针对有掩码防护 DES 的代数侧信道攻击

闫守礼 1 ，郭丽敏 1 ，王立辉 1 ，李清 1，2 ，俞军 1，2
（1 上海复旦微电子集团股份有限公司，上海 200433； 2 复旦大学 微电子学院，上海 201203）

摘 要：基于汉明重量泄漏模型，对带掩码防护的软件 DES 抗代数侧信道攻击能力进行了评估.首先研究了代数侧信道攻击的攻击原理，然后基于模板攻击得到了 DES 中间无防护轮次 S 盒输出的汉明重信息，将其作为可配置参数，利用脚本语言及 BAT 工具自动生成 DES 的合取范式表示，最后利用求解器进行密钥求解.结果表明：对仅掩码防护首两轮及尾两轮的软件 DES，利用中间连续 3 轮 S 盒输出汉明重泄漏即可恢复 56 比特 DES 根密钥.

关键词： DES；模板攻击；代数侧信道攻击

Algebraic side channel attack against DES with mask countermeasure

YAN Shou-li 1 ， GUO Li-min 1 ， WANG Li-hui 1 ， LI Qing 1，2 ， YU Jun 1，2
(1 Shanghai Fudan Microelectronics Group Company Limited， Shanghai 200433， China;
2 Institute of Microelectronics，Fudan University， Shanghai 201203， China)

Abstract：On the basis of the Hamming Weight leakage model， the anti algebraic side channel attack capability of a masked software DES is evaluated. The algebraic side channel attack principle is studied， and then the Hamming weight information of Sbox output of DES without protection is got based on the template attack， it is as the configurable parameters to generate conjunctive normal form of DES using script language and BAT tools， the key is retrieved by solver finally. The results show that the 56 bit DES root key can be recovered by using the Hamming weight of Sbox output from the middle 3 successive rounds， while the mask is only used to protect the first two rounds and the last two rounds of DES.

Key words： DES； Template Attack； Algebra Side Channel Attack

作者简介：
闫守礼 男，(1974-)，硕士，工程师.研究方向为密码芯片安全.
郭丽敏 女，(1986-)，硕士，工程师.研究方向为密码芯片安全.
王立辉（通讯作者） 男，(1982-)，博士，工程师.研究方向为密码芯片安全.E-mail:wanglihui@fmzh.com.cn.
李 清 女，(1968-)，硕士，高级工程师.研究方向为集成电路设计开发.
俞 军 男，(1968-)，硕士，高级工程师.研究方向为集成电路设计开发.