基于功耗感知隐藏技术的 SM4 算法 S 盒的实现

杨超群 1,殷树娟 1,李翔宇 2
（1 北京信息科技大学 理学院,北京 100192；2 清华大学 微电子所,北京 100084）

摘要： 功耗感知隐藏技术（PAH）是一种低功耗的抗功耗攻击方法，用于 AES 算法的 S 盒保护显示了安全性和能量效率上的优势.SM4 是我国自主设计的专用分组密码算法，在芯片实现中同样需要进行侧信道攻击防护.本文采用 PAH 技术，设计实现了 SM4 算法的 S 盒，设计了适用于 SM4 算法的补偿方案，并给出了自动化设计实现流程，将 PAH 技术推广应用到了 SM4 算法的 S 盒，版图后仿真结果表明所实现的 SM4 S 盒相对于其它方法功耗延时积降低了 76%，安全性达到与 AES S 盒电路相近的效果，证明了 PAH 方法的通用性.
关键词： SM4 算法；S 盒；PAH 技术；补偿方案；自动化设计实现流程

Implementation of SM4 Algorithm S-box Based on Power-aware Hiding Method

YANG Chao-qun1，YIN Shu-juan1，LI Xiang-yu2
(1 School of Applied Science, Beijing Information Science & Technology University, Beijing 100192, China;

2 Institute of Microelectronics, Tsinghua University, Beijing 100084,China)

Abstract： Power-aware hiding (PAH) is a low power and anti-power-analysis method. It shows the advantages in terms of security and energy efficiency when used for S box protection of AES algorithm. SM4 is a special block cipher algorithm designed independently in our country, and the protection of side channel attacks is also needed in the implementation of the chip. In this paper, the S box of SM4 algorithm is designed and implemented by using PAH method. The compensation scheme for SM4 algorithm is designed and the design flow of automation is given. The PAH technology is extended to the S-box of SM4 algorithm. The post-layout simulation results show that the power delay product of the implemented SM4 S box is 76% lower than other methods. And the security is similar to that of the AES S-box circuit. The generality of the PAH method is proved.
Key words： SM4 block cipher algorithm; S-box; PAH method; compensation scheme; automation design and implementation process

作者简介：
杨超群女，（1993-），硕士研究生.研究方向为密码集成电路.E-mail:yangcq0124@163.com.
殷树娟女，（1981-），副教授.研究方向包括混合信号集成电路设计、无源器件设计、核电子学和 IP 可重用设计.
李翔宇男，（1977-），副研究员.研究方向包括嵌入式系统安全和信息安全、超大规模集成电路、物联网设备和低功耗集成电路.