密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2018, 5(4): 376–382

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

侧信道分析专栏

侧信道分析专栏序言 (中英文)

白国强[1], 王 安[2]

1. 清华大学 微电子学研究所, 北京 100084
2. 北京理工大学 计算机学院, 北京 100081
通信作者: 白国强, E-mail: baigq@tsinghua.edu.cn; 王安, E-mail: wanganl@bit.edu.cn

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000248
中文引用格式: 白国强, 王安. 侧信道分析专栏序言 (中英文)[J]. 密码学报, 2018, 5(4): 376–382.
英文引用格式: BAI G Q, WANG A. Preface of side-channel analysis column (in Chinese and in English)[J]. Journal of Cryptologic Research, 2018, 5(4): 376–382.

Preface of Side-channel Analysis Column (in Chinese and in English)

BAI Guo-Qiang[1], WANG An[2]

1. Institute of Microelectronics, Tsinghua University, Beijing 100084, China
2. School of Computer Science, Beijing Institute of Technology, Beijing 100081, China
Corresponding author: BAI Guo-Qiang, E-mail: baigq@tsinghua.edu.cn;
WANG An, E-mail: wanganl@bit.edu.cn

密码学是现代信息安全的基石, 自 20 世纪 70 年代 DES 算法和 RSA 算法相继提出以来, 密码学得到了迅猛发展, 学者们主要采用数学手段设计密码算法, 并对其进行完全基于算法本身的安全性分析. 然而任何密码算法, 在被应用于工程实践以取得其算法功能时, 首先必须通过某种物理手段或方法来实现其计算流程. 在具体工程技术中, 为获取密码算法的功能, 通过某种物理手段来完成特定密码算法的具体加密或解密流程的过程, 我们称为密码算法的实现.

大约在 1844 年电报发明前的很长时期内, 人们主要是通过手工的方法完成加密和解密流程的, 这一时期的密码我们一般称作手工密码. 当人类文明进入到近代的机械和电气时代后, 人们有了相比于手工而言更先进的机械和电气技术. 借助于这种机械和电气技术, 人们可以较好地实现相对复杂的加密和解密流程, 从而推动人类的加解密技术上升到了机械电气密码时代. 第二次世界大战前, 以及二战之后较长一段时间内, 机械电气密码技术达到了鼎盛.

从 1944 年计算机发明和 1958 年集成电路发明后至今的几十年内, 人类的通讯技术飞速地步入了一个以计算机、集成电路和光纤技术为核心的新时代. 其中, 特别是集成电路技术的发明和发展, 在为数据提供强大、低廉的计算与存储能力的同时, 也为各种复杂密码算法的实现提供了全新的技术手段, 并引导人们不断提出各种新颖和复杂的密码算法, 以满足现代安全通讯技术的需求, 创造出新的安全供给, 使得现代密码学得以创立并在当代得到了蓬勃发展. 当下现代密码学空前繁荣, 但是我们不能忘记这种繁荣是以当前人类最先进的一种技术——集成电路技术为前提的. 近年来, 人们正在尝试以量子技术来取代集成电路技术以获取更高的计算能力. 这一情况使得目前量子计算、量子通信、量子密码等等成了最时髦的术

收稿日期: 2018-03-22 定稿日期: 2018-05-04

语. 然而, 这些量子密码、量子计算等技术是否最终能够击败当下的传统密码技术, 主要看量子技术能否成功取代集成电路技术, 目前我们只能拭目以待.

当前以集成电路技术为基础的密码算法的实现大致又可以分为两种方式, 一种是软件方式, 另一种是硬件方式. 所谓的软件方式是指以通用计算机指令集为基础的一种编程实现方法. 这一过程中, 实现通用计算机指令的物理载体仍然是集成电路芯片. 所谓的硬件方式是指针对特定密码算法所需的计算流程, 定制特定的集成电路来高效完成这种计算流程的一种方式. 当前硬件方式通常又分为 FPGA 方式和 ASIC 方式. FPGA 方式中提前预置了可编程逻辑电路, 该电路可通过现场编程方法生成用户需要的特定电路. 而 ASIC 方式则是完全依据需求来定制电路的一种方式. 无论是软件方式还是硬件方式, 在完成计算流程的过程中都需要花费时间、消耗能量和向外辐射电磁波. 1996 年, Paul Kocher 发现在手持密码设备的应用场景下, 攻击者一方面能够通过时间、能耗、电磁辐射、声音等侧信道来观测密码运算过程中的中间值信息, 另一方面可通过激光、电源毛刺、时钟毛刺、电磁脉冲等手段干扰密码运算, 从其错误输出中推导密钥信息. 这类 “旁门左道” 的攻击被称作侧信道分析 (side-channel analysis), 又称旁路分析.

从学术创新的角度来讲, 侧信道分析是一个天马行空、不拘一格的思维方式. 这是因为, 物质和信息进行传递的物理信道多种多样, 与密码算法结构相对应的分析模型花样繁多, 借助相关学科提高分析效率的方法也大相径庭. 在攻击方面, 简单能量分析、相关能量分析、模板攻击、碰撞攻击、差分聚类分析、互信息分析、差分故障分析、故障灵敏度分析等多种密钥恢复模型被提出; 相应地, 芯片设计方提出了掩码、伪操作、随机延时、乱序执行、功耗平衡、错误校验等多种抗侧信道攻击防护对策; 然而, 道高一尺魔高一丈, 攻击者随后发现差分频域分析、二阶侧信道攻击、组合攻击可以攻破某些防护对策; 进而, 设计者们又从设备级、芯片级、系统级、算法级、门级、晶体管级等多个层面来设计综合防护方案. 一时间, 侧信道分析学术领域呈现百花齐放、百家争鸣的局面.

只要密码算法的实现过程中未加入任何防护对策, 侧信道攻击几乎适用于所有的密码算法. 但即使一个密码设备完全没有进行侧信道防护, 侧信道攻击也未必能真正攻破它, 因为侧信道攻击通常有一定的假设条件, 例如攻击者需要持有设备、或跟设备的距离在一定范围内; 攻击者需要对密码算法实现方案有一定了解; 攻击者具备驱动设备快速多次重复加密的权限; 攻击者能够选择特定的明文进行加密等等.

对于密码产品的生产厂商而言, 他们通常会将各种先进的防护技术加入到自己的产品中, 并选择不公开其实现方案. 测评机构则对这些产品在白盒条件下进行安全性测试与评估, 并对产品赋予一定的安全等级. 然而, 即使是达到足够安全等级的产品, 仍然可能被学者或黑客们发现弱点, 并实施侧信道攻击. 厂商、测评机构、学者、黑客们分别从不同的角度开展研究, 相辅相成地推动着侧信道分析与防护技术的实用化.

我国侧信道分析领域已有十余年研究积累, 自 2010 年起, 中国密码学会密码芯片专委会每年组织一次密码芯片学术会议, 主要讨论以侧信道分析为代表的密码芯片相关研究领域中最新研究成果与进展. 然而, 我国在侧信道分析领域的研究水平较发达国家尚有一定差距. 侧信道分析领域公认的唯一顶级国际学术会议 CHES (International Workshop on Cryptographic Hardware and Embedded Systems) 自 1999 年创办至今已召开近 20 届, 中国大陆研究团队仅发表了 6 篇 CHES 论文, 期待我国优秀的密码学者们在侧信道分析领域创造更多前沿成果.

在本期《密码学报》的 “侧信道分析” 专栏中, 我们刊登了 6 篇论文, 希望给侧信道分析从业者带来理论支撑与实践帮助.

第 1 篇论文题目是《侧信道分析实用案例概述》. 由于时效、成本、技术等因素, 许多密码产品在设计时, 厂商并未考虑进行侧信道攻击的防护, 或者加入的防护对策并不足够强. 因而, 目前已经有多个商用产品被学者和黑客们用侧信道分析技术攻破. 文章总结了国际上商用密码产品被能量分析、电磁分析、故障分析、缓存分析等技术攻破的案例, 从技术上对其进行深入浅出的介绍, 同时也归纳了近年来出现的一些新奇的侧信道分析方法. 该文既可作为一篇侧信道分析的综述文章, 也能够为芯片厂商和测评机构提供丰富的经验参考.

第 2 篇论文题目是《Keccak 的一种新二阶门限掩码方案及实现》. Keccak 算法是美国国家标准局 2015 年发布的 SHA-3 杂凑算法标准, 文章基于 Keccak 算法的结构和 S 盒的性质, 用 3 个掩码分量构造了一种可抵抗二阶能量攻击的新型 Keccak 门限掩码方案. 作者基于 FPGA 环境给出了串行、并行的两

种具体实现方案, 以应用于不同的应用场景. 与现有方案相比, 新方案特点是面积小、所需随机数少, 这对于密码芯片厂商来讲, 有很高的实用价值.

第 3 篇论文题目是《一种高效的基于高阶 DPA 的掩码安全性评价方案》. 在侧信道分析测评过程中, 一些理论上安全的掩码方案, 在实测中可能会出现单变量泄露的现象, 从而导致防护失效. 文章从电路记忆效应的角度入手, 为单变量泄露的成因给出了理论解释, 并归纳出电路记忆效应的统一化描述. 同时, 借助多个共享因子的差分功耗特征, 提出了一种高阶侧信道攻击所需曲线量的预测算法. 该算法能够对高阶掩码方案的安全性提供可量化的评价标准, 对密码芯片安全性测评工作具有很高的参考价值.

第 4 篇论文题目是《针对 SM4 选择明文能量分析的选择明文算法》. SM4 算法是我国自主设计的商用分组密码算法, 其显著的雪崩效应给侧信道分析带来了很大的密钥搜索空间. 文章提出了一种选择明文能量分析, 对于无任何侧信道防护的 SM4 实现, 该方法能够高效恢复其密钥. 文章表明, SM4 算法本身是安全的, 但 SM4 芯片设计者需在芯片中加入掩码、伪操作等足够的抗侧信道攻击防护对策, 以确保其实现上的物理安全性.

第 5 篇论文题目是《SM4 密码算法的踪迹驱动 Cache 分析》. 文章同样针对国密 SM4 算法开展侧信道分析研究, 首先给出一种踪迹驱动 Cache 分析方法, 在只借助失效泄露信息的条件下, 用 25 个样本完成分析; 随后结合代数分析, 提出了一种踪迹驱动代数 Cache 分析方法, 用 10 个样本即可完成分析. 作者基于 ARM 处理器 LPC2124 进行了实验验证, 这意味着计算机、ARM 等平台中实现 SM4 算法时, 需要针对 Cache 分析做相应防护.

第 6 篇论文题目是《一种 AES 随机变换掩码方案及抗 DPA 分析》. 作者设计了一种基于随机选择变换的掩码方案 RSCM, 通过随机产生等概率汉明重量的掩码组, 在每次执行密码算法时随机选择一个组合进行防护. 同时, 可对 S 盒使用随机转置矩阵变换, 并结合固定值掩码方案, 对不同的轮函数加以相应的掩码防护. 该方案具有良好的普适性, 可用于多种常见分组密码算法.

上述 6 篇论文中, 2 篇讨论分析技术、2 篇讨论防护技术、1 篇讨论测评技术, 另有 1 篇综述. 攻和防一直是密码学关注的焦点, 虽然我国密码芯片的设计与测评水平较发达国家还有一定差距, 但国内学术界在侧信道攻防领域的研究已有较多积累. 希望本专栏能够为工业界设计安全高效的密码芯片提供理论依据, 并为测评机构带来前沿的分析技术和实验参考. 相信不久的将来, 我国密码芯片产业会有飞速的发展, 整体技术水平赶超发达国家.

Cryptography is the cornerstone of modern information security. It has rapidly developed since DES and RSA were put forward one after another in the 1970s. Scholars mainly use mathematical methods to design cryptographic algorithms and analyze them completely based on the security of the algorithm itself. However, any cryptographic algorithm when applied to engineering practice to achieve its algorithmic functions, must first achieve its computational flow through some physical means or methods. In specific engineering technology, the process of completing the specific encryption or decryption of a particular cryptographic algorithm is aimed at obtaining the function of the cryptographic algorithm through some physical methods, which is called the implementation of cryptographic algorithms.

For a long time before the invention of the telegraph in 1844, people mainly used manual methods to complete the encryption and decryption process. Thus, the ciphers of this period were generally known as manual ciphers. But people have more advanced mechanical and electrical technology than manual technology after human civilization entering the modern era of electrical and mechanical engineering. With this advanced technology, relatively complicated encryption and decryption process can be better implemented, thereby promoting human encryption and decryption technology into the era of mechanical electrical cipher. Before the World War II and after a long time of the war, mechanical electrical cipher technology reached a period of great prosperity.

In the decades since the invention of the computer in 1944 and the integrated circuit in 1958,

human communication technology has rapidly stepped into a new era which is cored on computers, integrated circuits and optical fiber. Among them, especially the invention and the development of integrated circuit technology, apart from providing powerful and inexpensive computing and storage capabilities for data, also provides brand new technical means for the implementation of various complex cryptographic algorithms. Besides, people are guided to constantly propose kinds of novel and complicated cryptographic algorithms to meet the needs of modern secure communication technology and create new security supplies, thus modern cryptography has been established and has flourished in the contemporary. Modern cryptography is unprecedentedly prosperous, but we cannot forget that this prosperity is premised on the most advanced technology——integrated circuit technology. In recent years, people are trying to replace integrated circuit technology with quantum technology to obtain better computing capability, in which case quantum computing, quantum communication, and post-quantum cryptography, etc. have become the most fashionable terms currently. However, whether such technology as post-quantum cryptography, quantum computing and so on can eventually defeat the current traditional cryptography technology, mainly depends on whether quantum technology can successfully replace integrated circuit technology. At present, we can only wait and see.

At the moment, the implementation of cryptographic algorithms based on integrated circuit technology can be roughly summarized into two ways. One is software method and the other is hardware method. The so-called software method refers to a programming method using a general computer instruction set as the foundation, yet the physical carrier for implementing general computer instructions is still integrated circuit chips in this process. The so-called hardware method is to customize specific integrated circuits to efficiently accomplish this calculation process which is required for specific cryptographic algorithms. Moreover, the current hardware method is usually divided into FPGA method and ASIC method. Programmable logic circuits are preset in advance in the FPGA method, and this circuit can generate the specialized circuits required by the users through an on-site programming approach. While the ASIC method customizes a circuit according the demand. Nevertheless, both of them take time, consume power, and radiate electromagnetic waves during the process of computation whether using a software approach or a hardware approach. In 1996, Paul Kocher discovered that in the application scenario of hand-held cryptographic devices, the attacker can observe the intermediate value information generated during cryptographic operations through time, power consumption, electromagnetic radiation, sound, etc. On the other hand, cryptographic operations may be disturbed by means of lasers, power glitches, clock glitches, electromagnetic pulses, etc. And then the key information may be derived from its faulty output. Such fantastic attack is called side-channel analysis.

From the perspective of academic innovation, side-channel analysis is an imaginative and eclectic approach of thinking, which is because that there are varieties of physical channels for the transfer of material and information, and there are many analytical models corresponding to different structures of cryptographic algorithms. In addition, the methods with related disciplines used to improve the analysis efficiency are also widely divergent. In terms of the attack, simple power analysis, correlation power analysis, template attack, collision attack, differential cluster analysis, mutual information analysis, differential fault analysis, fault sensitivity analysis and other key recovery models were put forward. Correspondingly, the chip designers proposed masking, dummy operation, random delay, shuffling, power balance, error checking and some other countermeasures against side-channel attacks. However, “while the priest climbs a foot, the devil climbs ten”, the attackers then discovered that some countermeasures can still be broken through differential frequency domain analysis, second-order side-channel attacks and some combination attacks. Furthermore, designers gave comprehensive protection schemes from the device level, chip level, system level, algorithm level, gate level, transistor level and

so on. For a while, the academic field of side-channel analysis presented a popular situation.

Side-channel attacks can be applied to almost all cryptographic algorithms so long as no countermeasures are added during the implementation of the cryptographic algorithm. However, even if a cryptographic device does not perform side-channel protection at all, side-channel attacks may not be able to actually break it. For instance, the attacker usually needs to hold the device or keep the distance to the device within a limited range; the attacker should have some knowledge of the implementation details of the cryptographic algorithm; the permission of driving the device to repeat encryption multiple times are supposed to obtained; and the attacker can choose specific plaintexts for encryption, etc.

For the manufacturers of cryptographic products, they generally add various advanced protection technologies to their products, and do not expose their implementation schemes. After the security of these products is evaluated under white-box conditions by evaluation institutions, they will be endowed a certain security level. Yet, scholars or hackers still may find out the weakness of products and then conduct side-channel attacks on them even if they have reached a sufficient security level. Manufactures, evaluation institutions, academics, and hackers carry out the research from different point of view, which complements and promotes the practical application of side-channel analysis and protection technology.

The research on side-channel analysis in China has lasted more than 10 years. Since 2010, the Society of Cryptographic Chip of the China Association for Cryptologic Research has organized annual conference on cryptographic chips, focusing on the latest research results and progress in research field of cryptographic chips such as side-channel analysis. Nevertheless, compared with developed countries in this field, China still has a certain gap in the research level. The only recognized top international academic conference in the field of side-channel analysis CHES (International Workshop on Cryptographic Hardware and Embedded Systems) was founded in 1999 and has been hold for nearly 20 times so far. But the research team of China mainland has only published 6 papers on CHES. Therefore, it is expected that Chinese excellent cryptographers will achieve more frontier achievements in the field of side-channel analysis.

In this special column of the "Side-channel Analysis" of the Journal of Cryptologic Research, we publish six papers and hope to bring theoretical support and practical help to the practitioners of side-channel analysis.

The title of the first paper is "Practical Cases of Side-channel Analysis". Due to factors of time, cost, technology, etc., some manufacturers do not consider the side-channel resistance in their products, or their countermeasures are not effective enough. Therefore, there are some commercial products that have been attacked by scholars and hackers by side-channel analysis. This paper summarizes the cases where international commercial cryptographic products were attacked by power analysis, electromagnetic analysis, fault attack, cache attack, and explains profound theories in simple language. In addition, the paper summarizes some of the novel side-channel analysis methods that have emerged in recent years. Apart from being served as a popular science reading about side-channel analysis, this paper can also provide a wealth of experience reference for chip manufacturers and evaluation institution.

The second paper titled "New Second Order Threshold Masking Scheme of Keccak and Its Implementation". The Keccak algorithm is the SHA-3 hash algorithm standard issued by the National Institute of Standards and Technology in 2015. Based on the structure of the Keccak algorithm and the S-box, this paper constructs a novel Keccak threshold masking scheme with three mask components that can resist second-order power attacks. The authors present two concrete implementation schemes of serial and parallel in view of FPGA environment for different applications scenarios. Compared with

existing solutions, the characteristics of the new solution are smaller area and few random numbers, which are of high practical value for cryptographic chip manufacturers.

The title of the third paper is "Efficient Evaluation Scheme for Mask Security Based on Higher Order DPA". During side-channel analysis and evaluation, some masking schemes which are theoretically secure may show univariate leakage in actual measurement, thereby leading to failure protection. The paper starts from the perspective of circuit memory effects, provides a theoretical explanation for the causes of univariate leakage, and summarizes the unified description of circuit memory effects. At the same time, based on differential power consumption characteristics of multiple sharing factors, a prediction algorithm for the amount of curve required for high-order side-channel attacks is proposed. This algorithm can provide a quantifiable evaluation standard for the security of high-order masking schemes, and has a high reference value for the evaluation of security of cryptographic chip.

The title of the fourth paper is "Chosen-plaintext Algorithm for the Chosen-plaintext Power Analysis Against SM4". SM4 algorithm is a commercial block cipher algorithm designed in China, and its significant avalanche effect brings a large key search space to side-channel analysis. This paper presents a chosen-plaintext power analysis, which can efficiently recover the key of SM4 implementation without any side-channel protection. It is showed that SM4 algorithm itself is secure, but SM4 chip designers should add masks, dummy-operations, and other countermeasures against side-channel attacks in the chip to ensure their physical security.

The title of the fifth paper is "Research on Trace Driven Cache Analysis on SM4". The paper also focuses on the side-channel analysis of SM4 algorithm. A trace-driven cache analysis method is first given, and 25 samples were employed for analysis under the condition of only using the invalid leakage information. Subsequently, combined with algebra analysis, a trace-driven algebra cache analysis method was proposed. As a result, 10 samples are enough for this analysis. The authors performed a verification on ARM processor LPC2124, which means that when implementing the SM4 algorithm in the computer, ARM and other platforms, it is necessary to perform corresponding countermeasures against cache analysis.

The title of the sixth paper is "On AES Random Transform Masking Scheme Against DPA". The authors design a masking scheme named RSCM which is based on the random selection transformation. It generates a mask group with equal probability Hamming weight, and then randomly selects a combination to defend power analysis during the operation of cryptographic algorithm. Furthermore, random transposed matrix can be applied to S-box, combining with fixed value mask scheme, so that different round functions can be protected by corresponding masking. This scheme is universal and can be applied to many block ciphers.

Among the six papers mentioned above, two discuss analysis, two discuss countermeasure, one discusses evaluation, and the rest is an overview. Attack and defense have always been the focus of cryptography. Although there is still a certain gap in the design and evaluation level of cryptographic chips between China and developed countries, domestic research on this field has been accumulated much. It is hoped that this column can provide a theoretical basis for the industry to design secure and efficient cryptographic chips, as well bring forward frontier analysis technology and experimental reference to the evaluation institutions. We believe that in the near future, China's cryptographic chip industry will develop rapidly, and the overall technological level will catch up with developed countries.

作者信息

白国强 (1963–), 陕西清涧人, 博士, 副教授, 中国密码学会密码芯片专业委员会副主任委员. 主要研究领域为密码算法的集成电路实现和密码芯片的安全保护.
baigq@tsinghua.edu.cn

BAI Guo-Qiang (1963–), born in Qingjian, Shaanxi Province, Ph.D., Associate Professor, Vice Chair of Society of Cryptographic Chip, Chinese Association for Cryptologic Research. Main research field covers integrated circuit realization of cryptology algorithm and security protection of cryptologic chips.
baigq@tsinghua.edu.cn

王安 (1983–), 山东莱州人, 博士, 讲师, 硕士生导师. 主要研究领域为密码工程与侧信道分析.
wanganl@bit.edu.cn

WANG An (1983–), born in Laizhou, Shandong Province, Ph.D., Lecturer, Tutor of Graduate for Master Degree. Main research field covers cryptologic engineering and side channel analysis.
wanganl@bit.edu.cn