Round5: merge of Round2 and HILA5

Hayo Baan[1], Sauvik Bhattacharya[1], Scott Fluhrer[5], Oscar Garcia-Morchon[1], Thijs Laarhoven[3], Ludo Tolhuizen[1], Ronald Rietman[1], Markku-Juhani O. Saarinen[2], and Zhenfei Zhang[4]

[1]Philips (Netherlands)
[2]PQShield (UK)
[3]TU/e (Netherlands)
[4]Algorand (US)
[5]Cisco (US)

November 30, 2018

Round5

Round5 is a merger of the Round2 [1] and HILA5[2] submissions. Basically, Round5 is Round2 with the error-correction code defined in HILA5.

This document summarizes which elements of Round2 and HILA5 are combined in Round5. It also describes the official comments on Round2, HILA5, and Round5 on the NIST PQC forum, and how they have been addressed.

Changes in Round5 compared to Round2 and HILA5

- **Error correction:** Round5 incorporates an error correction code based on that of HILA5 into the INDCPA-PKE scheme defined in Round2. The goal is to achieve the same target failure probability as Round2, but using smaller configuration parameters that lead to better performance. Direct application of HILA5's error correction in Round2 does not work well, as the decoder is confronted with correlated errors. These correlations are caused by the usage of a prime cyclotomic polynomial as reduction polynomial. Securely applying HILA5's code to Round2 requires performing operations on $\mathbf{v}$ in the NTRU ring and using balanced secrets. These are not major changes since Round2 – internally – already performs all operations on $\mathbf{v}$ in the NTRU ring, and Round2's implementation also uses balanced secrets.
  HILA5's error correction code avoids table look-ups and conditions altogether and it is, therefore, resistant to timing attacks.

- **Security targets:** Security targets in Round5 for NIST security levels I, III, and V are such that breaking Round5 requires a classical effort of at least 128, 192, and 256 bits, respectively. Similarly, the quantum-effort to break Round5 is bigger than 128 − MAXDEPTH, 192 − MAXDEPTH, and 256 − MAXDEPTH, respectively. Round5 encapsulates 128-, 192-, and 256- bit long keys in NIST security levels I, III, and V.

- **Parameter sets:** Round5 defines 21 parameter sets.

  - Six ring configurations (three each for INDCPA-KEM and INDCCA-PKE, each for NIST security levels I, III, and V) with a code capable of five error correction. Using XEf requires the reduction polynomial to be $\xi(x) = x^{n+1} - 1$ and that the sparse ternary secrets are balanced. These parameter choices are based on the merge of HILA5 with Round2 and show that the usage of error correction leads to the smallest public key and ciphertext sizes.
  - Six ring configurations (as above, three each for KEM and PKE, corresponding to NIST security levels I, III, and V) without error correction. These parameter choices can be considered more conservative than the previous ones, as they are only based on the Round2 design – no error correction used – that has received public review since its submission. However, since no error correction is applied, bandwidth requirements are around 33% higher than the previous parameters based on the merge of Round2 and HILA5 using error correction.
  - Six non-ring configurations (as above, three each for KEM and PKE, corresponding to NIST security levels I, III, and V) without error correction. These parameter choices rely on same design choices as the original Round2 submission.
  - Three application-tailored configurations.
    - A ring-based KEM configuration addressing Internet of Things applications that achieves even smaller bandwidth (736 Bytes in total) at the price of lower security and higher failure probability.
    - A ring-based KEM NIST level 1 configuration in which the encapsulated key is 192-bit long instead of just 128-bit long so that the difficulty of attacking the encapsulated key (by Grover) equals the difficulty of quantum lattice attack to Round5,
    - A non-ring-based NIST Level III PKE parameter set with a ciphertext size of only 988 Bytes, with very fast encryption and decryption, by taking $\overline{m} = 1$, at the cost of a larger public key. This configuration makes unstructured lattice configurations feasible in applications in which the public-key can remain static for a long time, e.g., email encryption.

- **Rounding constants:** In contrast to Round2, Round5 defines the rounding operation in terms of flooring and rounding constants. Round5 does so to guarantee the INDCPA security proof.
- **Power-of-two moduli:** All moduli in Round5 are powers of two. This allows for easy-to-implement modular arithmetic, and avoids the generation of random uniform noise otherwise required to guarantee uniform symbols in public keys and ciphertexts. Thus, Round5 does not provide support for NTT speed-ups that were applicable with both Round2 and HILA5.
- **Improved description:** Round5 specification is based on Round2 documentation to make it easier to identify changes with regard to the original submission. Specification is improved by including a broader security analysis and a detailed technical specification.

PQC comments

- **Constant time sorting in Round2:** On December 27, 2017, Daniel J. Bernstein addressed the constant-time generation of ternary secrets. Round5 addresses this by not requiring sorting in the generation of ternary secrets and using simple rejection sampling. Rejection sampling is not constant-time, but it is not related to the secret itself.
- **INDCCA security in HILA5:** On December 28, 2017, Lorenz Panny pointed out an error in HILA5's description that claimed IND-CCA security. Round5 addresses this by using the Fujisaki - Okamoto transformation proposed in Round2.
- **INDCPA-PKE proof in Round2:** On January 12, 2018, Jan-Pieter D'Anvers pointed out that the IND-CPA security proof of Round2 should be corrected using rounding constants. Round5 addresses this issue as suggested by D'Anvers.
- **Security levels:** On January 13, 2018, Michael Hamburg pointed out that the Round2 security levels did not match NIST definition. Round5 uses correct NIST security levels.
- **Correlated errors in prime cyclotomic polynomial:** On August 4th, 2018, Léo Ducas pointed out potential issues in the independence assumption in the failure probability analysis of the initial Round5 description.

  In a subsequent comment by Michael Hamburg on August 24, 2018, Hamburg discussed the correlation of failures in the prime cyclotomic ring. He concluded that it does not affect the original Round2 design, but it frustrates the direct application of XEf on Round2. In the same method, Hamburg also describes a ring switching trick, developed by himself and three members of the Round2 team, which addresses this issue and is used to securely apply HILA5's error correction to Round5.

References

[1] Hayo Baan, Sauvik Bhattacharya, Oscar Garcia-Morchon, Ronald Rietman, Ludo Tolhuizen, Jose-Luis Torre-Arce, and Zhenfei Zhang. Round2: KEM and PKE based on GLWR. Cryptology ePrint Archive, Report 2017/1183, 2017.

[2] Markku-Juhani O. Saarinen. HILA5: Key Encapsulation Mechanism (KEM) and Public Key Encryption Algorithm, November 2017.