摘要

尽管布尔函数和秘密分享都是密码学中较为成熟的经典课题，但布尔函数的秘密分享却是一个研究并不多的分支，针对侧信道攻击的分组密码算法安全实现就利用了后者。在本次讲座中，我们报告有限域 GF(2^8)上求逆映射的非平衡门限秘密分享，以及我们对国际高级加密标准算法 AES 和我国分组密码标准算法 SM4 的抗侧信道实现结果。这是到目前为止面积最小的 AES 掩码实现结果。