抗内存攻击的加密芯片双重动态混淆策略

景凤池 1 ，张金艺 1,2

（1 上海大学 微电子研究与开发中心，上海 200444；

2 上海大学 特种光纤与光接入网重点实验室，上海 200444）

摘　要： 目前，基于线性反馈移位寄存器(Linear Feedback Shift Register, LFSR)的动态混淆策略和测试授权策略是保护加密芯片免受扫描旁路攻击威胁的主流方法，然而存储在内存中的LFSR 种子或测试授权密钥极易受到针对内存的攻击.针对此问题，从应对扫描旁路攻击和应对内存攻击两个角度出发，设计双重动态混淆架构并基于此架构构建双重动态混淆策略.其中，构建基于 LFSR 自更新模块的扫描链数据动态混淆策略以应对扫描旁路攻击；构建 LFSR 输出序列动态混淆策略以应对内存攻击.实验表明，相较于目前主流的安全扫描策略，双重动态混淆策略在不影响芯片可测试性的同时，可以使加密芯片免受扫描旁路攻击和内存攻击的威胁；在 LFSR 自更新模块位数为 64 位、插入混淆逻辑门中异或门和同或门数量各为 8 位的的情况下，面积开销为 0.31%，攻击人员暴力破解双重动态混淆策略所需应用的测试向量至少为 6.29×10^{18} 个.

关键词： 加密芯片；扫描旁路攻击；内存攻击；动态混淆

Anti-memory attack encryption chip dual dynamic obfuscation strategy

JING Feng-chi 1 ，ZHANG Jin-yi 1,2

(1 Microelectronic Research and Development Center, Shanghai University, Shanghai 200444, China;2 Key Laboratory of Special Fiber Optics and Optical Access Networks,Shanghai University, Shanghai 200444, China)

Abstract： At present, the dynamic obfuscation strategy based on the Linear Feedback Shift Register (LFSR) and the test authorization strategy are the mainstream methods to protect the encryption chip from the threat of side scan-based attack. However, the LFSR seed or test authorization key stored in memory is extremely vulnerable to the attack on memory. To solve this problem, a dual dynamic obfuscation architecture is designed and a dual dynamic obfuscation strategy is constructed based on the two perspectives of side scan-based attack and memory attack. Among them, a dynamic obfuscation strategy of scan chain data based on LFSR self-update module is constructed to deal with side scan-based attack. Build an LFSR output sequence dynamic obfuscation strategy against memory attack. Experiments show that compared with the current secure scan strategy, the dual dynamic obfuscation strategy can protect the encryption chip from side scan-based attack and memory attack without affecting the testability of the chip. The area overhead is 0.31% when the LFSR self-update module number is 64 bits, and the number of XOR and XNOR gates in obviating logic gates are 8 bits each,it would needapplied at least 6.29×10^{18} test vectors for the attacker to brute force the dual dynamic obfuscation strategy.

作者简介：

景凤池 男，(1994-)，硕士.研究方向为集成电路可测试性设计.

张金艺（通讯作者） 男，(1965-)，研究员，博士生导师.研究方向 SOC/NOC 可靠性设计、无线通信类 ASIC 设计.E-mail: zhangjinyi@shu.edu.cn.