计算机工程与应用 2010 46 (6): 98-99 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

基于FPGA实现的DES抗能量攻击设计研究

温圣军，张鲁国

解放军信息工程大学 电子技术学院，郑州 450004

收稿日期 2008-9-12 修回日期 2008-11-7 网络版发布日期 2010-2-23 接受日期

摘要 针对文献[1]中提出的DES算法抗能量攻击设计方法，给出了对此方法的改进。改进后的设计方法与原方法相比，具有相同的能量攻击抵御能力。对改进算法的理论分析表明，此方法可适用于大多数分组密码算法的抗能量攻击设计，且相对于文献[1]中的方法，当基于FPGA具体实现时，改进算法可以在保持原有运行速度不变的情况下，节省约80%的硬件存储资源消耗。

关键词 三重数字加密标准算法（TDES） 能量攻击 逻辑资源 适用性

分类号 TP393

Design and research of DES against power analysis attacks based on FPGA

WEN Sheng-jun，ZHANG Lu-guo

Institute of Electronic Technology，the PLA Information Engineering University，Zhengzhou 450004，China

Abstract

Aimed at the DES design method against power analysis attacks mentioned in reference[1]，an improved one is proposed.Compared with the method of reference[1]，it has the same ability against the power analysis attacks.By analyzing the improved algorithm in theory，it is applicable for this method to make use of in the process of most of cipher algorithm’s design and implementation against power analysis attacks.The improved algorithm，while implemented based on FPGA，can not only save about eighty percent hardware storage resources，but also keep the operation rate in the same time.

Key words Triple Digital Encryption Standard（TDES） power analysis attack logic resource applicability

DOI: 10.3778/j.issn.1002-8331.2010.06.028

通讯作者 温圣军