抗二阶 DPA 分析的 ZUC 算法防护方案及硬件实现

朱文锋 [1]，郭 筝 [1,2]

（1 上海交通大学 微电子学院，上海 200010；2 智巡密码（上海）检测技术有限公司，上海 200010）

摘 要：对于不带防护的 ZUC 算法硬件实现，容易 DPA 攻击的影响.为此提出了基于二阶算术加、有限域 sbox 二阶全掩码、sbox 固定掩码以及伪轮防护方案的 ZUC 算法防护方案，理论上可以抗二阶 DPA 攻击，在 FPGA 上对其进行了实现，并在硬件实现进行了一定的优化，节省了功耗和面积.我们通过 FPGA 功耗采集平台，采集带防护的 ZUC 算法硬件实现的功耗曲线，对其进行 DPA 攻击，没有攻击出正确密钥，表明我们的防护方案实际有效，大大增加了功耗分析攻击的难度.

关键词：祖冲之算法；二阶 DPA；掩码方案；硬件实现

ZUC algorithm protection scheme and hardware implementation of against second-order DPA analysis

ZHU Wen-feng [1]，GUO Zheng [1,2]

(1 Microelectronics Institute, Shanghai Jiaotong University, Shanghai 20010, China;
2 Zhixing Password (Shanghai) Testing Technology Co., Ltd, Shanghai 200010,China)

Abstract：For the ZUC algorithm hardware implementation without protection, it is easy to influence the DPA attack.To this end, we propose a ZUC algorithm protection scheme based on second-order arithmetic addition, finite-domain sbox second-order full mask, sbox fixed mask and pseudo-wheel protection scheme, which can theoretically resist second-order DPA attacks.The ZUC algorithm protection scheme is implemented on the FPGA, and the hardware implementation is optimized to save power and area.We use the FPGA power consumption acquisition platform to collect the power consumption curve of the protected ZUC algorithm hardware, and perform DPA attacks on it. No correct key is attacked, indicating that our protection scheme is practical and effective, greatly increasing the power analysis attack difficulty.

Key words： ZUC algorithm; second order DPA; masking scheme; hardware implementation

作者简介：

朱文锋 男，(1994-)，硕士研究生.研究方向为分组密码算法掩码方案设计和攻击.
E-mail:zhuwenfengzi@formail:con.

郭 筝 男，(1980-)，博士，工程师.研究方向为集成电路安全分析和测试.