基于激光注入的FPGA加密防护设计验证研究

蔡 莹[1,2],朱 翔[1,2],王 舰[2,3],李昊远[2,3],韩建伟[1,2]
(1. 中国科学院国家空间科学中心,北京 100190; 2. 中国科学院大学,北京 100049; 3. 中国科学院软件研究所,北京 100190)

摘 要: 激光注入技术是评估安全芯片抗故障攻击能力的重要手段之一. 本文详细分析了激光故障注入的原理及激光诱发现场可编程门阵列(Field Programmable Gate Array,FPGA)触发器结构故障的机制,提出了一种FPGA激光注入评测方法. 分别采用随机和定点故障注入的方法,对基于FPGA实现的SM2算法的基点等数据进行了篡改,验证了防护设计的有效性. 针对28 nm工艺的FPGA,激光能够实现指定字节的单比特故障注入,同时也能实现快速的高覆盖率随机故障注入,是一种精确和高效的安全芯片评测手段.

关键词: 激光; FPGA; 故障注入; SM2; 防护验证
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112(2022)10-2381-06
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20210119

Verification of FPGA Encryption Protection Design Based on Laser Injection

CAI Ying[1,2],ZHU Xiang[1,2],WANG Jian[2,3],LI Hao-yuan[2,3],HAN Jian-wei[1,2]
(1. *National Space Science Center*, *Chinese Academy of Sciences*, *Beijing* 100190, *China*;
2. *University of Chinese Academy of Sciences*, *Beijing* 100049, *China*;
3. *Institute of Software Chinese Academy of Sciences*, *Beijing* 100190, *China*)

Abstract: Laser injection technology is one of the essential methods to evaluate the ability of security chips to resist failure attacks. In this paper, the principle of laser fault injection and the mechanism of laser-induced structural failure of FPGA(Fiele Programmable Gate Array) trigger are analyzed in detail, and an evaluation method of FPGA laser injection is proposed. The random and fixed-point fault injection method are adopted respectively to tamper with the basic point data of the SM2 algorithm based on FPGA, and the effectiveness of the protection design is verified. Aiming at the FPGA of 28nm process, the laser can achieve the single bit fault injection of specified byte and perform the fast random fault injection of high coverage rate. It is an accurate and efficient means of safety chip evaluation.

Key words: laser; FPGA; fault injection; SM2; protection verification

1 引言

随着信息化时代的不断发展,信息在传递、存储以及处理过程中遇到的安全问题越来越被重视. 信息安全的本质是密码算法的安全性,密码芯片作为信息安全产品的基础,应用越来越广泛,对于其安全性的验证研究非常重要. 现场可编程门阵列(Field Programmable Gate Array,FPGA)以其自身设计灵活、可靠性高等优点被广泛应用于安全领域中密码算法的实现. 但是,密码算法在物理实现的过程中,可能会造成时间、电磁以及功耗等侧信道信息泄露,除此之外,攻击者也可以通过激光、电压毛刺等手段诱发电路故障从而获取算法执行的中间值信息. 理论上根据其侧信道信息特征,可以借助不同的算法模型实现攻击. 1996年Boneh在欧密会上首次提出故障攻击[1]的概念,通过主动向密码设备中注入错误,分析错误获得密钥信息. 近年来,国际上有研究显示通过这种方法成功实现了对DES(Data Encryption Standard)算法、3DES算法、AES(Advanced Encryption Standard)算法等算法的攻击[2-6]以及利用椭圆曲线密码系统的故障来确定密钥[7]. 对于一些密码算法的签名过程来说,一旦签名私钥被攻击,由此带来的损失可能是灾难性的[8]. 其中故障攻击是一种比较有效的攻击手段,对

收稿日期:2021-01-18;修回日期:2021-08-29;责任编辑:孙瑶
基金项目:国防科工局技术基础科研项目(No.JSHS2019203B001);中国科学院青促会研究奖励基金(No.2018179)

其防护等的实验研究非常必要.

2015年,Selmke等人[9]提出90 nm和45 nm芯片的单个位激光故障注入的可行性. 近年来,激光作为一种精确有效的瞬时故障[10]注入手段,在FPGA等密码芯片的评测方面得到了应用. 本文以28 nm工艺的Kintex-7系列FPGA芯片为实验对象,通过激光手段对以SM2加密算法为例的防护设计进行了随机和指定比特辐照,实现了SM2算法数字签名中基点的单比特故障注入,验证了其防护算法的有效性.

2 Kintex-7系列FPGA

本文选用先进的28 nm工艺Kintex-7系列FPGA,该系列FPGA作为密码算法的典型载体,具有高性能、低功耗等特点,被广泛应用于航空航天、广播、通信、医疗等领域. 其中可配置逻辑块(Configurable Logical Block,CLB)是实现时序逻辑和组合逻辑电路的主要单元,也是Kintex-7系列FPGA中数量最多的逻辑资源[11]. 如图1所示,一个CLB单元由两个Slice组成,每个Slice主要包括6输入的查找表LUT、多路复用器、进位链、寄存器等结构单元. 按照功能划分,其可分为用于逻辑、算术、ROM功能的SliceL和另外可配置为分布式RAM或32位的移位寄存器的SliceM.

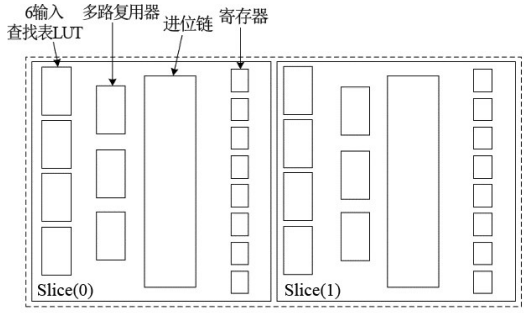

图1 Kintex-7系列FPGA CLB单元示意图

芯片封装会极大程度上影响激光的传输效率甚至阻碍激光传输,因此在芯片进行激光注入前,需对芯片进行合适的开封装处理. 不同的封装材料和封装形式需要采用不同的开封装手段,如图2所示.

Kintex-7系列FPGA芯片采用如图3所示的倒装芯片球栅阵列封装FC-BGA(Flip Chip Ball Grid Array),这种封装的金属布线层靠近焊球更便于走线,借助激光切割、物理拆卸等方法对芯片进行背部开封装处理后,如图4所示,裸露的硅衬底可以直接进行激光注入实验. 芯片背部开封装后测得裸芯片尺寸约为15 700 μm×9 000 μm,衬底厚度约705 μm.

图2 Kintex-7系列FPGA背部开封装图

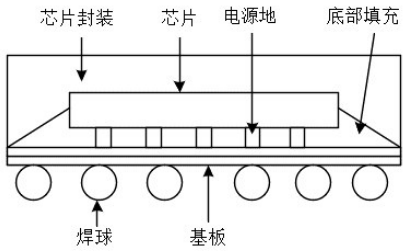

图3 FCBGA封装结构示意图

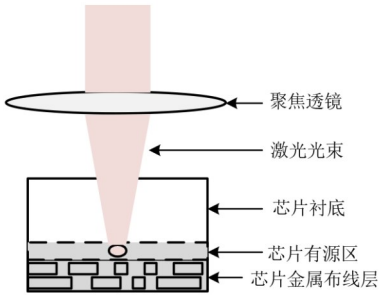

图4 开封装后激光注入示意图

3 激光故障注入实验原理及装置

3.1 激光故障注入实验原理

在常见的MOS工艺、双极工艺等集成电路中,激光辐照使其存储单元受到瞬态脉冲的影响导致双稳态结构[12,13]的关键节点电平发生改变,从而导致存储信息的改变. 从微观上来看,脉冲激光诱发故障的过程分为两步:电荷产生过程和电荷收集过程[14].

本实验聚焦的主要是Kintex-7系列FPGA基本逻辑单元中的寄存器,其主要由主锁存器和从锁存器两部分组成,以主锁存器中的I_1和I_2为例绘制其构成的交叉耦合反相器结构. 如图5所示,若D状态和时钟信号均处于高电平时,主锁存器维持,此时Q_M端输出信号为1. 当激光注入主锁存器的交叉耦合反向器结构,其MOS管中大量的反偏PN结不断的收集电荷. 这里以反相器I_3中的MOS管N_2为例,其漏极对激光辐照敏感,在收集电荷超过一定阈值时,发生高低电平的转换,此时原本截止的N_2受到瞬间电流的影响导通,Q_M的值从1跳变到0,并被交叉耦合结构锁存,而后直接传送到从级的输出端Q,导致Q值发生改变,也即成功完成故障注入.

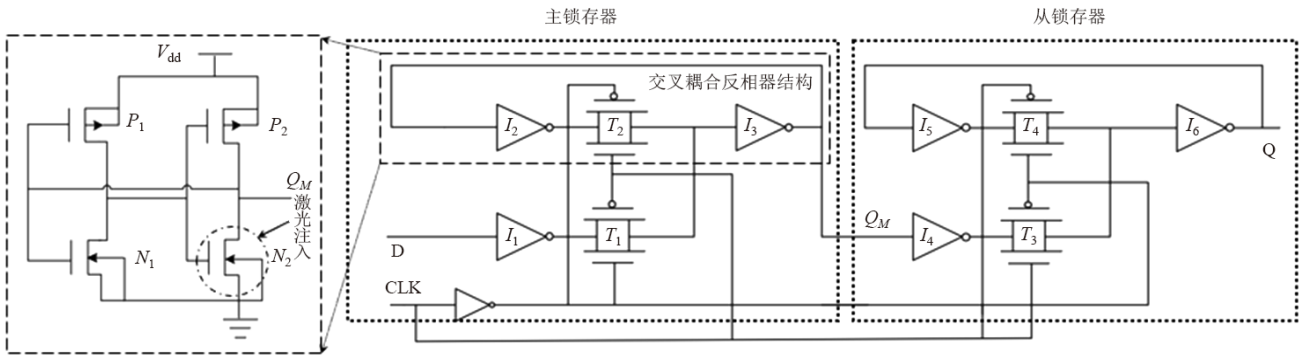

图5　CLB单元寄存器结构示意图

3.2　激光故障注入装置及激光参数选择

脉冲激光实验平台如图6所示,其中脉冲激光器用来产生激光,聚焦传导光路通过设计一系列的光路实现激光的传递和调节,三维精密移动台用来承载实验芯片,集成控制设备用来控制激光器以及其他实验组件等,其实物图如图7所示.

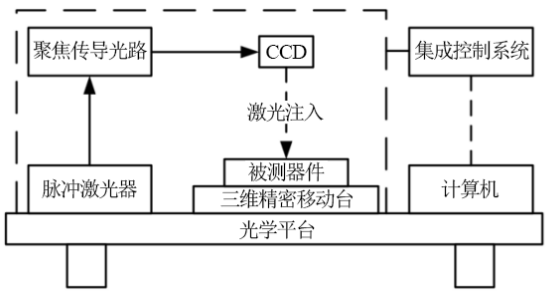

图6　激光故障注入装置示意图

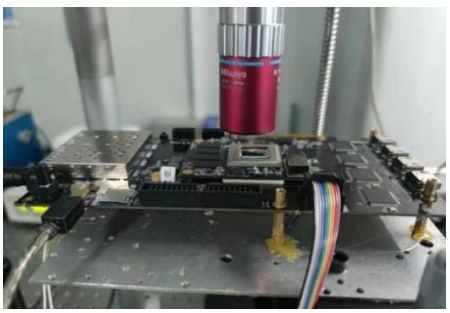

图7　激光故障注入装置实物图

激光在硅半导体器件背部辐照时,波长必须同时满足两个条件:首先,单个光子能量需要大于1.1 eV的禁带宽度,才能在硅中产生沉积能量并电离电荷,利用式(1)计算可得,激光波长必须小于1 130 nm,即

$$E=hc/\lambda \tag{1}$$

其次,激光入射到半导体材料时,激光强度I随入射深度x的变化满足Beer定律,即

$$I(x)=I_0\exp(-\alpha x) \tag{2}$$

其中,I_0为入射激光初始光强;$\alpha=4\pi k/n\lambda$为吸收系数,k为消光系数,λ为激光波长. 要使激光在硅中的穿透深度要足够穿透硅衬底,应使激光的波长尽可能长. 综合考虑激光故障注入选用的激光波长为1 064 nm,该波长为工业常用激光波长,激光设备较易获得.

脉冲宽度的选择也影响激光故障注入的效果,脉冲宽度太短会引起非线性效应造成双光子吸收且经济成本过高,脉冲宽度太长则超过芯片敏感结点的电荷吸收相应时间,甚至烧蚀器件. 最适宜进行故障注入的激光脉冲宽度一般在10~50 ps之间,本文选用激光器的脉冲宽度为25 ps. 为保证有足够的激光能量可调节范围,激光器输出平均激光能量的稳定性不低于95%,聚焦后激光光斑的直径约为2.2 μm.

4　实验过程及结果

4.1　加密算法防护设计实现

SM2算法是椭圆曲线体制下的一种公开密钥加密算法,被广泛应用于IPsec等安全协议的身份认证过程[15],其算法的主要过程包括公钥加密算法、数字签名算法以及密钥交换协议等. 它使用的椭圆曲线数字签名[16]和普通的数字签名有所区别,其计算过程基于有限域上椭圆曲线点群的运算规则[17],对该过程的故障攻击直接关系到私钥信息的获取. 相关防护算法针对SM2数字签名的生成算法中使用的标量乘方案进行设计,算法及具体防护点如算法1和表1所示. 该方案较全面的包含了参数校验、点校验、输出结果校验等目前常用的故障防护方法.

4.2　翻转能量测试与区域约束

首先对引起翻转的能量范围进行实验测试,小于600 pJ的能量基本不能引起翻转,大于1.2 nJ的激光能量可能会导致芯片出现硬错误. 因此设置激光能量800 pJ左右,该能量为选定芯片成功故障注入的最佳能量.

为针对性地对防护点进行故障注入,需精确定位

算法1 SM2数字签名生成算法标量乘故障防护方案

输入: k, G

输出: $Q=kG$

1. 验证G是否为椭圆曲线上的点(参数校验)
2. $R=$Randompoint(·),并验证R是否为椭圆曲线的点,且是否为非零值点(点校验)
3. $T_0=R, T_1=-R, T_2=G-R$,并验证G是否为椭圆曲线上的点(参数校验)
4. i等于$f-1$至0,依次执行$T_0=2T_0$,$T_0=T_0+T_{k_i+1}$
5. 验证T_2-T_1是否为G,T_0+T_1是否为椭圆曲线上的点并返回T_0+T_1(输出结果校验、点校验)

表1 SM2数字签名生成算法标量乘故障防护点

防护点	防护内容
1	标量乘开始阶段对于基点G的校验
2	标量乘中对于生成的随机点的校验
3	标量乘中使用基点G计算出T_0,T_1,T_2后,对基点G进行校验
4	标量乘中f轮迭代完成后,对T_2-T_1是否为G进行校验
5	标量乘中计算完成后,验证T_0+T_1是否为曲线上的点

激光扫描范围. 本实验根据标量乘防护的几个防护点,分别提取需要进行故障注入的256比特数据,将其约束到如图8所示指定位置,大小约为600 μm×700 μm.

根据故障防护点需求确定激光注入时间,结合激光聚焦点、芯片衬底厚度以及基点等需故障注入的约束范围确定故障注入的空间位置,利用逻辑位置与物理位置的映射关系确定如图9所示的激光扫描范围,配置激光注入参数后开始扫描,结束后调试回读故障注入后的值与目标原值进行对比,并观察防护算法的响应情况,实验中的各参数可根据不同的实验目的要求进行调整设置.

4.3 随机覆盖故障注入实验

本实验针对约束的256比特进行随机故障注入,利

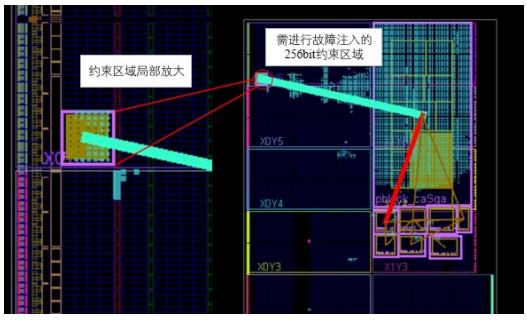

图8 FPGA故障注入位置约束图

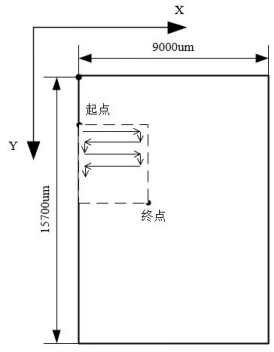

图9 激光扫描示意图

用合适的激光能量,2 μm的扫描间距以及5 000 μm/s的速度进行扫描,扫描区域大小为900 μm×900 μm,可完全覆盖约束区域,扫描一次用时约14 min. 具体防护验证实验参照SM2数字签名生成算法综合防护方案中的各个防护点进行设计. 五个防护点各选取一组数据记录如下,利用校验点1实验数据绘图,如图10所示.

在扫描速度间距合适且能量大小等条件控制得当的情况下,借助激光手段可成功完成故障注入,如表2所示,实验分别在五个防护点均成功实现了故障注入,并均能被防护算法检测拦截,整体上实现了SM2算法数字签名过程标量乘防护设计有效性验证.

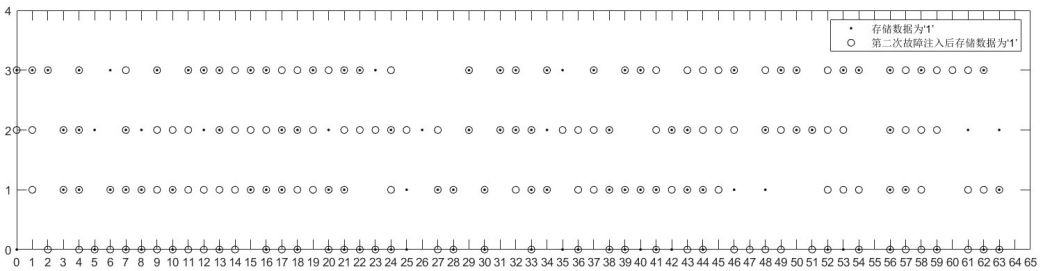

图10 防护点1故障注入对比图

图10中,"·"代表本次故障注入中存储数据从原来的1变成0,"○"表示存储数据从原来的0变成1,防护点1的实验中故障位数共计90位,其中基本每个字节的存储数据均能有所改变. 结合故障注入位数统计表3,从注入效率上来看,14 min平均完成了66.4位的故障注入,覆盖率达到25.9%. 缩小扫描间隔至1 μm,重复防护点1实验,故障数提升至107,覆盖率从25.9%提升至41.8%. 实验数据表明,缩小扫描间距可以有效提升激光注入故障覆盖率.

表2　防护实验结果记录

校验点	实验数据	
1	正确值	91167a5ee1c13b05d6a1ed99ac24c3c33e7981eddca6c05061328990f418029e
	故障值	8396fa17feb7bfffffffffbffc2e12c3fefa89ec7fe625d0af10ed90b3ff0dd6
2	正确值	aebe14e52e3aa5846f50e8c7c8ab955d6cdfa963002ff1e985d877e4c8181643
	故障值	aebe14e52e3aa5846750e8c7c8ab955d6cdfa963002000020000083ba5809603
3	正确值	91167a5ee1c13b05d6a1ed99ac24c3c33e7981eddca6c05061328990f418029e
	故障值	d51278dfe19fbb0dcffbe8e9a474cbc377fd93f9ddb001512c228cfef5fc039e
4	正确值	c87c322fd2c14fab3e44aac9403411b68cc84e0312d64943dbe8d34b964ef3e1
	故障值	5010030180c005a82604a20000001120848046031bd24943d8a8d3089762b300
5	正确值	50180002924d225bbb647dcb6f24b22076d666224a0a359aa66d093006f44f61
	故障值	545c801f9247327bf9ecf9f1ffa73f19bcd76f32da7e35afde7d39b8b6f25fe5

表3　各防护点实验故障位数结果统计表

实验	故障位数	故障覆盖率	平均故障注入位数
防护点1	90	35.2%	66.4
防护点2	47	18.4%	
防护点3	64	25%	
防护点4	61	23.8%	
防护点5	70	27.3%	

4.4　指定比特故障注入实验

激光故障注入的精确度可以通过改变扫描间距，控制扫描速度、精确定位敏感区域等实现．如图11和图12所示，数据1存储在slice(1)中的触发器结构中，激光聚焦的光斑等相关尺寸见标注．

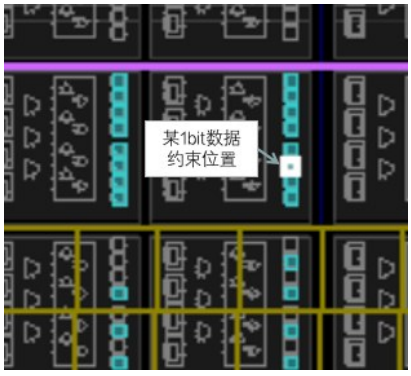

图11　SLICE中比特约束图

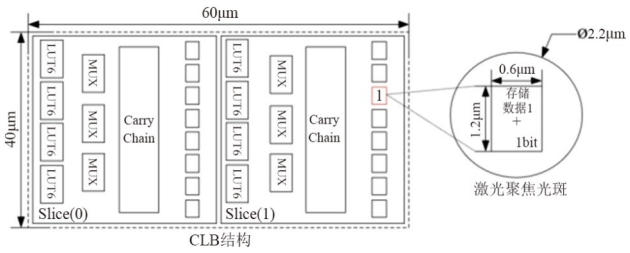

图12　CLB单元指定比特存储示意图

定位指定比特在物理版图上的对应位置，通过三维移动台控制激光辐照位置，可以控制故障注入的字节以及比特位信息．根据流程图(图13)操作，单比特敏感区定位后，重复多次利用激光注入，观察比特翻转情况．实验中以SM2算法数字签名过程中基点的第一个字节的最低位存储1的比特位为例，在敏感区附近进行多次注入激光可实现1到0的存储信息改变．完成单比特的故障注入后，执行防护算法仍有效．

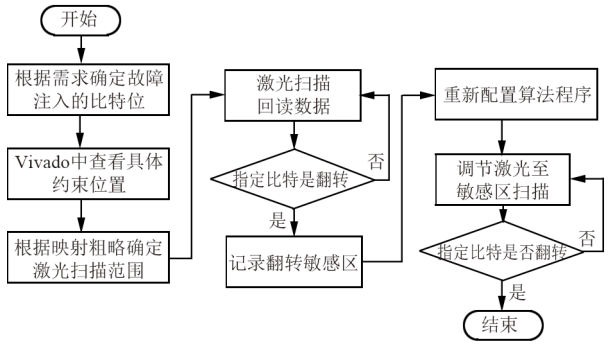

图13　单比特故障注入实验流程图

5　结束语

故障注入测试是高可靠安全芯片应用必经的测试环节，是密码算法防护设计验证的有效手段，也是判断电路系统容错能力的重要途径．本文通过脉冲激光实验装置对于背部开封装的28 nm FPGA芯片进行了激光故障注入实验，分别以随机故障注入和指定比特故障注入两种模式实现了SM2算法数字签名的故障注入，对其标量乘防护设计的效果进行了验证．

利用激光实现的故障注入不受接口条件约束，不需要介入内部的算法程序，直接在开封装的芯片外部即可完成，具有很好的真实性和覆盖性．针对评测所需的故障注入区域，激光既可以通过扫描方式实现高效率、高覆盖率的故障注入，也可以通过定点方式实现指定比特的可重复故障注入，满足密码评测需求．

参考文献

[1] BONEH D, DEMILLO R A, LIPTON R J. On the impor-

tance of checking cryptographic protocols for faults[C]// Advances in Cryptology-EUROCRYPT' 97. Berlin: Springer, 1997: 37-51.
[2] GIRAUD C. DFA on AES[J]. Lecture Notes in Computer Science, 2004, 3373: 27-41.
[3] HEMME L. A differential fault attack against early rounds of(triple) DES[C]//International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2004: 254-267.
[4] DUSART P, LETOURNEUX G, VIVOLO O. Differential fault analysis on AES[M]//Applied Cryptography and Network Security. Berlin: Springer, 2003: 293-306.
[5] HOCH J J, SHAMIR A. Fault analysis of stream ciphers [C]//International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2004: 240-253.
[6] CHEN C N, YEN S M. Differential fault analysis on AES key schedule and some countermeasures[M]//Information Security and Privacy. Berlin: Springer, 2003: 118-129.
[7] BIEHL I, MEYER B, MÜLLER V. Differential fault attacks on elliptic curve cryptosystems[M]//Advances in Cryptology–CRYPTO 2000. Berlin: Springer, 2000: 131-146.
[8] 侯红霞, 杨波, 张丽娜, 等. 安全的两方协作SM2签名算法[J]. 电子学报, 2020, 48(1): 1-8.
HOU H X, YANG B, ZHANG L N, et al. Secure two-party SM2 signature algorithm[J]. Acta Electronica Sinica, 2020, 48(1): 1-8. (in Chinese)
[9] SELMKE B, BRUMMER S, HEYSZL J, et al. Precise laser fault injections into 90 nm and 45 nm SRAM-Cells [M]//Smart Card Research and Advanced Applications. Cham: Springer International Publishing, 2016: 193-205.
[10] 王晶, 荣金叶, 周继芹, 等. 软硬件协同设计的SEU故障注入技术研究[J]. 电子学报, 2018, 46(10): 2534-2538.
WANG J, RONG J Y, ZHOU J Q, et al. The research on software-hardware co-designed SEU fault-injection technology[J]. Acta Electronica Sinica, 2018, 46(10): 2534-2538. (in Chinese)
[11] 陈环. FPGA功能测试研究[D]. 成都: 西华大学, 2020.
CHEN H. Research on FPGA Function Test[D]. Chengdu: Xihua University, 2020. (in Chinese)
[12] WIRTH G, KASTENSMIDT F L, RIBEIRO I. Single event transients in logic circuits–Load and propagation induced pulse broadening[J]. IEEE Transactions on Nuclear Science, 2008, 55(6): 2928-2935.
[13] DODD P E, MASSENGILL L W. Basic mechanisms and modeling of single-event upset in digital microelectronics [J]. IEEE Transactions on Nuclear Science, 2003, 50(3): 583-602.
[14] 黄建国, 韩建伟. 脉冲激光诱发单粒子效应的机理[J]. 中国科学G辑: 物理学、力学、天文学, 2004, 34(2): 121-130.
[15] 李凡, 李云峰, 翁天恒, 等. 基于FPGA的SM2点运算快速并行实现[J]. 电子测量技术, 2020, 43(15): 105-111.
LI F, LI Y F, WENG T H, et al. Implementation of parallel and fast SM2 point calculation on FPGA[J]. Electronic Measurement Technology, 2020, 43(15): 105-111. (in Chinese)
[16] JOHNSON D, MENEZES A, VANSTONE S. The elliptic curve digital signature algorithm(ECDSA)[J]. International Journal of Information Security, 2001, 1(1): 36-63.
[17] 侯鲁. 对SM2数字签名的攻击[D]. 济南: 山东大学, 2020.
HOU L. Attacking ECDSA of SM2[D]. Jinan: Shandong University, 2020. (in Chinese)

作者简介

蔡 莹 女,1997年12月出生,河南平顶山人. 2019年获中国地质大学(武汉)自动化专业学士学位及华中科技大学经济学双学士学位. 现为中国科学院国家空间科学中心硕士研究生. 主要从事芯片故障注入、硬件木马等方面的研究工作.
E-mail: fromcy@163.com

朱 翔(通讯作者) 男,1985年3月出生,安徽合肥人. 2005年和2008年在中国科学技术大学分别获得学士和硕士学位,2020年在中国科学院大学获博士学位. 现为中国科学院国家空间科学中心高级工程师,硕士生导师. 主要从事高可靠电子系统设计、芯片故障注入技术、抗辐射技术等方面的研究工作.
E-mail: zhuxiang@nssc.ac.cn