HAETAE 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 Contest 2nd Round Colloquium
August 28, 2024

HAETAE
HEAAN
CRYPTO LAB

1. Brief Intro:
   - Introduction

2. Advantages:
   - Complete Quantum Security Analysis
   - Unique and Efficient Design
   - Small Sizes

3. HAETAE Update v3.0:
   - Updates

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

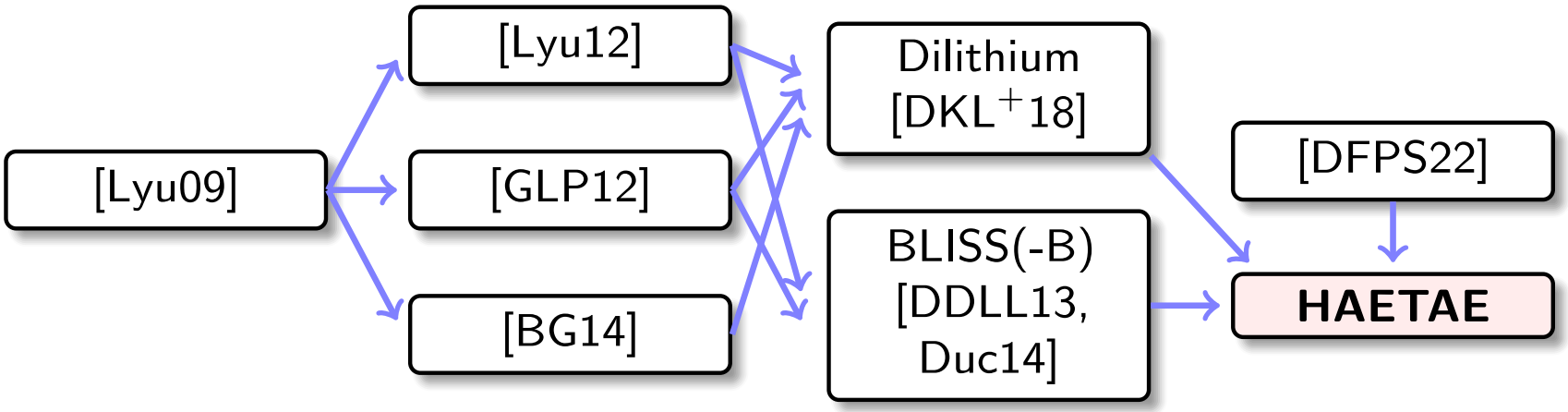
1. Brief Intro:
   - Introduction

2. Advantages:
   - Complete Quantum Security Analysis
   - Unique and Efficient Design
   - Small Sizes

3. HAETAE Update v3.0:
   - Updates

HAETAE Security

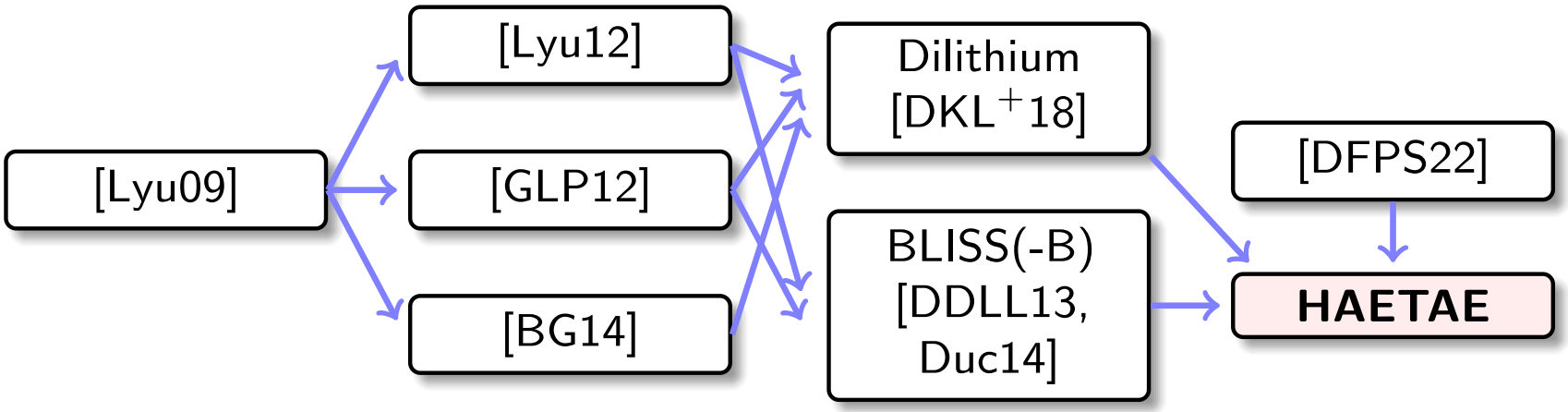
HAETAE is based on *Fiat-Shamir with Aborts (FSwA)* as ML-DSA (Dilithium).



- Well-studied quantum/classical security analyses [KLS18, GHHM21, DFPS23].
  - A complete security analysis of HAETAE is provided from v2.0.
- Side-channel security analysis
  - Constant-time implementation is provided from v2.0.
  - Analysis on masked implementation
    - Simpler than Hash-and-Sign signatures (Falcon, Mitaka, ...)
    - Fully fixed-point!

HAETAE Security

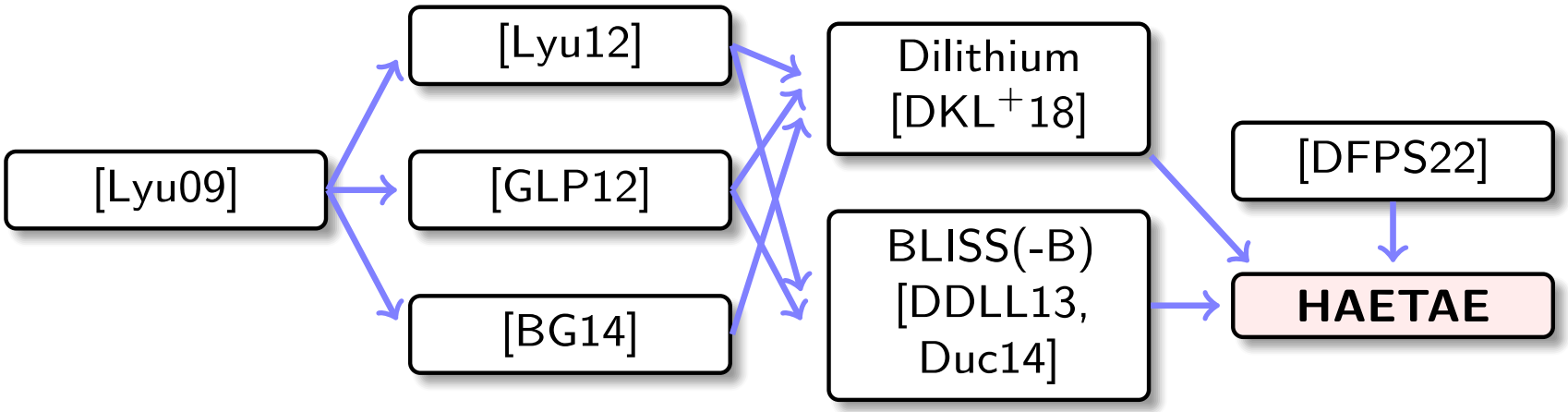
HAETAE is based on *Fiat-Shamir with Aborts (FSwA)* as ML-DSA (Dilithium).



- Well-studied quantum/classical security analyses [KLS18, GHHM21, DFPS23].
  - A complete security analysis of HAETAE is provided from v2.0.
- Side-channel security analysis
  - Constant-time implementation is provided from v2.0.
  - Analysis on masked implementation
    - Simpler than Hash-and-Sign signatures (Falcon, Mitaka, ...)
    - Fully fixed-point!

HAETAE Security

HAETAE is based on *Fiat-Shamir with Aborts (FSwA)* as ML-DSA (Dilithium).



- Well-studied quantum/classical security analyses [KLS18, GHHM21, DFPS23].
  - A complete security analysis of HAETAE is provided from v2.0.
- Side-channel security analysis
  - Constant-time implementation is provided from v2.0.
  - Analysis on masked implementation
    - Simpler than Hash-and-Sign signatures (Falcon, Mitaka, ...)
    - Fully fixed-point!

HAETAE Design

We combine the recent approaches:

- **Fiat-Shamir with Aborts** framework
- **Bimodal** rejection sampling
- randomness sampling from **Hyperball** distribution

$\Rightarrow$ Unique design of **Bimodal Hyperball**-based rejection sampling

Figure: Rejection from Left (Bimodal Hyperball) to Right (Hyperball)

with **NEW techniques**:

- Secret key rejections
- Bimodal verification key truncation
- Fixed-point discretized hyperball sampling

HAETAE Design

We combine the recent approaches:

- **Fiat-Shamir with Aborts** framework
- **Bimodal** rejection sampling
- randomness sampling from **Hyperball** distribution

⇒ Unique design of **Bimodal Hyperball**-based rejection sampling

Figure: Rejection from Left (Bimodal Hyperball) to Right (Hyperball)

with **NEW techniques**:

- Secret key rejections
- Bimodal verification key truncation
- Fixed-point discretized hyperball sampling

HAETAE Design

We combine the recent approaches:

- **Fiat-Shamir with Aborts** framework
- **Bimodal** rejection sampling
- randomness sampling from **Hyperball** distribution

⇒ Unique design of **Bimodal Hyperball**-based rejection sampling

Figure: Rejection from Left (Bimodal Hyperball) to Right (Hyperball)

with **NEW techniques**:

- Secret key rejections
- Bimodal verification key truncation
- Fixed-point discretized hyperball sampling

HAETAE Design

We combine the recent approaches:

- **Fiat-Shamir with Aborts** framework
- **Bimodal** rejection sampling
- randomness sampling from **Hyperball** distribution

$\Rightarrow$ Unique design of **Bimodal Hyperball**-based rejection sampling

Figure: Rejection from Left (Bimodal Hyperball) to Right (Hyperball)

with **NEW techniques**:

- Secret key rejections
- Bimodal verification key truncation
- Fixed-point discretized hyperball sampling

HAETAE Design

We combine the recent approaches:

- **Fiat-Shamir with Aborts** framework
- **Bimodal** rejection sampling
- randomness sampling from **Hyperball** distribution

$\Rightarrow$ Unique design of **Bimodal Hyperball**-based rejection sampling

Figure: Rejection from Left (Bimodal Hyperball) to Right (Hyperball)

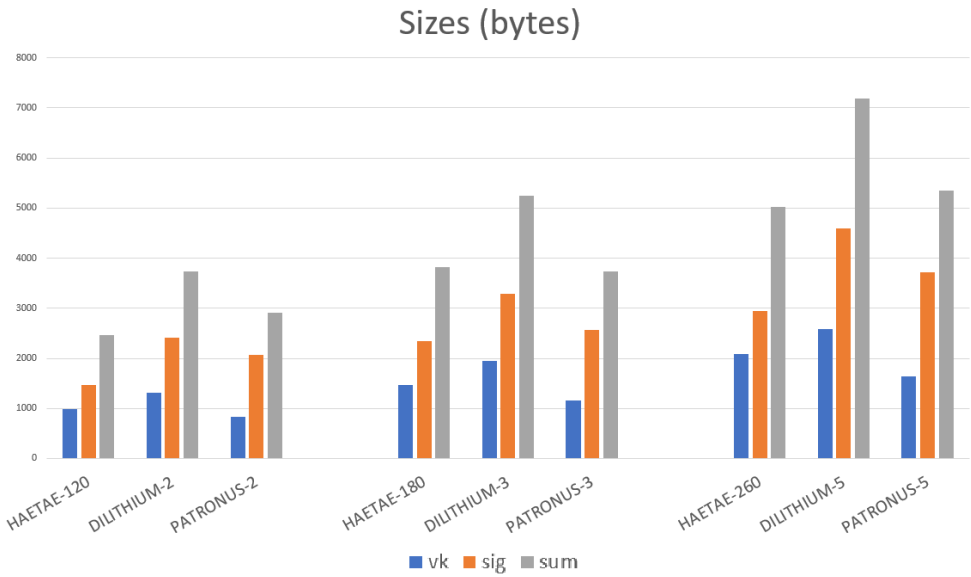
with **NEW techniques**:

- Secret key rejections
- Bimodal verification key truncation
- Fixed-point discretized hyperball sampling

HAETAE Sizes

HAETAE is the **smallest** among **Fiat-Shamir with Aborts (FSwA)** lattice signature.

Scheme	vk	sig	sum
HAETAE-120	992	1,474	2,466
HAETAE-180	1,472	2,349	3,821
HAETAE-260	2,080	2,948	5,028
Dilithium-2	1,312	2,420	3,732
Dilithium-3	1,952	3,293	5,245
Dilithium-5	2,592	4,595	7,187
Patronus-2	832	2,070	2,902
Patronus-3	1,152	2,575	3,727
Patronus-5	1,632	3,721	5,353



- Patronus (C'24) [BBRS24]: replace hyperball by hyper-polytope.
- HAETAE-120 fits into one TCP or UDP datagram (sig + vk $\leq$ 3,000B).

HAETAE Sizes

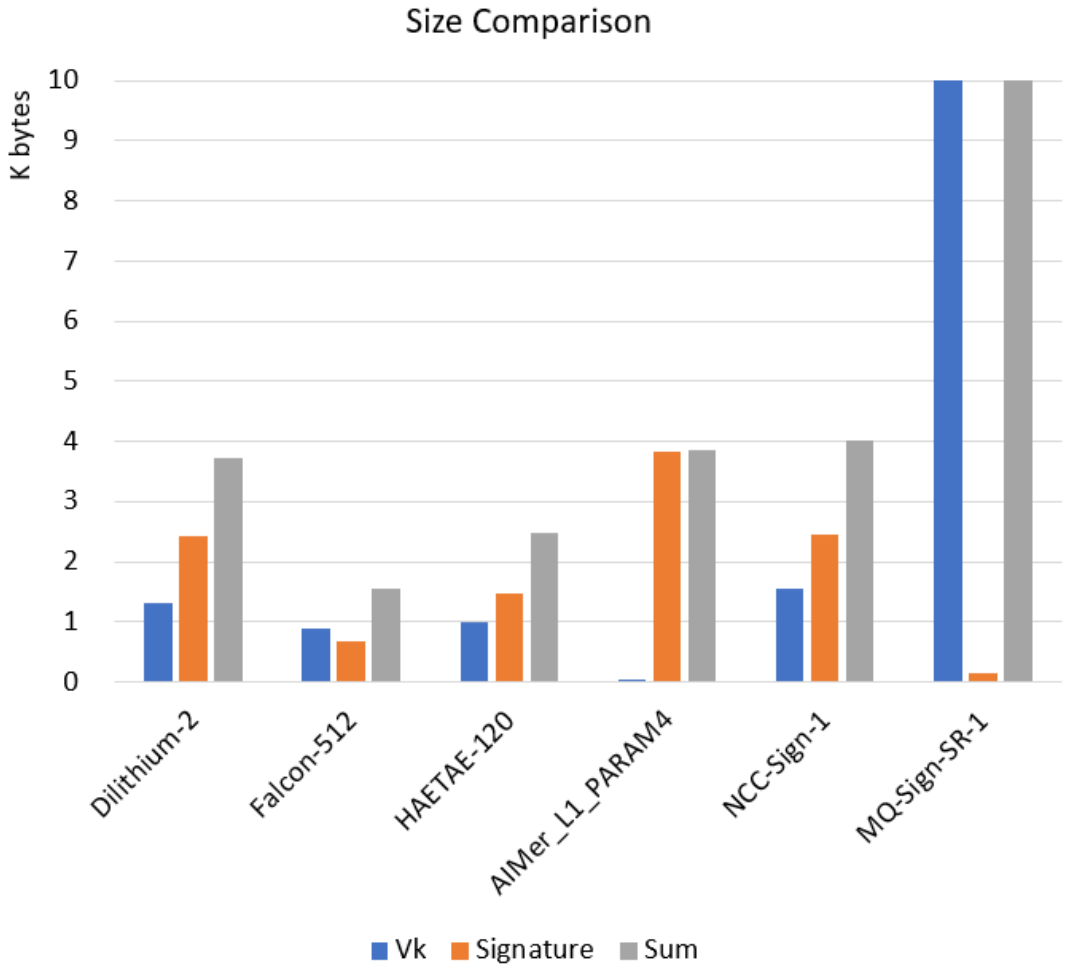


Figure: NIST standards and KpqC round 2 signatures

1. Brief Intro:
   - Introduction

2. Advantages:
   - Complete Quantum Security Analysis
   - Unique and Efficient Design
   - Small Sizes

3. HAETAE Update v3.0:
   - Updates

Introduction to HAETAE v3.0

HAETAE was updated last July!

- Private key size of SPEC. missing 32 bytes.
- Reduced B' (by 0.01) to satisfy Lemma 5.
  - Thanks to Nari Lee, Hansol Ryu, and Hochang Lee:
    - The previous B' did not satisfy Lemma 5 due to rounding error.
  - Negligible impact on the implementation/performance.
- Improved key generation procedure (40-60% reduced cycles)
  - Replace the 512-point FFT with a 256-point FFT.
  - No impact on security/sizes via equivalent equations.

Introduction to HAETAE v3.0

HAETAE was updated last July!

- Private key size of SPEC. missing 32 bytes.
- Reduced B' (by 0.01) to satisfy Lemma 5.
  - Thanks to Nari Lee, Hansol Ryu, and Hochang Lee:
    - The previous B' did not satisfy Lemma 5 due to rounding error.
  - Negligible impact on the implementation/performance.
- Improved key generation procedure (40-60% reduced cycles)
  - Replace the 512-point FFT with a 256-point FFT.
  - No impact on security/sizes via equivalent equations.

Introduction to HAETAE v3.0

HAETAE was updated last July!

- Private key size of SPEC. missing 32 bytes.
- Reduced B' (by 0.01) to satisfy Lemma 5.
  - Thanks to Nari Lee, Hansol Ryu, and Hochang Lee:
    - The previous B' did not satisfy Lemma 5 due to rounding error.
  - Negligible impact on the implementation/performance.
- Improved key generation procedure (40-60% reduced cycles)
  - Replace the 512-point FFT with a 256-point FFT.
  - No impact on security/sizes via equivalent equations.

Thank You!

HAETAE will be presented at CHES 2024, Halifax, Canada!

https://doi.org/10.46586/tches.v2024.i3.25-75

References I

[BBRS24] Henry Bambury, Hugo Beguinet, Thomas Ricosset, and Eric Sageloli.
Polytopes in the fiat-shamir with aborts paradigm.
Cryptology ePrint Archive, Paper 2024/411, 2024.

[BG14] Shi Bai and Steven D Galbraith.
An improved compression technique for signatures based on learning with errors.
In Cryptographers' Track at the RSA Conference, pages 28–47. Springer, 2014.

[DDLL13] Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky.
Lattice signatures and bimodal gaussians.
In Annual Cryptology Conference, pages 40–56. Springer, 2013.

[DFPS22] Julien Devevey, Omar Fawzi, Alain Passelègue, and Damien Stehlé.
On rejection sampling in lyubashevsky's signature scheme.
Cryptology ePrint Archive, Number 2022/1249, 2022.
To be appeared in Asiacrypt, 2022. https://eprint.iacr.org/2022/1249.

References II

[DFPS23] Julien Devevey, Pouria Fallahpour, Alain Passelègue, and Damien Stehlé.

A detailed analysis of fiat-shamir with aborts.

In Helena Handschuh and Anna Lysyanskaya, editors, CRYPTO 2023, Part V, volume 14085 of LNCS, pages 327–357. Springer, Heidelberg, August 2023.

[DKL+18] Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé.

Crystals-dilithium: A lattice-based digital signature scheme.

IACR Transactions on Cryptographic Hardware and Embedded Systems, pages 238–268, 2018.

[Duc14] Léo Ducas.

Accelerating bliss: the geometry of ternary polynomials.

Cryptology ePrint Archive, Paper 2014/874, 2014.

https://eprint.iacr.org/2014/874.

References III

[GHHM21] Alex B. Grilo, Kathrin Hövelmanns, Andreas Hülsing, and Christian Majenz.

Tight adaptive reprogramming in the QROM.

In Mehdi Tibouchi and Huaxiong Wang, editors, ASIACRYPT 2021, Part I, volume 13090 of LNCS, pages 637–667. Springer, Heidelberg, December 2021.

[GLP12] Tim Güneysu, Vadim Lyubashevsky, and Thomas Pöppelmann.

Practical lattice-based cryptography: A signature scheme for embedded systems.

In International Workshop on Cryptographic Hardware and Embedded Systems, pages 530–547. Springer, 2012.

[KLS18] Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner.

A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model.

In Jesper Buus Nielsen and Vincent Rijmen, editors, EUROCRYPT 2018, Part III, volume 10822 of LNCS, pages 552–586. Springer, Heidelberg, April / May 2018.

[Lyu09] Vadim Lyubashevsky.

Fiat-shamir with aborts: Applications to lattice and factoring-based signatures.

In International Conference on the Theory and Application of Cryptology and Information Security, pages 598–616. Springer, 2009.

References IV

[Lyu12] Vadim Lyubashevsky.

Lattice signatures without trapdoors.

In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 738–755. Springer, 2012.