改进的深度学习辅助密钥恢复框架：大状态分组密码的应用

李肖伟，任炯炯，陈少真
信息工程大学网络空间安全学院，中国郑州市，450000

摘要：在 2019 年的年度国际密码学会议上，Gohr 提出一种基于深度学习的密码分析技术，适用于分组较短的减轮轻量级分组密码 SPECK32/64。Gohr 遗留了一个关键问题，即如何实现基于深度学习的大状态分组密码密钥恢复攻击。本文设计了一种基于深度学习的大状态分组密码的密钥恢复框架。首先，提出基于深度学习的密钥比特敏感性测试(KBST)客观划分密钥空间。其次，提出一种新的构造神经区分器组合方法，以改进用于大状态分组密码深度学习辅助密钥恢复框架，并从密码分析角度证明其合理性和有效性。在改进的密钥恢复框架下，本文为 SIMON 和 SPECK 各大状态训练了一个有效的神经区分器组合，并执行了对 SIMON 和 SPECK 大状态成员的实际密钥恢复攻击。本文提出的 13 轮 SIMON64 攻击是迄今为止最有效的实际密钥恢复攻击方法。这是首次尝试在 18 轮 SIMON128、19 轮 SIMON128、14 轮 SIMON96 和 14 轮 SIMON64 上进行基于深度学习的实用密钥恢复攻击。此外，本文改进了针对 SPECK 大状态成员的实际密钥恢复攻击结果，提高了密钥恢复攻击的成功率。

关键词：深度学习；大状态分组密码；密钥恢复；差分分析；SIMON；SPECK
https://doi.org/10.1631/FITEE.2300848