HAETAE update v3.0

Jung Hee Cheon[1,2], **Hyeongmin Choe**[1], Julien Devevey[3], Tim Güneysu[4, 5], Dongyeon Hong, Markus Krausz[4], Georg Land[4], Junbum Shin[2], Damien Stehlé[2], MinJune Yi[1]

[1]Seoul National University, [2]CryptoLab Inc.,
[3]ANSSI, [4]Ruhr Universität Bochum, [5]DFKI

KpqC 9th Workshop
October 23, 2024

HAETAE
HEAAN
CRYPTO LAB

HAETAE

- Digital signature scheme secure against quantum attacks!
  - based on **lattice hard problems** MLWE and MSIS
  - follows **Fiat-Shamir with aborts** framework, secure in QROM
- Simple but short!
  - simpler than Falcon[1] & shorter than Dilithium[1]
  - optimal rejection rate with simple rejection condition
- Unique design rationale
  - **Bimodal Hyperball** rejection sampling
  - **New** size optimization and implementation techniques
- Candidate in *KpqC 2nd round & NIST PQC Additional Signatures*[2]

[1] NIST 2022 PQC signature standards

[2] NIST's on-ramp PQC signature competition, from 2023.

HAETAE
HEAAN CRYPTO LAB

HAETAE

- Digital signature scheme secure against quantum attacks!
  - based on **lattice hard problems** MLWE and MSIS
  - follows **Fiat-Shamir with aborts** framework, secure in QROM
- Simple but short!
  - simpler than Falcon[1] & shorter than Dilithium[1]
  - optimal rejection rate with simple rejection condition
- Unique design rationale
  - **Bimodal Hyperball** rejection sampling
  - **New** size optimization and implementation techniques
- Candidate in *KpqC 2nd round & NIST PQC Additional Signatures*[2]

[1] NIST 2022 PQC signature standards

[2] NIST's on-ramp PQC signature competition, from 2023.

HAETAE
HEAAN
CRYPTO LAB

HAETAE

- Digital signature scheme secure against quantum attacks!
  - based on **lattice hard problems** MLWE and MSIS
  - follows **Fiat-Shamir with aborts** framework, secure in QROM
- Simple but short!
  - simpler than Falcon[1] & shorter than Dilithium[1]
  - optimal rejection rate with simple rejection condition
- Unique design rationale
  - **Bimodal Hyperball** rejection sampling
  - **New** size optimization and implementation techniques
- Candidate in *KpqC 2nd round & NIST PQC Additional Signatures*[2]

[1] NIST 2022 PQC signature standards

[2] NIST's on-ramp PQC signature competition, from 2023.

HAETAE
HEAAN CRYPTO LAB

HAETAE

- Digital signature scheme secure against quantum attacks!
  - based on **lattice hard problems** MLWE and MSIS
  - follows **Fiat-Shamir with aborts** framework, secure in QROM
- Simple but short!
  - simpler than Falcon[1] & shorter than Dilithium[1]
  - optimal rejection rate with simple rejection condition
- Unique design rationale
  - **Bimodal Hyperball** rejection sampling
  - **New** size optimization and implementation techniques
- Candidate in *KpqC 2nd round & NIST PQC Additional Signatures*[2]

[1] NIST 2022 PQC signature standards

[2] NIST's on-ramp PQC signature competition, from 2023.

HAETAE
HEAAN
CRYPTO LAB

Introduction to HAETAE v3.0

HAETAE was updated last July!

- Secret key sizes of SPEC were missing 32 bytes.
- Improved key generation procedure (40-60% reduced cycles)
  - Replace the 512-point FFT with a 256-point FFT.
  - No impact on security/sizes proven via equivalent equations.
  - KeyGen performance benchmark:
    - HAETAE-120: 882k $\rightarrow$ 535k cycles (-40%).
    - HAETAE-180: $1{,}654$k $\rightarrow$ 821k cycles (-50%).
    - HAETAE-250: $2{,}200$k $\rightarrow$ 872k cycles (-60%).

Introduction to HAETAE v3.0

HAETAE was updated last July!

- Secret key sizes of SPEC were missing 32 bytes.
- Improved key generation procedure (40-60% reduced cycles)
  - Replace the 512-point FFT with a 256-point FFT.
  - No impact on security/sizes proven via equivalent equations.
  - KeyGen performance benchmark:
    - HAETAE-120: $882\text{k} \rightarrow 535\text{k}$ cycles (-40%).
    - HAETAE-180: $1{,}654\text{k} \rightarrow 821\text{k}$ cycles (-50%).
    - HAETAE-250: $2{,}200\text{k} \rightarrow 872\text{k}$ cycles (-60%).

Introduction to HAETAE v3.0

HAETAE was updated last July!

- Secret key sizes of SPEC were missing 32 bytes.
- Improved key generation procedure (40-60% reduced cycles)
  - Replace the 512-point FFT with a 256-point FFT.
  - No impact on security/sizes proven via equivalent equations.
  - KeyGen performance benchmark:
    - HAETAE-120: $882\text{k} \rightarrow 535\text{k}$ cycles (-40%).
    - HAETAE-180: $1{,}654\text{k} \rightarrow 821\text{k}$ cycles (-50%).
    - HAETAE-250: $2{,}200\text{k} \rightarrow 872\text{k}$ cycles (-60%).

Introduction to HAETAE v3.0

HAETAE was updated last July!

- Secret key sizes of SPEC were missing 32 bytes.
- Improved key generation procedure (40-60% reduced cycles)
  - Replace the 512-point FFT with a 256-point FFT.
  - No impact on security/sizes proven via equivalent equations.
  - KeyGen performance benchmark:
    - HAETAE-120: 882k $\rightarrow$ 535k cycles (-40%).
    - HAETAE-180: $1{,}654$k $\rightarrow$ 821k cycles (-50%).
    - HAETAE-250: $2{,}200$k $\rightarrow$ 872k cycles (-60%).

Introduction to HAETAE v3.0

- Reduced B' (by 0.01).
  - The previous B' did not satisfy Lemma 5
    - Mainly due to some rounding error that occurred in the Python script.
    - Thanks to Nari Lee, Hansol Ryu, and Hochang Lee for pointing this out.
  - We reduced B' by 0.01 which makes everything correct.
  - Negligible impact on the implementation/performance.

Lemma 5 (Bimodal Hyperball Rejection Sampling). *Let n be the degree of $\mathcal{R}$, $c > 1$, $r, t, m > 0$, and $B \geq \sqrt{B'^2 + t^2}$. Define $M = 2(B/B')^{mn}$ and set*

$$N \geq \frac{1}{c^{1/(mn)} - 1} \frac{\sqrt{mn}}{2} \left(\frac{c^{1/(mn)}}{B'} + \frac{1}{B} \right).$$

Introduction to HAETAE v3.0

- Reduced B' (by 0.01).
  - The previous B' did not satisfy Lemma 5
    - Mainly due to some rounding error that occurred in the Python script.
    - Thanks to Nari Lee, Hansol Ryu, and Hochang Lee for pointing this out.
  - We reduced B' by 0.01 which makes everything correct.
  - Negligible impact on the implementation/performance.

Lemma 5 (Bimodal Hyperball Rejection Sampling). *Let n be the degree of $\mathcal{R}$, $c > 1$, $r, t, m > 0$, and $B \geq \sqrt{B'^2 + t^2}$. Define $M = 2(B/B')^{mn}$ and set*

$$N \geq \frac{1}{c^{1/(mn)} - 1} \frac{\sqrt{mn}}{2} \left(\frac{c^{1/(mn)}}{B'} + \frac{1}{B} \right).$$

Introduction to HAETAE v3.0

- Reduced B' (by 0.01).
  - The previous B' did not satisfy Lemma 5
    - Mainly due to some rounding error that occurred in the Python script.
    - Thanks to Nari Lee, Hansol Ryu, and Hochang Lee for pointing this out.
  - We reduced B' by 0.01 which makes everything correct.
  - Negligible impact on the implementation/performance.

Lemma 5 (Bimodal Hyperball Rejection Sampling). *Let n be the degree of $\mathcal{R}$, $c > 1$, $r, t, m > 0$, and $B \geq \sqrt{B'^2 + t^2}$. Define $M = 2(B/B')^{mn}$ and set*

$$N \geq \frac{1}{c^{1/(mn)} - 1} \frac{\sqrt{mn}}{2} \left(\frac{c^{1/(mn)}}{B'} + \frac{1}{B} \right).$$

Thanks!

- The conference version of HAETAE can be found at tches.iacr.org/index.php/TCHES/article/view/11669

- Packages and specifications are available at kpqc.cryptolab.co.kr/haetae