密码产品的侧信道分析与评估

陈 华*①② 习 伟③ 范丽敏① 焦志鹏①④ 冯婧怡①④

①(中国科学院软件研究所可信计算与信息保障实验室 北京 100190)

②(密码科学技术国家重点实验室 北京 100878)

③(南方电网科学研究院 广州 510663)

④(中国科学院大学 北京 100049)

摘 要：作为一类重要的信息安全产品，密码产品中所使用的密码技术保障了信息的保密性、完整性和不可抵赖性。而侧信道攻击是针对密码产品的一类重要的安全威胁，它主要利用了密码算法运算过程中侧信息(如时间、功耗等)的泄露，通过分析侧信息与秘密信息的依赖关系进行攻击。对密码产品的抗侧信道攻击能力进行评估已成为密码测评的重要内容。该文从攻击性测试、通用评估以及形式化验证3个角度介绍了目前密码产品抗侧信道评估的发展情况。其中攻击性测试是目前密码侧信道测评所采用的最主要的评估方式，它通过执行具体的攻击流程来恢复密钥等秘密信息。后两种方式不以恢复秘密信息等为目的，而是侧重于评估密码实现是否存在侧信息泄露。与攻击性测试相比，它们无需评估人员深入了解具体的攻击流程和实现细节，因此通用性更强。通用评估是以统计测试、信息熵计算等方式去刻画信息泄露的程度，如目前被广泛采用的测试向量泄露评估(TVLA)技术。利用形式化方法对侧信道防护策略有效性进行评估是一个新的发展方向，其优势是可以自动化/半自动化地评估密码实现是否存在侧信道攻击弱点。该文介绍了目前针对软件掩码、硬件掩码、故障防护等不同防护策略的形式化验证最新成果，主要包括基于程序验证、类型推导及模型计数等不同方法。

关键词：密码产品；侧信道；信息泄露；形式化验证

中图分类号：TN918; TP309 **文献标识码**：A **文章编号**：1009-5896(2020)08-1836-10

DOI: 10.11999/JEIT190853

Side Channel Analysis and Evaluation on Cryptographic Products

CHEN Hua①② XI Wei③ FAN Limin① JIAO Zhipeng①④ FENG Jingyi①④

①(*TCA Laboratory*, *Institute of Software*, *Chinese Academy of Sciences*, *Beijing* 100190, *China*)

②(*State Key Laboratory of Cryptology*, *Beijing* 100878, *China*)

③(*Electric Power Research Institute*, *China Southern Power Grid*, *Guangzhou* 510663, *China*)

④(*University of Chinese Academy of Sciences*, *Beijing* 100049, *China*)

Abstract: As a kind of important information security products, the cryptographic technique adopted by cryptographic products guarantees the confidentiality, integrity and non-repudiation of information. The side channel attack is an important security threat against cryptographic products. It mainly utilizes the leakage of side information (such as time, power consumption, etc.) during the operation of cryptographic algorithm, and attacks by analyzing the dependence between side information and secret information. It has become an important test content to evaluate the ability of cryptographic products to defend against the side channel attack. The development of side channel evaluation of cryptographic products is introduced from three aspects of attack test, general evaluation and formal verification. The attack test is the most popular way adopted in side channel evaluation, which aims to recover the secret imformation such as the key by executing specific attack process. The latter two methods are not for the purpose of recovering secret information, but focus on assessing whether there is any side information leakage in the cryptographic implementation. They are more

收稿日期：2019-11-01；改回日期：2020-06-05；网络出版：2020-07-07

*通信作者： 陈华 chenhua@tca.iscas.ac.cn

基金项目：国家重点研发计划(2018YFB0904900, 2018YFB0904901)，十三五国家密码发展基金(MMJJ20170214, MMJJ20170211)

Foundation Items: The National Key R&D Program of China (2018YFB0904900, 2018YFB0904901), The National Cryptography Development Fund of China (MMJJ20170214, MMJJ20170211)

general than the attack test because they do not require the evaluator to go into the details of the attack process and implementation. The general evaluation is to describe the degree of information leakage by means of statistical test and information entropy calculation. For example, Test Vector Leakage Assessment (TVLA) technology is widely used at present. The formal method is a new development direction to evaluate the effectiveness of side channel protection strategy which has the advantage that it can automatically/semi-automatically evaluate whether the cryptographic implementation has side channel attack vulnerability. The latest results of formal verification for different protection strategies such as software mask, hardware mask and fault protection is introduced in this paper, mainly including program verification, type inference and model counting.

Key words: Cryptographic product; Side channel; Information leakage; Formal verification

1　引言

密码技术可以保障信息产品的保密性、完整性和不可抵赖性。所有利用密码技术的信息安全产品均可称为密码产品，如加密卡、智能密码钥匙、加密机、加密网关等。显然，安全性是密码产品最为重要的产品属性，任何针对它的安全威胁都可能对整个密码应用系统造成严重影响，从而可能引起个人隐私数据泄露、欺骗交易、数据篡改以及系统瘫痪等不良后果。影响密码产品安全性的因素有很多，无论是底层密码算法设计缺陷还是密码实现漏洞，均可导致密码产品被恶意攻击。其中侧信道攻击就是一类基于密码实现漏洞而发起的攻击方法。与其它方法相比，侧信道攻击具有攻击力度大、代价低、通用性强等优点，因此一经提出就引起了学术界、工业界和测评界的广泛关注。

侧信道攻击主要利用了密码算法运行过程中出现的各类信息泄露，通过分析信息泄露与秘密信息之间的数据依赖关系来恢复秘密信息，如密钥信息。按照泄露信息的不同表现形式，广义的侧信道攻击主要包括计时攻击[1]、能量攻击[2]、电磁攻击[3]以及故障攻击[4]等等。根据攻击对目标对象的物理破坏程度来分，侧信道攻击又可分为非侵入式攻击、半侵入式攻击和侵入式攻击[5]。非侵入式攻击不会对目标模块有任何物理接触，主要通过获得密码运行时间、能量信息以及电磁辐射等信息来进行攻击。半侵入式攻击会对密码产品做一定的物理处理，如对密码芯片去除封装，暴露其金属层，然后通过激光、电磁等手段干扰芯片运行并进行攻击。侵入式攻击对密码产品的破坏程度最大，通常会通过探针等形式去直接获取存储内容和密钥信息。

由于侧信道攻击对密码产品带来的广泛安全威胁，对密码产品的抗侧信道攻击能力进行评估已成为密码测评的重要内容。美国国家标准技术研究所NIST发布的密码模块安全标准FIPS140-3[6](也即ISO/IEC 19790[7])以及我国发布的GM/T 0028-2014《密码模块安全技术要求》[8]、GM/T0008-2012《安全芯片密码检测准则》[9]等已将抗侧信道攻击能力作为重要的测评依据。在FIPS140-3标准规范中，密码模块被分为4个等级，不同的等级对抗侧信道能力有不同的评估标准。等级越高，抗侧信道攻击能力评估要求越高。FIPS140-3将密码模块的安全性测试分为11个安全域，其中物理安全(physical security)和非侵入式攻击评估(non-invasive attacks)安全域主要涉及到了密码模块抗侧信道评估。物理安全主要考虑了密码模块对于半侵入式或侵入式攻击的保护。对于安全等级2级及以上的密码模块，物理安全方面要求显示拆卸的证据；对于安全3级以上的密码模块，需要提供对于温度和电压的异常保护；对于安全4级的密码模块，则要求提供对错误注入的保护。除此之外，对于抗非侵入式攻击的评估则是针对所有安全等级的，主要包括能量分析、计时分析以及电磁分析。我国发布的密码模块安全性检测技术要求《GM/T0028-2014》中关于抗侧信道攻击方面的评估要求和FIPS140-3是一致的。此外，GM/T0008-2012《安全芯片密码检测准则》主要分为3个安全等级，也要求密码芯片具有抵抗侧信道攻击的能力，主要包括对计时攻击、能量攻击、电磁攻击以及故障攻击的防护能力。表1给出了不同密码测评标准对密码产品抗侧信道防护的不同要求。

目前针对密码实现的侧信道评估形式中主要有3种类型，第1种是基于攻击的评估方法，即主要以各类物理攻击手段试图获取密钥或秘密参数信息，或者达到控制参数、扰乱执行流程等目的。该方法攻击性最强，评估力度最大，但很大程度依赖于具体的实现方式和设备特点。第2种评估方式不关注具体的攻击方法，而是判断密码实现是否存在某种秘密信息泄露。如果存在泄露，密码实现则被认为是不安全的。该类方法主要通过统计测试、信息熵等方式进行评估。该方法往往对实现方式和设备等信息依赖程度较低，因此通用性更强。第3种是利

表 1 密码测评标准中的抗侧信道防护要求比较

测评标准		FIPS140～3(1～4级)	GM/T0028(1～4级)	GM/T0008(1～3级)
非侵入/半侵入式	能量	1～4级	1～4级	2～3级
	计时	1～4级	1～4级	2～3级
	电磁	1～4级	1～4级	2～3级
	温度	3～4级	3～4级	2～3级
	电压	3～4级	3～4级	2～3级
	错误注入	4级	4级	3级
侵入式		2～4级	2～4级	2～3级

用形式化分析的方法对密码实现的抗侧信道攻击能力进行验证。该方法可以自动化/半自动化地评估密码实现的侧信道攻击脆弱点。以上3类方法没有严格的对应关系，因此在实际的密码产品测评中可以互为补充加以使用。下面将以能量攻击和故障攻击为例介绍下这3种评估方式，因为在所有的侧信道攻击中，能量攻击和故障攻击是两类使用最为广泛的侧信道攻击方法，评估方法和形式也最为丰富和多样化。

2 侧信道攻击测评

侧信道攻击测试是利用目前已有的侧信道攻击流程对密码产品进行攻击，如攻击成功，则说明密码产品没有达到安全要求，这也是目前密码测评主要采用的评估手段。

2.1 能量攻击测试

能量攻击属于非侵入式侧信道攻击方法，它是利用密码产品运行过程中泄露出的功耗信息进行攻击的一种方法，密码产品运行中的某一时刻功耗可以表示为[5]

$$P_{\text{total}=}P_{\text{op}}+P_{\text{data}}+P_{\text{el.noise}}+P_{\text{const}} \tag{1}$$

总的功耗主要由操作相关的功耗P_{op}、数据相关的功耗P_{data}、功耗测量时的电子噪声$P_{\text{el.noise}}$以及与操作、数据无关的常量能量消耗P_{const}组成，能量攻击正是利用功耗与敏感信息的依赖关系来分析获得密钥或其它秘密信息。最主要的能量攻击方法[2]包括简单能量分析方法(Simple Power Analysis, SPA)和差分能量分析方法(Differential Power Analysis, DPA)。FIPS140-3, GM/T0028-2014以及GM/T0008-2012等标准规范都明确要求密码产品需要具有抵抗这两种攻击的防护措施。简单能量分析方法的基本思想是，能量迹的轮廓与密码操作、密钥信息等之间如果存在直接简单的依赖关系，分析者可以通过观察能量迹就可以直接判断出加密轮数、密钥比特等信息。差分能量分析方法主要利用了密码运算中间值不同取值下的功耗差值在正确密钥假设下最为显著的特征，通过该特征可以筛选出正确密钥。相关能量分析(Correlation Power Analysis, CPA)[10]可以认为是差分能量分析的一种更为通用的攻击方法，它通过采集密码运算中间值的功耗曲线，然后计算假设密钥值下的预期曲线值，通过计算预期曲线值和实际曲线之间的相关性来筛选真实的密钥值。互信息分析(Mutual Information Analysis, MIA)[11]以猜测密钥对应的假设中间值和采集的功耗曲线的互信息作为区分器来进行正确密钥的猜测，其不需要将假设中间值映射为假设功耗值，具有更强的通用性，可以对功耗模型未知的设备进行能量分析。

以上介绍的攻击方法都属于Non-profiled攻击类别，即攻击者不需要额外拥有一台与攻击设备一样的设备进行数据建模，而是直接对攻击设备进行功耗采集并分析获得秘密信息。而Profiled攻击则需要攻击者拥有与攻击目标设备一样的训练设备，并且可以控制密码设备的运行情况，如可以任意选择明文和密钥。因此攻击者可以精确地建立密码运行信息泄露特征。在随后的攻击阶段，攻击者可以通过对两个设备的特征匹配来恢复出目标设备的密钥信息。最典型的Profiled攻击是模板攻击方法(Template Attack, TA)[12]。模板攻击包含模板构建和模板匹配两个步骤，首先对训练设备进行多元高斯分布特征建模，然后对攻击设备的实际采集功耗曲线进行高斯特征匹配，其中概率最大的即为正确密钥。与Non-profiled攻击相比，由于Profiled攻击假设最强，因此它的攻击力度也最大。

随着机器学习技术的发展，该技术也被用于能量分析中，并取得了不错的攻击效果。机器学习方法可以将能量攻击中的密钥恢复问题转化为分类问题，并且它本身的黑盒测试特性不需要密码实现满足任何数学分布假设，因此与传统能量攻击相比，它在许多场景下具有攻击力度更强、成功率更高、攻击复杂度更低等优点。初期的机器学习算法主要用了支持向量机、随机森林等算法[13,14]，研究表

明，这些算法在处理高维数据、小样本曲线量方面具有更大的攻击优势，另外在攻击一些防护实现的攻击效果还要优于传统的模板攻击、CPA或其组合形式。近年来，基于深度学习的能量分析技术更是得到了学术界与测评界的关注[15]。根据评估者是否拥有训练设备，基于机器学习的侧信道评估也分为Profiled攻击[15]和Non-profiled攻击[16]两类。虽然机器学习算法在很多攻击实例中展现出来了它的优势，但它仍然无法完全取代模板攻击等传统攻击方法。在实际检测中，需要根据具体的攻击条件去选择合适的攻击方式。

2.2 故障攻击测试

故障攻击是指利用一些物理手段对密码产品运行过程进行干扰，通过分析错误的运算结果来获取密钥信息。物理手段主要包括电压扰动、时钟注入、异常温度和激光注入等形式。目前的FIPS140-3等密码测评标准均要求产品应提供对电压、温度异常的防护措施。其中《安全芯片密码检测准则》中的安全3级要求密码产品提供对光攻击的防护能力。

依据故障注入对象的不同，故障攻击主要分为存储类和指令类两类攻击类型。存储类攻击是对存储算法中间运行结果或输入参数的存储器进行故障注入。存储器主要分为易失性存储区(如RAM)和非易失性存储区(如ROM和EEPROM)。存储类故障攻击会改变密码执行过程中的中间值、算法输入参数或系统参数。指令类故障注入针对的是指令执行控制部分，该类故障会导致指令被直接跳过或错误执行等。除此以外，还有一类故障类型是对算法数据处理过程进行故障注入，如在对存储器写过程中对传输总线进行故障注入，这会导致写操作失败而使得存储数据取值不变。

故障攻击在成功进行物理故障注入后，需要根据故障注入效果进行后期的密钥恢复。和能量攻击相比，故障攻击的密钥恢复方法更为复杂与多样化，更加依赖于被攻击算法的结构特点和实现细节。例如首个提出的故障攻击利用了CT-RSA算法的实现特点[4]，通过获得错误签名和正确签名可以得出私钥因子。而对于分组密码算法，目前最常用的故障分析技术为差分故障分析方法[17]，该方法利用了非线性部件S盒的差分分布性质，在获知正确密文和错误密文后，通过差分分析技术可以逐部分恢复出密钥信息。对于椭圆曲线来讲，针对签名算法标量乘的差分故障分析[18]则需要先猜测秘密指数部分比特的值，通过比较经过计算过的错误结果与实际错误结果是否一致来确定猜测比特是否正确。弱曲线攻击则是通过对基点注入若干比特的错误，使原曲线变为新的弱曲线，通过求解弱曲线上的ECDLP来获取秘密信息[18]。除此之外，格故障攻击也是针对椭圆曲线体制的一类重要的故障分析方法[19]，它是将格基约化算法用于故障分析过程中。其中最常用的格攻击模型是已知随机nonce k的部分比特值，则可通过求解格中最近向量问题来恢复签名中的私钥。此模型下的随机nonce k的部分比特值的获取可以通过直接进行故障注入(如部分比特清零)的方式，也可以通过组合其它类型的故障分析方法去获取，如差分故障分析或安全错误攻击。和能量攻击相比，故障攻击的攻击力度更强，所需的数据复杂度也很低(如针对分组密码算法的差分故障分析方法常常需要1～2次故障注入就会恢复出密钥)。但由于故障攻击的攻击条件相对比较强，故障注入精度很大程度影响了分析效果，因此尽管目前学术界已公开了很多种类的故障攻击方法，但在实际的密码评估过程所采用的方法仍十分有限。

3 基于信息泄露的通用评估

虽然攻击性测试是目前最主要的侧信道评估方式，但此种方式依赖于具体的攻击假设和攻击条件，因此存在着个体化、经验化、通用性差和评估周期长等问题。基于信息泄露的评估方式试图解决这些问题，它不以恢复密钥等秘密信息为目的，主要通过统计测试、信息熵评估等方式来判断密码运算过程是否存在某种秘密信息泄露。

3.1 基于能量攻击的通用评估

目前基于信息泄露的能量攻击通用评估技术主要包括基于t-test的TVLA(Test Vector Leakage Assessment)技术、基于χ^2-test的泄露评估技术以及基于深度学习的泄露评估技术。

2011年，第1个针对能量防护方案的通用评估方法被提出[20]。该方法不需要测试人员对于具体的能量攻击拥有额外的知识。2013年，上述方法被重新整理命名为测试向量泄露评估技术(TVLA)[21]。作为一个通用的能量评估技术，TVLA一经提出就得到了学术界和工业界的广泛重视。它利用了这样一个事实：能量攻击都是通过利用算法中间值泄露的敏感信息来进行攻击的，任何可造成统计特性上能量泄露的中间值计算都可能是潜在的攻击脆弱点。该方法利用了t-test技术评估待测设备特定采集的两组泄露曲线均值的差异性，从而判断是否有相应的秘密信息泄露，其统计量t按式(2)计算

$$t=\frac{X_{\mathrm{A}}-X_{\mathrm{B}}}{\sqrt{\dfrac{S_{\mathrm{A}}^2}{N_{\mathrm{A}}}+\dfrac{S_{\mathrm{B}}^2}{N_{\mathrm{B}}}}} \tag{2}$$

其中，A和B代表待测的两组功耗曲线，N_{A}和N_{B}表示两个集合的大小，X_{A}和X_{B}分别代表两组功耗曲线的均值，S_{A}和S_{B}分别代表两组功耗曲线的方差，将计算出的统计值和置信阈值相对比，超出阈值的样本点则认为出现了敏感信息的泄露。TVLA技术分为非特异性TVLA技术(non-specific TVLA)和特异性TVLA技术(specific TVLA)，其中非特异性TVLA技术使用固定和随机的两组明文，而特异性TVLA则要根据评估的运算部件专门设计明文。相比之下，非特异性TVLA技术因其简单高效、通用性强得到了更为广泛的应用。自从TVLA技术被提出以来，研究人员[22]针对该方法陆续开展了完善工作，旨在提高该方法的可靠性和实现性能。TVLA技术虽然具有简单高效、通用性等优点，但在实际评估过程中仍存在着一些问题[23]：首先是该方法简单地把评估曲线分为2组，而不是按照目标中间值的实际大小来分组(如S盒输出为4 bit，则通常需要16类分组的泄露情况)；其次是TVLA技术利用了简单的统计值构造形式来判断每一时刻是否存在泄露，这和一些信息泄露场景并不吻合(如门限实现中的高阶泄露场景)。以上问题会导致实际评估时出现假阳性或假阴性的测试结果。解决该问题需要将泄露曲线量大幅度地提高，因此很大程度降低了TVLA技术的实用性。

为了从原理上缓解TVLA技术存在的局限性，Moradi等人[23]提出了基于χ^2-test的评估方案。该方法将待测曲线集每一时刻的样本值存储为直方图的形式，记待测曲线集的数量为r，记录直方图的列数为c，第i个样本集第j列的频次为$F_{i,j}$，样本总数为N，其统计量T按照式(3)计算

$$T=\sum_{i=0}^{r-1}\sum_{j=0}^{c-1}\frac{\left(F_{i,j}-E_{i,j}\right)^2}{E_{i,j}} \tag{3}$$

其中，$E_{i,j}$表示频次期望值，自由度为$(r-1)(c-1)$，按照χ^2概率分布判定待测曲线集之间是否有差异。相对于t-test, χ^2-test可以自然地扩展到对多个分组进行泄露评估，这在评估多个特定明文相关性等场景下是很适用的。此外，χ^2-test基于完整的分布而不是某个统计距来评估独立性，因此在噪声较低或泄露信息在单个统计矩上差异不明显时，χ^2-test可探测到t-test漏报的安全脆弱点。然而随着信噪比变低，χ^2-test的优势逐渐变弱，甚至有时t-test可以基于更少的能量迹探测到泄露信息。因此χ^2-test可以作为TVLA技术的补充，和TVLA技术相结合使用进行评估，从而可以减少漏报率，提高评估的准确度。

χ^2-test评估和TVLA评估相结合可以有效提高评估准确度，但是相应的泄露检测尤其是针对多变量的泄露检测仍然较为繁琐，不能同时进行垂直和水平方向上的泄露检测，而且需要经过相应的预处理。针对这些缺陷，深度学习的思想被应用于泄露评估中，Wegener等人[24]提出了DL-LA(Deep Learning Leakage Assessment)技术。该方法通过监督学习的方法用训练集构造出一个神经网络，将神经网络作为待测数据集的区分器，当以不可忽略的概率区分成功的时候，那么将判定相应的侧信道信息存在着泄露。在某些场景中，DL-LA技术可以进行高效的单变量泄露评估，并且可以方便地扩展到多变量的泄露评估中。相对于TVLA和χ^2-test评估方法，它只需较少的功耗曲线就能检测到相应泄露的存在。但是其本身所使用的深度学习技术给泄露评估引入了新的变量，深度学习效果也影响着泄露检测结果的准确性，并且存在着概率适应性以及过拟合等问题，因此DL-LA也不能完全取代TVLA评估和χ^2-test评估，目前可作为泄露评估的补充技术进行使用。表2给出了以上3种通用评估方法的优缺点对比。

3.2 基于故障攻击的通用评估

在现有的众多故障分析方法中，差分故障攻击实现了对故障注入难度和结果分析复杂度的均衡，因此适用的注入场景最多，对密码算法带来的威胁最为广泛。分析密码算法及其防护措施对差分故障攻击的抵抗能力成为评估密码产品安全性的关键。2012年，Sakiyama等人[25]从S盒的差分分布特征入手，系统分析了分组密码算法在差分故障攻击场景下的密钥泄露情况，进而从提高故障信息利用率的角度定义出最优差分故障攻击。他们指出，每次故障注入所泄露的秘密信息的上界由故障传播过程中涉及的子密钥个数、故障模型的不确定度和密码算法S盒的差分分布特征共同决定。当计算出泄露信息的上界后，攻击者则可推断出恢复完整密钥所需的最少故障注入次数，并可判断现有攻击方法是否

表 2 能量攻击防护方案通用评估方法对比

评估方法	优点	缺点
TVLA	简单高效	低噪声情况下以及泄露信息分布在多个统计距情况下不适用
χ^2-test	有效弥补TVLA的不足，在低噪声以及泄露信息分布在多个统计距的情况下仍然适用	在信噪比较低的情况下，效率较低
DL-LA	无需预处理，更低的误报率	存在概率适应性以及过拟合等问题

正确或是否有改进空间。因为最优差分故障攻击不需要设计具体的密钥恢复策略，所以可实现高效的安全性评估，并且可作为基本元件用于分析分组密码防护实现抗故障攻击能力。

在抗故障攻击的防护实现中，有一类常用的方法是通过冗余运算检测故障注入进而阻止密文输出[26]，因为故障密文不被输出，所以敌手无法获取有效的信息用于密钥恢复。但考虑到冗余度有限的校验操作无法全面检测所有的故障类型，当故障被漏检时故障密文信息被完全泄露，因此现有研究通常采用检错成功率作为此类防护密码实现抗故障攻击的安全性指标。此外，另一类常见的防护通过随机化故障在加密过程中的混淆扩散情况，消除故障密文与注入故障的对应关系，其中代表性方法为感染类防护[27]。因为这类防护始终允许密文输出，所以Ghosh等人[28]提出使用正确、故障密文差分与密钥之间的互信息作为防护的安全性度量指标。若互信息为0，则判定防护密码实现可抵抗差分故障攻击；否则，不能抵抗故障攻击。然而在实际应用中，因为完整密码防护实现的构造比较复杂，所以对密钥和密文差分计算互信息并不容易。该方法除了被成功应用于基于中间值替换的感染防护[29]以外，目前未见关于其他感染防护方案的互信息评估结果。为实现量化评估，Feng等人[30]同样以信息泄露为指标，提出了一套更为通用的感染防护评估流程。该方法首先将防护密码实现划分成无防护密码算法和感染函数，然后利用故障在密码算法中的传播扩散特征刻画出感染函数需面对的攻击场景，利用密码算法最优差分故障攻击结果计算出安全感染函数输入需满足的不确定度下界。上述操作避免批量评估中对密码算法的重复性分析，降低了评估复杂度。接下来，在感染函数安全性量化分析中，感染函数被拆分为一系列重复且独立的随机非线性操作，从而有效地缩小了分析目标。通过复用单个随机非线性操作的分析结果，最终解决了感染函数输入的不确定度量化问题。

上述基于信息泄露的评估方法为密码产品抗故障安全性分析提供更加有效的评估手段。但它们大多只面向针对加密中间值的故障注入和依赖故障密文的密钥恢复方法。在判定密码算法抗指令故障注入攻击或其他不依赖故障密文具体值的攻击的安全性时，目前尚缺乏通用的评估方法。

4　侧信道防护的形式化分析

除了以上介绍的评估方法，利用形式化技术和方法对侧信道防护的有效性进行分析正在逐渐成为侧信道评估的一个新的发展方向。形式化方法的主要优势在于能够对防御方案进行自动或者半自动的分析，避免了手动分析的不全面及效率低等缺点，并且能够发现可能存在的潜在脆弱点。目前侧信道防护形式化分析主要是对掩码防护实现[31]的有效性进行验证，包括掩码的软件实现有效性和掩码硬件实现有效性。

在实际应用中，优化编译等因素会影响代码的操作和执行顺序，从而使得理论上证明是安全的掩码实际并不安全[32]。形式化方法分析的通常是编译后的汇编代码，因此能够更加准确地对掩码有效性进行评估。最具开创性的工作是Bathe等人[33]在CCS2016上提出的。该工作是对2015年欧密会上[34]提出不相干(Non-Interference, NI)属性的扩充，将其扩展为强不干扰(Strong Non-Interference, SNI)，从而实现了对高阶掩码的形式化验证。它允许证明更小的代码序列(称为gadget)在与其他代码部分的可组合性方面的安全性。实现SNI属性的代码片段可以与其他代码片段自由组合，而不会干扰整体抵抗侧信道攻击的防护能力。与此类似，Coron等人[35]在文献[33]工作的基础上给出了两种验证方法：第1种方法与Bathe的方法基本相同，但采用通用的LISP语言实现。第2种是使用初等变换方法判定NI和SNI属性来实现目标程序的验证。总而言之，Bathe和Coron的工作采用的都是程序验证的方法。除此之外，还有另外两种思路来对软件掩码的有效性进行形式化验证：基于类型推导的方法和基于模型计数的方法。

基于类型推导的典型工作有以下几个。在CHES2013上，Bayrak等人[32]将掩码方案的验证问题归约为布尔可满足问题。该方法的主要思路是分析掩码程序的数据流图，并将输入变量的类型分为3种：secret, public和random，通过敏感信息的检测判断掩码的安全性。如果密码实现中存在1个操作或者1组操作满足相关泄露至少依赖于1个秘密(密钥)信息且相关泄露不依赖于任何一个随机信息时，则可以判断出掩码实现是不安全的。最终将这两个条件判断转化为掩码实现中各个变量之间依赖关系的检测问题。该方法的优点在于快速高效，但其主要问题在于准确性和完全性有待提高。另一个基于类型推导的形式化的主要工作是Ouahma等人[36]给出的，该工作利用语义分析对掩码方案的汇编级代码进行验证。该方法针对的是值泄露模型，分析汇编程序中每条指令的目标寄存器内容的表达式。如果所有中间计算结果分布统计上独立于秘密变量，那么可以判定该程序能够抵抗1阶能量分析。

与文献[32]工作不同之处在于，该方法判断的是每一个中间变量的分布类型。

基于模型计数的方法工作主要是由Eldib等人[37,38]给出的，该方法分析的对象是掩码实现的布尔程序，主要思想是通过检测布尔程序中各个节点(对应的与、或、非等不同的布尔操作)的约束来进行验证，并将验证问题编码为SMT(Satisfiability Modulo Theories)可求解的一系列1阶逻辑公式。与文献[32]工作相比，该方法不但能够判断出敏感数据是否加了掩码，还能够判断出敏感信息所加掩码是否是完美掩码(perfect mask)，同时还可以直接定位易受攻击的代码部分。但它存在的主要问题在于需要求解的SMT公式规模与秘密变量呈指数关系，实用性和效率需要进一步提高。在此基础上，Zhang等人[39]结合语义推导和模型计数，在CAV2018上给出了一种基于反馈的掩码侧信道防御策略形式化验证方案，该方案可以看作是基于语义规则的类型推导和基于模型计数的协同集成。

相对于软件实现，硬件实现环境更加复杂，例如存在的毛刺(glitch)现象使得硬件掩码的实现更容易出现攻击脆弱点，常用的基于软件掩码的形式化验证方法不能直接应用于硬件掩码的评估中。Bertoni等人[40]在SPACE2016上给出了一种硬件掩码的验证方案，该工作考虑了电路输入端的所有可能瞬态，并对所有可能在门电路处发生的毛刺进行了建模，针对的是一阶掩码，侧重于纯组合逻辑。Bloem等人[41]在EUROCRYPT2018上给出了一种基于毛刺的硬件掩码形式化验证方法。该方法不需要对目标实现的任何中间步骤进行建模，直接分析探测模型下带毛刺的网表文件。通过将网表表示为布尔函数树，在带毛刺的探测模型下对每一个门的傅里叶系数进行合理但保守的估计，并根据每个门对输入的统计依赖预测可能的泄露。与Bertoni的工作相比，它不但考虑组合逻辑，还考虑时序门，能够覆盖更高阶泄露。

除了对能量掩码方案进行形式化验证之外，目前也有部分工作针对故障攻击的防御形式化验证展开。例如Goubet等人[42]在CARDIS2015上给出了一个评估软件防御错误注入攻击的形式化验证框架，采用有限自动机对指令进行描述，利用框架产生一系列输入到SMT求解器的等式，根据求解结果判断是否存在可能的攻击路径。相对于掩码方案，故障防御的形式化验证工作成果目前还不够丰富。

另外，对防御策略的形式化验证研究工作的特点在于：一种形式化建模方法的有效性与该方法对应的工具实现密切相关。因此，每一种形式化验证方法的提出通常都对应着相应的工具，例如Sleuth[32], SC snifer[38], SCInfer[39]和Rebacca[41]等。形式化验证工具研制需要关注的重点是所研制工具的实用性、易用性和实现效率。

5 结束语

侧信道攻击是针对密码产品的一类重要的攻击方法，对密码产品进行侧信道分析与评估是密码测评的重要环节。本文介绍了针对密码产品的3类侧信道分析评估方式，它们分别从不同的角度分析密码产品抗侧信道攻击的能力，具体包括侧信道攻击测评、基于信息泄露的通用评估和形式化验证技术。这3种方法各具特点，在实际的密码产品测评中可以互为补充加以使用，如表3。总的来说，目前针对密码产品的侧信道分析评估呈现如下趋势：首先，侧信道攻击的手段和方法日益丰富化、多样化并呈现出组合化的趋势；其次，机器学习技术在侧信道评估中发挥了越来越重要的作用；再次，由于具有效率高、通用性强等特点，基于信息泄露的侧信道评估技术与工具得到了日益广泛的关注。

与此同时，也存在着一些问题：(1)尽管目前已出现了种类繁多的侧信道分析方法，但实际测评标准采用的方法仍然有限，与最新侧信道攻击水平相比仍有一定的滞后性，从而很难全面涵盖密码产品的攻击脆弱点；(2)基于信息泄露的通用评估虽然提高了评估效率，降低了评估难度，但是与攻击性测试相比，其评估结果仍存在着可靠性与准确性等问题；(3)形式化验证技术提高了侧信道评估自动化水平，但存在着建模复杂、求解规模有限等问题，形式化验证工具的实用性和评估效率仍有待提高。

表 3 3种评估方法对比

评估方法	优点	缺点	适用场景
侧信道攻击测评	评估思路简单直接：利用现有攻击逐一尝试，攻击成功则不通过，失败则为通过	由于攻击方法繁多，实现繁琐，评估周期长，同时难以保障评估的完备性	符合攻击条件的侧信道泄露场景，也可作为其它评估技术的验证
基于信息泄露的通用评估	评估实现简单，评估结果可提供一定的理论安全依据	评估的准确度和解释性有待提高与增强	可单独作为评估技术使用，也可作为攻击测评中侧信息泄露点定位工具
形式化验证技术	可为防护实现提供安全性的理论评估，自动化程度高	实现代价大，评估效率较低	可作为可证明安全防护设计方案的验证工具

以上问题的有效解决需要学术界和测评界的共同努力，从而尽可能缩短实际密码测评能力与学术研究水平的差距，提升基于信息泄露的通用评估的可靠性与准确性，提高侧信道形式化分析与自动化评估能力，最终保证我国密码产品的整体安全水平。

参 考 文 献

[1] KOCHER P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[C]. The 16th Annual International Cryptology Conference Santa Barbara on Advances in Cryptology, Santa Barbara, USA, 1996: 104–113. doi: 10.1007/3-540-68697-5_9.

[2] KOCHER P, JAFFE J, and JUN B. Differential power analysis[C]. The 19th Annual International Cryptology Conference Santa Barbara on Advances in Cryptology, Santa Barbara, USA, 1999: 388–397. doi: 10.1007/3-540-48405-1_25.

[3] GANDOLFI K, MOURTEL C, and OLIVIER F. Electromagnetic analysis: Concrete results[C]. The 3rd International Workshop Paris on Cryptographic Hardware and Embedded Systems, Paris, France, 2001: 251–261. doi: 10.1007/3-540-44709-1_21.

[4] BONEH D, DEMILLO R A, and LIPTON R J. On the importance of checking cryptographic protocols for faults[C]. International Conference on the Theory and Application of Cryptographic Techniques Konstanz on Advances in Cryptology, Konstanz, Germany, 1997: 37–51. doi: 10.1007/3-540-69053-0_4.

[5] MANGARD S, OSWALD E, POPP T. 冯登国, 周永彬, 刘继业, 等译. 能量分析攻击[M]. 北京: 科学出版社, 2010: 3–4, 49–50.
MANGARD S, OSWALD E, and POPP T. FENG Dengguo, ZHOU Yongbin, LIU Jiye, *et al.* translation. Power Analysis Attacks[M]. Beijing: Science Press, 2010: 3–4, 49–50.

[6] NIST. FIPS 140–3 Security requirements for cryptographic modules[S]. NIST, 2019.

[7] ISO/IEC 19790: 2012. Information technology-security techniques-security requirements for cryptographic modules[S]. 2012.

[8] State Cryptography Administration. GM/T 0028–2014 Cryptography module security technical requirements[S]. Beijing: China Standard Press, 2014.

[9] 国家密码管理局. GM/T 0008–2012 安全芯片密码检测准则[S]. 北京: 中国标准出版社, 2012.
State Cryptography Administration. GM/T 0008–2012 Cryptography test criteria for security IC[S]. Beijing: China Standard Press, 2012.

[10] BRIER E, CLAVIER C, and OLIVIER F. Correlation power analysis with a leakage mode[C]. The 6th International Workshop Cambridge on Cryptographic Hardware and Embedded Systems, Cambridge, USA, 2004: 16–29. doi: 10.1007/978-3-540-28632-5_2.

[11] GIERLICHS B, BATINA L, TUYLS P, *et al.* Mutual information analysis[C]. The 10th International Workshop on Cryptographic Hardware and Embedded Systems, Washington, USA, 2008: 426–442. doi: 10.1007/978-3-540-85053-3_27.

[12] CHARI S, RAO J R, and ROHATGI P. Template attacks[C]. The 4th International Workshop Redwood Shores on Cryptographic Hardware and Embedded Systems, Redwood City, USA, 2002: 13–28. doi: 10.1007/3-540-36400-5_3.

[13] HOSPODAR G, GIERLICHS B, DE MULDER E, *et al.* Machine learning in side-channel analysis: A first study[J]. *Journal of Cryptographic Engineering*, 2011, 1(4): 293. doi: 10.1007/s13389-011-0023-x.

[14] LERMAN L, BONTEMPI G, and MARKOWITCH O. A machine learning approach against a masked AES[J]. *Journal of Cryptographic Engineering*, 2015, 5(2): 123–139. doi: 10.1007/s13389-014-0089-3.

[15] MAGHREBI H, PORTIGLIATTI T, and PROUFF E. Breaking cryptographic implementations using deep learning techniques[C]. The 6th International Conference on Security, Privacy, and Applied Cryptography Engineering, Hyderabad, India, 2016: 3–26. doi: 10.1007/978-3-319-49445-6_1.

[16] TIMON B. Non-profiled deep learning-based side-channel attacks with sensitivity analysis[J]. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2019(2): 107–131.

[17] BIHAM E and SHAMIR A. Differential fault analysis of secret key cryptosystems[C]. The 17th Annual International Cryptology Conference Santa Barbara on Advances in Cryptology, Santa Barbara, USA, 1997: 513–525. doi: 10.1007/BFb0052259.

[18] BIEHL I, MEYER B, and MÜLLER V. Differential fault attacks on elliptic curve cryptosystems[C]. The 20th Annual International Cryptology Conference Santa Barbara on Advances in Cryptology, Santa Barbara, USA, 2000: 131–146. doi: 10.1007/3-540-44598-6_8.

[19] SCHMIDT J M and MEDWED M. A fault attack on ECDSA[C]. The 2009 Workshop on Fault Diagnosis and Tolerance in Cryptography, Lausanne, Switzerland, 2009: 93–99. doi: 10.1109/FDTC.2009.38.

[20] GOODWILL G, JUN B, JAFFE J, *et al.* A testing methodology for side-channel resistance validation[C]. NIST

Non-Invasive Attack Testing Workshop, Nara, Japan, 2011: 115–136.

[21] BECKER G, COOPER J, DEMULDER E, *et al*. Test Vector Leakage Assessment (TVLA) methodology in practice[C]. International Cryptographic Module Conference, Gaithersburg, USA, 2013: 13.

[22] DING A A, CHEN Cong, and EISENBARTH T. Simpler, faster, and more robust t-test based leakage detection[C]. The 7th International Workshop on Constructive Side, Graz, Austria, 2016: 163–183. doi: 10.1007/978-3-319-43283-0_10.

[23] MORADI A, RICHTER B, SCHNEIDER T, *et al*. Leakage detection with the X^2-test[J]. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018(1): 209–237. doi: 10.13154/tches.v2018.i1.209-237.

[24] WEGENER F, MOOS T, and MORADI A. DL-LA: Deep learning leakage assessment[J]. *IACR Cryptology ePrint Archive*, 2019. https://eprint.iacr.org/2019/505.pdf.

[25] SAKIYAMA K, LI YANG, IWAMOTO M, *et al*. Information-theoretic approach to optimal differential fault analysis[J]. *IEEE Transactions on Information Forensics and Security*, 2012, 7(1): 109–120. doi: 10.1109/TIFS.2011.2174984.

[26] BERTONI G, BREVEGLIERI L, KOREN I, *et al*. Error analysis and detection procedures for a hardware implementation of the advanced encryption standard[J]. *IEEE Transactions on Computers*, 2003, 52(4): 492–505. doi: 10.1109/tc.2003.1190590.

[27] JOYE M, MANET P, and RIGAUD J B. Strengthening hardware AES implementations against fault attacks[J]. *IET Information Security*, 2007, 1(3): 106–110. doi: 10.1049/iet-ifs:20060163.

[28] GHOSH S, SAHA D, SENGUPTA A, *et al*. Preventing fault attacks using fault randomization with a case study on AES[C]. The 20th Australasian Conference on Information Security and Privacy, Brisbane, Australia, 2015: 343–355. doi: 10.1007/978-3-319-19962-7_20.

[29] TUPSAMUDRE H, BISHT S, and MUKHOPADHYAY D. Destroying fault invariant with randomization[C]. The 16th International Workshop on Cryptographic Hardware and Embedded Systems, Busan, Korea, 2014: 93–111. doi: 10.1007/978-3-662-44709-3_6.

[30] FENG Jingyi, CHEN Hua, LI Yang, *et al*. A framework for evaluation and analysis on infection countermeasures against fault attacks[J]. *IEEE Transactions on Information Forensics and Security*, 2020, 15: 391–406. doi: 10.1109/TIFS.2019.2903653.

[31] GOUBIN L and PATARIN J. DES and differential power analysis the "duplication" method[C]. The 1st International Workshop on Cryptographic Hardware and Embedded Systems, Worcester, USA, 1999: 158–172. doi: 10.1007/3-540-48059-5_15.

[32] BAYRAK A G, REGAZZONI F, NOVO D, *et al*. Sleuth: Automated verification of software power analysis countermeasures[C]. The 15th International Workshop on Cryptographic Hardware and Embedded Systems, Santa Barbara, USA, 2013: 293–310. doi: 10.1007/978-3-642-40349-1_17.

[33] BARTHE G, BELAÏD S, DUPRESSOIR F, *et al*. Strong non-interference and type-directed higher-order masking[C]. The 2016 ACM SIGSAC Conference on Computer and Communications Security, New York, USA, 2016: 116–129. doi: 10.1145/2976749.2978427.

[34] BARTHE G, BELAÏD S, DUPRESSOIR F, *et al*. Verified proofs of higher-order masking[C]. The 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology, Sofia, Bulgaria, 2015: 457–485. doi: 10.1007/978-3-662-46800-5_18.

[35] CORON J S. Formal verification of side-channel countermeasures via elementary circuit transformations[C]. The 16th International Conference on Applied Cryptography and Network Security, Leuven, Belgium, 2018: 65–82. doi: 10.1007/978-3-319-93387-0_4.

[36] EL OUAHMA I B, MEUNIER Q L, HEYDEMANN K, *et al*. Side-channel robustness analysis of masked assembly codes using a symbolic approach[J]. *Journal of Cryptographic Engineering*, 2019, 9(3): 231–242. doi: 10.1007/s13389-019-00205-7.

[37] ELDIB H, WANG Chao, and SCHAUMONT P. Formal verification of software countermeasures against side-channel attacks[J]. *ACM Transactions on Software Engineering and Methodology*, 2014, 24(2): 1–24. doi: 10.1145/2685616.

[38] ELDIB H, WANG Chao, and SCHAUMONT P. SMT-based verification of software countermeasures against side-channel attacks[C]. The 20th International Conference on Tools and Algorithms for the Construction and Analysis of Systems, Grenoble, France, 2014: 62–77. doi: 10.1007/978-3-642-54862-8_5.

[39] ZHANG Jun, GAO Pengfei, SONG Fu, *et al*. SCINFER: Refinement-based verification of software countermeasures against side-channel attacks[C]. The 30th International Conference on Computer Aided Verification, Oxford, England, 2018: 157–177. doi: 10.1007/978-3-319-96142-2_12.

[40] BERTONI G and MARTINOLI M. A methodology for the

characterisation of leakages in combinatorial logic[C]. The 6th International Conference on Security, Privacy, and Applied Cryptography Engineering, Hyderabad, India, 2016: 363–382. doi: 10.1007/978-3-319-49445-6_21.

[41] BLOEM R, GROSS H, IUSUPOV R, *et al*. Formal verification of masked hardware implementations in the presence of glitches[C]. The 37th Advances in Cryptology, Tel Aviv, Israel, 2018: 321–353. doi: 10.1007/978-3-319-78375-8_11.

[42] GOUBET L, HEYDEMANN K, ENCRENAZ E, *et al*. Efficient design and evaluation of countermeasures against fault attacks using formal verification[C]. The 14th International Conference on Smart Card Research and Advanced Applications, Bochum, Germany, 2015: 177–192. doi: 10.1007/978-3-319-31271-2_11.

陈　华：女，1976年生，正高级工程师，博士生导师，研究方向为侧信道分析与防护、密码检测.

习　伟：男，1980年生，高级工程师，研究方向为智能电网与电力芯片.

范丽敏：女，1978年生，高级工程师，硕士生导师，研究方向为侧信道分析与防护、密码检测.

焦志鹏：男，1992年生，博士生，研究方向为侧信道分析与防护.

冯婧怡：女，1991年生，博士生，研究方向为侧信道分析与防护.

责任编辑：马秀强