**后量子密码算法的安全性分析**

**关键词**：后量子密码，实际安全性，密码误用，微架构，侧信道攻击，分析评估

**摘要**：量子算法与量子计算的快速发展为当前密码体系带来革命性影响，后量子密码已经成为密码学备受关注的重要领域。由于后量子密码数学结构类型多样、设计范式新颖复杂、实现技术千差万别、部署平台结构各异等特点，开展后量子密码的安全性分析面临严峻挑战。本项目拟面向NIST公布的首批后量子密码标准算法，开展后量子密码算法的安全性分析研究，重点探索密码误用和微架构分析对后量子密码的安全性影响，研究具有使用条件弱、安全威胁大、影响范围广等特点的后量子密码误用分析方法、与具有远程攻击能力的后量子密码微架构分析方法及其防御方案，并从侧信道分析和故障注入分析两个角度审视后量子密码的实现安全性，形成后量子密码算法的具体安全强度评估框架，最终构建后量子密码安全性分析原型系统。项目研究旨在推动完善后量子密码安全性分析方法与技术体系，为后量子密码安全应用和分析业务的开展提供技术手段和核心工具支撑。

The National Institute of Standard Technology (NIST), for the first time, standardized four post-quantum cryptographic algorithms in July, 2022, to protect the existing cryptosystems from being attacked by quantum computers in the coming years. The security of post-quantum cryptography essentially depends not only on the computational complexity of the underlying mathematical problems, but also on the security in implementation and deployment of the cryptographic schemes. The project plans to conduct security analysis research on the current four standardized post-quantum cryptography algorithms by NIST and the latest candidate algorithms, focusing on breaking through methodologies of attack and defense misuse analysis, microarchitectural analysis, side channel analysis and fault injection analysis. In the meanwhile, based on theoretical computational complexity evaluation of underlying mathematical problems, and along with full consideration of auxiliary information from misuse analysis, side-channel analysis, fault injection analysis, as well as mapping relations of sensitive parameters, the project is expected to establish novel auxiliary information-assisted analytical methods against post-quantum cryptography, and develop prototype system platform for technical proof-of-concept in several significant applications scenarios. As a result, the project aims to develop the theoretical and practical security analysis methods and techniques for post-quantum cryptography, and at the same time provides technical solutions and core tools for security applications with post-quantum cryptography and business development of important the national departments.