计算机工程与应用 2009 45 (36): 63-65 ISSN: 1002-8331 CN: 11-2127/TP

研发、设计、测试

# AES密码电路抗差分功耗分析设计

邹 程，张 鹏，邓高明，赵 强

军械工程学院 计算机工程系，石家庄 050003

收稿日期 2008-12-29 修回日期 2009-2-16 网络版发布日期 2009-12-30 接受日期

摘要 针对差分功耗分析（DPA）攻击的原理及特点，分析了高级加密标准（AES）的DPA攻击弱点，采用掩盖（Masking）的方法分别对AES算法中字节代换部分（SubBytes）及密钥扩展部分进行了掩盖，在此基础上完成了AES抵御DPA攻击的FPGA硬件电路设计。通过对该AES的FPGA电路的差分功耗攻击实验验证，该方法能够很好地抵抗DPA攻击。

关键词 差分功耗分析（DPA） 掩盖 高级加密标准（AES）

分类号 TP309

# Differential Power Analysis resistant hardware implementation of AES cryptosystem

ZOU Cheng，ZHANG Peng，DENG Gao-ming，ZHAO Qiang

Department of Computer Engineering，Ordnance Engineering College，Shijiazhuang 050003，China

**Abstract**

This paper firstly declares the principle of the Differential Power Analysis（DPA） attack technology，and shows the vulnerability for power analysis attack straightforward AES.Then，it gets the method about masking to reduce the differential power signal of an AES circuit and completes the circuit.Finally，with experiment，it proves this circuit can lead to the failure of differential power analysis.

**Key words** Differential Power Analysis（DPA） masking Advanced Encryption Standard（AES）

DOI: 10.3778/j.issn.1002-8331.2009.36.019

通讯作者 邹 程 zc1980921@163.com