HAETAE: Rejecting on Hyperballs

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

[1]Seoul National University, [2]CryptoLab Inc.,
[3]École Normale Supérieure de Lyon, [4]Ruhr Universität Bochum,

KIAS-JBNU KpqC Workshop
May 18-19, 2023

Table of Contents

1. Brief Introduction to HAETAE:
   - Recap and summarizing HAETAE
   - “Fiat-Shamir with Aborts” paradigm

2. Rejection Sampling:
   - What is “Rejection Sampling?”
   - Rejection sampling in FS signatures
   - Rejection sampling in HAETAE

3. HAETAE updates:
   - Updates and current status

HAETAE

- Digital signature scheme, submitted to KpqC competition.
- Secure against quantum attacks
  - based on **lattice hard problems**, MLWE and MSIS
  - follows **Fiat-Shamir with aborts** framework, secure in QROM
- Goal:

Push Fiat-Shamir Signatures to the Limits!

Scheme	Lvl.	Sig.	vk	Const.-T.	Maskable
Falcon-512	1	666B	897B	✓ [Por19]	✗ [Pre23]
Dilithium-2	2	2,420B	1,312B	✓ [DKL+18a]	✓ [MGTF19]
HAETAE-120	2	1,463B	992B	✓	✓

Table: NIST security level, signature size, verification key size, and implementation security, with respect to constant-time and masking of selected signature schemes.

HAETAE

- Simple but short
  - simpler than Falcon[1] & shorter than Dilithium[1]
  - optimal rejection rate with simple rejection condition
- Design rationale: We combine the recent approaches,
  - **Fiat-Shamir with Aborts** framework
  - **Bimodal** rejection sampling
  - randomness sampling from **Hyperball** distribution

  with the NEW techniques,
  - secret key rejection sampling: efficient and easily maskable
  - verification key truncation: in bimodal setting
  - signature compression: in hyperball setting
  - discretized hyperball sampling: a fixed-point implementation

[1] NIST 2022 PQC signature standards

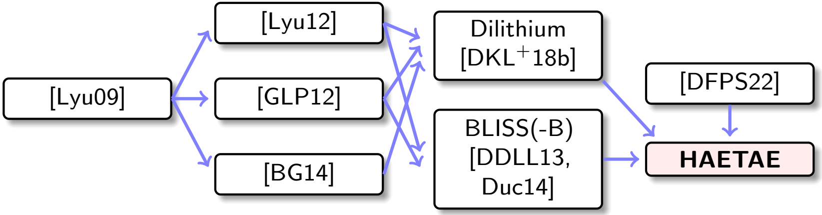
1. Brief Introduction to HAETAE:
   - Recap and summarizing HAETAE
   - “Fiat-Shamir with Aborts” paradigm

2. Rejection Sampling:
   - What is “Rejection Sampling?”
   - Rejection sampling in FS signatures
   - Rejection sampling in HAETAE

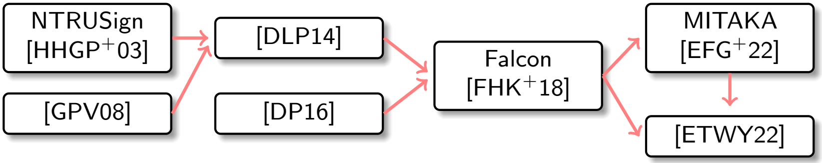
3. HAETAE updates:
   - Updates and current status

Lattice-based signatures

Fiat-Shamir with Aborts



Hash-and-Sign



Fiat-Shamir with Aborts

From an interactive identification protocol, FS transform provides a non-interactive ID protocol, say signature. E.g. Schnorr ID protocol $\xrightarrow{FS}$ Schnorr signature.

Basic "Fiat-Shamir with aborts" framework [Lyu09, Lyu12]

KeyGen : output $(\mathsf{sk} = \mathbf{s},\ \mathsf{vk} = \mathbf{A})$, where $\mathbf{t} = \mathbf{A}\mathbf{s} \bmod q$ and $\mathbf{s}$ is short.

Sign$(\mathsf{sk} = \mathbf{s},\ m)$: for short $\mathbf{y}$, compute $c = H(\mathbf{A}\mathbf{y} \bmod q,\ m)$ and $\mathbf{z} = \mathbf{y} + c\mathbf{s}$, then output $(c,\ \mathbf{z})$ via rejection sampling.

Verify$(\mathsf{vk} = \mathbf{A},\ m)$: check $c = H(\mathbf{A}\mathbf{z} - c\mathbf{t} \bmod q, m)$ and $\mathbf{z}$ is short.

Correctness:

- First, $\mathbf{y}$ and $\mathbf{s}$ are short. Since $c = H(\cdot)$ is binary, $c\mathbf{s}$ is also short. Thus, $\mathbf{z} = \mathbf{y} + c\mathbf{s}$ is short.
- It holds that $\mathbf{A}\mathbf{z} - c\mathbf{t} = \mathbf{A}(\mathbf{y} + c\mathbf{s}) - c\mathbf{t} = \mathbf{A}\mathbf{y} \bmod q$ since $\mathbf{A}\mathbf{s} = \mathbf{t} \bmod q$.

Fiat-Shamir with Aborts

Basic “Fiat-Shamir with aborts” framework [Lyu09, Lyu12]

Sign($\mathsf{sk} = \mathbf{s},\ m$) : for short $\mathbf{y}$, compute $c = H(\mathbf{A}\mathbf{y} \bmod q,\ m)$ and $\mathbf{z} = \mathbf{y} + c\mathbf{s}$, then output $(c,\ \mathbf{z})$ via rejection sampling.

Security:

- In the interactive setting, the signature $\mathbf{z} = \mathbf{y} + c\mathbf{s}$ can leak information about $\mathbf{s}$ if $\|\mathbf{y}\|$ is small. To avoid this, the noise flooding technique is generally used: setting $\|\mathbf{y}\| \approx 2^B \cdot \|c\mathbf{s}\|$ for B bit security.
- But using noise flooding makes the signature sizes much larger.
- “Aborting”, or “rejection sampling”, makes it possible to have a signature distribution independent of the secret, during the FS transforms.

1. Brief Introduction to HAETAE:
   - Recap and summarizing HAETAE
   - “Fiat-Shamir with Aborts” paradigm

2. Rejection Sampling:
   - What is “Rejection Sampling?”
   - Rejection sampling in FS signatures
   - Rejection sampling in HAETAE

3. HAETAE updates:
   - Updates and current status

Rejection sampling

- Rejection sampling is a widely studied and used, *folklore* technique from probabilities[2].
- In general, the signing procedure is given as:
  1. $\mathbf{y} \leftarrow Q_0$
  2. $c \leftarrow H(\mathbf{A}\mathbf{y}, m)$
  3. $\mathbf{z} \leftarrow \mathbf{y} + c\mathbf{s}$
  4. with probability $\min\left(1, \frac{P(c,\mathbf{z})}{M \cdot Q(c,\mathbf{z})}\right)$, return $\sigma = (c, \mathbf{z})$
  5. if it is not returned, go to step 1

  where Q is the probability distribution of $(c, \mathbf{z})$.
- Assuming $R_\infty(P\|Q) \leq M$ for some $M > 0$, the distribution of the signature in step 3 ($\sigma \sim Q$), turns into a distribution independent of $\mathbf{s}$ ($\sigma \sim P$).

[2] Julein Devevey, On Rejection Sampling in Lyubashevsky's Signature Scheme, Journées Codage et Cryptographie — Hendaye, 2022.

Rejection sampling: detailed analysis

Rejection sampling strategy can be rewritten as:

Given access to $X_1, X_2, \cdots \xleftarrow{i.i.d.} Q$, it is a family of randomized algorithms

$$\mathcal{A}_i : \mathsf{supp}(Q)^i \to [i] \cup \{\perp\},$$

finding the smallest i^* such that X_{i^*} is distributed following P, by defining

$$\mathcal{A}_i : (X_1, \cdots, X_i) \mapsto \begin{cases} i \text{ with prob. } \frac{P(X_i)}{R_\infty(P\|Q)\cdot Q(X_i)}, \\ \perp \text{ otherwise,} \end{cases}$$

from $i = 1, \cdots$, which ends if $\mathcal{A}_i \to i (= i^*)$, then finally outputs X_{i^*}.

Cf. Short recap on Rényi divergence: [3]for $\mathsf{supp}(P) \subseteq \mathsf{supp}(Q)$,

$$R_\infty(P\|Q) := \sup_{x \in \mathsf{supp}(P)} P(x)/Q(x).$$

[3] We can also consider $\mathsf{supp}(P) \not\subseteq \mathsf{supp}(Q)$, say smooth Rényi, but not here.

Rejection sampling: detailed analysis

- Running time: the expected run-time is $\mathbb{E}[i^*]$ since it ends when $\mathcal{A}_i$ outputs i. A quick computation shows $\mathbb{E}[i^*] = R_\infty(P\|Q)$:

$$\Pr[\mathcal{A}_i \to i] = \sum_{x_i} Q(x_i) \cdot \frac{P(x_i)}{R_\infty(P\|Q)\cdot Q(x_i)} = R_\infty(P\|Q)^{-1} (\text{let}, \ = p),$$

$$\begin{aligned} \mathbb{E}[i^*] &= \sum_{i\geq 1} i \cdot \Pr[i^* = i] \\ &= \sum_{i\geq 1} i \cdot \Pr[(\mathcal{A}_1, \cdots, \mathcal{A}_{i-1} \to \perp) \wedge (\mathcal{A}_i \to i)] \\ &= \sum_{i\geq 1} i \cdot p \cdot (1-p)^{i-1} = p^{-1} = R_\infty(P\|Q). \end{aligned}$$

- Distribution of final output X_{i^*}: the probability density function of the final output becomes P:

$$\begin{aligned} \text{pdf}[X_{i^*} = x] &= \sum_{i\geq 1} \Pr[\mathcal{A}_1, \cdots, \mathcal{A}_{i-1} \to \perp] \cdot \Pr[(\mathcal{A}_i \to i) \wedge (X_i = x)] \\ &= \sum_{i\geq 1} (1-p)^{i-1} \cdot Q(x) \cdot \frac{P(x)}{R_\infty(P\|Q)\cdot Q(x)} \\ &= P(x) \cdot \sum_{i\geq 1} p(1-p)^{i-1} = P(x). \end{aligned}$$

Rejection sampling: detailed analysis

So far, the transcripts (the final output) and the run-time (the number of iterations) of the rejection sampling strategy and that of the following algorithm are indistinguishable:

> Given access to $X \leftarrow P$, it samples $X \leftarrow P$, and outputs X with probability $R_\infty(P\|Q)^{-1}$, else re-sample it and repeat.

- run-time: $R_\infty(P\|Q)$,
- final output: $X \leftarrow P$.

Three simple facts:

- the same thing holds in the continuous domain,
- the Rényi divergence in the denominator can be replaced by $M > 0$ such that $R_\infty(P\|Q) \leq M$,
- more analysis is needed if we set a bound on i^*, say **bounded rejection**.

Rejection sampling: detailed analysis

Hence, if $R_\infty(P\|Q) \le M < \infty$, the following two games are indistinguishable:

$\mathcal{A}^{\text{real}}$:	$\mathcal{A}^{\text{ideal}}$:
1: $\mathbf{x} \leftarrow Q$	1: $\mathbf{x} \leftarrow P$
2: Return $\mathbf{x}$ with probability $\frac{P(\mathbf{x})}{M \cdot Q(\mathbf{x})}$	2: Return $\mathbf{x}$ with probability $\frac{1}{M}$
3: Else repeat 1–2	3: Else repeat 1–2

Imperfect rejection:

- Similar thing holds also for $M \approx R_\infty(P\|Q)$ or for smooth-Rényi divergence, i.e., when supp$(P) \nsubseteq$ supp(Q), with some statistical distance between the outputs.
- Since the fraction could have a value larger than 1, it should be replaced by $\min\left(\frac{P(\mathbf{x})}{M \cdot Q(\mathbf{x})}, 1\right)$.

Cf. HAETAE uses the **perfect, unbounded rejection**.

1. Brief Introduction to HAETAE:
   - Recap and summarizing HAETAE
   - "Fiat-Shamir with Aborts" paradigm

2. Rejection Sampling:
   - What is "Rejection Sampling?"
   - Rejection sampling in FS signatures
   - Rejection sampling in HAETAE

3. HAETAE updates:
   - Updates and current status

Rejection sampling in FS signatures

- The **FS signatures** are commonly given as follows:
  1. $\mathbf{y} \leftarrow Q_0$
  2. $c \leftarrow H(\mathbf{Ay}, m)$
  3. $\mathbf{z} \leftarrow \mathbf{y} + c\mathbf{s}$
  4. with probability $\min\left(1, \frac{P(c,\mathbf{z})}{M \cdot Q(c,\mathbf{z})}\right)$, return $\sigma = (c, \mathbf{z})$, else go to step 1
- The **ideal** signing can be given as:
  1. $c \leftarrow U(\mathcal{C})$
  2. $\mathbf{z} \leftarrow P^z$
  3. with probability $1/M$, return $(c, \mathbf{z})$, else go to step 1
- In the simulation-based proofs, the hash can be reprogrammed, and the challenge sampling can be treated as $c \leftarrow U(\mathcal{C})$.
- Then, it can be seen as $Q = Q_{c\mathbf{s}} \otimes U(\mathcal{C})$ and $P = P^z \otimes U(\mathcal{C})$.
- Then, the **real** and **ideal** signing algorithms are indistinguishable.

Rejection sampling in FS signatures

- The **FS signatures** are commonly given as follows:
  1. $\mathbf{y} \leftarrow Q_0$
  2. $c \leftarrow H(\mathbf{Ay}, m)$
  3. $\mathbf{z} \leftarrow \mathbf{y} + c\mathbf{s}$
  4. with probability $\min\left(1, \frac{P(c,\mathbf{z})}{M \cdot Q(c,\mathbf{z})}\right)$, return $\sigma = (c, \mathbf{z})$, else go to step 1
- The **ideal** signing can be given as:
  1. $c \leftarrow U(\mathcal{C})$
  2. $\mathbf{z} \leftarrow P^z$
  3. with probability $1/M$, return $(c, \mathbf{z})$, else go to step 1

Remark 1. The aborted transcripts can even be simulated [DFPS23].

Remark 2. The rewinding and reprogramming can not be directly treated in the QROM (see [KLS18, GHHM21, DFPS23]).

Rejection sampling in FS signatures

One important thing in practice is accepting a signature with probability $\frac{P(c,\mathbf{z})}{M\cdot Q(c,\mathbf{z})} = \frac{P^z(\mathbf{z})}{M\cdot Q_{c\mathbf{s}}(\mathbf{z})}$, which is also a challenging point.

- In [Lyu09] and Dilithium [DKL$^+$18b], the uniform distributions in hypercubes are used both for Q_0 and P^z, making it

$$\frac{P(c,\mathbf{z})}{M\cdot Q(c,\mathbf{z})} = \frac{\frac{1}{|I|^n}\cdot\chi(\mathbf{z}\in I^n)}{M\cdot\frac{1}{|J|^n}\cdot\chi(\mathbf{z}\in(J^n+c\mathbf{s}))} = \begin{cases} 1 & \text{if } \mathbf{z}\in I^n\cap(J^n+c\mathbf{s}) \\ 0 & \text{otherwise} \end{cases},$$

  where I and J are appropriate intervals, and χ is a characteristic function.

- In [Lyu12] and Bliss [DDLL13][4], the n-dimensional discrete Gaussian distributions are used. As a result, aborting the signature with Gaussian probability makes it hard to implement (See [EFGT17]).

[4] In fact, a bit different due to bimodal distribution

1. Brief Introduction to HAETAE:
   - Recap and summarizing HAETAE
   - “Fiat-Shamir with Aborts” paradigm

2. Rejection Sampling:
   - What is “Rejection Sampling?”
   - Rejection sampling in FS signatures
   - Rejection sampling in HAETAE

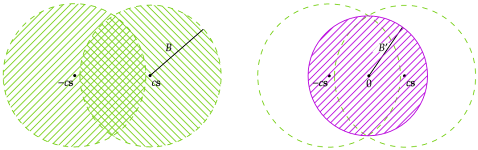
3. HAETAE updates:
   - Updates and current status

Hyperball bimodal rejection sampling

In HAETAE, we instead, use **uniform hyperball** distribution for sampling $\mathbf{y}$ following [DFPS22];

- $Q_{c\mathbf{s}}$ becomes a uniform distribution over a union of hyperballs with an intersection, $\mathcal{HB}_{-c\mathbf{s}}(B) \cup \mathcal{HB}_{c\mathbf{s}}(B)$,
- P becomes a hyperball uniform distribution, $\mathcal{HB}_{-c\mathbf{s}}(B')$,

as shown below.



Distribution of $Q_{c\mathbf{s}}$ and P.

Remark. The purple hyperball should be included in **every** $\mathcal{HB}_{-c\mathbf{s}}(B) \cup \mathcal{HB}_{c\mathbf{s}}(B)$ for the perfect rejection.

Hyperball bimodal rejection sampling

The use of hyperball distribution makes it possible

- to exploit optimal rejection rate, $\mathbb{E}[i^*]$,
- to reduce signature sizes, $\mathbb{E}[\|\mathbf{x}\|]$,

Figure: Distribution of P and Q

and use the **bimodal approach** [DDLL13];

- for more compact signature sizes,
- but with a simpler rejection condition, which leads to the easier implementation of secure rejection.

Hyperball bimodal rejection sampling: detailed analysis

The distributions can be expressed as follows:

- $Q_{c\mathbf{s}}(\mathbf{z}) = \frac{1}{2} \cdot \frac{1}{\mathsf{vol}(\mathcal{HB}(B))} \cdot \chi(\|\mathbf{z} - c\mathbf{s}\| < B) + \frac{1}{2} \cdot \frac{1}{\mathsf{vol}(\mathcal{HB}(B))} \cdot \chi(\|\mathbf{z} + c\mathbf{s}\| < B)$,
- $P(\mathbf{z}) = \frac{1}{\mathsf{vol}(\mathcal{HB}(B))} \cdot \chi(\|\mathbf{z}\| < B')$.

This leads to

$$\frac{P(\mathbf{z})}{M \cdot Q_{c\mathbf{s}}(\mathbf{z})} = \frac{\chi(\|\mathbf{z}\| < B')}{\chi(\|\mathbf{z} - c\mathbf{s}\| < B) + \chi(\|\mathbf{z} + c\mathbf{s}\| < B)}$$

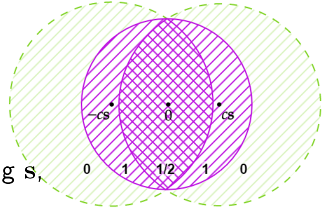
$$= \begin{cases} 0 & \text{if } \mathbf{z} \notin \mathcal{HB}(B'), \\ 1/2 & \text{if } \mathbf{z} \in \mathcal{HB}(B') \cap \mathcal{HB}_{c\mathbf{s}}(B) \cap \mathcal{HB}_{-c\mathbf{s}}(B), \\ 1 & \text{if } \mathbf{z} \in \mathcal{HB}(B') \setminus (\mathcal{HB}(B, c\mathbf{s}) \cap \mathcal{HB}(B, -c\mathbf{s})) \end{cases}$$

for some $M > 0$.

Hyperball bimodal rejection sampling

That is, we return $\mathbf{x} = (c, \mathbf{z})$ with probability

- 0: if $\|\mathbf{z}\| \geq B'$,
- 1/2: else if $\|\mathbf{z} - c\mathbf{s}\| < B$ and $\|\mathbf{z} + c\mathbf{s}\| < B$,
- 1: otherwise.



Since $\mathbf{z} = \mathbf{y} + (-1)^b c\mathbf{s}$, we can do this without using $\mathbf{s}$,

- if $\|\mathbf{z}\| \geq B'$, **reject**,
- else if $\|2\mathbf{z} - \mathbf{y}\| < B$,[5] **reject** with probability $1/2$,
- otherwise, **accept**,

resulting in a signature, distributed uniform in a hyperball $\mathcal{HB}(B')$.

[5] $\{\mathbf{z} \pm c\mathbf{s}\} = \{\mathbf{y}, 2\mathbf{z} - \mathbf{y}\}$ and always $\|\mathbf{y}\| < B$.

1. Brief Introduction to HAETAE:
   - Recap and summarizing HAETAE
   - “Fiat-Shamir with Aborts” paradigm
2. Rejection Sampling:
   - What is “Rejection Sampling?”
   - Rejection sampling in FS signatures
   - Rejection sampling in HAETAE
3. HAETAE updates:
   - Updates and current status

Updates

After submitting to KpqC Round 1, we had many further improvements, consisting of

- Missing parts inclusion:
  rANS encoding, rejection sampling for secret key sampling,
- New compressions:
  public key truncation and updated signature (especially the hint vector h) compression,
- New secret key rejection:
  security was underestimated due to a non-tight bound for $\|c\mathbf{s}\|$,
- Fully discretized hyperball:
  bound the statistical distance between 'continuous' and 'discretized' hyperballs and their effects on security,
- and some minor updates, adapted from Dilithium and others.

Considering the above changes, we update the parameters and implementation.

Updates

Implementation:

- **Fixed-Point** and **Constant-Time**[6],
- **Easily Maskable!**: detailed analysis is given in `ia.cr/2023/624`, and the masked implementation is ongoing,

Sizes and Performance:

		Sizes (bytes)		Cycles (med)		
Param. set	Lvl.	Sig.	vk	KeyGen	Sign	Verify
HAETAE-120/Dilithium-2	2	60%	76%	408%	548%	106%
HAETAE-180/Dilithium-3	3	71%	75%	383%	484%	123%
HAETAE-260/Dilithium-5	5	63%	80%	181%	363%	94%
Falcon-512/HAETAE-120	1/2	46%	90%	3,885%	277%	27%
Falcon-1024/HAETAE-260	5	44%	86%	9,110%	423%	25%

Table: Relative comparison between HAETAE, Dilithium, and Falcon using their constant-time reference implementation[7].

[6] available at HAETAE website: `kpqc.cryptolab.co.kr`.

[7] not yet optimized, yet ongoing with some basic optimizations.

Thanks!

Any question?

References I

[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.

[DFPS23] Julien Devevey, Pouria Fallahpour, Alain Passelègue, and Damien Stehlé.
A detailed analysis of fiat-shamir with aborts.
Cryptology ePrint Archive, Paper 2023/245, 2023.
https://eprint.iacr.org/2023/245.

[DKL+18a] Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé.
CRYSTALS-Dilithium: A lattice-based digital signature scheme.
IACR TCHES, 2018(1):238–268, 2018.
https://tches.iacr.org/index.php/TCHES/article/view/839.

[DKL+18b] 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.

[DLP14] Léo Ducas, Vadim Lyubashevsky, and Thomas Prest.
Efficient identity-based encryption over ntru lattices.
In International Conference on the Theory and Application of Cryptology and Information Security, pages 22–41. Springer, 2014.

References III

[DP16] Léo Ducas and Thomas Prest.
Fast fourier orthogonalization.
In Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation, pages 191–198, 2016.

[Duc14] Léo Ducas.
Accelerating bliss: the geometry of ternary polynomials.
Cryptology ePrint Archive, Paper 2014/874, 2014.
https://eprint.iacr.org/2014/874.

[EFG+22] Thomas Espitau, Pierre-Alain Fouque, François Gérard, Mélissa Rossi, Akira Takahashi, Mehdi Tibouchi, Alexandre Wallet, and Yang Yu.
Mitaka: A simpler, parallelizable, maskable variant of.
In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 222–253. Springer, 2022.

References IV

[EFGT17] Thomas Espitau, Pierre-Alain Fouque, Benoît Gérard, and Mehdi Tibouchi.

Side-channel attacks on BLISS lattice-based signatures: Exploiting branch tracing against strongSwan and electromagnetic emanations in microcontrollers.

In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, ACM CCS 2017, pages 1857–1874. ACM Press, October / November 2017.

[ETWY22] Thomas Espitau, Mehdi Tibouchi, Alexandre Wallet, and Yang Yu.

Shorter hash-and-sign lattice-based signatures.

In Yevgeniy Dodis and Thomas Shrimpton, editors, Advances in Cryptology – CRYPTO, 2022.

[FHK+18] Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang.

Falcon: Fast-fourier lattice-based compact signatures over ntru.

Submission to the NIST's post-quantum cryptography standardization process, 36(5), 2018.

References V

[GHHM21] Alex B. Grilo, Kathrin Hövelmanns, Andreas Hülsing, and Christian Majenz.
Tight adaptive reprogramming in the QROM.
In Mehdi Tibouchi and Huaxiong Wang, editors, Advances in Cryptology - ASIACRYPT, pages 637–667. Springer, 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.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan.
Trapdoors for hard lattices and new cryptographic constructions.
In Proceedings of the fortieth annual ACM symposium on Theory of computing, pages 197–206, 2008.

[HHGP+03] Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H Silverman, and William Whyte.
Ntrusign: Digital signatures using the ntru lattice.
In Cryptographers' track at the RSA conference, pages 122–140. Springer, 2003.

References VI

[KLS18] Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner.
A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model.
In Advances in Cryptology – EUROCRYPT, pages 552–586. Springer, 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.

[Lyu12] Vadim Lyubashevsky.
Lattice signatures without trapdoors.
In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 738–755. Springer, 2012.

[MGTF19] Vincent Migliore, Benoît Gérard, Mehdi Tibouchi, and Pierre-Alain Fouque.
Masking Dilithium - efficient implementation and side-channel evaluation.
In Robert H. Deng, Valérie Gauthier-Umaña, Martín Ochoa, and Moti Yung, editors, ACNS 19, volume 11464 of LNCS, pages 344–362. Springer, Heidelberg, June 2019.

References VII

[Por19] Thomas Pornin.
New efficient, constant-time implementations of falcon.
Cryptology ePrint Archive, Paper 2019/893, 2019.

[Pre23] Thomas Prest.
A key-recovery attack against mitaka in the t-probing model.
Cryptology ePrint Archive, Report 2023/157, 2023.
https://eprint.iacr.org/2023/157.