doi: 10.1631/FITEE.1500460

题目：边信道攻击和学习向量量化

概要：尽管加密算法已得到改进，加密系统的安全性仍然是密码系统设计者关注的重点。边信道攻击可利用加密系统的物理漏洞来获取秘密信息。目前提出的多种边信道信息分析方法中，机器学习被认为是一种有前景的方法。基于神经网络的机器学习可获得指令标志（功耗与电磁辐射），并自动识别。本文对椭圆曲线加密（Elliptic curve cryptography, ECC）的现场可编程门阵列（field-programmable gate array, FPGA）实现展开了新的实验研究，探讨了基于学习向量量化（Learning vector quantization, LVQ）神经网络的边信道信息表征的效率。LVQ 作为多类分类器的主要特点是它具有学习复杂非线性输入-输出关系、使用顺序训练程序和适应数据的能力。实验结果表明基于 LVQ 的多类分类是边信道数据表征的强大且有前景的方法。

关键词：边信道攻击；椭圆曲线加密；多类分类；学习向量量化