HAETAE: Shorter Lattice-based Fiat-Shamir Signatures

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

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

https://ia.cr/2023/624

Sungshin Women's University
May 21, 2024

HAETAE
HEAAN
CRYPTO LAB

Table of Contents

1. Digital Signatures:
   - What is a digital signature?
   - Lattice-based digital signatures
   - Rejection sampling

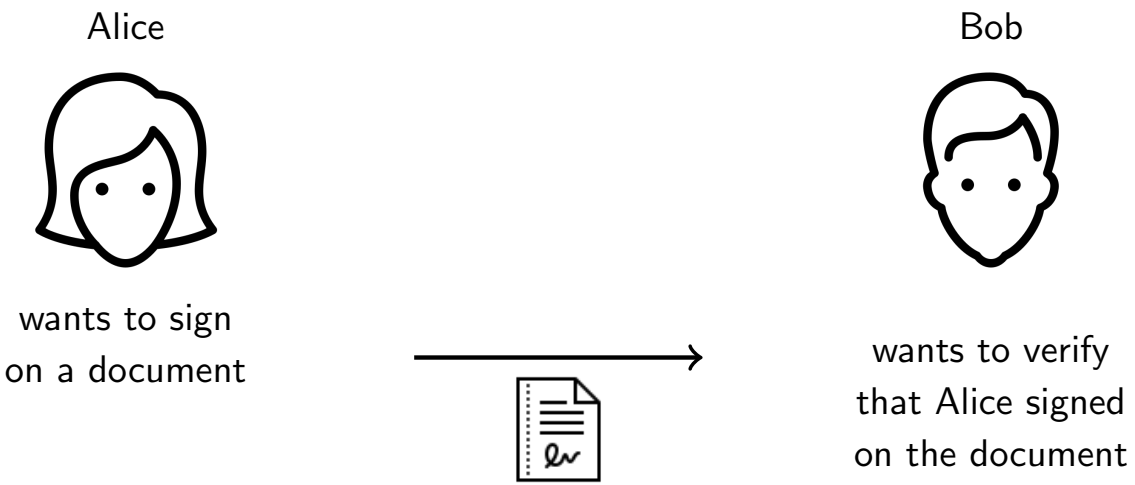
2. HAETAE:
   - Hyperball bimodal rejection sampling
   - Parameter choices
   - Comparison to SotA lattice signatures
   - Current status

1. Digital Signatures:
   - What is a digital signature?
   - Lattice-based digital signatures
   - Rejection sampling

2. HAETAE:
   - Hyperball bimodal rejection sampling
   - Parameter choices
   - Comparison to SotA lattice signatures
   - Current status

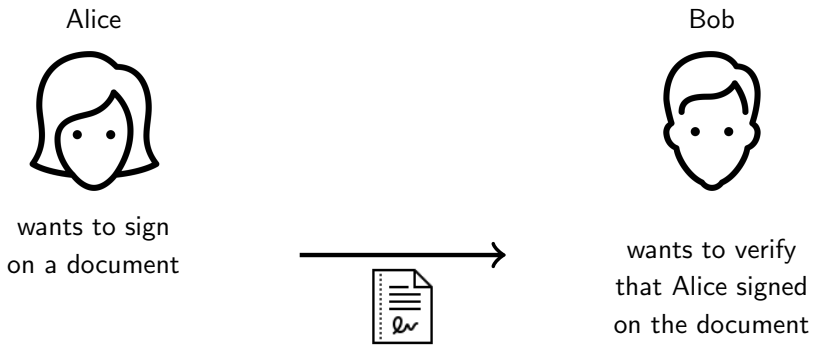
Digital signatures

Conventional signatures work as:



Digital signatures

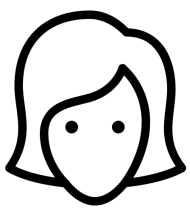
Conventional signatures work as:



Digital signatures work as:

$(\mathsf{sk}, \mathsf{vk}) \leftarrow$ KeyGen and broadcast vk

Alice (knows sk)



signature $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, m)$

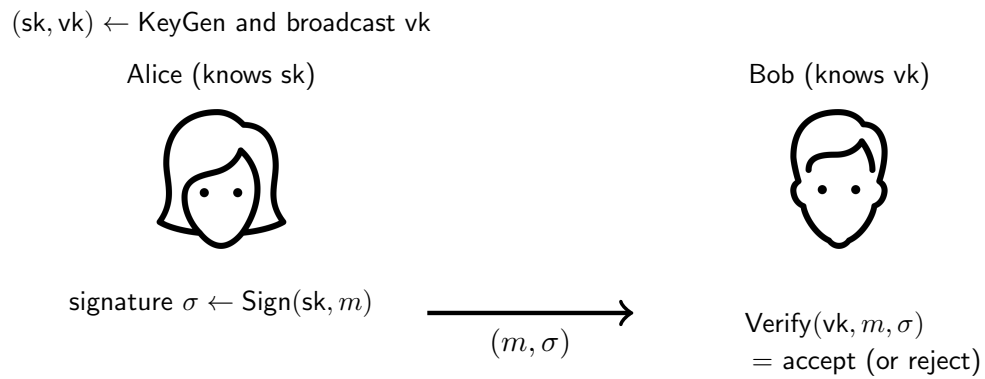
(m, σ)

Bob (knows vk)

$\mathsf{Verify}(\mathsf{vk}, m, \sigma)$
$=$ accept (or reject)

Digital signatures

Digital signatures work as:



- **Correctness**: Verify(vk, m, Sign(sk, m)) = accept
- **Unforgeability**: Only Alice can make a new valid signature. More formally,

  for given vk *and valid message-signature pairs* $\{(m_i, \sigma_i)\}_i$*, no adversary can forge a new valid signature* σ *for some message* m*.*

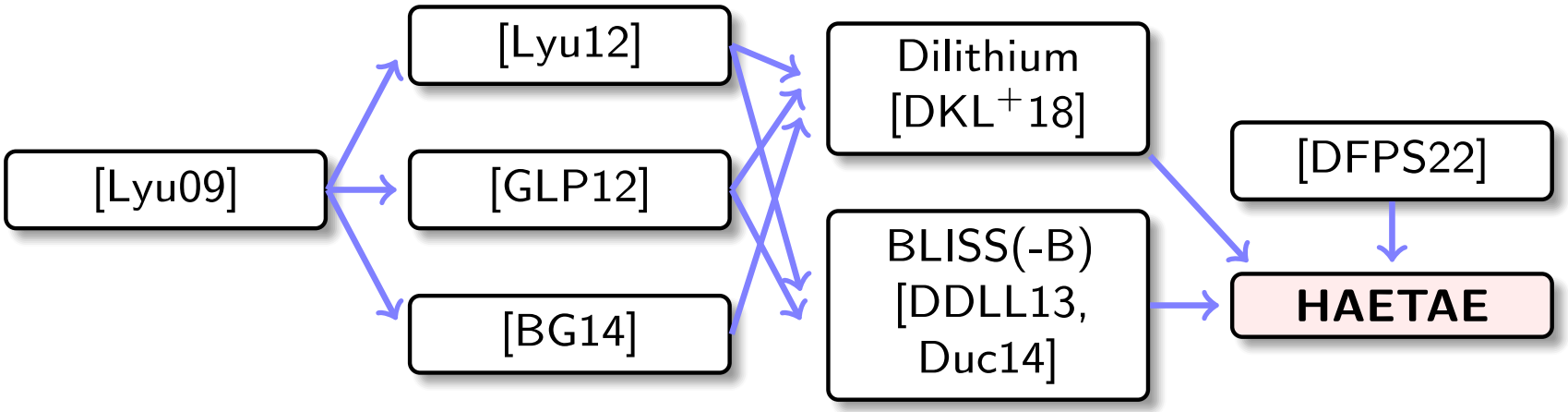
vk and $\{(m_i, \sigma_i)\}_i$ ⟶  ⟶̸ new m and σ

1. Digital Signatures:
   - What is a digital signature?
   - Lattice-based digital signatures
   - Rejection sampling

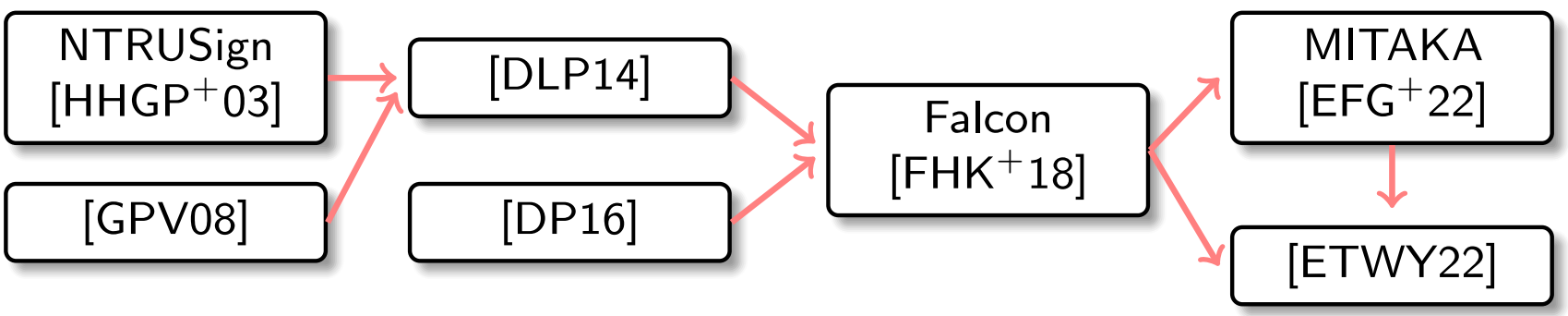
2. HAETAE:
   - Hyperball bimodal rejection sampling
   - Parameter choices
   - Comparison to SotA lattice signatures
   - Current status

Lattice-based signatures

Fiat-Shamir with abort



Hash-and-Sign



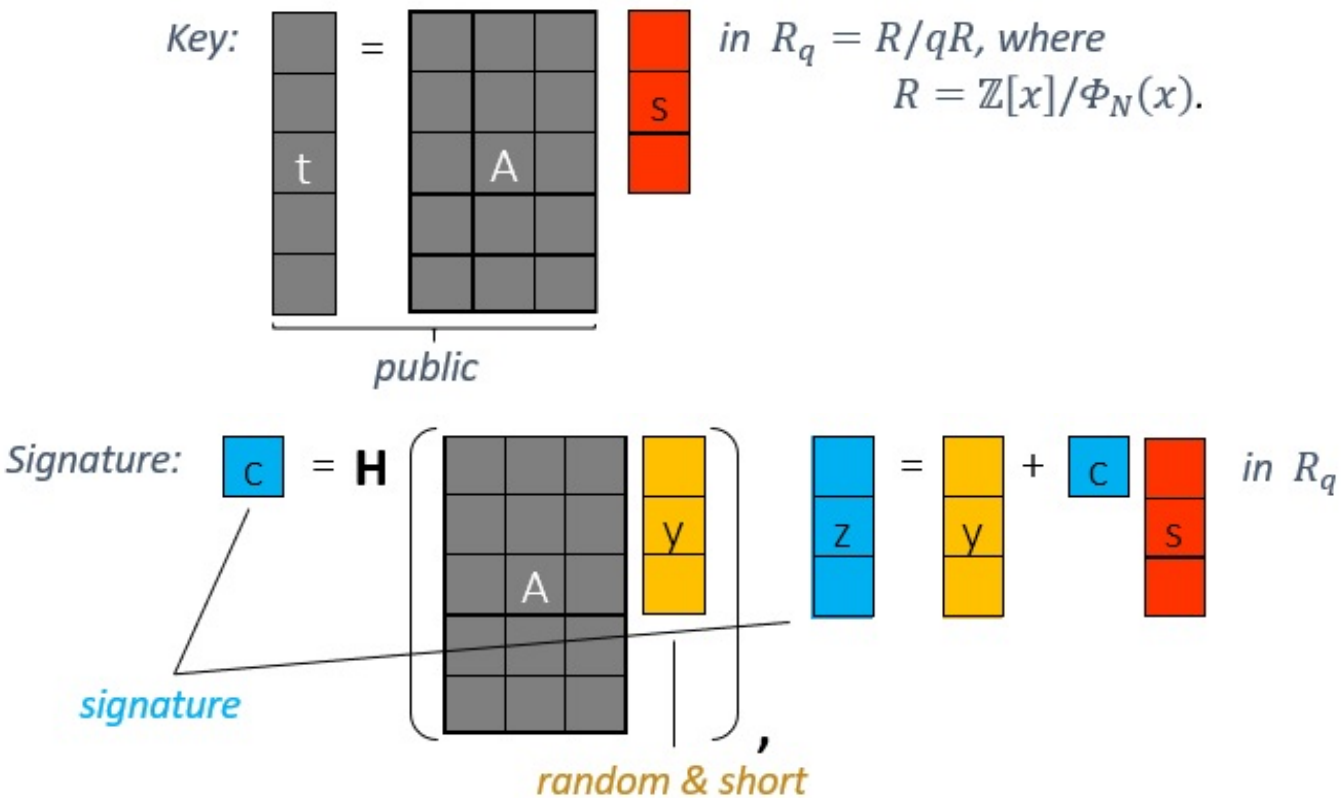
Lattice-based signatures

Fiat-Shamir with Aborts (FSwA):

Key: (secret key: 'short' $\mathbf{s}$, public key: $\mathbf{t} = \mathbf{A}\mathbf{s} \bmod q$)

Sign: $\sigma = (c = H(\mathbf{A}\mathbf{y} \bmod q,\ m),\ \mathbf{z} = \mathbf{y} + c\mathbf{s})$ for short $\mathbf{y}$, with rejection sampling

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



Lattice-based signatures

Fiat-Shamir with abort:

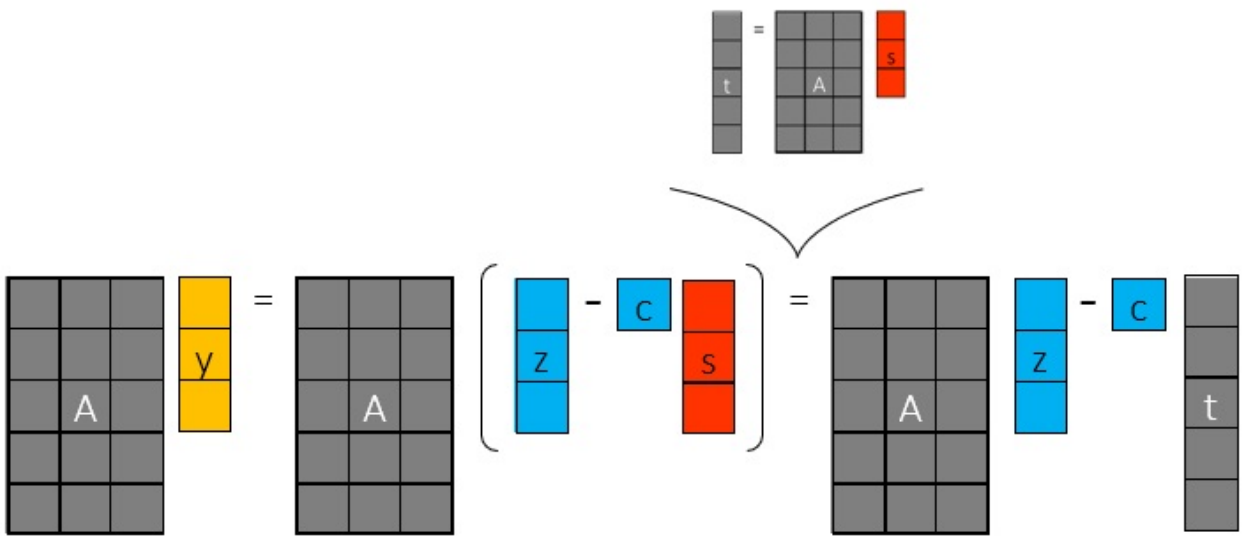
Key: (secret key: 'short' $\mathbf{s}$, public key: $\mathbf{t} = \mathbf{A}\mathbf{s} \bmod q$)

Sign: $(c = H(\mathbf{A}\mathbf{y} \bmod q,\ m),\ \mathbf{z} = \mathbf{y} + c\mathbf{s})$ for short $\mathbf{y}$, with rejection sampling

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

Correctness of FSwA:

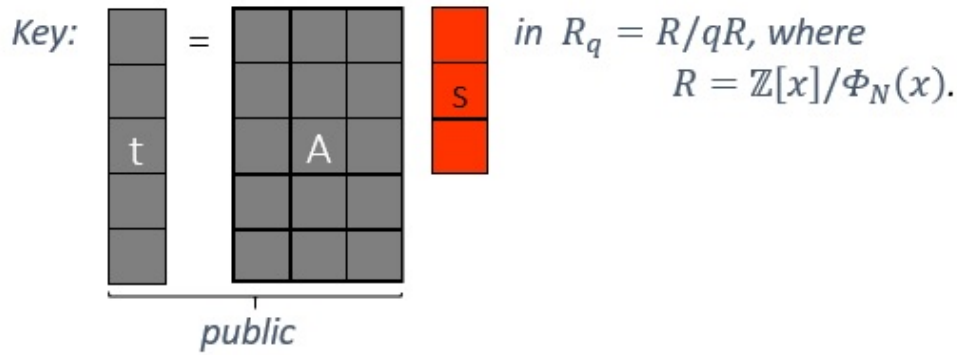
- $\mathbf{y}$, $\mathbf{s}$: short, and $c = H(\cdot)$: binary hash value $\Rightarrow c\mathbf{s}$: short.
  $\Rightarrow \mathbf{z} = \mathbf{y} + c\mathbf{s}$: short.
- $\mathbf{A}\mathbf{y} = \mathbf{A}(\mathbf{z} - c\mathbf{s}) = \mathbf{A}\mathbf{z} - c\mathbf{A}\mathbf{s} = \mathbf{A}\mathbf{z} - c\mathbf{t} \bmod q$.



Lattice-based signatures

Unforgeability of FSwA:

- **Public key** does not leak secret $\Leftarrow$ Module-SIS: it is hard to find a short vector $\mathbf{s}$ satisfying $\mathbf{As} = \mathbf{t} \mod q$.[1]



- **Signature** $(c, \mathbf{z})$ does not leak secret $\Leftarrow$ rejection sampling,
- **No new signatures** can be sampled **without** $\mathbf{s}$ $\Leftarrow$ Module-SIS (assuming ROM and rewinding...): it is hard to find short $\mathbf{z}_1 \neq \mathbf{z}_2$ satisfying $\mathbf{A}(\mathbf{z}_1 - \mathbf{z}_2) = 0 \mod q$.

[1] Both HAETAE and Dilithium use MLWE instead of MSIS.

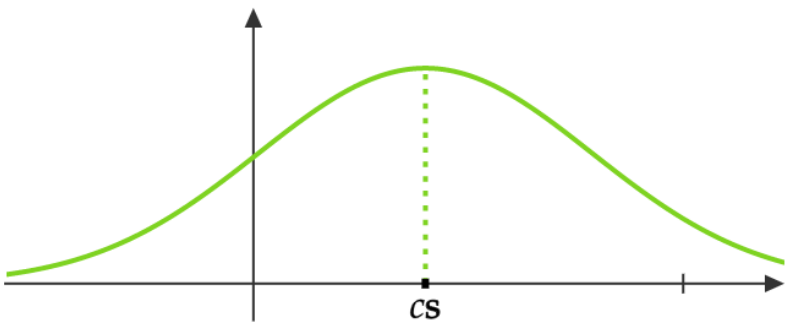
1. Digital Signatures:
   - What is a digital signature?
   - Lattice-based digital signatures
   - Rejection sampling

2. HAETAE:
   - Hyperball bimodal rejection sampling
   - Parameter choices
   - Comparison to SotA lattice signatures
   - Current status

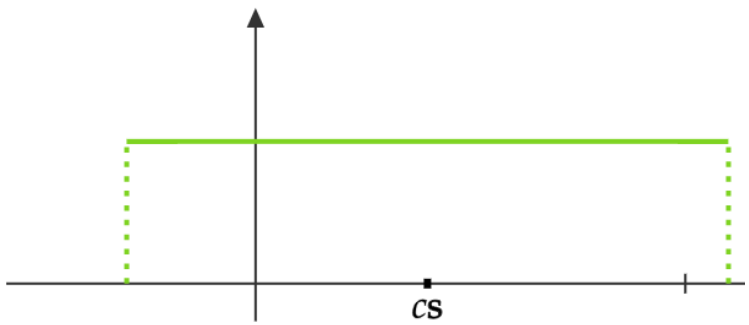
Rejection sampling

Leakage from $(c, \mathbf{z} = \mathbf{y} + c\mathbf{s})$?

With ∞ pairs of $(c, \mathbf{z} = \mathbf{y} + c\mathbf{s})$, we can collect $\mathbf{z}$ for the same c:



$y \leftarrow \mathcal{N}(0, \sigma^2)$



$y \leftarrow U[-a, a]$

$\Rightarrow$ Recover $\mathbf{s}$ from $c\mathbf{s}$.

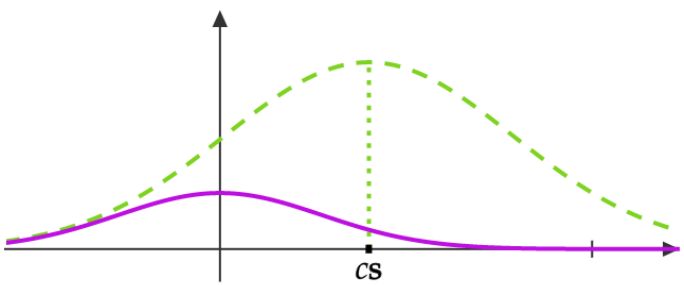
Rejection sampling

Rejection sampling

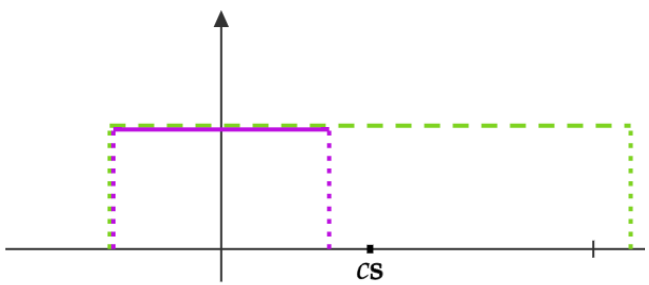
$D_{\text{source}} = \{(c, \mathbf{z})\}$ $\xrightarrow[\text{prob. } p(c,\mathbf{z})]{\text{reject with}}$ D_{target}

distribution of $(c, \mathbf{z})$, possibly leak $\mathbf{s}$

new distribution, independent of $\mathbf{s}$



$y \leftarrow \mathcal{N}(0, \sigma^2)$



$y \leftarrow U[-a, a]$

Rejection sampling

The **FSwA signatures** are generated as follows:

1. $\mathbf{y} \leftarrow D_0$
2. $c \leftarrow H(\mathbf{A}\mathbf{y} \bmod q, m)$
3. $\mathbf{z} \leftarrow \mathbf{y} + c\mathbf{s}$
4. with probability $\frac{p_{\text{target}}(c,\mathbf{z})}{M \cdot p_{\text{source}}(c,\mathbf{z})}$, return $\sigma = (c, \mathbf{z})$, else go to step 1

M: bounding factor for the probability to be ≤ 1.

Final distribution $\sim D_{\text{target}}$.

Run-time $\propto M$.

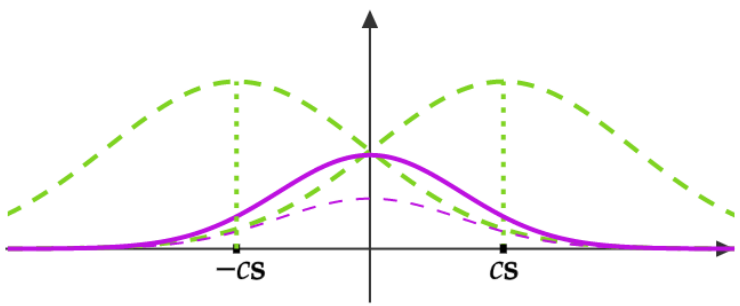
Bimodal rejection sampling

Run-time $\propto M$ ($\approx$ green area / purple area).

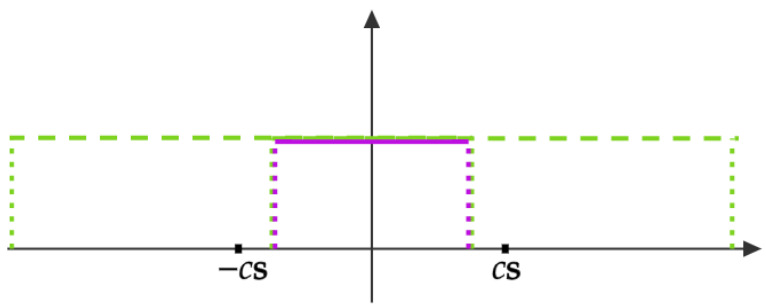
To decrease M, [DDLL13] uses

$$\mathbf{z} = \mathbf{y} + (-1)^b c\mathbf{s} \bmod 2q$$

instead of $\mathbf{z} = \mathbf{y} + c\mathbf{s} \bmod q$:



$y \leftarrow \mathcal{N}(0, \sigma^2)$



$y \leftarrow U[-a, a]$

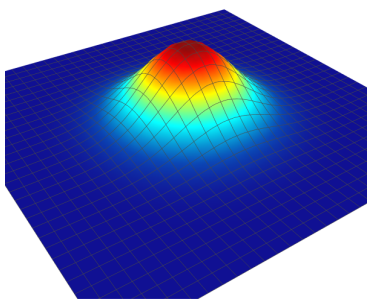
Note, no change for the uniform case.

1. Digital Signatures:
   - What is a digital signature?
   - Lattice-based digital signatures
   - Rejection sampling

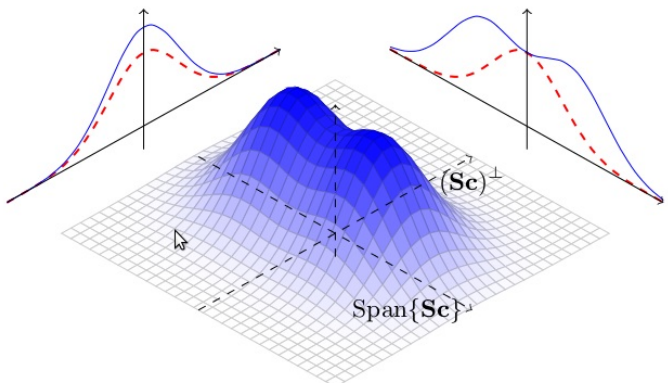
2. HAETAE:
   - Hyperball bimodal rejection sampling
   - Parameter choices
   - Comparison to SotA lattice signatures
   - Current status

Hyperball bimodal rejection sampling

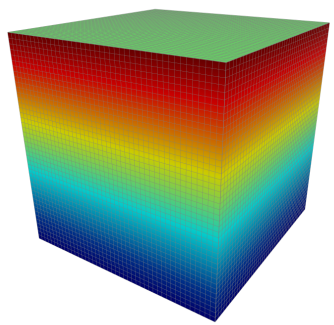
Previously, the randomness $\mathbf{y}$ was chosen from either discrete Gaussian (or its bimodal version) or uniform hypercube.[2]



[Lyu12]



[DDLL13]



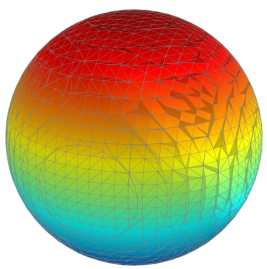
[Lyu09], Dilithium

[2] The vectors $\mathbf{y}$ and $\mathbf{z}$ are high-dimensional vectors, so uniform in an interval is indeed a uniform hypercube.

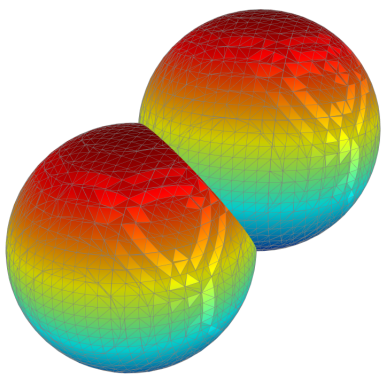
Hyperball bimodal rejection sampling

HAETAE uses **uniform hyperball** distribution for sampling $\mathbf{y}$ [DFPS22], based on the **bimodal approach** [DDLL13],

- to exploit optimal M, which reduces signature and verification key sizes.



unimodal hyperball

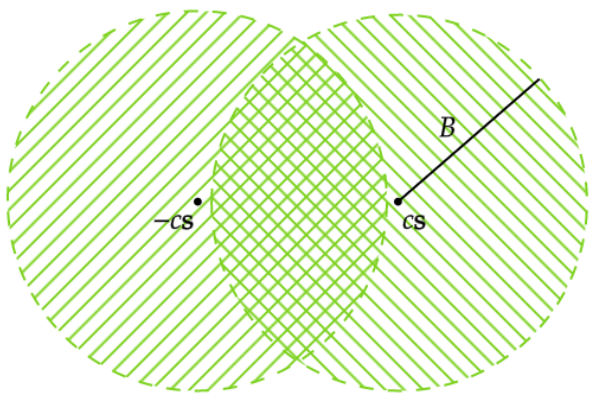


bimodal hyperball

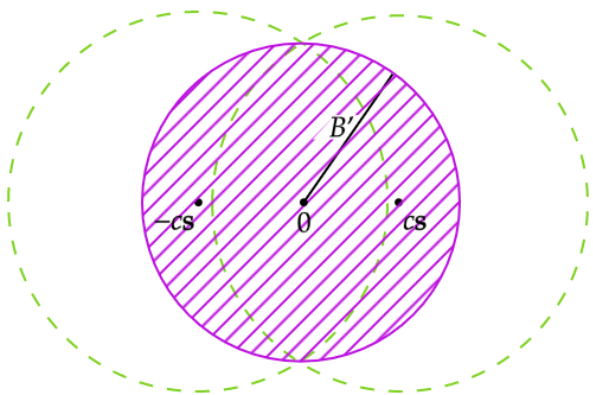
Hyperball bimodal rejection sampling

We reject $(c, \mathbf{z}) \sim D_{\mathsf{s}}$ (with p.d.f. p_{s}) to a target distribution D_{t} (with p.d.f. p_{t}), where

- p_{s}: uniform in hyperballs of radii B centered at $\pm c\mathbf{s}$
  - union of two large balls
- p_{t}: uniform in a smaller hyperball of radii B' centered at zero
  - a smaller ball in the middle



p_s



p_t

Hyperball bimodal rejection sampling

- $p_{\mathsf{s}}(\mathbf{x}) = \frac{1}{2 \cdot \mathsf{vol}(\mathcal{B}(B))} \cdot \chi_{\|\mathbf{z}-c\mathbf{s}\|<B} + \frac{1}{2 \cdot \mathsf{vol}(\mathcal{B}(B))} \cdot \chi_{\|\mathbf{z}+c\mathbf{s}\|<B}$,
- $p_{\mathsf{t}}(\mathbf{x}) = \frac{1}{\mathsf{vol}(\mathcal{B}(B))} \cdot \chi_{\|\mathbf{z}\|<B'}$.

$$\Rightarrow p(\mathbf{x}) = \frac{p_{\mathsf{t}}(\mathbf{x})}{M \cdot p_{\mathsf{s}}(\mathbf{x})} = \frac{\chi_{\|\mathbf{z}\|<B'}}{\chi_{\|\mathbf{z}-c\mathbf{s}\|<B} + \chi_{\|\mathbf{z}+c\mathbf{s}\|<B}}$$

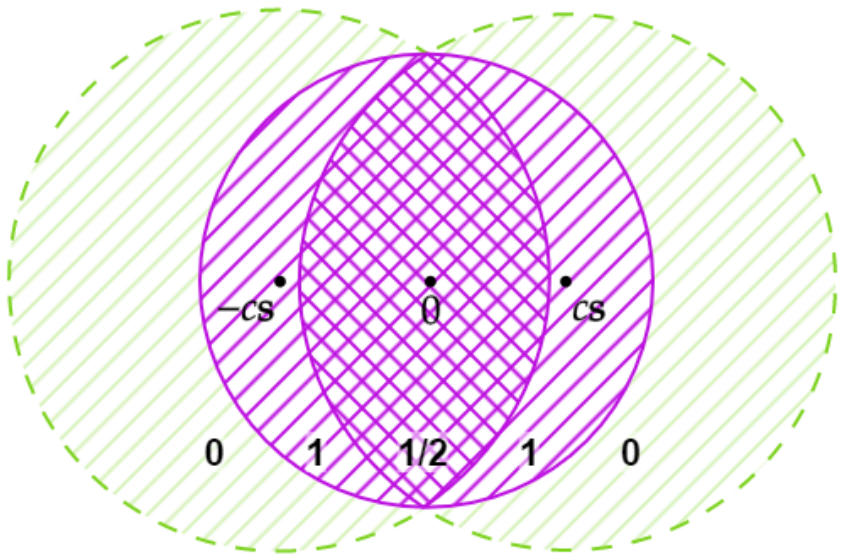
$$= \begin{cases} 0 & \text{if } \mathbf{z} \notin \mathcal{B}(B'), \\ 1/2 & \text{if } \mathbf{z} \in \mathcal{B}(B') \cap \mathcal{B}(B, c\mathbf{s}) \cap \mathcal{B}(B, -c\mathbf{s}), \\ 1 & \text{if } \mathbf{z} \in \mathcal{B}(B') \setminus (\mathcal{B}(B, c\mathbf{s}) \cap \mathcal{B}(B, -c\mathbf{s})),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

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.



1. Digital Signatures:
   - What is a digital signature?
   - Lattice-based digital signatures
   - Rejection sampling

2. HAETAE:
   - Hyperball bimodal rejection sampling
   - Parameter choices
   - Comparison to SotA lattice signatures
   - Current status

Parameter choices

Basic parameters:

- Ring degree of $\mathcal{R}$: $n = 256$
- MLWE, MSIS moduli: $q = 64513 = 2^{16} - 2^{10} + 1$
- Module dimension: k, ℓ $(\mathbf{A} \in \mathcal{R}_{2q}^{k \times (k+\ell+1)})$
- Ternary secret: $\eta = 1$
- Hamming weight of $c = H(\cdot)$: τ

✓ Entropy for c should be large enough, for e.g., $\approx 2^{\{192,\ 225,\ 255\}}$ for security parameters $\lambda = 128$, 192, and 256, respectively.

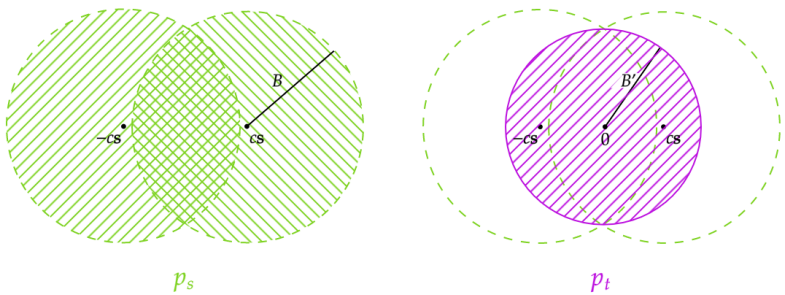
$\Rightarrow \binom{n}{\tau}$ is set to have $\approx 2^{\{192,\ 225\}}$ for $\lambda = 128$ and 192. For $\lambda = 256$, however, we need $\sum_{k=0}^{n/2-1} \binom{n}{k} = 2^{255}$.

Parameter choices

Rejection sampling parameters

- Radii for $\mathbf{y}$ and $\mathbf{z}$: B and B'
- Parameter for sk rejection: γ

✓ B'-hyperball is contained in the two B-hyperballs, centered at $\pm\|c\mathbf{s}\|_2$:



$\Rightarrow B'^2 + \|c\mathbf{s}\|_2^2 \leq B^2$.

✓ To further reduce B and B', we use good sk satisfying $\|c\mathbf{s}\|_2 \leq \gamma\sqrt{\tau}$, via sk rejection sampling (use $1/10$ among uniform ternary secret vectors).

$\Rightarrow B'^2 + \gamma^2\tau \leq B^2$.

Parameter choices

Compression parameters

- Parameter for vk truncation: d
- Parameter for $\mathbf{z}$ and vk compression: α and α_{h}
- Radius for $\tilde{\mathbf{z}}$ (decompressed $\mathbf{z}$ with some error): B''

✓ HAETAE uses various compression techniques to reduce signature sizes:

- Entropy encoding (rANS) on signatures in B-ball
- HighBits, LowBits, LSB compression with hints
- Final rejection after signing (rejects 0.1% signatures)

1. Digital Signatures:
   - What is a digital signature?
   - Lattice-based digital signatures
   - Rejection sampling

2. HAETAE:
   - Hyperball bimodal rejection sampling
   - Parameter choices
   - Comparison to SotA lattice signatures
   - Current status

Comparison to SotA lattice signatures.

For 120-bit classical security. Sizes are in bytes.

Scheme	sig	vk	KeyGen	Sign	
				sampling	rejection
Dilithium-2	2420	1312	fast	Hypercube	$\|\cdot\|_\infty < B$
Bliss-1024[3]	1700	1792	fast	dGaussian at 0	reject with prob. $f(\mathsf{sk}, \mathsf{Sig})$
HAETAE120	1468	1056	fast	dHyperball at 0	$\|\cdot\|_2 < B$
Mitaka-512[4]	713	896	slow	dGaussian at 0 & intGaussian at $H(m)$	none
Falcon-512	666	897	slow	dGaussian at $H(m)$	none

Table: Comparison between different lattice-based signature schemes.

[3] modified Bliss (to ≥ 120 bit-security) in Dilithium paper.
[4] Mitaka-512 has 102 bits of security

1. Digital Signatures:
   - What is a digital signature?
   - Lattice-based digital signatures
   - Rejection sampling

2. HAETAE:
   - Hyperball bimodal rejection sampling
   - Parameter choices
   - Comparison to SotA lattice signatures
   - Current status

Current Status

NIST PQC

- Competition for USA standard PQC schemes.
- HAETAE is one of the candidates in *Additional Signatures* track.

KPQC

- Competition for Korean standard PQC schemes.
- HAETAE is advanced to Round 2, one of four candidates in *Digital Signatures* track.

✓ HAETAE will appear in CHES 2024.

Thank you!

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.

[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.

[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 II

[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.

[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.

References III

[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.

[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 IV

[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.