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

吴震,陈运,陈俊,王敏.真实硬件环境下幂剩余功耗轨迹指数信息提取[J].通信学报,2010,(2):17~21

真实硬件环境下幂剩余功耗轨迹指数信息提取

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
吴震	
陈运	
陈俊	
王敏	

中文摘要：

为获取真实硬件上实现的公钥密码密钥信息，提出了实用功耗分析模型，并归纳出指数信息提取的信息处理方法；利用自主设计实现的功耗分析平台获取了幂剩余算法功耗轨迹图，成功提取出其32bit指数信息；推翻了Messerges等关于使用SPA攻击难以在真实硬件环境下直接获取RSA密钥信息的论断；此外，还验证了静态掩盖算法抗SPA攻击的有效性。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭