NTRU Prime: modifications for round 2

20190330

Streamlined NTRU Prime parameter sets: Added smaller parameter set and larger parameter set to accompany the existing parameter set.

NTRU LPRime parameter sets: Added smaller parameter set and larger parameter set to accompany the existing parameter set. As before, the primes are shared between Streamlined NTRU Prime and NTRU LPRime.

No changes to trapdoor functions (now named "Core"). Changes to CCA conversion:

- Encodings are now more space-efficient, and are defined in a unified way across sizes.
- To enforce unique encodings of ciphertexts and public keys, the public-key string is included as an input to the confirmation hash, and the ciphertext string—including the confirmation—is included as an input to the session-key hash.
- Explicit rejection of invalid ciphertexts is replaced with implicit rejection as a second layer of defense against chosen-ciphertext attacks, beyond the existing layer of plaintext confirmation. The hashing details are redesigned.

Our new test script `ntruprime.sage` covers all three sizes for both Streamlined NTRU Prime and NTRU LPRime, and has a `round1` option to switch back to the previous CCA conversion. Various tests of `round1` match the round-1 software.

Further modifications to documentation:

- Section 2, "General algorithm specification", is reorganized and expanded. The section now describes Streamlined NTRU Prime in two layers, separating the mathematics of Streamlined NTRU Prime Core from the outer layer of CCA conversion. For NTRU LPRime there are three layers: NTRU LPRime Core is again the mathematics, NTRU LPRime Expand handles derandomization and seed expansion, and the outer layer handles the CCA conversion.
- Section 3, "List of parameter sets", presents shared parameter choices in a modularized and generalized way, simplifying the specification of each parameter set.
- Section 4, "Design rationale", is extended (starting "Modifications for round 2").
- Section 5, "Detailed performance analysis", is expanded and updated.
- Section 6, "Analysis of known attacks", is expanded and updated. This section explains a variety of security estimates that we have computed, including some for comparison to the "Estimate" page and some for improvements.
- Section 7, "Expected strength in general", is expanded and updated.
- Section 8, "Expected strength for each parameter set", is expanded and updated.
- Section 9, "Advantages and limitations", is extended (starting "Additional comments for round 2").