基于微控制器的AES激光注入攻击研究

姜会龙[①②] 朱 翔*[①②] 李 悦[①] 马英起[①] 上官士鹏[①②]
韩建伟[①] 蔡 莹[①②]

[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)

摘 要：密码设备面临故障攻击的威胁，针对密码芯片的故障攻击手段研究是密码学和硬件安全领域的重要研究方向。脉冲激光具有较好的时空分辨性，是一种准确度较高的故障攻击手段。该文详细描述了激光注入攻击的原理和方法，以集成AES-128算法的微控制器(MCU)为例实施了激光注入攻击实验。实验以微控制器的SRAM为攻击目标，分别成功实现了差分故障攻击和子密钥编排攻击，恢复了其16 Byte的完整密钥，其中后一种攻击是目前首次以激光的手段实现。研究表明，激光注入攻击能准确定位关键数据存放的物理位置，并能在任意的操作中引入错误，实现单比特的数据翻转，满足故障攻击模型的需求。激光注入攻击能在较短时间内完成自动攻击和密文收集，攻击过程贴近真实场景，对密码芯片具有极大的威胁。

关键词：故障攻击；微控制器；AES；激光注入；SRAM

中图分类号：TN918.2 **文献标识码**：A **文章编号**：1009-5896(2021)05-1357-08

DOI: 10.11999/JEIT200163

Research on Laser Injection Attack for AES Based on Micro-Controller Unit

JIANG HuiLong[①②] ZHU Xiang[①②] LI Yue[①] MA Yingqi[①]
SHANGGUAN Shipeng[①②] HAN Jianwei[①] CAI Ying[①②]

[①](*National Space Science Center*, *Chinese Academy of Sciences*, *Beijing* 100190, *China*)
[②](*University of Chinese Academy of Sciences*, *Beijing* 100049, *China*)

Abstract: The security of cryptosystem is threatened by fault attacks, and implementation of fault attacks for crypto chips become an important research direction in the field of cryptography and hardware security. The pulse laser is a method with high accuracy for its high temporal-spatial resolution. In this paper, the principle and method of laser injection attacks are described in detail, and experiments are carried out on a Micro-Controller Unit (MCU) with AES-128 algorithm as an example. The SRAMs of the MCU are taken as the attack targets. Differential fault attack and the subkey expansion attack are successfully implemented, and the 16 Byte complete keys are recovered respectively. The latter attack is first implemented by the laser. The research shows that laser injection attack has many benefits to meet the requirements of fault attack models, including accurate location of critical data, error injection in any operation, and generation of single bit flip. The laser injection attacks and ciphertext collection can be completed automatically in a short time in a nearly real-life scenario, which has a great threat to the crypto chips.

Key words: Fault attack; Micro-Controller Unit (MCU); Advanced Encryption Standard (AES); Laser injection; SRAM

收稿日期：2020-03-10；改回日期：2020-10-25；网络出版：2020-11-19
*通信作者： 朱翔 zhuxiang@nssc.ac.cn
基金项目：中国科学院重点部署项目(KGFZD-135-16-005)，中国科学院空间科学预先研究项目(XDA15014600)
Foundation Items: The Key Deployment Projects of Chinese Academy of Sciences (KGFZD-135-16-005), The Space Science Advance Research Projects of Chinese Academy of Sciences (XDA15014600)

1 引言

以智能卡为代表的密码芯片广泛应用于通信、金融、交通、政务、社保等领域，是维持和保障网络信息安全的核心载体之一。一般而言，密码芯片的安全性取决于所采用的密码体制。然而，自1996年Kocher提出时间攻击以来，针对密码算法在物理实现上存在的信息泄露隐患，在密码芯片运算过程中实施各种旁路攻击，就有可能获得其存储的秘密信息。旁路攻击按攻击方式可分为被动攻击和主动攻击。被动攻击一般不干扰密码芯片的正常运行，通过收集芯片运行时的功耗、电磁辐射等信息进行分析，主要包括时间攻击、能量攻击和光辐射分析等[1]。主动攻击一般指故障攻击，即在芯片运行时有意诱发故障，通过故障分析恢复密钥。诱发故障的手段包括电压或时钟毛刺、电磁扰动、温度变化、聚焦离子束(Focused Ion Beam, FIB)、紫外光辐照、激光注入等[2]，其中激光注入因具有较高的时间和空间分辨性，通常被认为是最有潜力的故障注入手段之一。当前，国际上商业化的激光注入装置已在密码芯片测评行业中使用，取得了一定的效果。国内激光注入技术的研究相对较少。因此，自行设计密码芯片的激光攻击安全性测试系统，对国内集成电路和信息安全领域的研究至关重要。本文依托中国科学院国家空间科学中心自主研制的单粒子效应脉冲激光实验平台，通过优化设计形成密码芯片激光注入攻击实验装置，具备较高的时间和空间精准度，并且有一定的自主测试和故障识别的能力，适合开展激光注入攻击实验研究。

智能卡的核心为微控制器，本文以智能卡常用的ATMEGA163型微控制器及AES-128为例，详细论述脉冲激光攻击密码芯片的流程和方法，具体从以下几个部分展开：(1)第2节介绍AES算法及两种故障攻击模型；(2)第3节讨论密码芯片的激光故障注入原理，并介绍激光注入的实验装置；(3)第4节介绍微控制器激光攻击的实践以及攻击的结果；(4)第5节为结束语。

2 AES算法及故障攻击

2.1 AES算法

高级加密标准(Advanced Encryption Standard, AES)是美国国家标准技术协会(National Institute of Standards and Technology, NIST)于2001年发布的用于取代数据加密标准(DES)的分组密码算法。其数据分组长度为128 bit，密钥长度可以为128, 192或256 bit，分别对应加密轮数为10轮、12轮以及14轮，这里关注的是128 bit版本。AES是基于有限域运算的SPN结构迭代分组密码，输入的明文数据被描述为4×4状态矩阵(state)，首先与初始密钥执行异或操作，再进行10轮迭代运算。AES以字节或字为单位进行操作，每轮的操作为：字节变换(SubBytes)、行移位(ShiftRows)、列混淆(MixClumns)以及轮密钥加(AddRoundKey)，最后一轮不执行列混合操作。因其较高的安全性和执行效率，AES算法是目前使用最广泛的加密算法之一。

2.2 故障攻击

故障攻击最早在针对CRT-RSA的攻击中被研究者提出，之后广泛应用到各类密码算法的攻击研究中。针对AES算法的DFA攻击在2003年被首次提出，攻击者使用不超过50个密文对即可恢复128 bit完整密钥[3]。同年，另一研究指出在第8轮和第9轮列混合之间注入单字节故障，使用2个密文对可将密钥候选空间降为2^{40}[4]。针对AES密钥编排过程的攻击方法在2008年被提出，使用2个密文对可将密钥搜索空间降为2^{32}；使用4个密文对则可以降为1[5]。2009年，研究者提出在AES的第7轮和第8轮列混合之间注入1个字节故障，可将密钥候选空间降为2^{32}，若再用一条同一字节的故障密文，可将候选空间降为1。2011年，研究者又在上述研究的基础上利用第9轮和第10轮的子密钥之间的关系，仅使用1条密文即可将候选空间降为2^8[6]，这是目前已知针对AES效率最高的DFA攻击方法。以上的研究为单字节或单比特故障模型，此外还有针对AES的多字节故障模型[7]。2018年，文献[8]针对分组密码提出了持久故障攻击(Permanent Fault Attack, PFA)的方法。对AES的S盒注入持久错误后使用大约2000条密文可恢复完整密钥，对基于双冗余防护的AES算法攻击依然有效。近年来，轻量级算法备受人们关注，一些针对该类算法的故障攻击方法也被提出[9–11]。

故障攻击的第1步是通过不同的手段诱导设备产生特定类型的故障并收集信息。毛刺和电磁脉冲手段产生的故障一般是随机多字节错误，而激光则兼具时空精准度，能产生单比特或单字节类型的故障[12]。故障攻击的第2步是通过合适的故障模型来分析取得的信息，常见的故障模型有差分故障攻击(Differential Fault Attack, DFA)、子密钥编排攻击、碰撞故障攻击(Collision Fault Attacks, CFA)、无效故障攻击(Invalid Fault Attack, IFA)、代数故障攻击(Algebra Fault Attack, AFA)等。差分故障攻击和子密钥编排攻击是两种效率较高的故障模型，本文以这两种故障模型展开了攻击的实验。

2.2.1 差分故障攻击

差分故障攻击利用故障注入后的故障密文对来建立差分方程，通过求解方程来恢复密钥。图1是第9轮输入第1个字节的故障差分传播模型，设密文第i个字节对应第10轮输入的差分为δ_i，以C_i和$\tilde{C}_i$分别表示正确值和错误值，以K_i^{10}表示第10轮的子密钥的第i字节，则可以得到式(1)关于δ和K_i^{10}的关系

$$\mathrm{Sub}^{-1}(C_i \oplus K_i^{10}) \oplus \mathrm{Sub}^{-1}(\tilde{C}_i \oplus K_i^{10}) = \delta_i,\quad i = 0,1,\cdots,15 \tag{1}$$

攻击者首先需要为式(1)等号右侧建立一个查找表，由δ取遍0x01～0xFF并利用4个故障字节在第9轮列混合后产生的差分比例关系，进一步筛选得到4 Byte的密钥候选值。

2.2.2 子密钥编排攻击

对第9轮子密钥编排的过程引入故障，故障将引发第10轮子密钥和密文产生多个错误字节。图2展示了Kim等人[5]的攻击模型，故障引入第9轮子密钥的第1个字节，将造成第10轮子密钥的6个字节出错，密文8个字节出错。如图2设第9轮子密钥第1个字节注入故障产生差分a，经过第9轮的密钥扩展后子密钥K^9及错误值$\tilde{K}^9$的第1行满足：$K^{9,1} \oplus \tilde{K}^{9,1} = (a,a,a,a)$，同时第9轮输出的第1行的差分也满足$(a,a,a,a)$，经字节变换和行移位操作后差分变为$(b_1,b_2,b_3,b_4)$；接下来经过第10轮的子密钥扩展，第10轮子密钥将产生6个故障字节，密文对$(C,\tilde{C})$的差分满足

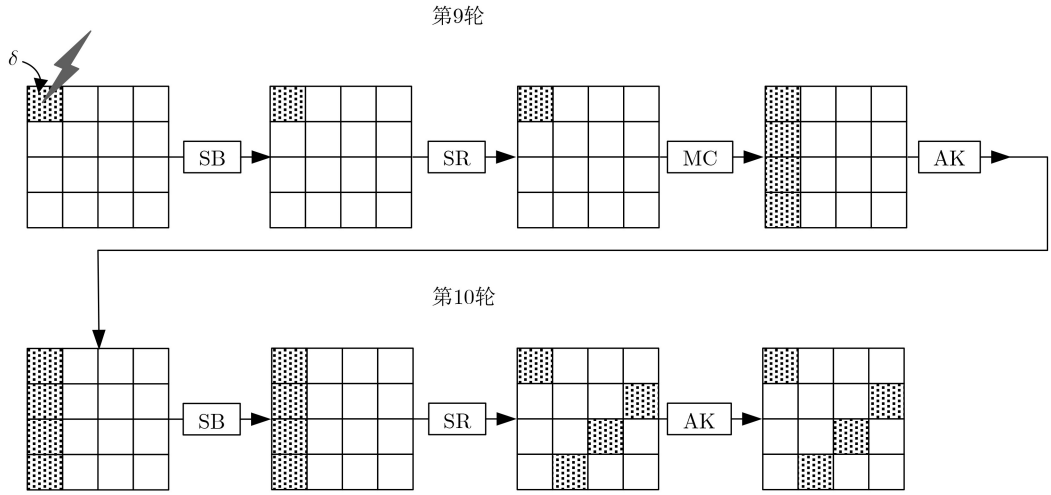

图 1 第9轮输入的故障差分传播

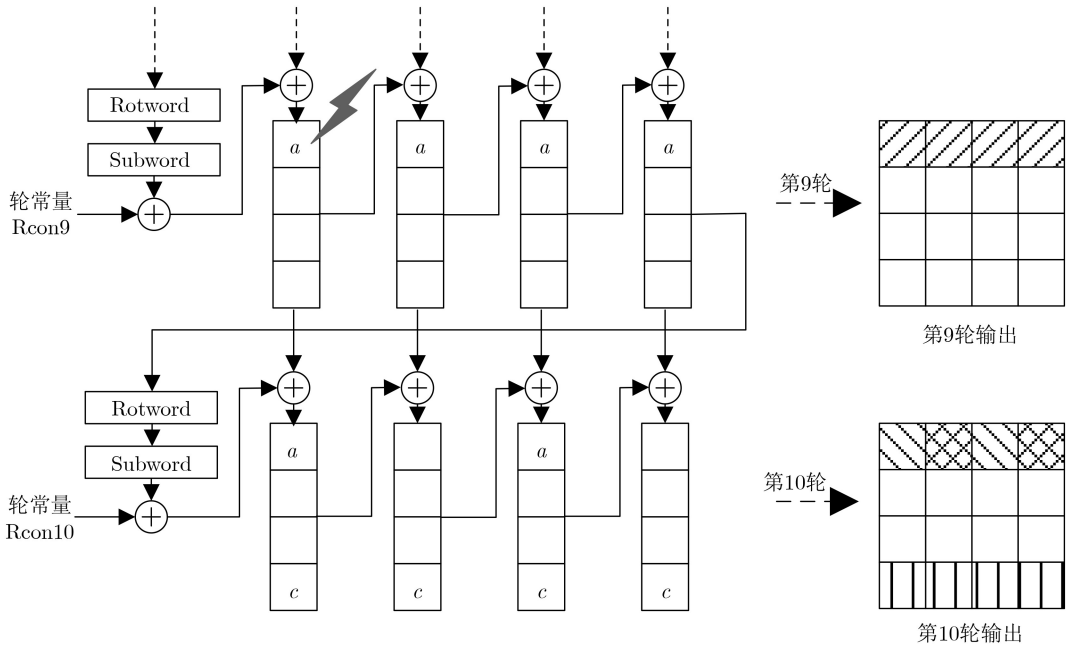

图 2 攻击第9轮子密钥编排的第1个字节

$$C \oplus \tilde{C} = \begin{bmatrix} a \oplus b_1 & b_2 & a \oplus b_3 & b_4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ c & c & c & c \end{bmatrix} \tag{2}$$

Kim等人给出了该模型下恢复第10轮子密钥的思路，以$K_i^9, K_i^{10}(i=0,1,2,\cdots,15)$分别表示第9轮、10轮的子密钥第$i$个字节，以图2中故障为例，使用两对密文$(C,\tilde{C})$和$(D,\tilde{D})$恢复第10轮4 Byte密钥$(K_0^{10}, K_4^{10}, K_8^{10}, K_{12}^{10})$的步骤可概括如下：

(1) 考虑(K_4^{10}, K_{12}^{10})两个字节所对差分关系

$$\begin{aligned}(\alpha_1,\alpha_2) = &\mathrm{SB}^{-1}[\mathrm{SR}^{-1}(C_4 \oplus K_4^{10}, C_{12} \oplus K_{12}^{10})] \\ &\oplus \mathrm{SB}^{-1}[\mathrm{SR}^{-1}(\tilde{C}_4 \oplus K_4^{10}, \tilde{C}_{12} \oplus K_{12}^{10})]\end{aligned} \tag{3}$$

遍历两个密钥字节，将(α_1,α_2)中满足$\alpha_1=\alpha_2$的密钥字节及相应差分值放入集合M。

(2) 计算下一个字节K_8^{10}，同样应满足式(3)的差分关系，此时差分值从集合M中遍历即可，将得到的候选密钥和差分值放入集合N。

(3) 计算第4个字节K_0^{10}，依照式(3)的关系从集合N中遍历差分值即可。

可以证明只需2对密文即可将4个字节的密钥候选值数目降为1，因此将完整密钥候选数目降为1需要8对密文[5]。

3 激光注入攻击原理和实验装置

3.1 激光注入攻击

利用激光诱发集成电路故障始于对单粒子效应(Single Event Effect, SEE)的研究，后来作为一种主动式的故障注入手段被应用于侧信道攻击领域。2007年，Schmidt等人用波长为785 nm的低成本激光设备为一款8 bit的微控制器注入故障，成功恢复了CRT-RSA的密钥。2010年，Agoyan等人[13]首次实现对无防护的AES算法的激光注入攻击，攻击目标是事先生成并存放在SRAM中的10轮子密钥。2013年，Roscian等人[14]使用光斑直径达到100 μm的激光束对一款130 nm的微控制器正面实施了激光注入攻击。该实验表明，即使使用大尺寸的光斑仍可能进行单比特类型的故障注入，他们解释这一现象是金属层遮挡了部分SRAM单元的敏感区导致。2011年Canivet等人首次利用激光对FPGA实现的AES算法注入故障。2014年，Courbon等人[15]借助扫描电子显微镜对微控制器实施了比特级精准的置位/复位的攻击。2018年，Breier等人[16]提出了针对微控制器的指令跳过等故障模型，并对流密码ChaCha实施了激光注入攻击。2020年，Zhang等人[17]利用1064 nm的激光器对AES算法的S盒实施了故障攻击，验证了PFA攻击的现实可行性。国内方面，也有少部分的学者从事该领域的研究。2015年，王红胜等人[18]对CRT-RSA成功实施了激光注入攻击。近些年，一些机构和公司团体也对激光攻击的方法进行了研究[19]。

鉴于激光注入攻击对技术和成本的较高要求，国内外相关领域的研究尚存在诸多困难，多数的攻击往往借助理想化的条件来降低攻击难度，国内相关领域的研究仍处于起步阶段。本文所开展的激光注入攻击实验具备较高的时空精准度，针对子密钥编排的攻击更贴近真实场景，也是目前已知资料中首次利用激光对密钥编排过程展开的攻击。

3.2 激光注入攻击的原理和辐照芯片的方式

对于硅半导体，光子能量大于1.14 eV的辐照光可以激发光致载流子，即电子-空穴对。在PN结附近的电荷会在电场作用下被收集，光电流可使得处在截止状态的PN结导通。在典型的SRAM 6管单元中，处在锁存状态的两对MOS管分别处于开启和截止的状态，光电流会使处在截止状态的MOS管逐渐开启，另外一对MOS管则逐渐关断，随后电路进入另一种稳定状态，此时电路存储的比特发生改变。这种现象称为单粒子翻转(Single Event Upset, SEU)。因此，激光攻击SRAM单元要辐照到关断的MOS管区域。需要注意的是，能量过高时可能会出现单粒子闩锁(Single Event Latchup, SEL)现象，芯片因内部持续的大电流而无法工作，甚至烧毁，应避免这种情况出现。攻击的第1步是将芯片去封装，可以选择从正面或背面辐照激光，近年来甚至有研究提出了从侧面辐照激光的技术[20]。正面开封时有源区较浅，可使用可见光波段进行攻击，但存在金属层的阻碍。背部开封可避免金属层的干扰，但有源区较深，需要使用穿透能力更强的激光。本实验采用1064 nm的红外激光，在硅中的穿透深度可达1000 μm，普通芯片的硅衬底一般为几十或几百μm，能轻易辐照到芯片的有源区。

3.3 实验装置

3.3.1 脉冲激光实验平台

实验装置依托单粒子效应脉冲激光实验平台，主要包括脉冲激光器、光路系统、3维移动台、同步控制系统及控制计算机，如图3所示。激光器产生1064 nm的脉冲激光，脉冲宽度为15 ps，窄脉宽可以避免多余激光能量对器件的影响；脉冲激光通过光路系统辐照待测器件，光路系统还可用于观测器件结构及光斑位置；3维移动台用于搭载待测器件，可以实现分辨率为0.1 μm激光注入位置定位，通过设置起始点和终点可以完成自动扫描实验；同步控制系统接受计算机指令，实现对激光器和移动台的

同步控制，完成目标区域和时刻的自动激光注入。

3.3.2 ATMEGA163L型微控制器及实验电路

实验对象为Atmel公司的ATMEGA163L商用MCU，其具有1 kB的内部SRAM、16 kB的Flash及4 MHz最大频率。为方便实现对MCU的数据通信和功耗分析，基于MCU专门设计了智能卡形式的电路板，可插入SASEBO-W侧信道开发板使用。对MCU来说，激光注入故障的区域可以是寄存器、SRAM或者Flash。考虑到MCU在执行AES加密时会将每轮运算的子密钥和中间数据存放在SRAM区，激光注入的目标选择MCU的SRAM区。实验前对MCU背面进行去封装并利用红外CCD拍摄了版图，如图4所示，通过版图分析可以确定MCU各功能单元的大致分布。作为存储单元，SRAM和Flash通常都有规则的结构，另外相比于SRAM, Flash通常具有更大面积的控制电路。

4　实验过程及攻击结果

4.1 攻击时序和位置控制

故障攻击实现的关键在于把握故障注入的时间和位置。SRAM中存放的中间数据和子密钥数据随算法的执行而不断刷新，需要把握好时机将故障注入到指定的操作，同时不能影响接下来的操作。故障注入的目标数据只有16 Byte，因而也需要提前确定SRAM中故障注入的位置。实验测量了MCU的实时功耗，通过简单功耗分析来确定算法的执行状态。图5是经滤波后的功耗图，从中可以很容易识别出AES的10轮操作和每轮的子操作，通过改变激光触发的延迟时间可将故障注入到特定的操作中，图中红色信号是用于触发激光的使能信号。通过3维移动台搭载待测MCU配合测试系统可以完成对整个SRAM的攻击，进行自动故障注入、故障识别和密文收集。

4.2 攻击结果

4.2.1 差分故障攻击结果

MCU背面开封后测得芯片尺寸大约为4500 μm×4500 μm，通过版图的比例可判断SRAM区域的尺寸大约为900 μm×1800 μm。如图6，以芯片的右下角作为参考点，分别沿着如图所示的X和Y方向移动300 μm和2400 μm后作为移动台的起点(0,0)，

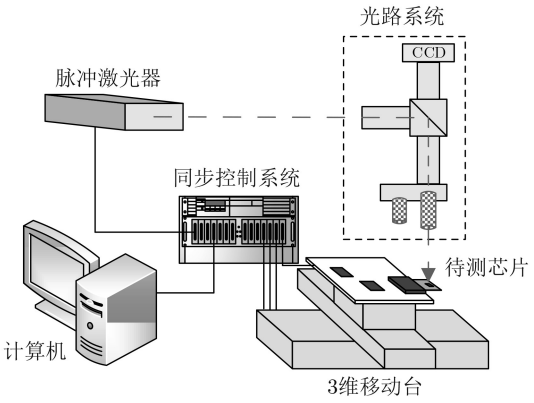

图 3 实验平台

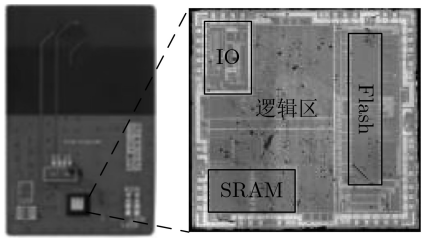

图 4 ATMEGA163L型微控制器及背部的版图

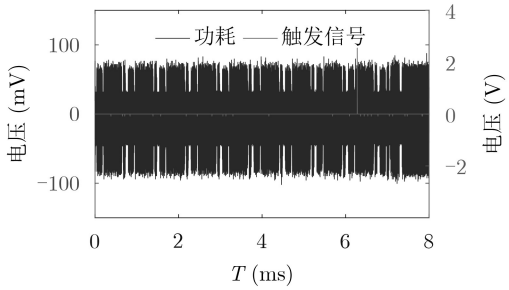

图 5 10轮AES功耗曲线(黑)及触发激光的方波信号(红)

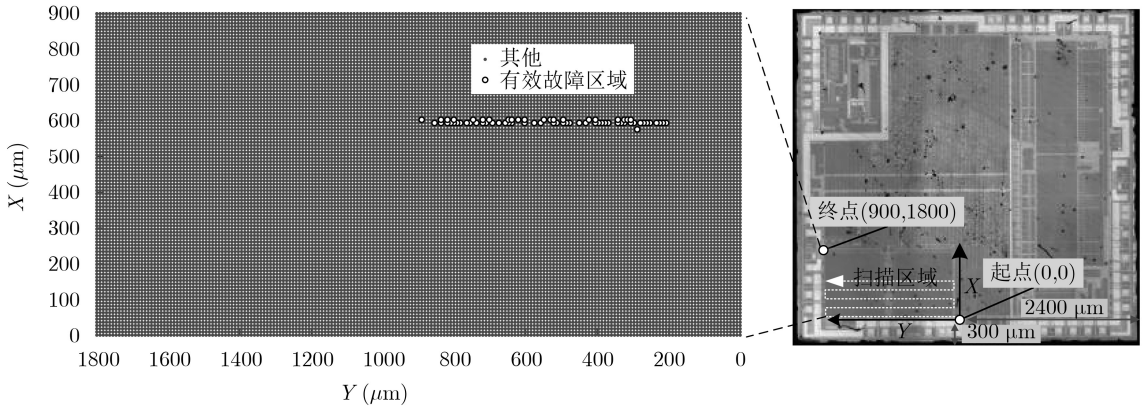

图 6 差分故障攻击的有效区域

并设置终点为(900,1800)，从而覆盖整个SRAM。虚线为移动台的运动轨迹，对整个SRAM进行激光扫描注入。设定激光触发的时刻到第8轮与第9轮的列混合之间，将移动台的位置节点间距设置为9 μm，在该区域总共产生了101×201=20301个攻击位置，每个位置耗时大约0.4 s，完成全部位置的激光注入扫描大约用时8000 s。图6展示了差分故障攻击的有效区域，该区域在不同加密时刻注入激光得到的故障密文符合差分故障攻击的密文差分特点，可以断定该区域存放了16 Byte的中间数据。

表1展示了对第9轮输入注入故障后最终恢复完整子密钥的攻击结果，实验利用15对密文将密钥候选数目降为1。

将移动台的步距设为45 μm，在该区域只使用20×40=800个攻击位置，平均可以找到约2.9个故障位置，这两个位置可以满足第8轮故障注入的要求，耗时仅320 s。考虑到普通计算机的算力，在绝大多数情况下，应用第8轮的故障模型完成首次攻击的时间不超过350 s。在得到攻击有效区域后，实验可以被准确地复现，这一时间会大大缩短。

4.2.2 对子密钥编排的攻击结果

考虑到芯片的资源限制和数据安全等因素，子密钥一般在每轮临时生成，找到子密钥存放的位置，在合适的时机将故障注入到指定字节是攻击成功的关键。图7中t_1和t_2对应两个密钥扩展操作之间的时间段，实验发现在此段时间内注入激光可引入错误至第9轮子密钥。进一步实验发现在t_1时间内注入故障产生密文有10 Byte出错，这是因为对子密钥注入的错误影响了第9轮的密钥加操作，因而注入错误的合适时间应该选择在t_2内。

选择两对密文：

$$\left.\begin{cases} C = \text{6F9B0CFE948D12DCDDB248940346DC4E} \\ \tilde{C} = \text{6F9BBC97948DA2A1DDB2F84203466CED} \end{cases}\right\} \left.\begin{cases} D = \text{C57C46A6AE15A393D8517911312630CE} \\ \tilde{D} = \text{C57CF6F9AE1513BFD851C95B3126806B} \end{cases}\right\} \tag{4}$$

根据式(2)，这两对密文的差分可以表示为

$$S^3 \oplus \tilde{S}^3 = \begin{bmatrix} a \oplus b_1 & b_2 & a \oplus b_3 & b_4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ c & c & c & c \end{bmatrix} \tag{5}$$

经过2.2.2节步骤(1)筛选后候选值情况如表2所示，K_7^{10}和K_{15}^{10}包含两个候选值。在经过步骤(2)和步骤(3)后候选值情况分别如表3和表4所示。实际上，在步骤(1)后的候选值可以直接只保留表2中的第1个，这是因为在实验中可以保证每次都能将激光注入到相同的比特位置，因此两次加密中第9轮子密钥注入故障前后差分值相等，也即$a_1 = a_2$可以作为筛选的判断条件，另外此差分为0x20说明注入的故障类型是单比特，可用于进一步缩小候选空间。对其他12 Byte的密钥采用相同的办法，实验利用8对密文将第10轮的子密钥候选值数目降为1。

4.3 攻击小结

该攻击实验花费较低的时间成本和较少的密文代价，完成了针对AES的DFA攻击和子密钥编排攻击。对于后者，对攻击的字节要求更严格，传统的电压和时钟毛刺、电磁脉冲手段比较难实现，激光则凭借其时空精准度的优势足以胜任该类型的攻

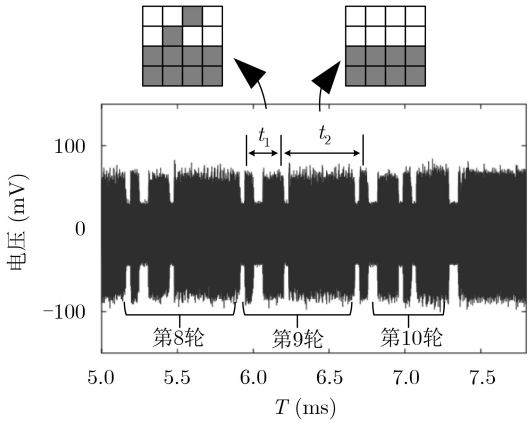

图 7 后3轮功耗及攻击子密钥的有效时间段

表 1 攻击第9轮输入的字节位置及恢复的密钥字节

输入错误字节位置	恢复字密钥字节	密文对数目	最终候选值(0x)
10	$K_0^{10}, K_7^{10}, K_{10}^{10}, K_{13}^{10}$	3	13, 17, A7, 2B
3	$K_1^{10}, K_4^{10}, K_{11}^{10}, K_{14}^{10}$	4	11, E3, 8B, 30
7	$K_2^{10}, K_5^{10}, K_8^{10}, K_{15}^{10}$	4	1D, 94, F3, C5
11	$K_3^{10}, K_6^{10}, K_9^{10}, K_{12}^{10}$	4	7F, 4A, 07, 4D

表 2 经步骤(1)筛选后的候选值情况

	K_7^{10}	K_{15}^{10}	a_1	a_2
1	0x17	0xC5	0x20	0x20
2	0x53	0xC3	0x77	0x9C

表 3 经步骤(2)筛选后的候选值情况

	K_7^{10}	K_{11}^{10}	K_{15}^{10}	a_1	a_2
候选	0x17	0x8B	0xC5	0x20	0x20

表 4 经步骤(3)筛选后的候选值情况

	K_3^{10}	K_7^{10}	K_{11}^{10}	K_{15}^{10}	a_1	a_2
候选	0x7F	0x17	0x8B	0xC5	0x20	0x20

击。对攻击的结果分析发现每次注入的故障类型均为单比特翻转，表明在该芯片的工艺尺寸下激光光斑可以覆盖单个存储单元的敏感区域，能够满足故障模型对指定字节或比特攻击的要求。

5　结束语

本文总结了激光注入攻击的实验原理和方法，以一款实现有AES-128算法的MCU为例，实施了激光注入攻击，定位了关键数据在SRAM区的物理位置。对第8轮的差分故障攻击表明，首次攻击仅使用1个明文进行大约800次激光注入，即可完成对该型号MCU的整个SRAM区的攻击恢复出完整密钥，耗时不超过350 s。实验首次利用激光的手段完成对子密钥编排过程的攻击，实验方法更符合密码芯片真实的工作场景，具有可重复性。实验表明，以微控制器为代表的密码芯片SRAM存储的变量数据受激光攻击的威胁很大，有必要考虑防护对策。针对激光注入攻击的防护对策可以分为时间冗余、空间冗余和信息冗余3类[21,22]，时间冗余包括加入随机延迟、多次加密校验密文等措施。空间冗余包括并行加密块、光传感器等措施，其中并行加密防护多针对硬件平台的算法实现。信息冗余包括算法执行过程的数据校验等措施。但无论是哪种防护措施，都会给设备带来成本增加、性能损失等缺点。针对激光注入攻击的研究，能揭示密码芯片在现实场景运行的薄弱环节，指导芯片设计从更安全的角度来实现。

参 考 文 献

[1] 陈华, 习伟, 范丽敏, 等. 密码产品的侧信道分析与评估[J]. 电子与信息学报, 2020, 42(8): 1836–1845. doi: 10.11999/JEIT190853.
CHEN Hua, XI Wei, FAN Limin, *et al*. Side channel analysis and evaluation on cryptographic products[J]. *Journal of Electronics & Information Technology*, 2020, 42(8): 1836–1845. doi: 10.11999/JEIT190853.

[2] 王安, 葛婧, 商宁, 等. 侧信道分析实用案例概述[J]. 密码学报, 2018, 5(4): 383–398. doi: 10.13868/j.cnki.jcr.000249.
WANG An, GE Jing, SHANG Ning, *et al*. Practical cases of side-channel analysis[J]. *Journal of Cryptologic Research*, 2018, 5(4): 383–398. doi: 10.13868/j.cnki.jcr.000249.

[3] DUSART P, LETOURNEUX G, and VIVOLO O. Differential fault analysis on A. E. S[C]. The 1st International Conference on Applied Cryptography and Network Security, Kunming, China, 2003: 293–306. doi: 10.1007/978-3-540-45203-4_23.

[4] PIRET G and QUISQUATER J J. A differential fault attack technique against SPN structures, with application to the AES and KHAZAD[C]. The 5th International Workshop on Cryptographic Hardware and Embedded Systems, Cologne, Germany, 2003: 77–88. doi: 10.1007/978-3-540-45238-6_7.

[5] KIM C H and QUISQUATER J J. New differential fault analysis on AES key schedule: Two faults are enough[C]. The 8th International Conference on Smart Card Research and Advanced Applications, London, UK, 2008: 48–60. doi: 10.1007/978-3-540-85893-5_4.

[6] TUNSTALL M, MUKHOPADHYAY D, and ALI S. Differential fault analysis of the advanced encryption standard using a single fault[C]. The 5th IFIP WG 11.2 International Conference on Information Security Theory and Practice: Security and Privacy of Mobile Devices in Wireless Communication, Heraklion, Crete, Greece, 2011: 224–233. doi: 10.1007/978-3-642-21040-2_15.

[7] LIAO Nan, CUI Xiaoxin, LIAO Kai, *et al*. Improving DFA attacks on AES with unknown and random faults[J]. *Science China Information Sciences*, 2017, 60(4): 042401. doi: 10.1007/s11432-016-0071-7.

[8] ZHANG Fan, LOU Xiaoxuan, ZHAO Xinjie, *et al*. Persistent fault analysis on block ciphers[J]. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018, 2018(3): 150–172. doi: 10.13154/tches.v2018.i3.150-172.

[9] GRUBER M and SELMKE B. Differential fault attacks on KLEIN[C]. The 10th International Workshop on Constructive Side-Channel Analysis and Secure Design, Darmstadt, Germany, 2019: 80–95. doi: 10.1007/978-3-030-16350-1_6.

[10] VAFAEI N, BAGHERI N, SAHA S, *et al*. Differential fault attack on SKINNY block cipher[C]. The 8th International Conference on Security, Privacy, and Applied Cryptography Engineering, Kanpur, India, 2018: 177–197. doi: 10.1007/978-3-030-05072-6_11.

[11] 袁庆军, 张勋成, 高杨, 等. 轻量级分组密码PUFFIN的差分故障攻击[J]. 电子与信息学报, 2020, 42(6): 1519–1525. doi: 10.11999/JEIT190506.
YUAN Qingjun, ZHANG Xuncheng, GAO Yang, *et al*. Differential fault attack on the lightweight block cipher PUFFIN[J]. *Journal of Electronics & Information Technology*, 2020, 42(6): 1519–1525. doi: 10.11999/JEIT190506.

[12] 王如燕. 针对AES结构的差分故障分析方法效率改进研究[D]. [硕士论文], 南京航空航天大学, 2019. doi: 10.27239/d.cnki.gnhhu.2019.001818.
WANG Ruyan. Research on efficiency improvement of differential fault analysis for AES structure[D]. [Master dissertation], Nanjing University of Aeronautics and Astronautics, 2019. doi: 10.27239/d.cnki.gnhhu.2019.001818.

[13] AGOYAN M, DUTERTRE J M, MIRBAHA A P, *et al*. Single-bit DFA using multiple-byte laser fault injection[C]. 2010 IEEE International Conference on Technologies for Homeland Security, Waltham, USA, 2010: 113–119. doi: 10.1109/THS.2010.5655079.

[14] ROSCIAN C, DUTERTRE J M, and TRIA A. Frontside laser fault injection on cryptosystems – Application to the AES' last round[C]. 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Austin, USA, 2013: 119–124. doi: 10.1109/HST.2013.6581576.

[15] COURBON F, LOUBET-MOUNDI P, FOURNIER J J A, *et al*. Increasing the efficiency of laser fault injections using fast gate level reverse engineering[C]. 2014 IEEE International Symposium on Hardware-oriented Security and Trust (HOST), Arlington, USA, 2014: 60–63. doi: 10.1109/HST.2014.6855569.

[16] BREIER J, JAP D, and CHEN C N. Laser-based Fault Injection on Microcontrollers[M]. PATRANABIS S and MUKHOPADHYAY D. Fault Tolerant Architectures for Cryptography and Hardware Security. Singapore: Springer, 2018: 81–100. doi: 10.1007/978-981-10-1387-4_5.

[17] ZHANG Fan, ZHANG Yiran, JIANG Huilong, *et al*. Persistent fault attack in practice[J]. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2020, 2020(2): 172–195. doi: 10.13154/tches.v2020.i2.172-195.

[18] 王红胜, 纪道刚, 张阳, 等. 针对RSA-CRT数字签名的光故障攻击研究[J]. 电子设计工程, 2015, 23(6): 12–15. doi: 10.14022/j.cnki.dzsjgc.2015.06.004.

WANG Hongsheng, JI Daogang, ZHANG Yang, *et al*. Optical fault attack on RSA-CRT signatures[J]. *Electronic Design Engineering*, 2015, 23(6): 12–15. doi: 10.14022/j.cnki.dzsjgc.2015.06.004.

[19] 朱磊, 陈力颖. 低成本eSIM芯片抗激光故障注入攻击的防护设计[J]. 电子元器件与信息技术, 2019, 3(11): 7–10. doi: 10.19772/j.cnki.2096-4455.2019.11.004.

ZHU Lei and CHEN Liying. Protection design of low cost eSIM chip against laser fault injection attack[J]. *Electronic Component and Information Technology*, 2019, 3(11): 7–10. doi: 10.19772/j.cnki.2096-4455.2019.11.004.

[20] RODRIGUEZ J, BALDOMERO A, MONTILLA V, *et al*. LLFI: Lateral laser fault injection attack[C]. 2019 Workshop on Fault Diagnosis and Tolerance in Cryptography, Atlanta, USA, 2019: 41–47. doi: 10.1109/FDTC.2019.00014.

[21] YUCE B, SCHAUMONT P, and WITTEMAN M. Fault attacks on secure embedded software: Threats, design, and evaluation[J]. *Journal of Hardware and Systems Security*, 2018, 2(2): 111–130. doi: 10.1007/s41635-018-0038-1.

[22] 王沛晶. 集成电路奇偶校验故障注入检测方法研究[D]. [硕士论文], 天津大学, 2018. doi: 10.27356/d.cnki.gtjdu.2018.002203.

WANG Peijing. Research on parity code-based fault detection of integrated circuit against fault injection attack[D]. [Master dissertation], Tianjin University, 2018. doi: 10.27356/d.cnki.gtjdu.2018.002203.

姜会龙：男，1994年生，博士生，研究方向为密码芯片激光故障攻击.

朱 翔：男，1985年生，高级工程师，研究方向为器件辐射效应.

李 悦：女，1987年生，助理研究员，研究方向为数字集成电路可靠性分析方法.

责任编辑：马秀强