通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

首页　| 期刊简介 | 编委会 | 投稿须知 | 在线订阅 | 资料下载 | 编委论坛

甘刚,王敏,杜之波,吴震.基于Montgomery算法安全漏洞的SPA攻击算法[J].通信学报,2013,(Z1):156~161

基于Montgomery算法安全漏洞的SPA攻击算法

Simple power analysis attack against cryptosystemsbased on Montgomery algorithm

投稿时间： 2013-06-14

DOI： 10.3969/j.issn.1000-436x.2013.Z1.020

中文关键词：模幂运算 侧信道攻击 简单能量分析攻击 Montgomery算法

英文关键词：modular exponentiation side-channel attack simple power analysis Montgomery algorithm

基金项目：“十二五”国家密码发展基金资助项目（MMJJ201101022）；四川省科技支撑计划基金资助项目（2011GZ0170）；四川省教育厅重点科研基金资助项目（13ZA0091）

作者	单位
甘刚，王敏，杜之波，吴震	成都信息工程学院 网络工程学院，四川 成都 610225

摘要点击次数：98

全文下载次数：42

中文摘要：

公钥密码体制的算法大多基于有限域的幂指数运算或者离散对数运算。而这些运算一般会采用Montgomery算法来降低运算的复杂度。针对Montgomery算法本身存在可被侧信道攻击利用的信息泄露问题，从理论和实际功耗数据2方面分析了Montgomery算法存在的安全漏洞，并基于该漏洞提出了对使用Montgomery算法实现的模幂运算进行简单能量分析（SPA, simple power analysis）攻击算法。利用该算法对实际模幂运算的能量曲线进行了功耗分析攻击。实验表明该攻击算法是行之有效的。

英文摘要：

The Montgomery algorithm is widely used to reduce the computational complexity of large integer modular exponentiation. The SPA (simple power analysis) attacks against public-key cryptosystems based on Montgomery algorithm implementation were presented by exploitation of the inherent security vulnerability which that sensitive information leakage could be used by side-channel attack. The chosen-message SPA attacks were focused on, which enhance the differences of operating wave-forms between multiplication and squaring correlated to the secret key by using the input of particular messages. In particular, a SPA attack against RSA cryptosystem was showed based on large integer modular exponentiation. The results show that the attack algorithm is correct and effective.

查看全文 查看/发表评论 下载PDF阅读器

关闭

版权所有：《通信学报》
地址：北京市丰台区成寿寺路11号邮电出版大厦8层 电话：010-81055478，81055479
81055480，81055482 电子邮件：xuebao@ptpress.com.cn
技术支持：北京勤云科技发展有限公司