一种抗物理攻击防篡改检测技术

张　赟 1，赵毅强 1，刘军伟 1,2，李雪民 1，杨　松 1
(1 天津大学 电子信息工程学院，天津 300072；
2 信息工程大学 密码工程学院，河南 郑州 450002）

摘　要： 提出一种应用于高安全芯片的抗侵入式物理攻击防篡改检测技术，利用芯片顶层金属对侵入式攻击进行主动实时监测，可有效地防止侵入式攻击对电路存储关键信息的提取.提出了针对大规模电路的随机哈密顿回路版图优化加速生成算法，能够在较短时间内生成高无序、大格点量的拓扑结构.本方法可增加攻击者实施侵入式攻击所需的时间与成本，提升大尺寸高安全芯片的物理防护能力.

关键词： 信息安全；物理攻击；屏蔽探测层；随机哈密顿回路；信息熵

A Temper-Resistant Detecting Technique Against Physical Attack

ZHANG Yun1, ZHAO Yi-qiang1, LIU Jun-wei1,2, LI Xue-min1, YANG Song1
(1 School of Electronic Information Engineering, Tianjin University, Tianjin 300072, China; 2 School of Cryptography Engineering, Information Engineering University, Zhengzhou 452400, China)

Abstract： A temper resistant detecting technique applied in high security chips is proposed in this paper. The method utilize the topmost layer to monitor attack behaviors in real time, which prevents the key information stored in circuits from being stolen. An optimized algorithm for generating a random hamilton path of the layout in VLSI circuits is proposed. Using this algorithm, a highly disordered topology with a large area can be generated in a short time. The proposed method can increase the time and cost for the invasive attacks and improve the physical defense ability.

Key words： information security; physical attack; shield; random hamilton path; entrop

作者简介：
张　赟　男，（1991-），硕士研究生.研究方向为集成电路设计.
赵毅强（通讯作者）　男，（1964-），博士，教授，博士生导师.研究方向为集成电路设计.E-mail: yq_zhao@tju.edu.cn
刘军伟　男，（1977-），博士研究生.研究方向为集成电路设计.
李雪民　男，（1990-），硕士研究生.研究方向为集成电路设计.
杨　松　男，（1990-），硕士研究生.研究方向为数字集成电路设计、算法设计.