

基于人工智能的侧信道攻击研究

何利文, 国海轮, 安 聪

(南京邮电大学, 江苏 南京 210000)

摘 要:随着密码技术和信息技术的发展,目前的密码算法本身已足够强大,能够对抗传统的密码分析手段,但由于设备本身的工艺特性,其运行时会泄露如功耗、电磁、时间等侧信道信息,这些信息可以被攻击者利用,破解密钥。因为这种攻击效果好,所以最开始比较受欢迎。模板攻击由 Rohatgi 等人首次提出,和差分功耗攻击不同的是,它需要攻击者预先刻画密码芯片的模板,然后进行模板匹配,攻击时攻击者可以提取感兴趣的部分,因为监督学习和这种攻击过程很类似,所以机器学习在侧信道领域应用越来越广。之后 Martinask 等人将深度学习方法引入模板攻击,结果表明攻击效果优于其他训练算法。该文首先介绍了侧信道攻击的发展情况、概述、分类,之后结合最近几年机器学习技术的发展,阐述了人工智能在侧信道攻击技术方面的应用。

关键词:侧信道攻击;人工智能;故障攻击;功耗攻击;模板攻击

中图分类号:TP31

文献标识码:A

文章编号:1673-629X(2022)06-0106-06

doi:10.3969/j.issn.1673-629X.2022.06.018

Research on Side Channel Attack Based on Artificial Intelligence

HE Li-wen, GUO Hai-lun, AN Cong

(Nanjing University of Posts and Telecommunications, Nanjing 210000, China)

Abstract: With the development of cryptography and information technology, the current cryptographic algorithm itself is strong enough to fight against the traditional cryptanalysis methods. However, due to the process characteristics of the device itself, it will leak side channel information such as power consumption, electromagnetic, time and so on, which can be used by attackers to crack the key. In many side channel information, the acquisition of power consumption information is relatively simple and low cost, but it has a strong attack effect. The template attack was first proposed by Rohatgi et al. Different from the differential power attack, it requires the attacker to characterize the template of the cryptographic chip in advance, and then match the template to the attacking device. During the attack, the attacker can extract the interested part, because the attack process of the template attack is similar to supervised learning, so many machine learning algorithms are introduced into the field of side channel attack. After that, Martinask and others introduced the deep learning method into the template attack, and the results show that the attack effect is better than other training algorithms. In this study, we first introduce the development, overview and classification of side channel attack, and then combined with the development of machine learning technology in recent years, expound the application of artificial intelligence in side channel attack technology.

Key words: side channel attack; artificial intelligence; failure attack; power consumption attack; template attack

0 引 言

随着信息的快速发展,信息的智能化对大家的生
活有很大影响,同时信息安全方面衍生出很多缺陷。
密码有关的设备安全变得尤为重要,密码技术在生活
中到处可见。这些技术对终端设备产生巨大威胁。侧
信道攻击^[1]起源于20世纪末。1996年,P. Kocher等
提出了Timing Attack,运用此项技术攻破了RSA公钥
体系、Diffie-Hellman密钥交换协议的加密系统。该

方法通过分析时间的信息泄露来得出密钥,是出现的
最早的SCA攻击。随着技术的发展,近几年将人工智
能技术应用到侧信道攻击里面,增强了侧信道攻击的
破解效率,节省了更多人力物力。在攻击方面有很多
的对抗侧信道的方法,包括硬件方面和软件方面。硬
件方面比如重新对电路的逻辑单元进行设计;算法方
面的话主要是加入随机掩码,使真实功耗和理论功耗
相关性变弱。机器学习的发展对侧信道起到了重要作

收稿日期:2021-04-08

修回日期:2021-08-12

基金项目:2018年国家重点研发计划项目(2018YFB2100200)

作者简介:何利文(1968-),男,博士,教授,研究方向为网络、信息安全、云计算大数据分析与应用;通信作者:安 聪(1996-),男,硕士研究生,研究方向为信息安全。

用,因此该文首先介绍侧信道的发展;然后介绍其分类,先对其进行整体分类,再根据不同的指标对其进行详细的分类说明;接着介绍侧信道攻击在人工智能方面的应用,包括结合深度学习还有机器学习等,还分析了各种模型成功率还有经典模型和人工智能模型的对比。

1 侧信道攻击发展介绍

侧信道分析(side-channel analysis, SCA):通过加密软件或硬件运行时产生的各种泄漏信息获取密文信息。

1997年,D. Boneh等^[2]最先提出了Fault Attack。主要思想是采用物理手段,攻击加密设备,让它运行的时候出问题,最后根据错误的信息更改算法结构,然后对算法逻辑进行分析,最后得出密钥。主要的物理方法有:电压变化、光辐射、低温、电磁辐射等。自此以后,故障攻击有了新的进步,在攻击范围上做了优化,使得范围变大了。鉴于它的攻击方式特殊,所以它逐渐成熟,通过不断的发展,成为一项新技术。

之后两年,P. Kocher等第一次将功耗攻击的想法运用到侧信道攻击中。主要原理是:CPU执行不同指令的时候会有不同的功耗特征,这是因为不同的指令触发的半导体数量不同,有的指令还会访问内存、缓存等等,有的复杂的指令需要的时钟周期(clock cycles)比别的指令要长,各种各样的因素会导致不同的指令执行的时候会产生不同的功耗特征。P. Kocher等在很多文献中研究了关于智能卡功耗的内容,最终总结出其中的系统不能抵抗功耗攻击。根据功耗分析方法的不同,功耗攻击主要有如下两类:

和系统有关的能量消耗和处理器的执行不同的命令有关联,算法的不同模块对应的能量消耗也不一样。正因为这个原因,攻击者可以猜测出对应的命令,最终破解密码。称为简单功耗分析^[3],另一类经过大量数据曲线分析,最后而得出密钥,包括差分功耗、相关系数功耗^[4]、方差功耗分析,这些方法都属于这一类攻击范畴。CPA有很多优点:如容易操作,效果显著,所以大家都比较青睐这种方法,慢慢的成为一种很常见的功耗方法。功耗分析方法在AES、DES、RSA这几种加密方法中的应用是比较成熟的。

21世纪,侧信道攻击技术有了新的发展,然而侧信道信息收集设备也随之发展起来,产生了新类型的攻击方法:Electromagnetic Analysis。这种分析方法通过采集加密时产生的电磁辐射来分析出密钥,优点:噪音小、效果显著。

2002年,C. Suresh等^[5]提出了Template Attack。模板的思想首次被使用,对密钥经过模拟收集,创建功

耗曲线数据库,接下来让真实的功耗曲线和数据库中的比较,根据最相似的分析出密钥。这种思想的优点是需要真实功耗曲线量少,在效率方面也很高。

2004年Eric Brier等^[6]在CHES会议上提出了CPA;2008年大会决定DPA比赛,第一届比赛由法国举办,这次比赛为相关的技术提供了一个平台。

最近侧信道在很多方向有进一步的探索发现,主要有以下方面:

(1) 信息预处理。

在收集相关信息的时候,如果不是很准确或者噪声太多,会对最后成功率有很大影响。

所以只有收集到准确的侧信道信息才能更快地得到密钥。然而实际操作中有很多不是想获取的信息比如噪音等,结果会导致曲线和时间对不齐,最终不能得出密钥。这就需要在正式开始前对收集的信息进行处理。Jip Hogenboom等^[7]在2010年提出了一种数学方面的统计方法—主成分分析,这种方法对最开始收集的曲线信息进行处理,处理完后降低曲线维度,提高了攻击效率。

(2)模型分析。CPA的思想最早在2004年被提出,它通过计算真实功耗和理论功耗的相关性,分析出密钥。后面对这种方法的研究比较重视。2009年,Emmanuel Prouff等^[8]提出了互信息分析方法,这种方法主要是通过分析真实功耗和理论功耗的互信息,破解密钥;Yuichi Komano等提出了BS-CPA方法,其在分析的时候是通过不断迭代来实现的,每次得出一个子密钥,这样就可以带入下一轮然后进行分析,最终能使信噪比有所降低;2010年,Youssef Souissi等人构建了主成分分析法的一个新应用模式,正确密钥区分器。

(3)高阶功耗。研究者对侧信道攻击做了深入研究,提出了很多关于抗侧信道的方法,比较有名的是高级功耗方面的进展。

(4)复合式攻击。这种方法是一种将好多种方法柔和在一起的方式。有密码学和侧信道攻击的结合;不同类型SCA方法的结合;蔡泽明等^[9]在2014年提出了一种新的基于代数表达式功耗模型的差分功耗分析攻击方法,对功耗曲线样本量由以前的很多到现在只需少量,而且没有增加时间复杂度,提高了攻击效率。

2 侧信道攻击分类

侧信道分析方法可以分为四大类^[10]:简单侧信道分析(simple side-channel analysis, SSCA)、差分侧信道分析(different side-channel analysis)、相关侧信道分析(correlation side-channel analysis, CSCA)等。

侧信道攻击有两种分类:

第一种攻击可以根据是否对芯片造成物理损坏,分为入侵、非入侵、半入侵三类。入侵方法是对内部设计进行了解,之后采取措施。例如,检测芯片内部互联线的数据变化,或者直接读内存的内容。包括探测攻击(probing attack)、逆向版图提取分析(reverse engineering, layout extraction and analysis)。非入侵攻击不需要解剖芯片而是通过检测芯片工作时从外部表现出的特征进行分析,包括运行时间(timing)、电流(current)、电磁辐射等。Skorobogatov 和 Anderson 发明了半入侵攻击:需要了解芯片内部信息,但是不用都拆开,也不用操作金属表面。

第二种攻击根据是否干扰芯片正常运行分类有主动和被动两种。第一类主要是通过让设备不能正常运行,最常见的就是故障攻击了。第二类就是我们比较熟悉的简单、差分等功耗方法。

还有一些常用的能量攻击,如简单功耗攻击、差分功耗^[11]攻击、CPA(connection power analysis)攻击和模板攻击^[12]等。

SPA攻击(简单功耗分析):设备的功耗和算法执行的不同指令有关。在加密算法运行的时候,采集芯片功耗,然后通过推断可以猜测到数据命令和操作的关系,进而分析出密钥。通过这种攻击方法获得密钥,需要对芯片设备足够了解,才能判断所对应的操作进而发现特征。对于算法加密细节,这种方法效果更好,比如数据加密标准和公钥加密。SPA显示了乘法和平方运算的差异,所以能用于恢复RSA的密钥。SPA还能得出DES算法实现中的置换和移位产生的能量差异,最后得出DES算法的密钥。这种方法有一个缺点就是,当防御技术变强的时候,比较难破解,必须结合别的方法进行攻破。

DPA:加密设备在运行的时候会有不同的命令被执行,每个命令产生的功率也会相应变化,可以用特殊的仪器和一些数学方法来分析这些信息。它是通过电流的前后变化来进行分析的,和上面一种攻击方法不一样,这种方法不要求对设备很了解,但要收集很多更好的曲线来分析。当实际操作时要有加密设备,实际上收集的曲线有很多噪声,主要有内、外部噪声,算法噪声^[13]。与功耗能量相比,本征和量化噪声很小,当然也有减少噪声的方法,比如使用测量设备;DPA策略能有效减少算法方面产生的噪声。

当然也可以通过增加功耗曲线数减少DPA中产生的噪声,既可以在时域进行也可以在频域来分析。主要是通过电流电压的变化分析出最终密钥。

CPA:在DPA上进行了一定的优化,当然也是要提前猜测密钥的,之后计算理论功耗和实际功耗的相关性,后面就是对所有猜想进行同样计算,如果存在一

条曲线,在某时的相关系数比别的要高,此条曲线对应的就是正确密钥。

模板攻击:通过计算两者的相关值来验证猜测密钥的正确性,最后得出密钥。CPA是常用的功耗攻击方法。模板攻击和功耗攻击不同,它需要攻击者准备一个设备,该设备应该和被攻击设备相似,用它来采集功耗,之后提取特征,最后构建模板。它和机器学习模型训练差不多。之后就能进行模板匹配了,多数情况下一次只能得到部分密钥。对于使用汉明重量这种模型,需要很多能量迹的从而减少密钥空间,最后得出密钥。

最近几年也兴起了一些较新奇的SCA方法。碰撞攻击利用不同明文产生碰撞,进行关系推导,最后得出密钥。随后人们将密码学与SCA结合,提出了代数侧信道分析,把两者的优点结合,使SCA攻击范围变大。攻击方法越来越成熟,大家对密码设备很重视,有很多防御方面的技术被提出,例如在算法执行时加入时延、对加密过程中的中间值加入掩码。攻击方法也出现了很多,针对加入时延的可以采用傅里叶变换,对于加入掩码的可以用高阶DPA^[14]。

3 侧信道攻击在人工智能方面的分析

近年来,基于深度学习的SCA吸引了许多研究者。Maghrebi等人在2016年首次将深度学习应用于侧信道攻击。2017年,Cagli等人^[15]提出了一种基于卷积神经网络的建模类攻击方法,这种方法对轨迹要求很低,可以不预先进行处理,对特征点的选取要求也不高。而且他们将数据增强的方法运用到CNN中,提高了网络的性能。2019年,Robyns等人提出了一种新的相关优化方法,这种方法在电磁轨迹^[16]中选择有用的泄漏样本,然后将它看作是优化问题,然后进一步改进该方法。

机器学习^[17]已经运用到能量分析中,且成效很好,对侧信道有深远影响。再后面,深度学习开始和密码学相结合,为侧信道攻击提供了新思路。机器学习在信号多分类上和深度学习是有区别的:是否需要人的参与。

神经网络是人工智能研究领域的一部分,现在流行的是深度卷积神经网络,虽然卷积网络存在浅层结构,但因为准确度等一些原因,很少使用。学术界和工业界说的CNN和CNNs一般都是深层的。它可以从大规模数据里面学习,可以把结果向同类型数据泛化。它包含卷积层、池化层,在图像处理领域有不错的效果。CNN有一个很好的特性就是平移不变,因为它使用了二种方法,池化和权重共享。所以它在训练功耗曲线时,如果存在曲线没有对齐的情况,它也能很好的

学习和训练。

深度学习^[18]慢慢地渗入侧信道技术中,对解决侧信道方面的技术问题提供了新思路。Template attack^[19]介绍了一种新型类模板攻击方法,主要用了深度学习的思想,搭建卷积神经网络之后对模型验证。第一种是没有加掩码的 AES 的功耗信息,第二种是加入随机掩码的 AES 的信息。将 SVM 攻击和第一种卷积神经网络作比较发现,SVM 的成功率是较高的,但是时间复杂度也相应提高了。比基于 CNN 模型高几百倍。图 1 是 CNN 模型对 RSM 掩码方案^[20]的破解,以 offset 值为假设中间值计算与功耗曲线相关系数,选择那种相关系数高的特征点,使用 CNN 多分类模型把 Offset 功耗曲线值分成 16 类。将数据集分为测试和训练两种。

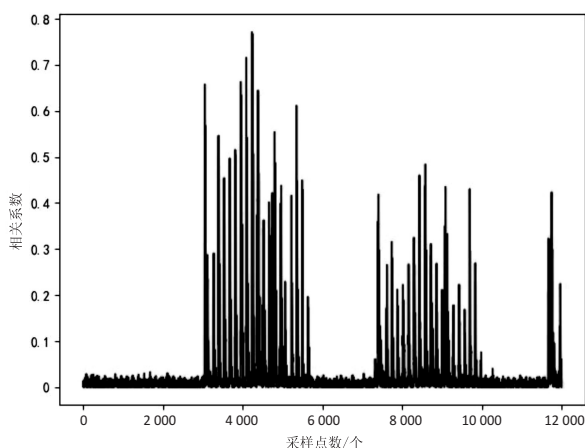


图 1 Offset 值与功耗曲线的关系

文献^[21]公开了一组具有不同程度抖动防御的侧信道数据集 ASCAD。该数据集是 AES 加掩码算法实现的一种电磁信号泄露数据。

它选用没有加入掩码的 S 盒的输出为攻击点,之后对感知器和 CNN 做了完整测试。

其采用的方法是通过实验对比逐一发现神经网络超参数的最佳值,在每一个超参数寻优的实验研究中,其余超参数均保持不变。但神经网络超参数很难找,是因为超参数的最佳会受到别的超参数的影响,不存在独立的最佳超参数。只有对所有的参数进行遍历才能发现最合适的组合,因为超参数很多所以实验的代价是非常大的。事实上,根据实验研究,依据简单的原则设计的卷积神经网络也会具有 CNN-best 的攻击效果。

CNN-best 结构:每一层的 filte 分别是 64, 128, 256, 512, 512, 每一层采用 relu 函数和平均化函数。它有很多参数,在卷积神经网络里面,参数越多,越容易有过拟合的情况发生。过拟合是指训练误差和测试误差之间有很大差距,换句话说就是模型复杂度高于实

际问题,模型在训练集上表现好,但在测试集上表现差。从侧信道的各个研究方向来看,深度学习技术^[18]在每个领域都有不错的发展,尤其是和模板有关的在人工智能技术的引导下,后面又加入大数据分析,让侧信道可以发展得更好。这种模型建立类攻击需要从设备中采集能量迹,这种设备必须和目标设备类似,这是 CNN 技术在侧信道领域应用的前提条件。多层感知机在运用到侧信道领域后,基于神经网络的侧信道攻击方法出现了很多,部分侧信道数据集也慢慢地在网络上开放,使得基于深度学习的模板攻击^[22]发展迅速。目前,得益于卷积神经网络在能量迹足够、特征数量多的前提下处理能力强,所以基于卷积神经网络侧信道攻击方面还是做了很多研究。但在能量迹预处理 CNN 方面的研究很少,尽管这方面研究很少,但文献^[23]提出了一种基于卷积神经网络的能量迹预处理方案。它是利用 Sinc 卷积层和传统卷积层构建 Sinc-CDAE^[24],然后通过能量迹估计算法获得足够的数据来训练。而且能量迹可以在自动滤波后获取,这种方法在非失调能量迹上的攻击效果是很好的。作为对比,实验设计了一个具有 4 个卷积层,3 个平均池化层和 1 个全连接隐层、1 个输出层的神经网络。该网络参数数量只有 CNN-best 的 80%。证明验证集精度与训练集精度同步上升。

对于模板攻击来说,传统的模板攻击有如下步骤:确定信息泄露位置还有提取相关信息。之后进行模板创建。选择合适的模板。这种攻击方法的成功率和创建模板的质量有关系,当然还有一些别的因素如曲线数量也至关重要。选择最合适的模板。

模型的成功率都是随着功耗曲线的增多在不断增长,因为模板不一样,成功率波动也很大。PCA-SVM 主要依赖于功耗曲线数目,而经典模板攻击的依赖较小;SVM 多分类在前期对功耗曲线数依赖性很大,当功耗曲线达到一定数量时,分类成功率相对稳定;CNN 模型对功耗曲线数的依赖情况和 SVM 基本相同。总结一下就是,信号特征和功耗曲线数目成正相关,当然对于模板攻击基本上没影响。SVM 模型在有些情况下达不到很好的效果,比如采集的功耗曲线比较少的时候,当然了如果数量足够多,就和该因素相关性不是很大了。CNN 模型和机器学习模型有相似的地方。

从表 1 可以看出,基于 CNN 的时间复杂度最小,SVM 模型的是最大的。在特征点数目一样的情况下,CNN 所需时间和功耗曲线数都是比较少的,体现了它可以在少样本情况下训练出更好的模型。使用很少的参数就能代表高级的函数,这是多层的优点。CNN 的本质是一个多层复合函数,和普通的神经网络不同的

是它的某些权重参数是共享的,训练时依然采用反向传播算法来学习更有用的特征,从而提升了分类的准确性。

表 1 CNN 攻击方法和其他方法的对比

比较项目	经典模板	SVM	CNN
功耗曲线数	15 000	2 000	4 500
特征点数	621	621	621
运行时间/h	8	8	0.5

如图 2 所示,卷积神经网络模型迭代大概 50 次的时候就可以达到模型最优解。较传统的模板攻击和机器学习,这种模型在训练的时候收敛速度比其他模型快,模型的时间和空间复杂度都较低,所以对于高维度的数据集在处理方面有不错的效果。

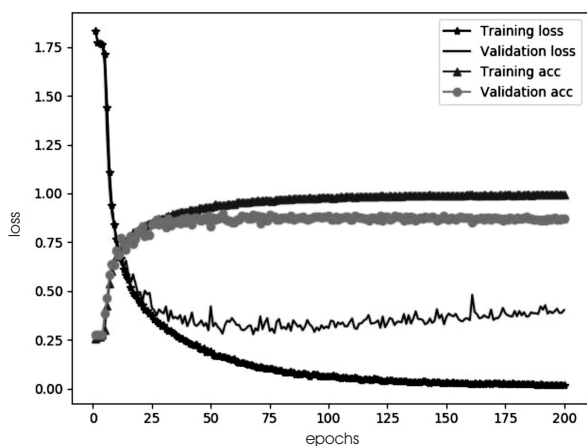


图 2 CNN 模型损失函数和算法攻击准确率

基于主成分分析特征提取的 SVM 分类,它的特征提取算法在时间和空间复杂度上都是优于相关系数提取算法的。因为贝叶斯概率模型计算起来十分复杂,它的时间和空间复杂度也大,在实践攻击的时候效果不是很好。

深度学习应用在侧信道领域^[25],是符合当前技术趋势的,借助模型训练,可以更好地进行攻击,选择最合适的攻击方法,这方面的研究也越来越多。Housseem Maghrebi 和 Thibault Portigliatti 等人的研究内容主要是通过机器学习提出新的攻击方法。但是他们的实验是在具体的环境里面实现的,相比于传统的模板攻击机器学习方法还是不错的。传统模板攻击在同样情况下模板匹配准确率较低。这是因为其对功耗特征精确刻画效果差,对功耗曲线的数量有很大依赖。因为各大高校和科研机构对人工智能的贡献,机器学习和深度学习这两种技术在安全方向也越来越受欢迎。

4 结束语

该文对侧信道攻击技术进行了全面的分析,首先

从其发展历史开始介绍,阐述了其详细发展过程及发展过程中的技术进步;对侧信道攻击技术有了一定了解之后,接下来对其分类,按照攻击手段是否破坏物理损坏芯片,将其分为入侵、非入侵、半入侵三种;按照是否干扰芯片正常运行分类,将其分为主动(active)和被动(passive)两种;最后阐述了侧信道攻击和人工智能的结合,基于深度学习的知识,结合算法优化还有各种新的数据集的推出,让侧信道攻击在破解加密算法方面效率更高。

机器学习算法和上述的模板分析有类似的地方,它们都由学习和测试构成。在处理分类和回归算法方面机器学习是比较有优势的,人工智能算法通过对数据训练,通过训练得出的结论来对接下来的数据处理,模板分析和这个过程是有点像的。

算法方面,大数据分析、机器学习甚至深度学习都是不错的方法,从而建立更为有效的分析模型,可以为后面的进一步研究奠定基础。在攻击方面,在这个信息安全的时代,保护好个人信息也尤为重要,所以在对攻击有研究的同时,也需要对防御方面采取一定措施,比如之前的固定值掩码、RSM 掩码等都是保护加密算法不被侧信道攻击的,后面也希望有更多的防御方面的研究者投入这方面的研究,这将是一个新的方向。

信息安全是国家发展的后盾,所以,无论是软件或硬件,都应该对密码算法进行优化,使得信息被更好地保护。所以,不仅要在传统密码学方面做深入研究,更应结合新技术如侧信道来增强自身防御力。

参考文献:

- [1] KOCHER P, JAFFE J, JUN B. Differential power analysis [C]//Advances in cryptology – crypto: 1999. [s. l.]: Springer-Verlag, 1999: 388–397.
- [2] MARTINASEK Z, ZEMAN V. Innovative method of the power analysis [J]. Radio Engineering, 2013, 22 (2): 586–594.
- [3] 成 为, 谷大武, 郭 箬, 等. 一种针对 RSA-CRT 的功耗分析攻击方法 [J]. 通信技术, 2011, 44 (6): 123–125.
- [4] 蔡泽民, 王 奕, 李仁发. 基于代数表达式功耗模型的差分功耗分析攻击 [J]. 计算机应用, 2014, 34 (2): 448–451.
- [5] ZHUANG Z, CHEN J, ZHANG H. A countermeasure for DES with Both rotating masks and secured s-boxes [C]//2014 tenth international conference on computational intelligence and security (CIS). Kunming, Yunnan, China: IEEE, 2014: 410–414.
- [6] FEI Y, LUO Q, DING A A. A statistical model for DPA with novel algorithmic confusion analysis [M]//Cryptographic hardware and embedded systems – CHES. Berlin: Springer, 2012: 45.
- [7] 易 涛. 入侵检测中神经网络及 D-S 理论的研究 [D]. 成

- 都:成都理工大学,2006.
- [8] 庞 贝,刘飞帆. 集众智,造“中国芯”[J]. 科技创新与品牌,2013(5):66–67.
- [9] 涂 皓. 基于旁路分析的硬件木马设计实现[D]. 长沙:国防科技大学,2010.
- [10] 刘长龙. 基于侧信道分析的硬件木马检测技术研究[D]. 天津:天津大学,2013.
- [11] LIU P C, CHANG H C, LEE C Y. A true random-based differential power analysis countermeasure circuit for an AES engine[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2012, 59(2):103–107.
- [12] CHOUDARY O, KUHN M G. Efficient template attacks [C]//International conference on smart card research & advanced applications. Berlin, Germany: Springer, 2013: 253–270.
- [13] YAROM Y, FALKNER K. FLUSH+RELOAD: a high resolution, low noise, L3 cache side-channel attack [C]//Proceedings of the 23rd USENIX conference on security symposium. Vancouver: USENIX, 2014: 719–732.
- [14] 童元满, 王志英, 戴 葵, 等. 一种抗 DPA 及 HO-DPA 攻击的 AES 算法实现技术[J]. 计算机研究与发展, 2009, 46(3): 377–383.
- [15] PICEK S, HEUSER A, JOVIC A, et al. Climbing down the hierarchy: hierarchical classification for machine learning side-channel attacks [C]//International conference on cryptology in Africa. Dakar, Senegal: Springer, 2017: 61–78.
- [16] PEETERS E, STANDAERT F X, QUISQUATER J J. Power and electromagnetic analysis: Improved model, consequences and comparisons[J]. Integration, the VLSI Journal, 2007, 40(1): 52–60.
- [17] LERMAN L, POUSSIER R, BONTEMPI G, et al. Template attacks vs. machine learning revisited (and the curse of dimensionality in side-channel analysis) [C]//Constructive side-channel analysis and secure design. Berlin, Germany: Springer, 2015: 20–33.
- [18] MAGHREBI H, PORTIGLIATTI T, PROUFFE. Breaking cryptographic implementations using deep learning techniques [C]//Security, privacy, and applied cryptography engineering. Hyderabad, India: Springer, 2016: 3–26.
- [19] RAVANELLI M, BENGIO Y. Speaker recognition from raw waveform with SincNet [C]//Proceedings of 2018 IEEE spoken language technology workshop (SLT). Athens (GR): IEEE, 2018: 1021–1028.
- [20] 于 赛. 基于分组密码算法的侧信道分析与实现[D]. 成都: 电子科技大学, 2015.
- [21] AGRAWAL D, RAO J R, ROHATGI P, et al. Templates as master keys[J]. Lecture Notes in Computer Science, 2005, 36(59): 15–29.
- [22] ARCHAMBEAU C, PEETERS E, STANDAERT F X, et al. Template attacks in principal subspaces [C]//Cryptographic hardware and embedded systems – CHES. Yokohama, Japan: Springer, 2006: 1–14.
- [23] GIERLICH B, LEMKERUST K, PAAR C. Templates vs. stochastic methods [C]//Proceedings of the workshop on cryptographic hardware and embedded systems (CHES06). Yokohama: [s. n.], 2006: 70.
- [24] BENADJILA R, PROUFF E, STRULLU R, et al. Study of deep learning techniques for side-channel analysis and introduction to ASCAD database [J]. Journal of Cryptographic Engineering, 2020, 10: 163–188.
- [25] ZHOU W H, KONG F T. Electromagnetic side channel attack against embedded encryption chips [C]//2019 19th IEEE international conference on communication technology. Xi'an: IEEE, 2019: 30.
- +++++
- (上接第 78 页)
- generative adversarial networks for small object detection [J]. arXiv:1706.05274, 2017.
- [15] 朱张莉, 饶 元, 吴 渊, 等. 注意力机制在深度学习中的研究进展[J]. 中文信息学报, 2019, 33(6): 1–11.
- [16] JADERBERG M, SIMONYAN K, ZISSERMAN A. Spatial transformer networks[J]. arXiv:1506.02025, 2015.
- [17] WANG Fei, JIANG Mengqing, QIAN Chen, et al. Residual attention network for image classification[J]. arXiv:1704.06904, 2017.
- [18] EVERINGHAM M. The PASCAL visual object classes challenge (VOC2012) [EB/OL]. [2021-06-21]. <http://pascal-voc2012.eecs.soton.ac.uk/challenges/VOC/voc2012/index.html>.