基于电压毛刺故障扰动的分组密码安全性度量方法研究

欧庆于,罗 芳,吴晓平,杨 鹏
(海军工程大学信息安全系,湖北武汉 430033)

摘 要: 随着信息体系对抗强度的升级,网络空间已演变为由各类信息平台及控制网络互联而成的复杂网电环境,所面临的安全威胁日趋复杂.作为网络空间安全的基石,各类密码算法实现不可避免地受到由环境引入或攻击者恶意施加的故障扰动影响,进而引发密码安全性问题.本文以电压毛刺故障扰动手段为基础,对分组密码算法实现的故障产生机理及安全扰动机制进行了分析和研究;构建了用于刻画密码电路故障传播概率性波动模型;结合不可区分性理论、活动字节传播概率的统计分布技术,提出了能够充分反映故障扰动场景下分组密码实际安全特性的度量框架.实验表明,该度量框架能够充分反映实际故障概率传播特性与攻击者区分优势之间的关联性,并对分组密码实现在遭受故障攻击下的安全性实施客观分析.

关键词: 电压毛刺;故障注入;故障扰动;分组密码;安全性分析;信息泄露
中图分类号: TP309.1 **文献标识码:** A **文章编号:** 0372-2112 (2021)03-0417-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.12263/DZXB.20200514

Research on the Metric Method for the Security of the Block Cipher Based on the Voltage Glitch Fault Disturbance

OU Qing-yu, LUO Fang, WU Xiao-ping, YANG Peng
(*Department of Information Security, Naval University of Engineering, Wuhan, Hubei* 430033, *China*)

Abstract: With the upgrade of the information system confrontation, the cyberspace has developed to a complicated network electricity environment, composed of kinds of interconnected information platforms and control networks. Its security threats has been more complicated. As the security base of the cyberspace, the fault disturbance to the implementation of the cipher, caused by the environment and the malicious attacker, can not be avoided, so the security problem of the cipher will be induced. In this paper, based on the voltage glitch fault injection, the fault generation and the security disturbance mechanism of the block cipher chip, is analyzed. The fluctuant model, used for characterizing the fault propagation probability of the cipher chip, is constructed. Applying the indistinguishable theory, and the statistical distribution of the propagation probability to the active bytes, the metric model of the actual physical security for the block cipher chip, is proposed. It is experimented that, the relevance, between the actual fault propagation probability and the distinguish advantage, can be reflected by the model, so the security of the block cipher, in the scene of the fault attack, can be analyzed objectively.

Key words: voltage glitch; fault injection; fault disturbance; block cipher; security evaluation; information leakage

1 引言

在诸多故障扰动手段中,电压毛刺(瞬态电脉冲信号)凭借其超宽带特性,可突破 VLSI 中的耦合电容网络及各类滤波机制,在核心电路中形成瞬时电压上冲/下冲,破坏系统原有时间约束条件,引发中间状态的翻转,并最终形成故障密文输出.此外,由于电压毛刺下降沿/上升沿陡峭(可达到皮秒级)、持续时间短(一般为纳秒级),使得其在适当的触发条件下能够对特定时刻/位置的密码操作实施扰动.

Zussa. L 等人[1~3]对电压毛刺的注入效果进行了定性比较,并对扰动效果作了定量分析; Flynn. C. O[4]对基于可调电压降(crowbars)的故障扰动技术进行了研究;文献[5]以能带隙、锁相环、时钟信号发生模块为对象,对电压毛刺在数模混合电路中的行为模型进行了研究;文献[6]对基于电磁发射形式的电压毛刺故障扰动技术进行了研究;文献[7]提出了一种基于电压毛刺的远程注入方法;文献[8]对基于电压毛刺的半永久故

收稿日期:2020-05-28;修回日期:2020-08-06;责任编辑:覃怀银
基金项目:国家自然科学基金(No.61672531);保密通信国防科技重点实验室基金(No.614210301030117)

障(permanent fault)注入技术进行了研究. 为进一步明确故障扰动对密码电路安全性的影响,文献[9]、[10]对基于扰动的信息泄露表征及区分器的构造进行了研究;文献[11]提出了一种刻画分组密码算法层面故障扰动传播特性的传播轨迹框架;文献[12]提出了一种适用于分组密码算法层面的自动化安全特性分析框架.

上述研究构建了一系列以故障注入为背景的正向安全性测试技术、分析方法和度量框架,能够在算法层面较好地说明故障扰动安全特性. 但由于缺乏与具体实现方式及物理载体中故障传播特性的关联,使得其难以全面真实地反映各类密码算法实现在实际故障扰动下的信息泄露情况.

本文围绕电压毛刺故障扰动场景下分组密码实现的安全性测试及分析问题,对由约减结构和区分难度表征的分组密码安全扰动机制进行了研究;以此为基础,提出了一种能够刻画电压毛刺故障扰动沿实际网表路径传播的概率性波动模型,并对其与分组密码安全特性的关联进行了研究;最后,提出了一种适用于电压毛刺故障扰动场景下的安全度量框架,实现了对由实际故障扰动引起的约减结构动态变化与密码算法信息泄露的综合表征和度量.

2 基于电压毛刺的分组密码安全扰动机制

基于电压毛刺的分组密码安全扰动,其本质是利用电压毛刺的瞬变特性,在极短(纳秒级甚至是皮秒级)时间内改变局部晶体管电路的偏置状态,破坏密码算法电路时序约束条件,从而对分组密码中间值进行篡改.

从映射的角度,分组密码算法实现了明文空间 M 与密文空间 C 在密钥 k 控制下经过一系列中间值空间的映射. 在密码算法、明文及密钥确定的前提下,假设故障在中间值空间 I^i 被成功注入,使得正常情况下的局部映射 $U^k:I_l^i\to I_i^i$ 被篡改为 $\tilde{U}^k:I_l^i\to I_k^j$,并进而造成后续中间值空间至密文空间的映射被篡改.

基于不可区分性理论,故障扰动下密码算法安全性可形式化表述为:

$$\Delta^D(k,k^*)=\left|P[D(U^k,\tilde{U}^k)=1]-P[D(U^{k^*},\tilde{U}^{k^*})=1]\right| \tag{1}$$

其中,U^k、$\tilde{U}^k$ 分别为在密钥 k 作用下的正常局部映射和故障局部映射;$\Delta^D(k,k^*)$ 为基于区分器 D 对猜测密钥 k^* 的区分优势. 以差分故障分析(DFA)为例,基于差分区分器 D_{diff},通过对中间值差分 Δi 在差分表中的命中情况的,对正确密钥 k 进行猜测,如式(2)所示:

$$P^{k^*}_{\text{collision}}(\Delta i,\mathrm{S})=D_{\text{diff}}(E_{\text{pr}}(i,k^*_{\text{pr}}),E_{\text{pr}}(\tilde{i},k^*_{\text{pr}})) \tag{2}$$

$P^{k^*}_{\text{collision}}(\Delta i,\mathrm{S})$ 为基于猜测密钥 k^* 构造的中间值差分 Δi 在差分表 S 中的碰撞概率,E_{pr} 为故障注入点之后的局部加密操作,k^*_{pr} 为局部加密操作的猜测密钥、i 为正常中间数据、$\tilde{i}$ 为被故障注入干扰的中间数据. 显然,当 $P^k_{\text{collision}}(\Delta i,\mathrm{S})\neq P^{k^*}_{\text{collision}}(\Delta i,\mathrm{S})$ 时,攻击者可对正确密钥 k 进行区分. 其区分的难度如式(3)所示

$$\Delta^D(k,k^*)=\left|[P^{k^*}_{\text{collision}}=1]-[P^k_{\text{collision}}=1]\right| \tag{3}$$

基于以上讨论可知,对分组密码算法成功实施故障扰动的必要条件是:

(1)通过故障注入能够构造区分器 D,使得 $|P[D(U^k,\tilde{U}^k)=1]-P[D(U^{k^*},\tilde{U}^{k^*})=1]|\geqslant 0$;

(2)基于区分器 D 对正确密钥 k 进行分析在计算上可行.

当对密码算法运行过程中的中间值实施扰动时,从中间值空间 I^i 至密文空间 C 形成了密码算法的约减结构. 该约减结构,实际上决定了攻击者所能够获取的区分优势上限[14~16]. 因此,为成功实施故障攻击,通过故障扰动所形成的约减结构的轮数应小于该分组密码算法可证明安全的最小轮数 $R_{\min}$—即分组密码算法的可证明安全最小轮数就形成了电压毛刺安全扰动的边界.

3 分组密码安全扰动度量

在遭受电压毛刺故障扰动时,密码算法电路故障传播特性受网表联接关系的影响. 此外,由于在芯片制造过程中,工艺参数在一定范围内波动,使得实际电路在环境因素变化时,表现出与初始设计的概率性偏差[17]. 因此,在电压毛刺故障扰动场景下,故障传播本质上是一种受网表联接关系影响的路径选择概率行为.

3.1 电压毛刺扰动的概率性波动模型

图1 局部路径示例

以图 1 为例,设局部路径中节点 n_i 的入射路径延时概率密度函数(PDF)为 $p_i(t)$. 由于各路径延时 PDF 与路径所跨越的物理区域相关,各节点入射路径延时可视为独立,则 n_i 至 n_j 的路径延时 PDF 为

$$f(t)=\prod_0^t p_i(t_i)\cdots p_j(t_j),t_i+\cdots t_j=t \tag{4}$$

与之对应的延迟累积分布函数为

$$F(t)=\int_{-\infty}^t f(t)\,\mathrm{d}t \tag{5}$$

设引发该路径时间约束违背的阈值为 T_{th},则该局部路径正常运行的概率为 $F(T_{\text{th}})$.

在电压毛刺故障扰动场景下,设路径节点 n_i 的延迟在区间 $\Delta d_i(\Delta d_i\geqslant 0)$ 内波动的 PDF 为 $p_{n_i}(t)$ $(0\leqslant t\leqslant \Delta d_i)$,则节点 n_i 至 n_j 的路径延迟 PDF 可重新定义为

$$f'(t)=\prod_0^t p_{n_i}(\Delta t_i)p_i(t_i-\Delta t_i)\cdots p_{n_j}(\Delta t_j)p_j(t_j-\Delta t_j),\quad t_i+\cdots+t_j=t,\Delta t_i>0 \tag{6}$$

局部路径正常运行的概率为

$$F'(t) = \int_{-\infty}^{t} f'(t)\,\mathrm{d}t \tag{7}$$

在单纯考虑路径延时(不考虑节点延迟)的情况下,当故障注入时,路径时间约束违背的阈值 T'_{th} 将小于正常情况下的路径时间约束违背阈值 T_{th},导致路径时间违背的概率增加,如式(8)所示

$$P'_{\mathrm{fault}}(T'_{\mathrm{th}}) = 1 - F(T'_{\mathrm{th}}) > P_{\mathrm{fault}}(T_{\mathrm{th}}) = 1 - F(T_{\mathrm{th}}) \tag{8}$$

除由节点 n_i 引入的延时波动外,再汇聚扇出节点会造成节点延迟与前端扇出节点延迟相关,破坏各节点延迟独立性,引入路径延时的波动[17].

图 2 中,n_f 存在扇入节点 n_d、n_e,两节点扇入子图的交集为图中阴影部分. 由于节点 n_c 的两条扇出路径不同时属于节点 n_d 和 n_e 的扇入子图,则节点 n_f 为再汇聚扇出节点,其依赖节点为 n_c.

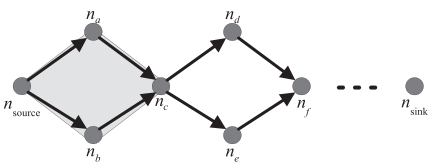


图2　局部路径的再汇聚扇出

由于依赖节点具有多个扇出路径,且位于扇入子图交集的边缘,将造成其与再汇聚扇出节点的概率相关性. 因此,为对路径交叉情况下的故障传播进行分析,需要考虑依赖节点的扇出路径选择概率. 设依赖节点的扇出路径选择概率为 p_{path},各扇出路径关联的局部路径延时 PDF 为 $f_i(t)$,则

$$P_{\mathrm{fault}} = 1 - F(t) = 1 - \sum_{i=0}^{n} p_{\mathrm{path}} \int_{-\infty}^{t} f_i(t)\,\mathrm{d}t \tag{9}$$

现实中,由于电压毛刺扰动的概率波动特性,故障扰动形成的约减结构也具备概率波动特性. 设考虑扰动概率波动情况下,攻击者基于区分器 D 对猜测密钥 k^* 的区分难度如式(10)所示

$$\Delta'^{D}(k,k^*) = \left|\left[P'^{k^*}_{\mathrm{collision}} = 1\right] - \left[P'^{k}_{\mathrm{collision}} = 1\right]\right| \tag{10}$$

则区分难度的概率性波动用 σ_D 表示

$$\sigma_D = \left|\Delta^{D}(k,k^*) - \Delta'^{D}(k,k^*)\right| \tag{11}$$

3.2　分组密码安全扰动度量

电压毛刺扰动的概率波动特性所引发的区分难度波动,造成了同一分组密码算法在不同实现方式、不同攻击环境下,抗故障攻击能力表现的差异. 由于在现实中难以准确测量路径延时 PDF、电路网表分布等参数,使得必须借由其他途径以统计方式反映.

设电压毛刺故障扰动情况下获得故障中间值与正常中间值的差分为 Δi,并进而产生故障密文差分 Δc,则基于第 2 节的分析可知

$$\Delta c = \mathrm{Struct}_{\mathrm{cut}}(\Delta i) = B_l(B_m^{r-1}(\Delta i)),\ r < R_{\min} \tag{12}$$

其中,$\mathrm{Struct}_{\mathrm{cut}}$ 表示形成的约减结构,由 $r-1$ 个中间单轮结构 B_m 和 1 个末轮结构 B_l 构成,$R_{\min}$ 为分组密码算法可证明安全的最小轮数.

基于分组密码算法约减轮活动字节概率传播特性[18~20]可知,$(\Delta c,\Delta i)$ 差分对所代表的故障模式传播概率为

$$T(\Delta c,\Delta i) = P(\mathrm{Struct}_{\mathrm{cut}}(\Delta i) = \Delta c \mid \Delta i) \tag{13}$$

该传播概率受电压毛刺故障扰动概率波动的影响. 具体而言,不同故障模式的出现概率由具体故障点位置的概率决定. 此外,当故障传播概率存在偏置时,分组密码中的非线性部件(如 Sbox)平衡特性被破坏,为候选密钥提供了可区分性. 因此,对偏置存在情况下的信息泄露进行度量,能够较为充分地表征分组密码实现的实际安全扰动情况.

基于文献[21],分组密码在故障扰动场景下单字节差分信息泄露可基于条件熵表示为

$$\begin{aligned}\mathrm{Info}_{\mathrm{leak}} &= H(k_b \mid \Delta c)\\ &= H(\Delta i \mid \Delta c) + H(i \mid \Delta c \Delta i))\end{aligned} \tag{14}$$

其中,k_b 表示正确密钥字节;Δc 表示正常密文字节与故障密文字节的差分;i 表示正常情况下的中间值;Δi 表示故障对正常情况下的中间值 i 的扰动.

在实际故障扰动中,由于故障概率性波动的原因,使得式(14)中的 Δi 和 Δc 不可避免的存在偏置现象,从而造成故障输出模式的偏置;此外,由于不同故障输出模式所造成的信息泄露存在差异,因此对分组密码电路在实际故障扰动中的信息泄露情况进行度量,需要综合考虑各故障输出模式的发生概率,以及不同故障模式产生信息泄露对系统总体安全的影响.

$$\begin{aligned}\mathrm{Info}_{\mathrm{leak}} &= H(k \mid \Delta C)\\ &= \sum_{m\in M} P_m \times (H(\Delta I_m \mid \Delta C_m) + H(I_N \mid \Delta C_m \Delta I_m)) \times \sigma_m\\ &= \sum_{m\in M} P_m \times \Big(\sum_{\Delta c\in\Delta C,\Delta i\in\Delta I} P(\Delta c,\Delta i)\,\log_2 T(\Delta c,\Delta i)\\ &\quad + \sum_{\Delta c\in\Delta C} \sum_{\Delta i\in\Delta I} H(i_N \mid \Delta c\Delta i) \times T(\Delta c,\Delta i) \Big) \times \sigma_m\end{aligned} \tag{15}$$

其中,k 表示正确密钥;ΔC 表示正常密文与故障密文的差分集;P_m 表示特定故障输出模式 m 的出现概率;M 为全体故障输出模式总体;ΔC_m 表示故障输出模式 m 下攻击者获得的密文差分集;ΔI_m 表示与 ΔC_m 相对应的中间值差分集;I_N 表示正常情况下的中间值集;$T(\Delta c,\Delta i)$ 为差分对 $(\Delta c,\Delta i)$ 的传播概率;σ_m 为对故障输出模式 m 指定的惩罚因子.

4　实验及分析

4.1　电压毛刺故障注入测试实验环境

如图 3 所示,电压毛刺故障注入测试实验环境主要

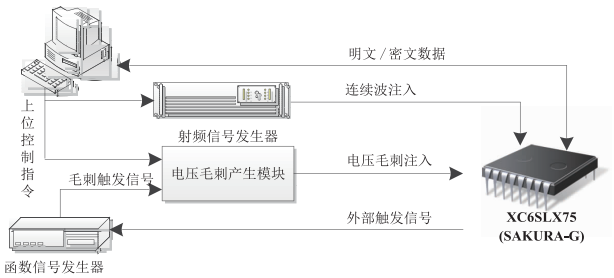
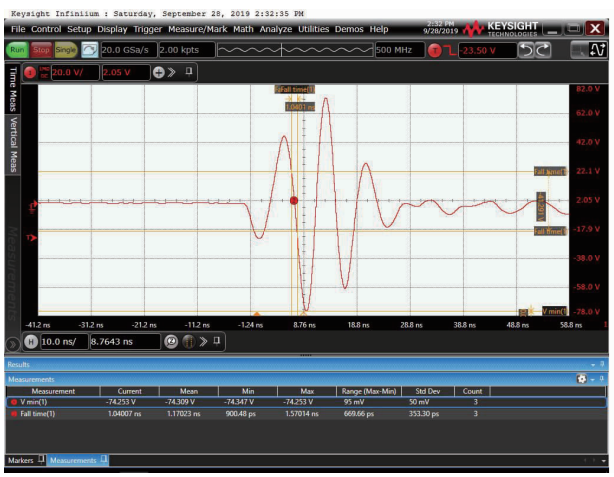
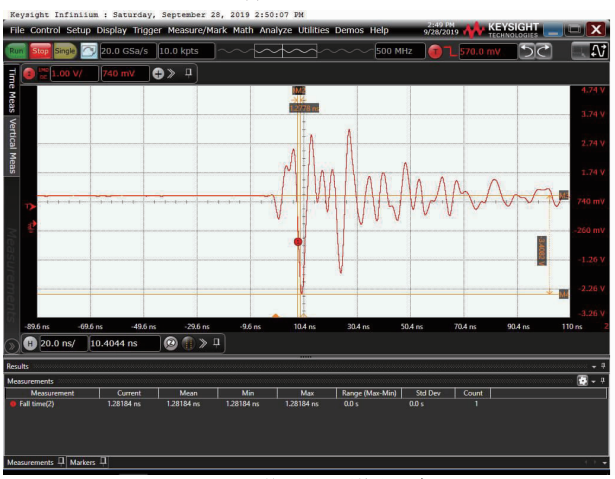


图3 电压毛刺故障注入测试实验环境组成

包括:射频信号发生器、电压毛刺产生模块、函数信号发生器及 SAKURA_G 攻击验证平台等. 由射频信号发生器、功率放大器和注入钳组成的测试系统对 SAKURA-G(运行 AES-128 密码算法)实施连续正弦波注入,射频信号源扫频范围设定为 80 ~ 300MHz,幅度为 130dBμV;电压毛刺产生模块对 AES-128 密码算法实现进行时机选定的或随机的故障注入,基准电压为 50V,外部触发信号由 AES 各轮时钟上升沿产生. 空载电压毛刺下降沿(10% ~ 90%)为 1.0401ns,负脉冲幅值为 -74.253V,如图 4(*a*)所示. 该电压毛刺在 FPGA 核心电源系统形成下降沿为 1.28184ns,幅度为 -3.4082V 的电压降,如图 4(*b*)所示.



(*a*) 电压毛刺注入



(*b*) FPGA核心电源系统电压降

图4 电压毛刺故障注入测试实验环境组成

4.2 基于电压毛刺的故障传播概率估计

密钥固定前提下,基于连续正弦波对 SAKURA-G 平台进行高次谐波故障扰动,外部主频为 48MHz,运行基于串行方式实现的 AES-128 密码算法. AES-128 密码算法通过内部锁相环倍频方式在 100MHz 频率下运行,单轮迭代运算耗时约为 10ns. 通过故障扰动共获得 3286 条故障密文,各比特位翻转情况如图 5 所示.

输出密文第 14 字节的第 2bit 共翻转 619 次;第 13 字节的第 5bit 共翻转 586 次;第 15 字节的第 5bit 翻转 497 次;第 12 字节的第 5bit 翻转 495 次;第 11 字节的第 3bit 翻转 485 次. 对以上各字节的翻转概率估计如表 1 所示.

表 1 输出密文字节翻转概率

字节序号	翻转次数	样本数	故障传播概率
11	485	3286	0.148
12	495		0.151
13	586		0.178
14	619		0.188
15	497		0.151

在明文随机输入,且随机变更密钥的情况下,进行随机电压毛刺故障注入. 基于 455556 次故障注入共获得 35889 条故障密文输出. 按故障字节在输出密文中的位置,故障模式可划分为 18 类,如图 6 所示.

表 2 故障点位置分析结果

故障模式	故障密文数	故障模式	故障密文数
1	11917	5	16
2	9622	6	29
3	959	7	2
4	896		
故障点分析	故障模式 1 ~ 7 中,密文故障字节数均小于 4,说明故障传播未经过列混合轮运算扩散,故障点位于末轮运算		
故障模式	故障密文数	故障模式	故障密文数
8	5858	10	1
9	4924		
故障点分析	故障模式 8 ~ 10 中,密文故障字节数为 4,且各故障字节位于不同列. 说明其故障点位置位于倒数第 2 轮列混合运算之前		
故障模式	故障密文数	故障模式	故障密文数
11	127	14	65
12	13	15	108
13	11		
故障点分析	故障模式 11 ~ 15 中,密文故障字节数为 5,为模式 8/9 与末轮单字节故障的混杂模式		
故障模式	故障密文数	故障模式	故障密文数
16	211	18	1129
17	1		
故障点分析	故障模式 16 ~ 18 中,密文除一个字节外,均发生故障,故障点位于倒数第 2 轮列混合运算之前,且存在多种模式重叠的现象		

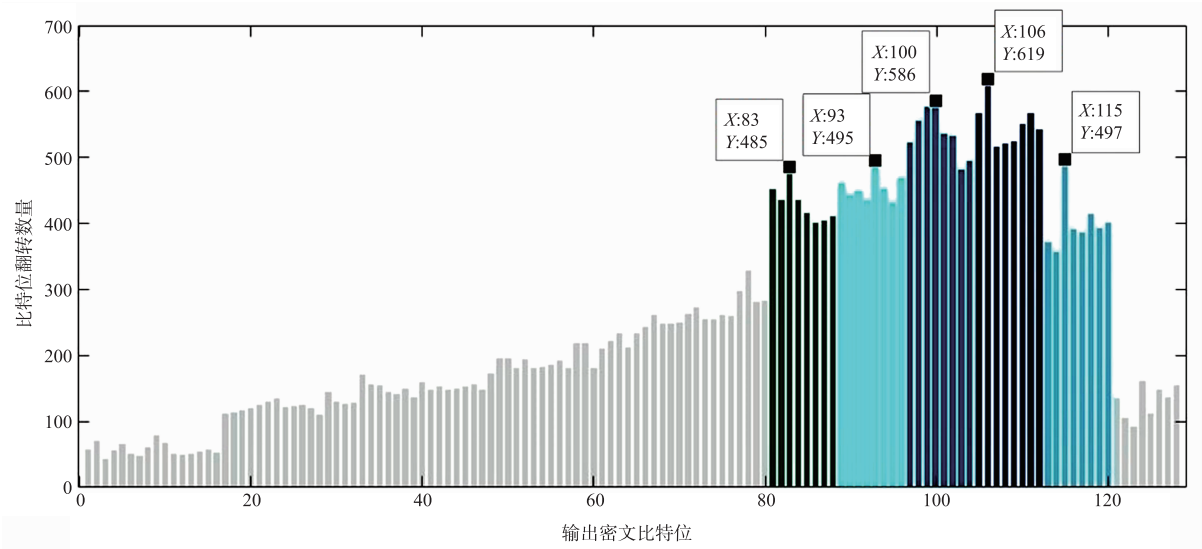


图5　传输路径故障传播概率

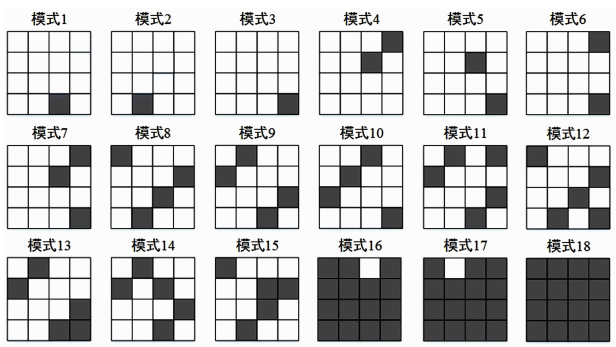


图6　密文故障模式

如表2 所示,故障扰动位置主要分布于 AES-128 的最后三轮中. 通过与图 5 和表 1 的比较,验证了基于连续正弦波进行故障传播概率估计的可行性. 此外,通过对故障点位置进行分析可以发现,故障在末轮中出现的频率最高. 基于 4. 1 节的分析可知,由于各局部路径延迟概率的叠加,必然造成末端路径时间条件约束违背概率的增加.

4. 3　密码安全扰动度量

如式(16)所示,单一字节差分 Δx 经 Sbox 变换后的获得 Δy,差分对(Δx,Δy)对应的正常字节 x_1 的解的分布如文献[21]中所述(解为 2 的项数为 126,为 0 的项数为 128,为 4 的项数为 1).

$$\Delta y = \mathrm{Sbox}(x_1) \oplus \mathrm{Sbox}(x_1 \oplus \Delta x) \tag{16}$$

虽然 x_1 均匀分布,但由于实际故障扰动的概率性波动,在 Δy 中已形成非常明显的偏置. 当 Δx 固定时,与各 Δy 对应的 x_1 的解必不相同[21];同样,当 Δy 固定时与各 Δx 对应的 x_1 的解也必不相同. 因此,Δy 的偏置情况实际上反映了 Δx 的偏置信息.

以故障模式 1 为例,基于文献[21]中的方法进行分析可知,Δy 仅在 63 个位置出现. 由于 x_1 为均匀分布,可知与 Δy 命中次数为 0 时相对应的 Δx 非零值均不可能出现,且 $\Delta x = 2$. 基于式(15)可计算

$$\begin{aligned} T(\Delta c, \Delta i) &= 1, \quad \Delta c \in \Delta C_1 \\ \mathrm{Info}^1_{\mathrm{leak}} &= N - H(K \mid \Delta Z) \\ &= 8 - H(\Delta X \mid \Delta Y = y) \\ &\quad - H(X \mid \Delta X \Delta Y = \Delta y) \\ &= 8 - 0 - 0 = 8 \end{aligned}$$

其中 ΔC_1 表示故障输出模式 1 下的密文差分集,即基于模式 1 已完全泄露 8bit 轮密钥字节.

各故障模式下的信息泄露情况如表 3 所示. 在模式 18、19 中,由于故障点出现于多个位置,且经过剩余混乱扩散,导致无法提取有效信息.

表 3　各故障输出模式的信息泄露情况

模式	泄露	概率	模式	泄露	概率
1	8 bit	0. 33	10	32 bit	0. 0007
2	8 bit	0. 27	11	32 bit	0. 003
3	8 bit	0. 027	12	32 bit	0. 0004
4	16 bit	0. 025	13	32 bit	0. 0003
5	16 bit	0. 0004	14	32 bit	0. 0016
6	16 bit	0. 0008	15	32 bit	0. 0031
7	16 bit	0. 00006	16	0 bit	0. 00003
8	32 bit	0. 16	17	0 bit	0. 00003
9	32 bit	0. 14	18	0 bit	0. 032

在模式 7 中,第 16 字节的故障点位于轮密钥加操作之后,泄露 2 字节轮密钥;在模式 11、12、13、14、15 中,其位于末轮的故障点位于密钥加操作之后,故其仅基于倒数第 2 轮的故障注入泄露 4 字节轮密钥. 则该 AES-128 实现的平均泄露为

$$\begin{aligned}\mathrm{Info}_{\mathrm{leak}}^{\mathrm{total}} &= 0.33\times 8 + 0.27\times 8 + 0.027\times 8 + 0.025\times 16\\ &\quad + 0.0004\times 16 + 0.0008\times 16 + 0.00006\times 16\\ &\quad + 0.16\times 32 + 0.14\times 32 + 0.0007\times 32\\ &\quad + 0.003\times 32 + 0.0004\times 32 + 0.0003\times 32\\ &\quad + 0.0016\times 32 + 0.0031\times 32\\ &\approx 15.33\mathrm{bit}\end{aligned}$$

在实际故障扰动情况下,该密码算法实现基于故障密文输出平均泄露的密钥信息量为 15.33bit. 平均泄露信息量体现了具体密码算法实现的实际难度.

基于现有分析方法对 4.2 中随机故障注入下的信息泄露情况进行分析,并与本文结果进行比较,如表 4 所示. 通过比较可知,文献[9,10,12,21]中所提出的分析模型,实际上只针对最差情况下(故障模式 8、9、10)的安全扰动情况进行了度量,而并未考虑故障概率性波动造成的信息泄露动态变化. 文献[11]所使用的特征空间衰减率模型,虽然能够反映多次故障注入场景下密钥空间的变化规律,但并未考虑实际故障注入过程中的成功率问题,且给出的分析结果更多的表明了在多次故障注入下的信息泄露趋势,不便于实施具体的定量分析. 本文所提出的度量框架,充分考虑了故障的概率性波动特性,其度量结果能够反映在现实应用环境中由密码算法和实现方式耦合呈现的安全特性,便于对具体密码产品的抗故障安全性进行客观评价.

表 4 与其他分析方法的对比

分析方法	分析模型	分析结果	出处
基于候选密钥估计的偏差香农熵	$H(p_s) = -\sum_{e=0}^{255} p_s(e)\times\log_2 p_s(e)$	32bit	文献[9]
基于候选密钥的极大似然估计	$l(\hat{K}) = \prod_{i=1}^{n} P(\tilde{S}_{\mathrm{ak}_r^i} = \hat{S}_{\mathrm{ak}_r^i})$	32bit	文献[10]
基于候选密钥的平均汉明重量	$h(\hat{K}) = \frac{1}{n}\sum_{i=1}^{n}\mathrm{HW}(\hat{S}_{\mathrm{ak}_r^i})$	32bit	
平方欧氏距离非平衡度估计	$s(K) = \sum_{\delta=0}^{255}\left(\frac{\#\{i \mid \hat{S}_{\mathrm{ak}_r^i}[j] = \delta\}}{n} - \frac{1}{256}\right)$	32bit	
状态差分的最大香农熵	$H_{\max}(\delta_j^i) = \sum_{z=1}^{l}\left(-\sum_{q=0}^{2^m-1} p_q^{w_z^{ij}}\log_2(p_q^{w_z^{ij}})\right)$	32bit	文献[12]
基于故障输出的密钥条件熵	$H(K \mid \Delta Z) = H(\Delta X \mid \Delta Z) + H(X \mid \Delta Z\Delta X))$	32bit	文献[21]
考虑概率波动特性的泄露度量	$\sum_{m\in M} P_m \times (H(\Delta I_m \mid \Delta C_m) + H(I_N \mid \Delta C_m \Delta I_m)) \times \sigma_m$	15.33bit	本文

5 结论

与单纯基于密码算法控制流、数据流的故障扰动进行度量的方法相比,本文提出的安全扰动度量框架充分考虑了实际情况中故障的概率传播特性与攻击者区分优势之间的关联性,能够较好地反映分组密码算法实现的安全扰动程度,并可为具体密码算法实现在抗故障注入攻击方面的优劣评判提供客观依据.

参考文献

[1] Zussa L, Dutertre J M, Clediere J, Robisson B, Tria A. Investigation of timing constraints violation as a fault injection means[A]. XVII Conference on Design of Circuits and Integrated Systems[C]. Santander, Spain: IEEE, 2012. 63 – 71.

[2] Zussa L, Dutertre J M, Clediere J, Robisson B. Analysis of the fault injection mechanism related to negative and positive power supply glitches using an on-chip voltmeter[A]. IEEE International Symposium on Hardware-oriented Security & Trust[C]. Arlington, USA: IEEE, 2014. 151 – 159.

[3] Zussa L, Dutertre J M, Clediere J, Tria A. Power supply glitch induced faults on FPGA: an in-depth analysis of the injection mechanism[A]. IEEE 19th International On-line Testing Symposium[C]. Chania, Greece: IEEE, 2013. 73 – 81.

[4] Flynn C O. Fault Injection Using Crowbars on Embedded Systems[DB/OL]. http://eprint.iacr.org/2016/810.pdf, 2016.

[5] Boher B N, Beroulle V, Hly D, Damiens J, Candelier P. Clock generator behavioral modeling for supply voltage glitch attack effects analysis[J]. Microprocessors & Microsystems, 2016, 47(PA): 37 – 43.

[6] Vincent I, Robert S, Florian U. Your rails cannot hide from localized EM: How dual-rail logic fails on FPGAs[A]. Cryptographic Hardware and Embedded Systems—CHES 2017[C]. Taipei, China: Springer, 2017. 403 – 424.

[7] Krautter J, Dennis R E G, Tahoori M B. FPGA hammer:

Remote voltage fault attacks on shared FPGAs, suitable for DFA on AES[A]. Cryptographic Hardware and Embedded Systems—CHES 2018[C]. Amsterdam, the Netherlands: Springer, 2018. 44 – 68.

[8] Zhang Fan, Lou Xiaoxuan, Zhao Xinjie, Bhasin S, He Wei, Ding Ruyi, Samiya Q, Ren Kui. Persistent fault analysis on block ciphers[A]. Cryptographic Hardware and Embedded Systems—CHES 2018[C]. Amsterdam, the Netherlands: Springer, 2018. 150 – 172.

[9] Lashermes R, Reymond G, Dutertre J, Fournier J, Robisson B, Tria A. A DFA on AES based on the entropy of error distributions[A]. Fault Diagnosis and Tolerance in Cryptography—FDTC 2012[C]. Leuven, Belgium: Springer, 2012. 34 – 43.

[10] Fuhr T, Jaulmes E, Lomn V, Thillard A. Fault attacks on AES with faulty ciphertexts only[A]. Fault Diagnosis and Tolerance in Cryptography—FDTC 2013[C]. Santa Barbara: Springer, CA, 2013. 108 – 118.

[11] 欧庆于,罗芳,叶伟伟,周学广. 分组密码算法抗故障攻击能力度量方法研究[J]. 电子与信息学报,2017,39(5):1266 – 1270.
Ou Qing-yu, Luo Fang, Ye Wei-wei, Zhou Xue-guang. Metric for defences against fault attacks of block ciphers[J]. Journal of Electronics & Information Technology, 2017, 39(5): 1266 – 1270. (in Chinese)

[12] Sayandeep S, Debdeep M, Pallab D. ExpFault: An automated framework for exploitable fault characterization in block ciphers[J]. Journal of Cryptographic Engineering, 2019, 9: 203 – 219.

[13] Behzad Razavi. Fundamentals of Microelectronics[M]. Boston: Wiley, 2008. 796 – 801.

[14] Dziembowski S, Pietrzak K. Leakage-resilient cryptography[A]. 49th Annual IEEE Symposium on Foundations of Computer Science[C]. Philadelphia, PA, USA: IEEE, 2008. 293 – 302.

[15] Sun Bing, Liu Meicheng, Guo Jian, Qu Longjiang, Rijmen V. New insights on AES-like SPN ciphers[A]. 2016 International Cryptology Conference[C]. Santa, Barbara, UCSB: Springer, 2016. 605 – 624.

[16] Chen Shan, Steinberger J. Tight security bounds for key – alternating ciphers[A]. 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques[C]. Copenhagen, Denmark: Springer, 2014. 116 – 124.

[17] Srivastava A, Sylvester D, Blaauw D. Statistical Analysis and Optimization for VLSI: Timing and Power[M]. Ann Arbor: Springer, 2005. 114 – 118.

[18] Grassi L, Rechberger C, Ronjom S. A new structural-differential property of 5-round AES[A]. 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques[C]. Paris, France: Springer, 2017. 289 – 317.

[19] Grassi L, Rechberger C. Rigorous Analysis of Truncated Differentials for 5-round AES[DB/OL]. https://eprint.iacr.org/2018/182.pdf, 2018.

[20] Bao Z, Guo J, List E. Extended Expectation Cryptanalysis on Round-reduced AES[DB/OL]. https://eprint.iacr.org/2019/622.pdf, 2019.

[21] Sakiyama K, Li Yang, Iwamoto M, Ohta K. Information-theoretic approach to optimal differential fault analysis[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(1): 109 – 120.

作者简介

欧庆于　男,1978 年生于江西靖安,现为海军工程大学信息安全系副教授,获军队科技进步二等奖 3 项,主要研究方向为密码应用安全性测评、旁路攻击防御.
E-mail:ouqingyv@163.com

罗　芳(通信作者)　女,1983 生于江西吉安,现为海军工程大学信息安全系讲师,主要研究方向为序列密码及分组密码设计、密码安全性分析.
E-mail:lf_0215@sina.com

吴晓平　男,1961 年生于山西新绛,现为海军工程大学信息安全系教授、博士生导师,主要研究领域为信息安全、系统决策.
E-mail:wxp8@sohu.com

杨　鹏　男,1996 年 2 月生于湖南岳阳,现为海军工程大学信息安全系硕士研究生,主要研究方向为密码芯片安全性评估.
E-mail:849593165@qq.com