计算机工程与应用 2007 43 (22): 103-105 ISSN: 1002-8331 CN: 11-2127/TP

产品、研发、测试

FPGA密码芯片差分功耗分析仿真研究

丁国良，赵 强，褚 杰，邓高明

军械工程学院 计算机工程系，石家庄 050003

收稿日期 修回日期 网络版发布日期 2007-7-20 接受日期

摘要 在分析FPGA组成结构特点的基础上，根据FPGA功耗产生的机理，提出了一种FPGA功耗模型。针对DES加密的DPA，实现了DPA仿真平台，并利用该模型和仿真平台验证了FPGA实现DES加密算法对DPA攻击的脆弱性。

关键词 旁路攻击 功耗泄漏模型 差分功耗分析 FPGA

分类号

Research of simulation DPA for FPGA cryptographic chips

DING Guo-liang，ZHAO Qiang，ZHU Jie，DENG Gao-ming

Dept. of Computer Engineering，Ordnance Engineering College，Shijiazhuang 050003，China

Abstract

Through analyzing architectural features of FPGA，a power consumption model of FPGA on the basis of the mechanism for power consumption is put forward.A DPA simulation platform is realized for DPA to DES.The model and platform validate the vulnerability of the realization of DES with FPGA for DPA attacks.

Key words side-channel attacks power leakage model Differential Power Analysis（DPA） FPGA

DOI:

通讯作者 丁国良 E-mail：DGL998@163.com