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

李 浪,李仁发,李 静,吴克寿.PFM：一种抗高阶功耗攻击的SMS4算法[J].通信学报,2010,(5):87~92

PFM：一种抗高阶功耗攻击的SMS4算法

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
李 浪	
李仁发	
李 静	
吴克寿	

中文摘要：

针对已有的SMS4功耗攻击方法，设计了一种适合低功耗小面积的伪随机固定值掩码SMS4算法（PFM）。首先，对SMS4算法结构及内部加密运算流程进行研究；设计了一种SMS4原子掩码算法来抗高阶功耗攻击，该方法使各中间变量均被掩码；在此方法的基础上，为了减少芯片的面积和功耗以适应特殊环境下的加密应用（如特殊环境的传感器加密通信节点），提出了一种改进的固定值掩码算法：伪随机固定值掩码算法（PFM）及其实现技术。实验结果证明，该方法在芯片面积和功耗增加不大的情况下，可以有效抵抗二阶差分功耗攻击。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭