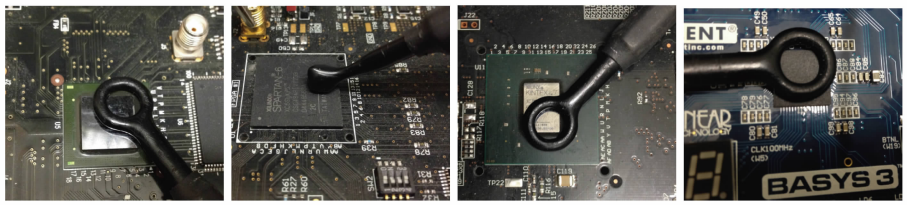


图 6 对多款 FPGA 芯片进行电磁探测实验图

该实例的分析对象是 Xilinx 公司的商用 FPGA 芯片，主要利用这些芯片的 bitstream encryption 机制中的密码算法，分别包括 3DES，AES-128，AES-256. 根据目前所公开的资料，上述密码算法仍然采用无保护的方式进行实现，因此攻击者很容易想到对其进行侧信道分析的方法. 但是由于 FPGA 芯片 bitstream encryption 机制的特殊性，对于上述密码算法实现的侧信道分析点与传统的经典侧信道分析点有所不同，攻击者需要更强的条件才能实施攻击. 早期的攻击中，攻击者需要更多的能量/电磁消耗曲线和更强的计算分析能力（使用 GPU），才能恢复密钥信息. 在最新的攻击中，攻击者利用选择明文的方式，使该攻击对曲线数量和计算能力的要求下降到与经典侧信道分析相同的水平. 因此，这种攻击是一种具有实际应用价值的攻击手段，在未来将会对 FPGA 厂商产生影响.

2.7 针对 IEEE 802.15.4 协议节点的能量分析破解

IEEE 802.15.4 协议是一族在无线网络中经常要使用的通信协议，包括 ZigBee，WirelessHART，MiWi，ISA100.11a，6LoWPAN，Nest Weave，JenNet，IEEE 802.15.5，Thread，Atmel Lightweight Mesh 以及 DigiMesh 等协议. 加载有片上系统（SoC）芯片的无线传感器有很多都支持 IEEE 802.15.4 协议，并且具有专门的 AES 加速器来实现 AES-CCM 算法，通过 AES-CCM 对发送或接收到的消息进行加密或鉴别，保障协议通信安全.

加拿大戴尔豪斯大学的研究团队在 2016 年利用能量分析，破解了运行在 Atmel 公司的 ATMega128RFA1 智能卡上的 AES 加速器，获取了在执行 IEEE 802.15.4 协议时所使用的 AES 密钥. 此外，该团队还证明即便 AES 加速器不放置在智能卡，而是放置于无线传感器节点上，同样可以利用电磁分析的方法对其进行类似的破解[40].

上述分析实例主要针对无线个域网协议族 IEEE 802.15.4 中使用的无保护 AES-CCM 算法方案来进行侧信道分析. 类似于前面几个实例，对于无保护方案的侧信道分析在目前已经不足为奇，特别是对于智能卡或者无线传感器节点等资源受限设备，增添防御机制十分困难. 从能量曲线

的采集角度来看，该方案主要采用了传统的能量采集电路构造技术来进行能量曲线采集，采用的分析方法属于传统的相关能量分析.

2.8 计时分析(包括 cache 攻击)实例

为了减少系统的内存占用，运行在系统上的不同进程会共享相同的内存页. 这种共享可以基于共享页的来源，例如共享库中的函数. 此外，共享还可以基于主动搜索和合并相同的内容. 为了保持非信任进程之间的隔离，系统依赖于对共享页强制执行只读权限或者写时复制的硬件机制. 但是，由于共享 cache 的使用，这种共享内存页存在巨大的安全隐患.

来自澳大利亚阿德莱德大学的研究人员在 2014 年展示了一种 cache 攻击技术——FLUSH+RELOAD，它利用处理器的弱点监视共享页内存行的访问[5]. 与已出现的 cache 攻击不同，FLUSH+RELOAD 以最后一级 cache 为攻击目标. 因此，攻击程序和被攻击进程不需要运行在一个处理器核心上.

阿德莱德大学的研究团队对 GnuPG 1.4.13 中的程序实施了 FLUSH+RELOAD 攻击，证明了这种方法的破解效果，图 7 是其攻击实验结果图. 该实验是在一个操作系统上的不同进程以及不同虚拟机上的不同进程上进行的. 平均而言，他们的攻击能够通过观察单个签名或解密轮来回复 96.7%的密钥位.

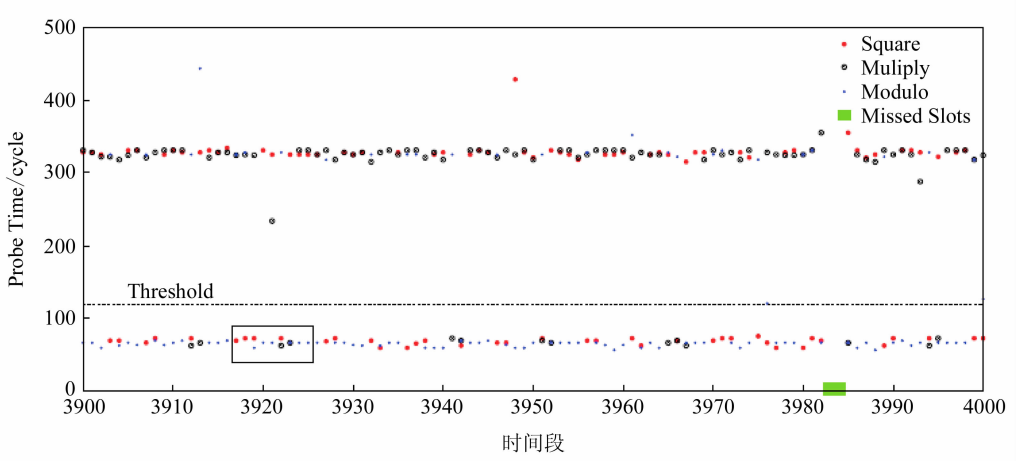


图 7 FLUSH+RELOAD 的攻击实验结果

除了以上提到的 FLUSH+RELOAD 攻击以外，cache 攻击还有很多种类，如 Evict+Time 攻击 Prime+Probe 攻击以及 Flush+Flush 攻击. 最近，由于现代 CPU 的推测执行机制，Meltdown 和 Spectre 两种攻击被广泛报道并引起了学术界和企业界的巨大关注，而实施这 2 种攻击的手段就是典型的 cache 时间攻击.

3 总 结

目前，针对密码设备的侧信道分析案例屡见报端，侧信道分析也逐步从一种实验室攻击手段转变为对实际系统具有严重安全威胁的实际攻击方法. 对此，学术界和产业界也设计提出了多种不同类型的防御机制，比如双轨机制、掩码机制等. 但是受限于密码设备的性能要求，防御机制所带来的资源开销往往会极大地影响密码设备的可用性. 因此，对于密码设备而言，侧信道防御机制将是未来重要的研究方向之一；安全能力高、资源开销小的防御机制也将成为密码设备产品的重要特点和技术指标.

参 考 文 献

[1] Kocher P. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems [C] //Proc of CRYPTO'96. Berlin: Springer, 1996: 104-113

[2] Kelsey J, Schneier B, David Wagner, et al. Side channel cryptanalysis of product ciphers [C] //Proc of ESORICS'98. Berlin: Springer, 1998: 97-110

[3] Osvik D A, Shamir A, Tromer E. Cache attacks and countermeasures: The case of AES [C] //Proc of CT-RSA'06. Berlin: Springer, 2006: 1-20

[4] Bangerter E, Gullasch D, Krenn S. Cache games-Bringing access-based cache attacks on AES to practice [C] //Proc of S&P'11. Piscataway, NJ: IEEE, 2011: 490-505
[5] Yarom Y, Falkner K. Flush+Reload: A high resolution, low noise, L3 cache side-channel attack [C] //Proc of USENIX'14. Berkeley, CA: USENIX Association, 2014: 719-732
[6] Gruss D, Maurice C, Wagner K, et al. Flush+Flush: A fast and stealthy cache attack [C] //Proc of DIMVA'16. Berlin: Springer, 2016: 279-299
[7] Kocher P, Jaffe J, Jun B. Differential power analysis [C] //Proc of CRYPTO'99. Berlin: Springer, 1999: 388-397
[8] Lemke K, Schramm K, Paar C. DPA on n-bit sized boolean and arithmetic operations and its application to IDEA, RC6, and the HMAC-construction [C] //Proc of CHES'04. Berlin: Springer, 2004: 205-219
[9] Agrawal D, Archambeault B, Rao J R, et al. The EM side-channel(s) [C] //Proc of CHES'02. Berlin: Springer, 2003: 29-45
[10] Gandolfi K, Mourtel C, Olivier F. Electromagnetic analysis: Concrete results [C] //Proc of CHES'01. Berlin: Springer, 2001: 251-261
[11] Hutter M, Mangard S, Feldhofer M. Power and EM attacks on passive 13.56MHz RFID devices [C] //Proc of CHES'07. Berlin: Springer, 2007: 320-333
[12] Biham E, Shamir A. Differential fault analysis of secret key cryptosystems [C] //Proc of CRYPTO'97. Berlin: Springer, 1997: 513-525
[13] Boneh D, DeMillo R A, Lipton R J. On the importance of checking cryptographic protocols for faults [C] //Proc of EUROCRYPT'97. Berlin: Springer, 1997: 37-51
[14] Piret G, Quisquater J-J. A differential fault attack technique against SPN structures, with application to the AES and khazad [C] //Proc of CHES'03. Berlin: Springer, 2003: 77-88
[15] Biryukov A, Bogdanov A, Khovratovich D, et al. Collision attacks on AES-based MAC: Alpha-MAC [C] //Proc of CHES'07. Berlin: Springer, 2007: 166-180
[16] Biryukov A, Khovratovich D. Two new techniques of side-channel cryptanalysis [C] //Proc of CHES'07. Berlin: Springer, 2007: 195-208
[17] Bogdanov A. Improved side-channel collision attacks on AES [C] //Proc of SAC'07. Berlin: Springer, 2007: 84-95
[18] Bogdanov A. Multiple-differential side-channel collision attacks on AES [C] //Proc of CHES'08. Berlin: Springer, 2008: 30-44
[19] Ledig H, Muller F, Valette F. Enhancing collision attacks [C] //Proc of CHES'04. Berlin: Springer, 2004: 176-190
[20] Moradi A. Statistical tools flavor side-channel collision attacks [C] //Proc of EUROCRYPT'12. Berlin: Springer, 2012: 428-445
[21] Schramm K, Leander G, Felke P, et al. A collision-attack on AES: Combining side channel-and differential-attack [C] //Proc of CHES'04. Berlin: Springer, 2004: 163-175
[22] Schramm K, Wollinger T, Paar C. A new class of collision attacks and its application to DES [C] //Proc of FSE'03. Berlin: Springer, 2003: 206-222
[23] Oren Y, Kirschbaum M, Popp T, et al. Algebraic side-channel analysis in the presence of errors [C] //Proc of CHES'10. Berlin: Springer, 2010: 428-442
[24] Oren Y, Renauld M, Standaert F-X, et al. Algebraic side-channel attacks beyond the Hamming weight leakage model [C] //Proc of CHES'12. Berlin: Springer, 2012: 140-154
[25] Renauld M, Standaert F-X, Nicolas V-C. Algebraic side-channel attacks on the AES: Why time also matters in DPA [C] //Proc of CHES'09. Berlin: Springer, 2009: 97-111
[26] Genkin D, Shamir A, Tromer E. RSA key extraction via low-bandwidth acoustic cryptanalysis [C] //Proc of CRYPTO'14. Berlin: Springer, 2014: 444-461
[27] Fischer W, Gammel B M, Kniffler O, et al. Differential power analysis of stream ciphers [C] //Proc of CTRSA'07. Berlin: Springer, 2007: 257-270
[28] Bonneau J, Mironov I. Cache-collision timing attacks against AES [C] //Proc of CHES'06. Berlin: Springer, 2006: 201-215
[29] 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 [C] //Proc of CRYPTO'08. Berlin: Springer, 2008: 203-220
[30] Zhou Yuanyuan, Yu Yu, Standaert F-X, et al. On the need of physical security for small embedded devices: A case study with COMP128-1 implementations in SIM cards [C] //Proc of FC'13. Berlin: Springer, 2013: 230-238
[31] Genkin D, Pipman I, Tromer E. Get your hands off my laptop: Physical side-channel key-extraction attacks on PCs [C] //Proc of CHES'14. Berlin: Springer, 2014: 242-260
[32] Genkin D, Pachmanov L, Pipman I, et al. Stealing keys from PCs using a radio: Cheap electromagnetic attacks on windowed exponentiation [C] //Proc of CHES'15. Berlin: Springer, 2015: 207-228
[33] Korak T, Plos T. Applying remote side-channel analysis attacks on a security-enabled NFC tag [C] //Proc of CT-RSA'13. Berlin: Springer, 2013: 207-222
[34] Liu Junrong, Yu Yu , Standaert F-X, et al. Small tweaks do not help: Differential power analysis of MILENAGE implementations in 3G/4G USIM cards [C] //Proc of ESORICS'15. Berlin: Springer, 2015: 468-480
[35] BalaschJ, Gierlichs B, Reparaz O, et al. DPA, bitslicing and masking at 1GHz [C] //Proc of CHES'15. Berlin: Springer, 2015: 599-619

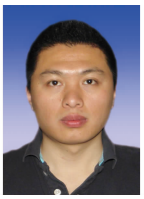
[36] Moradi A, Barenghi A, Kasper T. On the vulnerability of FPGA bitstream encryption against power analysis attacks: Extracting keys form Xilinx Virtex-II FPGAs [C] //Proc of CCS'11. New York: ACM, 2011: 111-124

[37] Moradi A, Kasper M, Paar C. Black-box side-channel attacks highlight the importance of countermeasures [C] // Proc of CT-RSA'12. Berlin: Springer, 2012: 1-18

[38] Moradi A, Oswald D, Paar C, et al. Side-channel attacks on the bitstream encryption mechanism of AlteraStratix II: Facilitating black-box analysis using software reverse-engineering [C] //Proc of FPGA'13. New York: ACM, 2013: 91-100

[39] Moradi A, Schneider T. Improved side-channel analysis attacks on Xilinx bitstream encryption of 5, 6, and 7 series [C] //Proc of COSADE'16. Berlin: Springer, 2016: 71-87

[40] O'Flynn C, Chen Zhizhang. Power analysis attacks against IEEE 802.15.4 nodes [C] //Proc of COSADE'16. Berlin: Springer, 2016: 55-70



葛景全

博士研究生，主要研究方向为网络与空间安全.

gejingquan@iie.ac.cn

屠晨阳

博士，助理研究员，主要研究方向为网络与空间安全.

tuchenyang@iie.ac.cn

高　能

博士，研究员，主要研究方向为网络与空间安全.

gaoneng@iie.ac.cn