一种针对 SM2 规整点乘算法的新型 SPA 攻击

王立辉 1，赵兵 2，李清 1，梁晓兵 2，刘静 3
（1 上海复旦微电子集团股份有限公司，上海 200433； 2 中国电力科学研究院，北京 100192；3 国网宁夏电力公司电力科学研究院， 宁夏 银川 750002）

摘要： 相比于 RSA 密码算法，SM2 在同样的安全强度下需要更短的密钥长度，因此更适合于应用到资源受限的智能卡中.为了 SM2 应用的安全性，人们研究出多种具有抗侧道攻击能力的 SM2 点乘算法.本文提出了一种基于条件减法的新型简单功耗分析方法，可以对常用的两种防护实现进行密钥的破解.实验结果表明，该方法只需要一条功耗曲线，即可在几秒钟内破解出 SM2 密钥.同时本文也给出了几种可以抵御该攻击的防护方法.

关键词： SM2；SPA；蒙哥马利模乘；条件减法
中图分类号： TP393.08
文献标识码： A
文章编号： 1000-7180(2018)08-0026-05

A Novel SPA Attack on SM2 with Regular Point Multiplication

WANG Li-hui1, ZHAO Bing2, Li Qing1, LIANG Xiao-bing2, LIU Jing3
(1 Shanghai Fudan Microelectronics Group Company Limited, Shanghai 200433, China; 2 China Electric Power Research Institute, Beijing 100192, China; 3 Power Research Institute of State Grid Ningxia Power Co.，Yinchuan 750002，China)

Abstract： Compared with the RSA, the shorter key length is needed in the same security strength, so SM2 is more suitable for the application to the resource limited smart card. For the security of application of SM2, people study the variety point multiplication algorithms with countermeasures to resist the side channel attacks. This paper proposes a new simple side-channel analysis (SPA) method based conditional subtraction to attack two usual SM2 algorithms with countermeasures. Experimental results show that this method only needs a power trace, which can be used to break the SM2 key in a few seconds. At the same time, this paper also demonstrates some countermeasures to resist the attack.

Key words： SM2; SPA; montgomery modular multiplication; conditional subtraction

作者简介：
王立辉男，(1982-)，博士，工程师.研究方向为密码芯片安全.E-mail:wanglihui@fmsh.com.cn.
赵兵男，(1971-)，硕士，高级工程师.研究方向为信息学.
李清女，(1968-)，硕士，高级工程师.研究方向为集成电路设计开发.
梁晓兵男，(1978-)，博士，高级工程师.研究方向为信息学.