Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Seminar

Overview of different NTRU Variants

Established public key cryptography can be considered broken in the presence of a large scale quantum computer. In order to act on this emerging threat the National Institute of Standards and Technology (NIST) has started a competition [1] to standardize possible post-quantum cryptography algorithms.
A promising candidate algorithm is the NTRU cryptosystem which was first introduced by Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman in 1996. Since then it several different variants of the system were developed:
- NTRUEncrypt [2]
- NTRU-HRSS-KEM [3]
- NTRU Prime [4]

In the second round of the contest NTRUEncrypt and NTRU-HRSS-KEM merged to form NTRU [5]. Each algorithm is accompanied with its respective reference implementation, while several variants are integrated in the open source library pqm4 [6] and PQClean [7].

This work should given an overview of the difference and similarities between the different algorithms with a focus on:
- Parameters of the algorithm (e.g. “Which basic ring do they use? Is there a reason why?”)
- Did the authors mention why they changed something in their algorithms
- How are the algorithms implemented in practice using the respective reference implementations and [6,7] (e.g. “Which multiplication method do they use?”)

[1] https://csrc.nist.gov/Projects/post-quantum-cryptography
[2] NTRUEncrypt
[3] NTRU-HRSS-KEM
[4] NTRU Prime
[5] NTRU
[6] https://github.com/mupq/pqm4
[7] https://github.com/PQClean/PQClean

Prerequisites

Request Topic

Advisors

Thomas Schamberger