doi:10.1631/FITEE.1601652

题目：基于 Feistel 动态网络映射的非易失存储内存安全增强方法

概要：作为构建未来主存系统的替代方案，新兴的非易失性存储器 NVM （non-volatile memory）技术可用高能效和低开销方式提高内存容量。然而，非易失存储器有限的耐久性导致其面临安全威胁：若恶意攻击者持续对一小部分物理行进行写操作，整个系统会很快失效。为解决该问题，提出几个磨损均衡方案，以安全感知的方式将写负载均匀分布到整个内存空间。提出一种基于重映射时间差异信息泄露的时间探测攻击 RTA（remapping timing attack）。分析和实验结果表明，RTA 可攻击 3 种最新磨损均衡方案（例如，基于区域的 start-gap、安全刷新和多路磨损均衡），使它们在很短时间内失效（例如，几天甚至几分钟）。为抵抗该攻击，提出一种新的磨损均衡方案，即基于安全区域的 start-gap（security RBSG）。该方案采用动态 Feistel 网络的两级策略，利用可调节安全保障增强简单的 start-gap。理论分析和评估结果表明，提出的安全 RBSG 方案不仅可以抵抗传统攻击，也可以很好地抵抗 RTA。

关键词：非易失存储（NVM）；耐久性；磨损均衡；时间攻击