电子科学与工程学院国家ASIC工程中心宽电压IC设计团队在2020年JSSC期刊发表机器学习抗旁路攻击电路成果

发布者：杨婷婷 发布时间：2021-02-26 浏览次数： 1270

2020年，东南大学国家ASIC中心宽电压IC设计团队在集成电路领域国际旗舰期刊IEEE Journal of Solid-State Circuits （JSSC）上发表了题为“Machine Learning Assisted Side-Channel-Attack Countermeasure and Its Application on a 28-nm AES Circuit”的研究论文。论文作者为单伟伟、张帅、徐嘉铭、陆旻熠、杨军、时龙兴。

JSSC为集成电路领域影响力最大、难度最大的国际顶级学术期刊。自1966年创刊至今50余年时间内，在2019年之前，中国大陆高校在此期刊上总计发表论文仅40余篇。

论文主要研究密码电路的抗旁路攻击方法。旁路攻击（SCA）的硬件对策对于保护加密电路十分必要。许多对策会消耗较大的存储和面积开销。ASIC中心宽电压IC设计团队提出了一种基于机器学习的抗SCA方法，该方法可直接补偿中间数据的汉明距离（HD）概率，从而使得通过汉明距离（HD）概率无法区分正确和错误的子密钥。其原理是通过机器学习寻找到最优的汉明概率重映射矩阵，之后输入到补偿电路中进行补偿。

将该电路应用于高级加密标准（AES）-128电路，整个补偿电路在28nm上实现，可有效提升抗攻击效果。此外，它对于频率和吞吐率并不会有影响，其功耗和面积开销都相对较低，因此非常适合用于资源受限的加密电路。

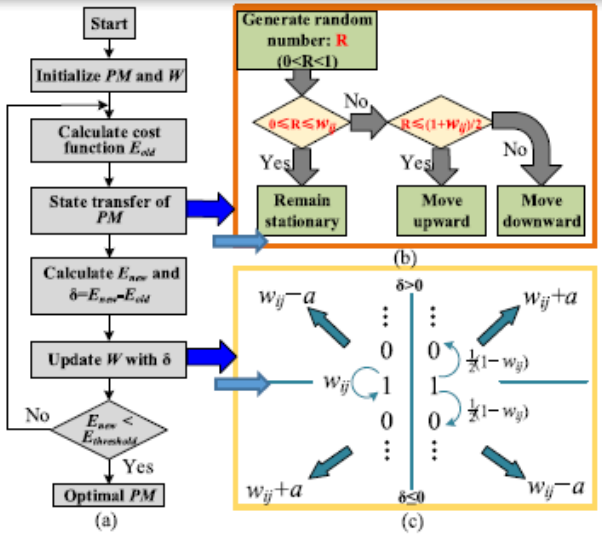

图1 利用机器学习方法获得HD重分布

TABLE II

CHARACTERISTICS OF AES CIRCUIT

Metrics	Unprotected AES		Protected AES	
CMOS Process	28 nm			
Supply Voltage (V)	1.1	0.42	1.1	0.42
Frequency (MHz)	870	25	870	25
Throughput (Gb/s)	11.14	0.32	11.14	0.32
Power (mW)	21.3	0.13	29.8 (+39.9%)	0.18 (+38.4%)
Energy Efficiency (pJ/bit)	1.913	0.42	2.77	0.59
CPA resistance (MTD)	3,367		>1,500,000	

图2 本工作和未受保护的AES系统对比

供稿人：陆亦诚 单伟伟

地址：南京市玄武区四牌楼2号东南大学
邮编：210096

管理入口

联系我们