**报告题目：**Unsupervised Hierarchical Side-Channel Analysis on ML-KEM Cryptographic Algorithms

**报告人：**孙绍飞，博士，北京邮电大学网络空间安全学院

摘要：Post-quantum cryptography (PQC) is a new generation of cryptographic schemes designed to resist attacks from quantum computers on existing cryptographic algorithms. Among current PQC proposals, lattice-based cryptography has emerged as the most promising solution due to its simple structure, fast computation speed, and high security. Consequently, it has garnered significant attention from side-channel analysis researchers in recent years. Our work focuses on ML-KEM, and applies unsupervised learning techniques for its side-channel analysis. By collecting trace leakages during its inverse Number Theoretic Transform (NTT) operation, and using specific ciphertext traces for simple power analysis, we successfully recover the key using unsupervised learning algorithms. Compared to existing techniques, our proposed method can recover the key using a small number of traces.



孙绍飞，博士，现为北京邮电大学网络空间安全学院副研究员，主要从事芯片安全、侧信道分析、硬件木马及人工智能等领域的研究工作，在国内外知名学术期刊上以第一作者或通信作者身份发表了多篇高水平学术论文。主持/参与多项国家自然科学基金项目、国家重点研发计划子课题、国家重点实验室开放课题等项目，参与起草了两项安全芯片的行业标准，已在侧信道分析领域积累了丰富的知识和经验。

Sun Shaofei is currently an associate researcher at the School of Cyberspace Security, Beijing University of Posts and Telecommunications. His main research areas include chip security, side-channel analysis, hardware trojans, and artificial intelligence. He has published multiple academic papers in well-known domestic and international academic journals. He has hosted and participated in several projects, including National Natural Science Foundation of China projects, the National Key R&D Program, and open projects from national key laboratories. He has also contributed to drafting two industry standards for security chips and has accumulated extensive knowledge and experience in the field of side-channel analysis.