报告名称：基于周期性质的新型密钥恢复攻击方法

报告专家：邹剑

专家单位：福州大学

报告时间：2023 年 6 月 10 日上午 9：00

报告地点：数学与统计学学院 201

专家简介：邹剑，福州大学计算机与大数据学院副教授，硕士生导师。2015 年于中国科学院软件所获博士学位，毕业后作为福建省引进人才进入福州大学计算机与大数据学院承担教学与科研工作。主持国家级项目两项。现主要从事分组密码、量子计算等方面的研究，相关成果发表于 ASIACRYPT 2020、 IET Information Security、 Journal of Information Science and Engineering 等会议和期刊。

报告摘要:本文针对 Feistel、Misty 与 Type-1/2 型广义 Feistel 等结构，创新性地将 Simon 算法的周期性质与生日攻击思想相结合，提出了一种新型传统密钥恢复攻击。与 Simon 算法可以在多项式时间内恢复周期值不同，我们在传统计算环境下至少需要生日攻击界才能恢复出对应的周期值。利用我们的新方法，本文可以在$O(2^{n/4})$的选择明文和密文条件下，以$O(2^{3n/4})$的时间复杂度恢复出 5 轮 Feistel-F 结构的密钥，对应的存储复杂度为$O(2^{n/4})$。上述结果比 Isobe 和 Shibutani 的工作结果多扩展了 1 轮，并且所需的存储复杂度也更少。对于 Feistel-FK 结构，本文构造了 7 轮密钥恢复攻击。此外，我们还将上述方法应用于构造 Misty 结构和 Type-1/2 型广义 Feistel 结构的密钥恢复攻击。对于不同的 Misty 密码方案，本文分别给出了 5 轮 Misty L-F 和 Misty R-F 结构的密钥恢复攻击，以及 6 轮 Misty L-KF/FK 和 Misty R-KF/FK 结构的密钥恢复攻击。对

于 d 分支 Type-1 型广义 Feistel 结构，本文给出了 d^2 轮的密钥恢复攻击。当 $d \geq 6$ 时，本文对于 d 分支 Type-2 型广义 Feistel 结构的新型密钥恢复攻击轮数会优于现有密钥恢复攻击轮数。