Popular science summary of the PhD thesis

PhD student	Fabrizio Sisinni
Title of the PhD thesis	Decryption Failures and Rigidity for Post-Quantum Public-Key Encryption
PhD school/Department	Department of Applied Mathematics and Computer Science

Science summary

As powerful quantum computers become a reality, many of today's cryptographic tools will no longer be secure. This has sparked a global effort to design "post-quantum" cryptography—new techniques that remain safe even against quantum attacks. One of the most promising directions is lattice-based cryptography, and a method called the Fujisaki–Okamoto (FO) transform plays a central role in securing many of these systems.

This thesis addresses two major questions about the security of FO-based schemes.

The first concerns reliability.
Lattice-based systems can occasionally produce small errors during decryption. While these errors do not affect normal operation, an attacker may try to exploit them to extract secret information. Researchers therefore developed tests to measure how difficult it is to trigger such failures. In this thesis, we analyze these tests for several widely used schemes and show that they satisfy the required security guarantees—both for the underlying mathematical problems and for the main constructions expected to secure future internet communications.

The second question deals with real-world attacks.
Even a mathematically sound system can leak information through its implementation—for example through timing, power use, or electromagnetic signals. A specific step of the FO transform, called re-encryption, is especially vulnerable to such side-channel attacks, and protecting it can be expensive.

This thesis introduces a new way to understand what re-encryption checks for and why it matters. We develop a general framework that captures this behavior and supports alternative checks that are less prone to side-channel leakage. At the same time, our analysis shows that in some situations the weaknesses of re-encryption are unavoidable, highlighting when stronger protections are necessary.

Together, these contributions offer a clearer and more complete picture of the security of FO-based post-quantum cryptography—helping ensure that the systems protecting our digital world remain secure in the age of quantum computers.

Please submit the summary to the department PhD coordinator together with your thesis