doi:10.1631/FITEE.1800312

题目：针对一种基于 SM3 算法的消息验证码的相关能量攻击

概要：基于哈希函数的消息验证码（HMAC）被广泛应用于身份认证和消息完整性领域。SM3函数作为中国的哈希函数在国内具有很高市场价值。基于SM3的HMAC（HMAC-SM3）侧信道安全性依旧处于被评估阶段，尤其在硬件实现下的侧信道安全性更具研究价值。在硬件实现下，存储在寄存器的中间值有明显的汉明距离泄漏。此外，SM3算法结构决定了HMAC-SM3侧信道分析难度。针对HMAC-SM3的硬件实现，提出一种技巧性的基于比特值的选择明文相关能量攻击策略。在一款现场可编程门阵列（FPGA）开发板上进行实际攻击实验。实验结果表明，利用所提选择明文攻击策略，可从2256的密钥猜测空间中恢复正确密钥。

关键词：HMAC-SM3；侧信道分析；相关能量攻击；基于比特值的选择明文