Compact Lattice Signatures via Iterative Rejection Sampling

Joel Gärtner[1,2]
[1]KTH Royal Institute of Technology
[2]Swedish NCSA, Swedish Armed Forces, Stockholm, Sweden

Aug 17, 2025

Summary

- Compact lattice-based Fiat–Shamir with Aborts signature scheme
- Enabled by new rejection sampling and iterative signature construction
- New scheme still compact when parametrized without aborts

Scheme	VK + Signature Size
With aborts	928 + 775 = 1703
Without aborts	1056 + 1059 = 2115
HAETAE-120	992 + 1474 = 2466
G+G-120	1472 + 1677 = 3149
Dilithium-2	1312 + 2420 = 3732

Lyubashevsky's Signature Scheme [Lyu09, Lyu12]

- Origin of the basic idea behind Dilithium
- Fiat–Shamir based signatures similar to Schnorr signatures
- Lattice-based schemes security relies on variant of SIS to be hard

Short Integer Solutions (SIS)

Given $\boldsymbol{A}$ uniformly random in $\mathbb{Z}_q^{m \times n}$, find short $\boldsymbol{x}$ such that $\boldsymbol{Ax} \equiv 0 \mod q$.

Overview of Lyubashevsky's Scheme

Private key

Matrix $\boldsymbol{S}$ with short columns

Public key

Random matrix $\boldsymbol{A}$ and $\boldsymbol{T} = \boldsymbol{A}\boldsymbol{S} \bmod q$

Overview of Lyubashevsky's Scheme

Private key

Matrix $\boldsymbol{S}$ with short columns

Public key

Random matrix $\boldsymbol{A}$ and $\boldsymbol{T} = \boldsymbol{AS} \bmod q$

Sign message μ

- Sample short $\boldsymbol{y}$ and derive a short challenge $\boldsymbol{c} = \mathcal{H}(\boldsymbol{Ay} \bmod q, \mu)$
- Signature: $(\boldsymbol{z}, \boldsymbol{c})$ where $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{Sc} \bmod q$

Overview of Lyubashevsky's Scheme

Private key

Matrix $\boldsymbol{S}$ with short columns

Public key

Random matrix $\boldsymbol{A}$ and $\boldsymbol{T} = \boldsymbol{AS} \bmod q$

Sign message μ

- Sample short $\boldsymbol{y}$ and derive a short challenge $\boldsymbol{c} = \mathcal{H}(\boldsymbol{Ay} \bmod q, \mu)$
- Signature: $(\boldsymbol{z}, \boldsymbol{c})$ where $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{Sc} \bmod q$

Verify signature $(\boldsymbol{z}, \boldsymbol{c})$

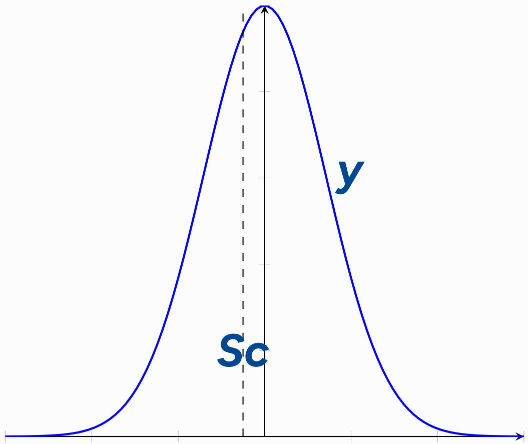
Check that $\|\boldsymbol{z}\|$ small and $\mathcal{H}(\boldsymbol{Az} - \boldsymbol{Tc} \bmod q, \mu) = \boldsymbol{c}$

Aborts to Ensure Security of Scheme

- Signatures leak information about $\boldsymbol{S}$ as $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{S}\boldsymbol{c}$ dependent on $\boldsymbol{S}$
- Solution is to not always emit $(\boldsymbol{z}, \boldsymbol{c})$ instead sometimes aborting and restarting
- Corresponds to rejection sampling from distribution of $\boldsymbol{y} + \boldsymbol{S}\boldsymbol{c}$

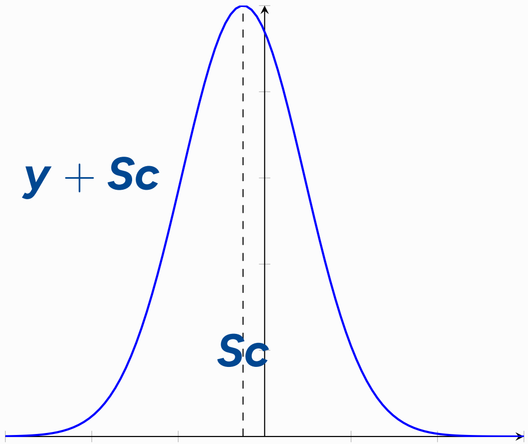
One-Dimensional Illustration

- $\boldsymbol{y}$ Gaussian, $\boldsymbol{Sc}$ small shift



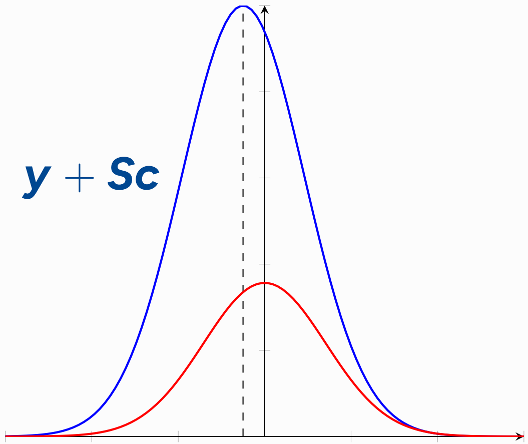
One-Dimensional Illustration

- $\boldsymbol{y}$ Gaussian, $\boldsymbol{Sc}$ small shift
- $\boldsymbol{y} + \boldsymbol{Sc}$ non-centered Gaussian



One-Dimensional Illustration

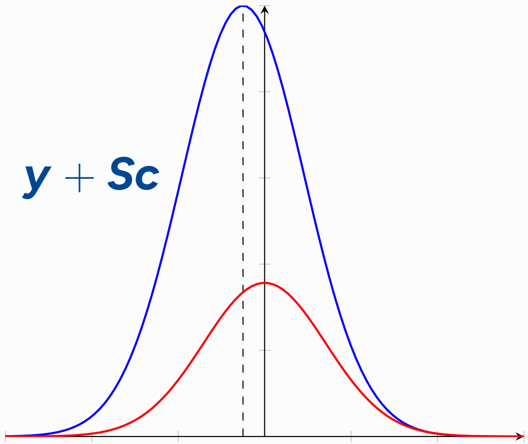
- $\boldsymbol{y}$ Gaussian, $\boldsymbol{Sc}$ small shift
- $\boldsymbol{y} + \boldsymbol{Sc}$ non-centered Gaussian
- Gaussian function $\rho_r(\boldsymbol{z})/M$ in red



One-Dimensional Illustration

- $\boldsymbol{y}$ Gaussian, $\boldsymbol{Sc}$ small shift
- $\boldsymbol{y} + \boldsymbol{Sc}$ non-centered Gaussian
- Gaussian function $\rho_r(\boldsymbol{z})/M$ in red
- Emit signature with probability

$$\frac{\rho_r(\boldsymbol{z})}{M\rho_r(\boldsymbol{z} - \boldsymbol{Sc})} = \frac{\rho_r(\boldsymbol{y} + \boldsymbol{Sc})}{M\rho_r(\boldsymbol{y})}$$



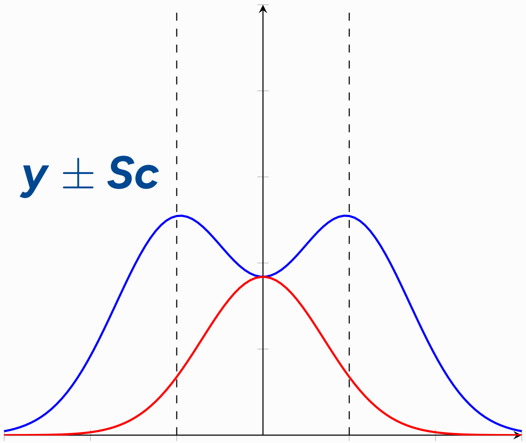
Parametrization Tradeoffs

Smaller Gaussian parameter r leads to

- More secure scheme
- More compact signatures
- Higher rejection probability and signing time

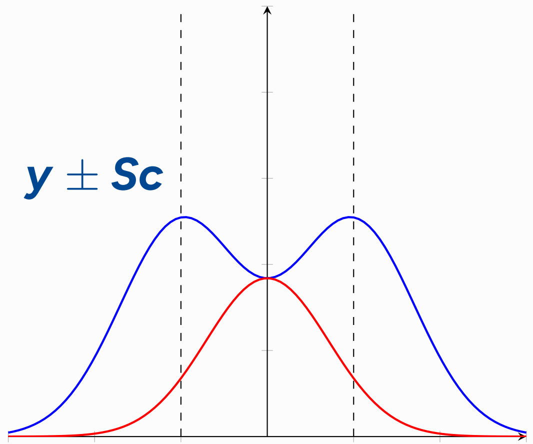
BLISS [DDLL13]

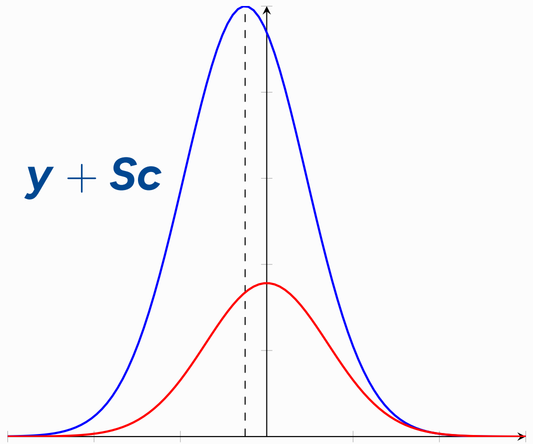
- Different public key construction allowing signatures to be constructed as $(\boldsymbol{z}, \boldsymbol{c})$ with $\boldsymbol{z} = \boldsymbol{y} \pm \boldsymbol{Sc}$
- Equal probability for the different choices leads to bimodal distribution



Benefit of Bimodal Rejection Sampling

- Possible to handle much larger $\|\boldsymbol{Sc}\|$ with the same rejection probability
- Corresponds to handling smaller $\|\boldsymbol{z}\|$ with the same $\|\boldsymbol{Sc}\|$





Reformulation of Bimodal Rejection Sampling

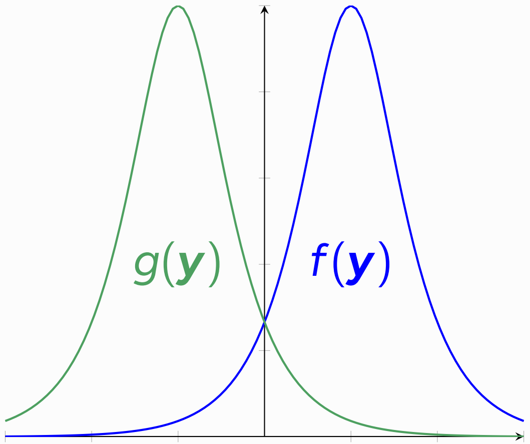
Typical formulation

- Construct $\boldsymbol{z}$ as $\boldsymbol{y} \pm \boldsymbol{Sc}$ with probability $1/2$
- Accept $\boldsymbol{z}$ with probability $R(\boldsymbol{z})$

Combined formulation

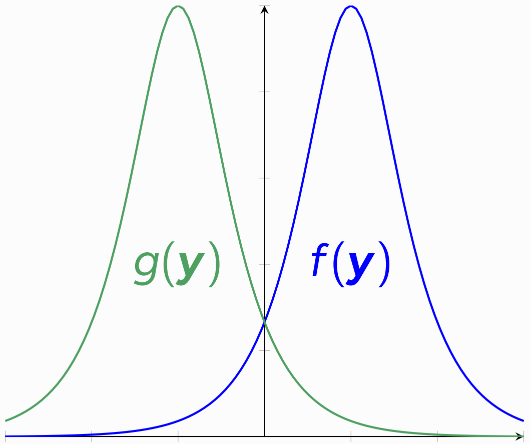
Given $\boldsymbol{y}$ construct $\boldsymbol{z}$ as

- $\boldsymbol{y} - \boldsymbol{Sc}$ with probability $f(\boldsymbol{y}) = R(\boldsymbol{y} - \boldsymbol{Sc})/2$
- $\boldsymbol{y} + \boldsymbol{Sc}$ with probability $g(\boldsymbol{y}) = R(\boldsymbol{y} + \boldsymbol{Sc})/2$
- Reject otherwise



More General Functions $f(\boldsymbol{y})$ and $g(\boldsymbol{y})$

- $\boldsymbol{z} = \boldsymbol{y} - \boldsymbol{Sc}$ with probability $f(\boldsymbol{y})$
- $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{Sc}$ with probability $g(\boldsymbol{y})$
- Probability of $\boldsymbol{y}$ proportional to $\rho_r(\boldsymbol{y})$, a Gaussian function with parameter r

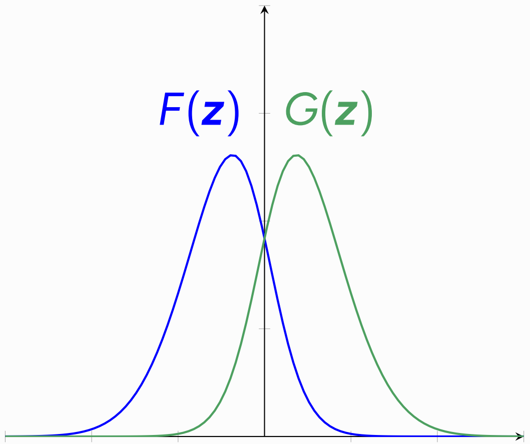


More General Functions $f(\boldsymbol{y})$ and $g(\boldsymbol{y})$

- $\boldsymbol{z} = \boldsymbol{y} - \boldsymbol{Sc}$ with probability $f(\boldsymbol{y})$
- $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{Sc}$ with probability $g(\boldsymbol{y})$
- Probability of $\boldsymbol{y}$ proportional to $\rho_r(\boldsymbol{y})$, a Gaussian function with parameter r

Probability of $\boldsymbol{z}$ proportional to

- $F(\boldsymbol{z}) = \rho_r(\boldsymbol{z} + \boldsymbol{Sc})f(\boldsymbol{z} + \boldsymbol{Sc})$ via f
- $G(\boldsymbol{z}) = \rho_r(\boldsymbol{z} - \boldsymbol{Sc})g(\boldsymbol{z} - \boldsymbol{Sc})$ via g
- $F(\boldsymbol{z}) + G(\boldsymbol{z}) = \dfrac{\rho_r(\boldsymbol{z})}{M}$ in total

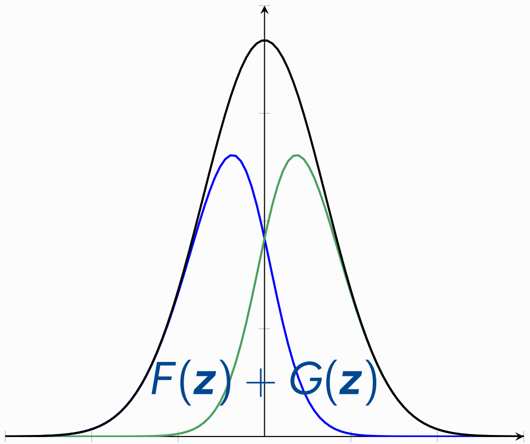


More General Functions $f(\boldsymbol{y})$ and $g(\boldsymbol{y})$

- $\boldsymbol{z} = \boldsymbol{y} - \boldsymbol{Sc}$ with probability $f(\boldsymbol{y})$
- $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{Sc}$ with probability $g(\boldsymbol{y})$
- Probability of $\boldsymbol{y}$ proportional to $\rho_r(\boldsymbol{y})$, a Gaussian function with parameter r

Probability of $\boldsymbol{z}$ proportional to

- $F(\boldsymbol{z}) = \rho_r(\boldsymbol{z} + \boldsymbol{Sc})f(\boldsymbol{z} + \boldsymbol{Sc})$ via f
- $G(\boldsymbol{z}) = \rho_r(\boldsymbol{z} - \boldsymbol{Sc})g(\boldsymbol{z} - \boldsymbol{Sc})$ via g
- $F(\boldsymbol{z}) + G(\boldsymbol{z}) = \dfrac{\rho_r(\boldsymbol{z})}{M}$ in total



Our Rejection Sampling Functions

Functions are defined as

$$f(\boldsymbol{y}) = \begin{cases} \dfrac{S(\boldsymbol{y})}{M} & \text{If } \langle \boldsymbol{y}, \boldsymbol{Sc} \rangle \geq \|\boldsymbol{Sc}\|^2 \\ \dfrac{1 - S(-\boldsymbol{y})}{M} & \text{If } \langle \boldsymbol{y}, \boldsymbol{Sc} \rangle < \|\boldsymbol{Sc}\|^2 \end{cases} \qquad g(\boldsymbol{y}) = \begin{cases} \dfrac{1 - S(\boldsymbol{y})}{M} & \text{If } \langle \boldsymbol{y}, \boldsymbol{Sc} \rangle \geq -\|\boldsymbol{Sc}\|^2 \\ \dfrac{S(-\boldsymbol{y})}{M} & \text{If } \langle \boldsymbol{y}, \boldsymbol{Sc} \rangle < -\|\boldsymbol{Sc}\|^2 \end{cases}$$

where

$$S(\boldsymbol{y}) = \sum_{k \geq 0} \frac{(-1)^k \rho_r(\boldsymbol{y} + k\boldsymbol{Sc})}{\rho_r(\boldsymbol{y})}$$

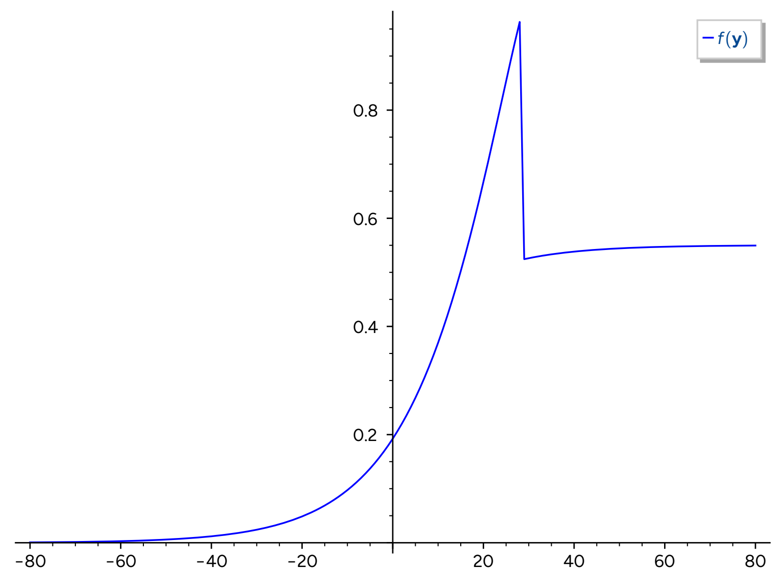
which in the relevant regime can be efficiently approximated

Rejection Parameter M

- Rejects with probability $1/M$
- Selected to ensure that $f(\boldsymbol{y}) + g(\boldsymbol{y}) \leq 1$
- Depends on parameter $\alpha \leq r/\|\boldsymbol{Sc}\|$

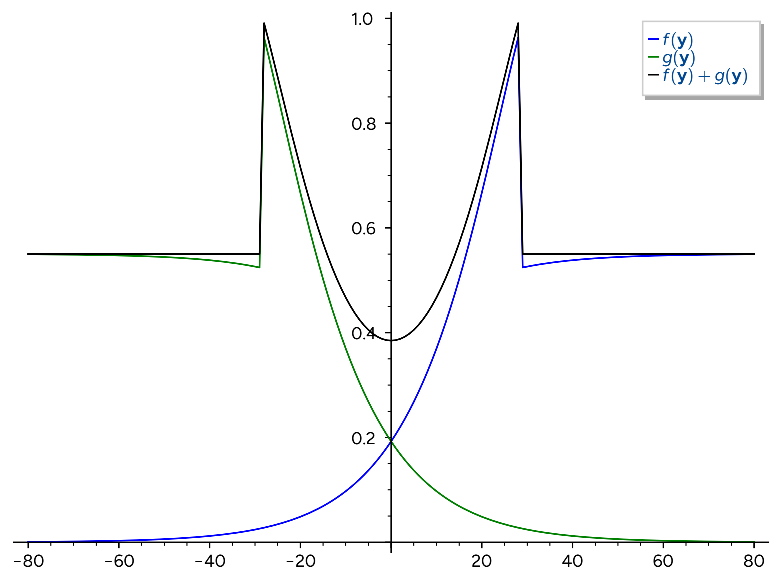
One-Dimensional Illustration: Functions

- Function f provides more complicated redistribution of probability than in BLISS



One-Dimensional Illustration: Functions

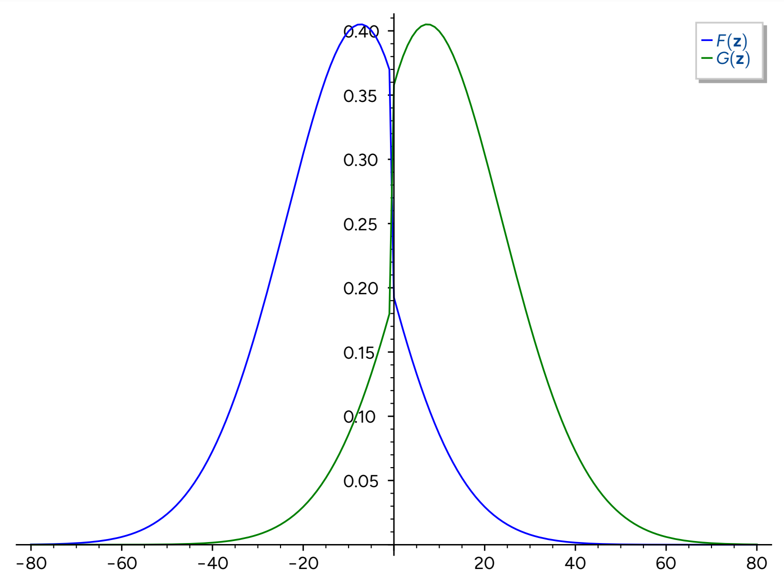
- Function f provides more complicated redistribution of probability than in BLISS
- Rejection parameter M selected such that $\max_y f(y) + g(y) \approx 1$



One-Dimensional Illustration: Outputs

Probability of $\boldsymbol{z}$ proportional to

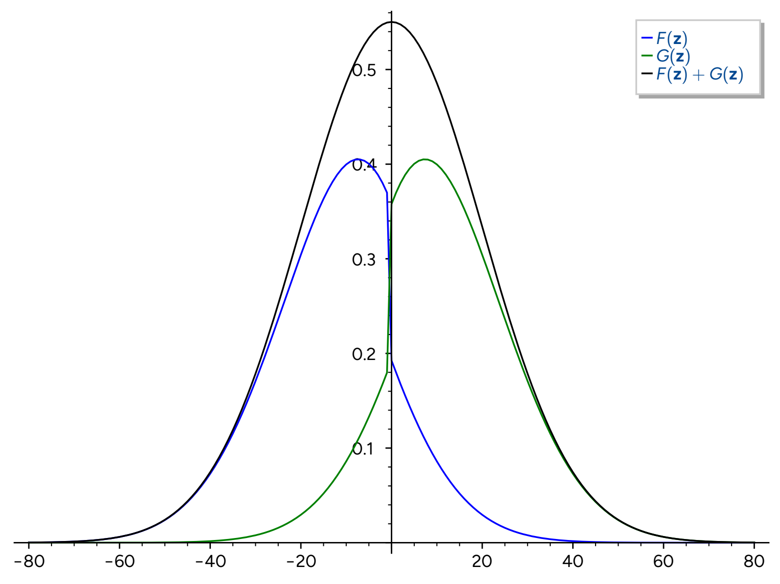
- $F(\boldsymbol{z}) = \rho_r(\boldsymbol{y} + \boldsymbol{Sc}) f(\boldsymbol{z} + \boldsymbol{Sc})$ via f
- $G(\boldsymbol{z}) = \rho_r(\boldsymbol{y} - \boldsymbol{Sc}) g(\boldsymbol{z} - \boldsymbol{Sc})$ via g



One-Dimensional Illustration: Outputs

Probability of $\mathbf{z}$ proportional to

- $F(\mathbf{z}) = \rho_r(\mathbf{y} + \mathbf{Sc})f(\mathbf{z} + \mathbf{Sc})$ via f
- $G(\mathbf{z}) = \rho_r(\mathbf{y} - \mathbf{Sc})g(\mathbf{z} - \mathbf{Sc})$ via g
- $F(\mathbf{z}) + G(\mathbf{z}) = \frac{\rho_r(\mathbf{z})}{M}$ in total



Comparison to Bimodal Rejection Sampling

- Parameter $\alpha \leq r/\|\mathbf{Sc}\|$.
- Smaller α leads to more compact scheme

BLISS

- Uses $\alpha \in [0.5, 1]$
- Repetition rate between 7.4 and 1.6

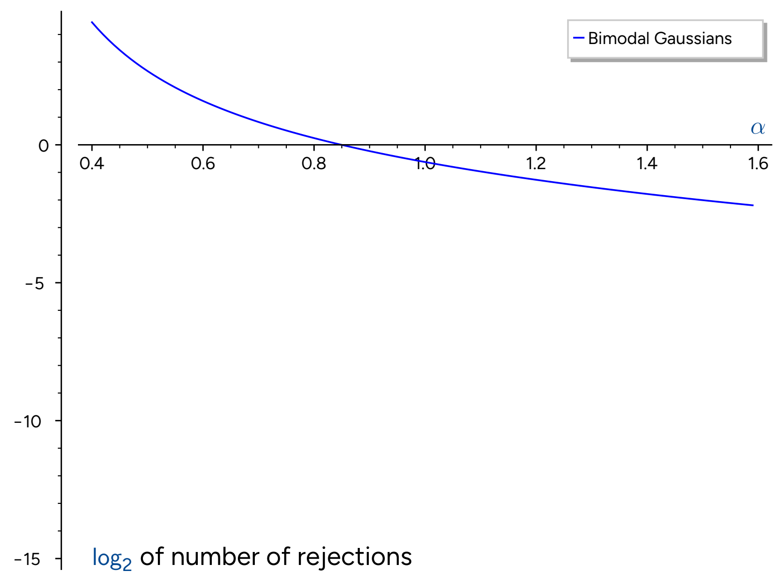


Figure: Base two logarithm of the expected number of rejections.

Comparison to Bimodal Rejection Sampling

- Parameter $\alpha \leq r/\|\mathbf{Sc}\|$.
- Smaller α leads to more compact scheme

BLISS

- Uses $\alpha \in [0.5, 1]$
- Repetition rate between 7.4 and 1.6

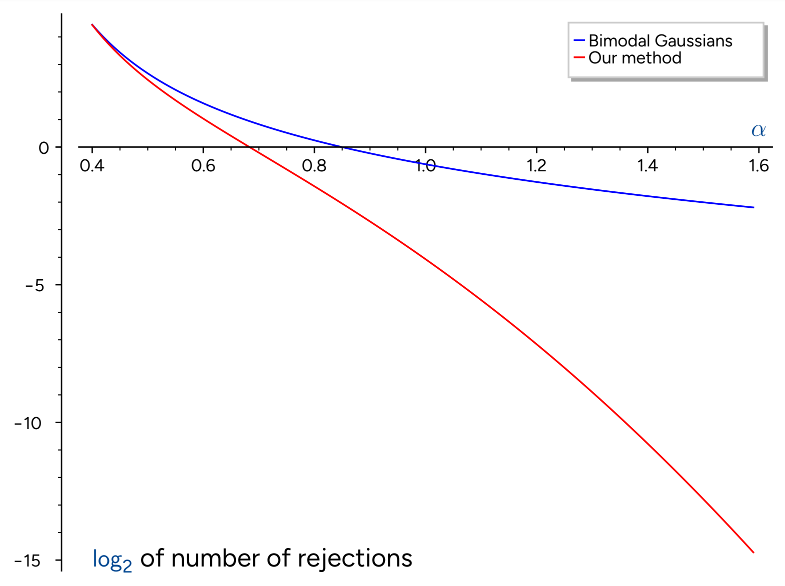


Figure: Base two logarithm of the expected number of rejections.

Iterative Signature Construction

- Can construct signature with $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{S}\boldsymbol{c}'$ for any $\boldsymbol{c}' \equiv \boldsymbol{c} \mod 2$
- Select signs of entries in the $\{0, 1\}$ challenge vector $\boldsymbol{c}$ independently

$$\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{S}\boldsymbol{c}' = \boldsymbol{y} + \sum_{i=1}^{n} (\pm)\boldsymbol{s}_i c_i$$

- Columns $\boldsymbol{s}_i$ of $\boldsymbol{S}$ on expectation much shorter than $\boldsymbol{S}\boldsymbol{c}$

Iterative Signature Construction

- Can construct signature with $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{S}\boldsymbol{c}'$ for any $\boldsymbol{c}' \equiv \boldsymbol{c} \mod 2$
- Select signs of entries in the $\{0, 1\}$ challenge vector $\boldsymbol{c}$ independently

$$\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{S}\boldsymbol{c}' = \boldsymbol{y} + \sum_{i=1}^{n} (\pm)\boldsymbol{s}_i c_i$$

- Columns $\boldsymbol{s}_i$ of $\boldsymbol{S}$ on expectation much shorter than $\boldsymbol{S}\boldsymbol{c}$

1. Let $\boldsymbol{z}_0 = \boldsymbol{y}$

Iterative Signature Construction

- Can construct signature with $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{S}\boldsymbol{c}'$ for any $\boldsymbol{c}' \equiv \boldsymbol{c} \mod 2$
- Select signs of entries in the $\{0, 1\}$ challenge vector $\boldsymbol{c}$ independently

$$\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{S}\boldsymbol{c}' = \boldsymbol{y} + \sum_{i=1}^{n} (\pm)\boldsymbol{s}_i c_i$$

- Columns $\boldsymbol{s}_i$ of $\boldsymbol{S}$ on expectation much shorter than $\boldsymbol{S}\boldsymbol{c}$

1. Let $\boldsymbol{z}_0 = \boldsymbol{y}$
2. Perform rejection sampling to construct $\boldsymbol{z}_i = \boldsymbol{z}_{i-1} \pm \boldsymbol{s}_i c_i$

Iterative Signature Construction

- Can construct signature with $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{S}\boldsymbol{c}'$ for any $\boldsymbol{c}' \equiv \boldsymbol{c} \mod 2$
- Select signs of entries in the $\{0, 1\}$ challenge vector $\boldsymbol{c}$ independently

$$\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{S}\boldsymbol{c}' = \boldsymbol{y} + \sum_{i=1}^{n} (\pm)\boldsymbol{s}_i c_i$$

- Columns $\boldsymbol{s}_i$ of $\boldsymbol{S}$ on expectation much shorter than $\boldsymbol{S}\boldsymbol{c}$

1. Let $\boldsymbol{z}_0 = \boldsymbol{y}$
2. Perform rejection sampling to construct $\boldsymbol{z}_i = \boldsymbol{z}_{i-1} \pm \boldsymbol{s}_i c_i$
3. If any step rejects, reject iterative procedure

Iterative Signature Construction

- Can construct signature with $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{S}\boldsymbol{c}'$ for any $\boldsymbol{c}' \equiv \boldsymbol{c} \mod 2$
- Select signs of entries in the $\{0, 1\}$ challenge vector $\boldsymbol{c}$ independently

$$\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{S}\boldsymbol{c}' = \boldsymbol{y} + \sum_{i=1}^{n} (\pm)\boldsymbol{s}_i c_i$$

- Columns $\boldsymbol{s}_i$ of $\boldsymbol{S}$ on expectation much shorter than $\boldsymbol{S}\boldsymbol{c}$

1. Let $\boldsymbol{z}_0 = \boldsymbol{y}$
2. Perform rejection sampling to construct $\boldsymbol{z}_i = \boldsymbol{z}_{i-1} \pm \boldsymbol{s}_i c_i$
3. If any step rejects, reject iterative procedure
4. $\boldsymbol{z}_n = \boldsymbol{y} + \boldsymbol{S}\boldsymbol{c}'$ follows Gaussian distribution and $\boldsymbol{c}' \equiv \boldsymbol{c} \mod 2$

Iterative Signature Construction Performance

+ Each iterative step uses rejection sampling with larger $\alpha \leq r/\|\mathbf{s}_i\|$
- All steps must succeed

Provides significant benefit in combination with our new method

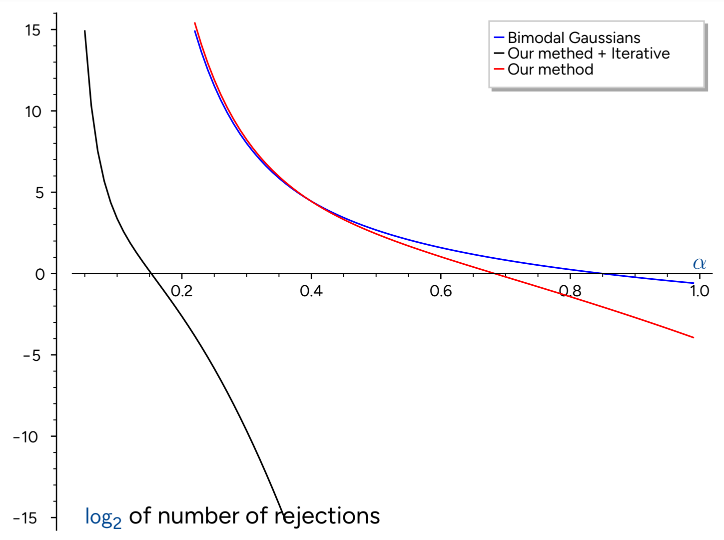


Figure: Rejection rates when $\mathbf{c}$ has 10 non-zero entries.

Concrete Scheme

Structured Scheme

- NTRU-based and MLWE-based schemes possible
- NTRU-based scheme somewhat more compact
- MLWE-based scheme more flexible to parametrize

NTWE-based scheme

- NTWE problem [Gär23] natural combination of NTRU and MLWE problems
- Provides flexibility benefit of MLWE and compactness benefits of NTRU

NTWE problem

- Parameters ℓ, m, q and $\mathcal{R} = \mathbb{Z}_q[X]/(X^n + 1)$
- Secret and small $\boldsymbol{s} \in \mathcal{R}^\ell$, $\boldsymbol{e} \in \mathcal{R}^m$ and invertible $f \in \mathcal{R}$
- Distinguish $\boldsymbol{A} \leftarrow U(\mathcal{R}^{m \times \ell})$ and $\boldsymbol{b} = (\boldsymbol{A}\boldsymbol{s} + \boldsymbol{e})f^{-1}$ from uniformly random

NTWE-based scheme

- NTWE problem [Gär23] natural combination of NTRU and MLWE problems
- Provides flexibility benefit of MLWE and compactness benefits of NTRU

NTWE problem

- Parameters ℓ, m, q and $\mathcal{R} = \mathbb{Z}_q[X]/(X^n + 1)$
- Secret and small $\boldsymbol{s} \in \mathcal{R}^\ell$, $\boldsymbol{e} \in \mathcal{R}^m$ and invertible $f \in \mathcal{R}$
- Distinguish $\boldsymbol{A} \leftarrow U(\mathcal{R}^{m \times \ell})$ and $\boldsymbol{b} = (\boldsymbol{As} + \boldsymbol{e})f^{-1}$ from uniformly random

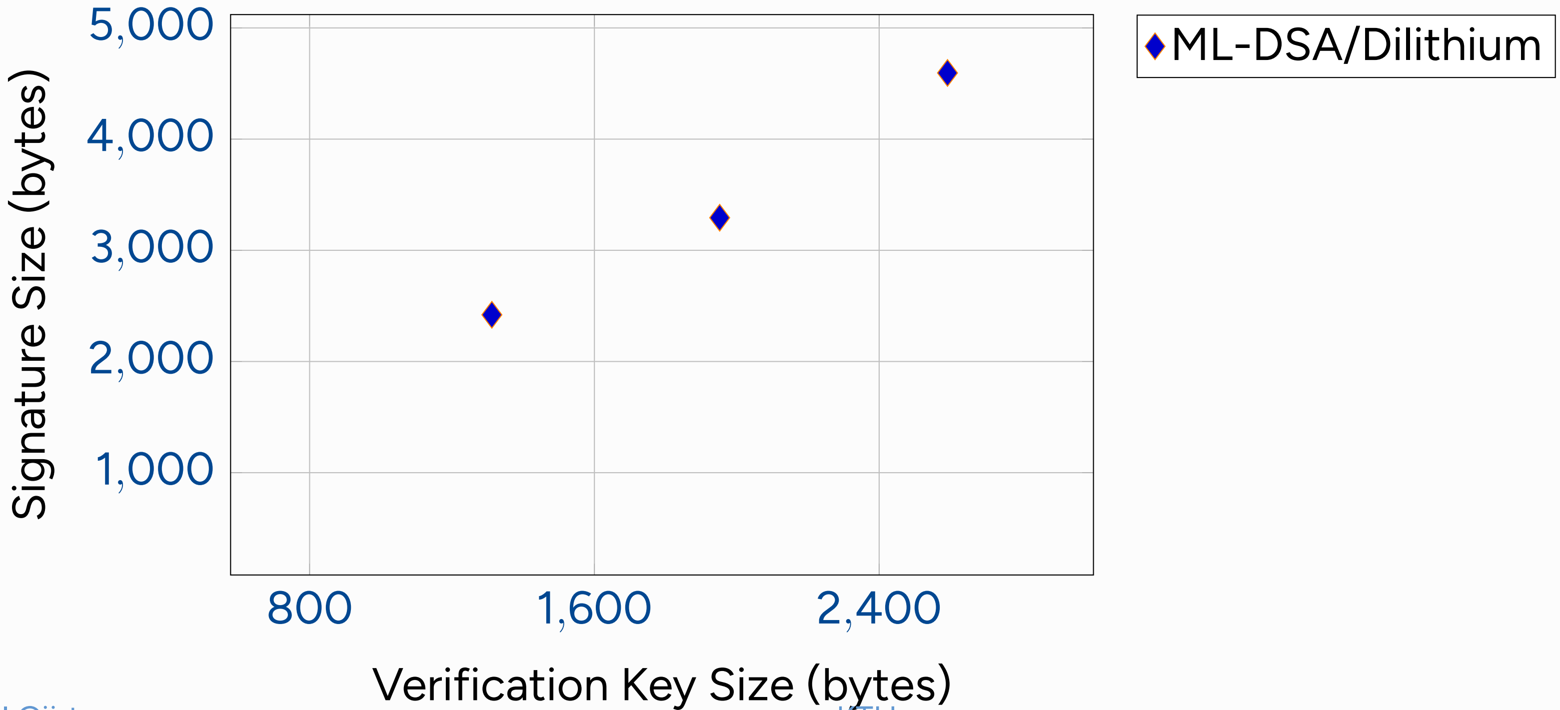
MLWE-based alternative

Would have at most 300 bytes larger signatures

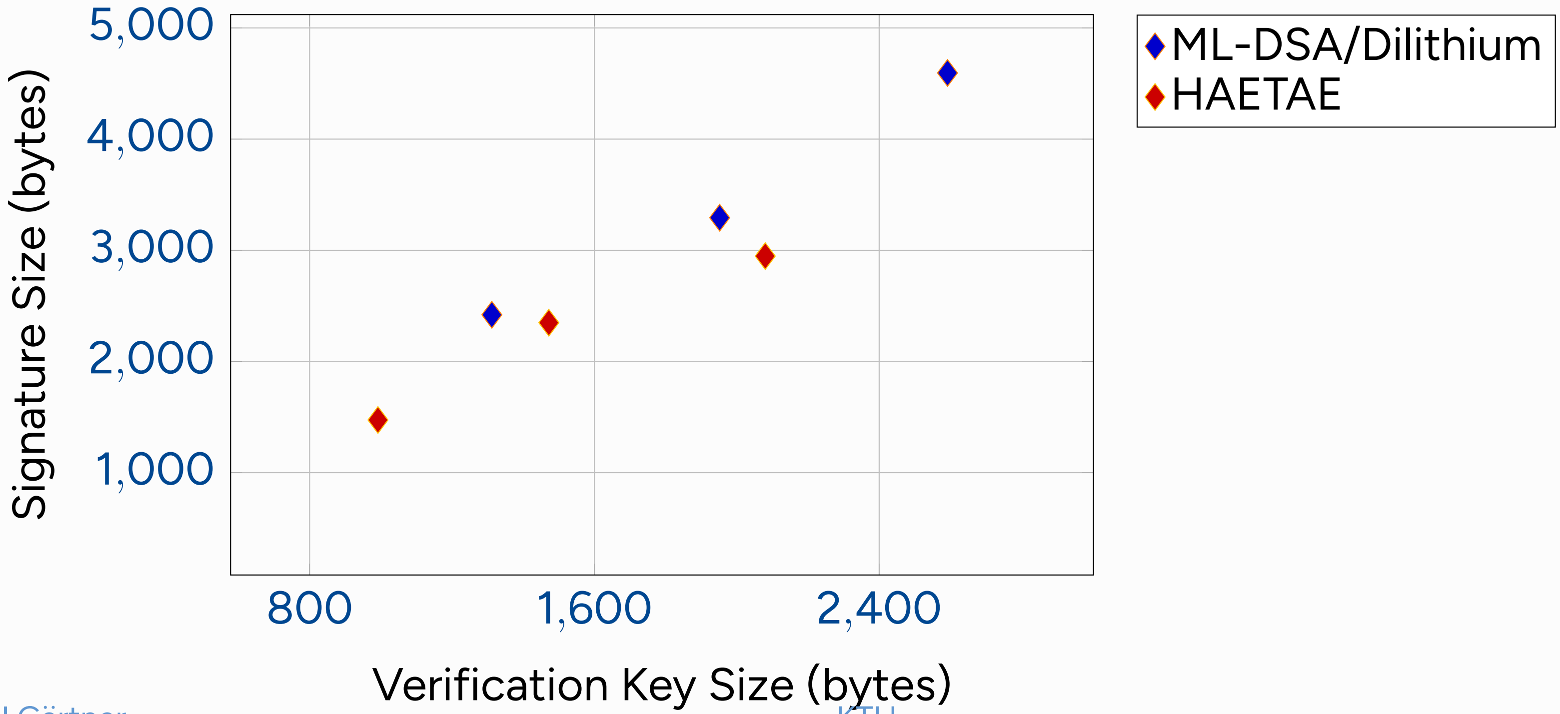
Proposed Scheme

- Use $n = 256$ and a prime q that allows efficient NTT
- Various standard tricks for compressing scheme
- Variants with rejection probability of $\approx 50\%$ and with $< 2^{-100}$

Comparison

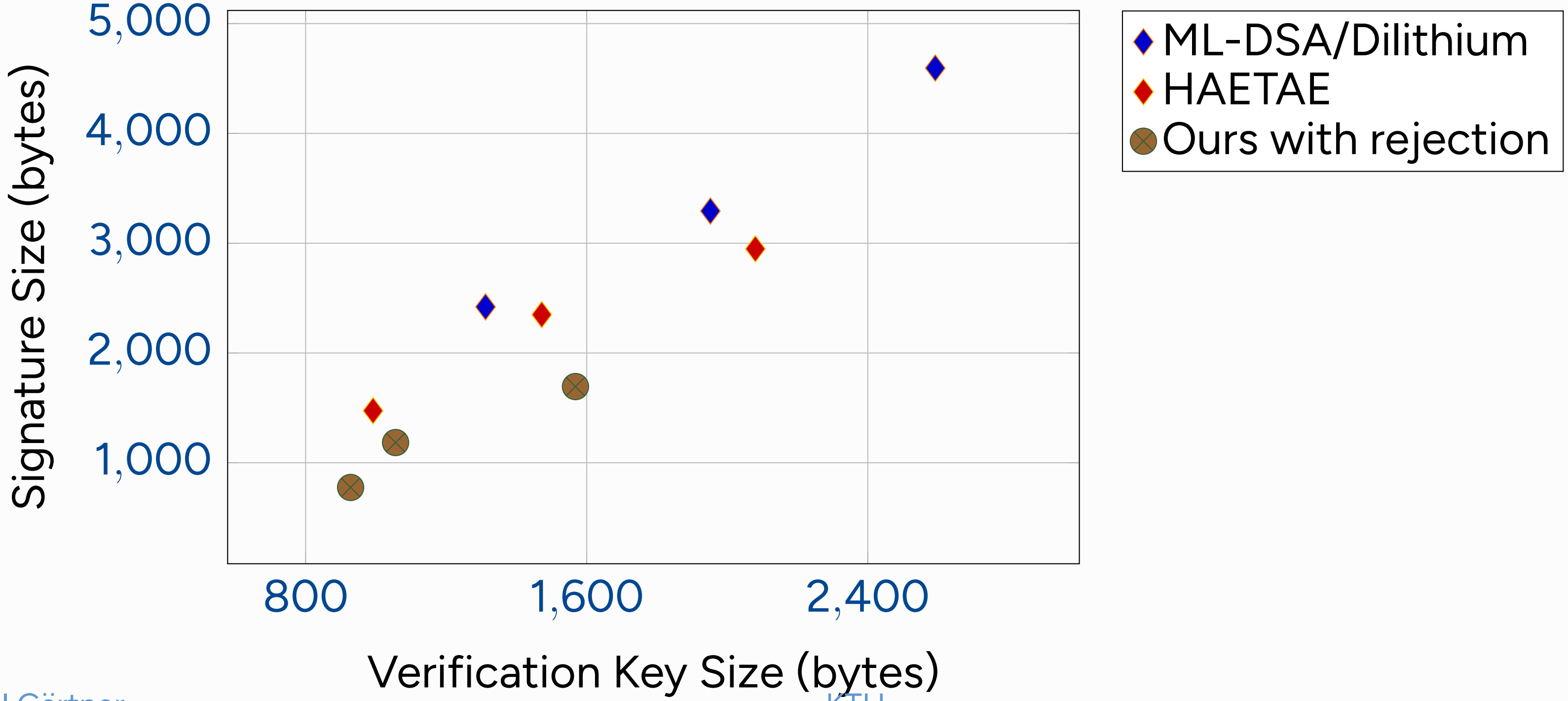

5,000
4,000
3,000
2,000
1,000
Signature Size (bytes)
800
1,600
2,400
Verification Key Size (bytes)
ML-DSA/Dilithium

Comparison



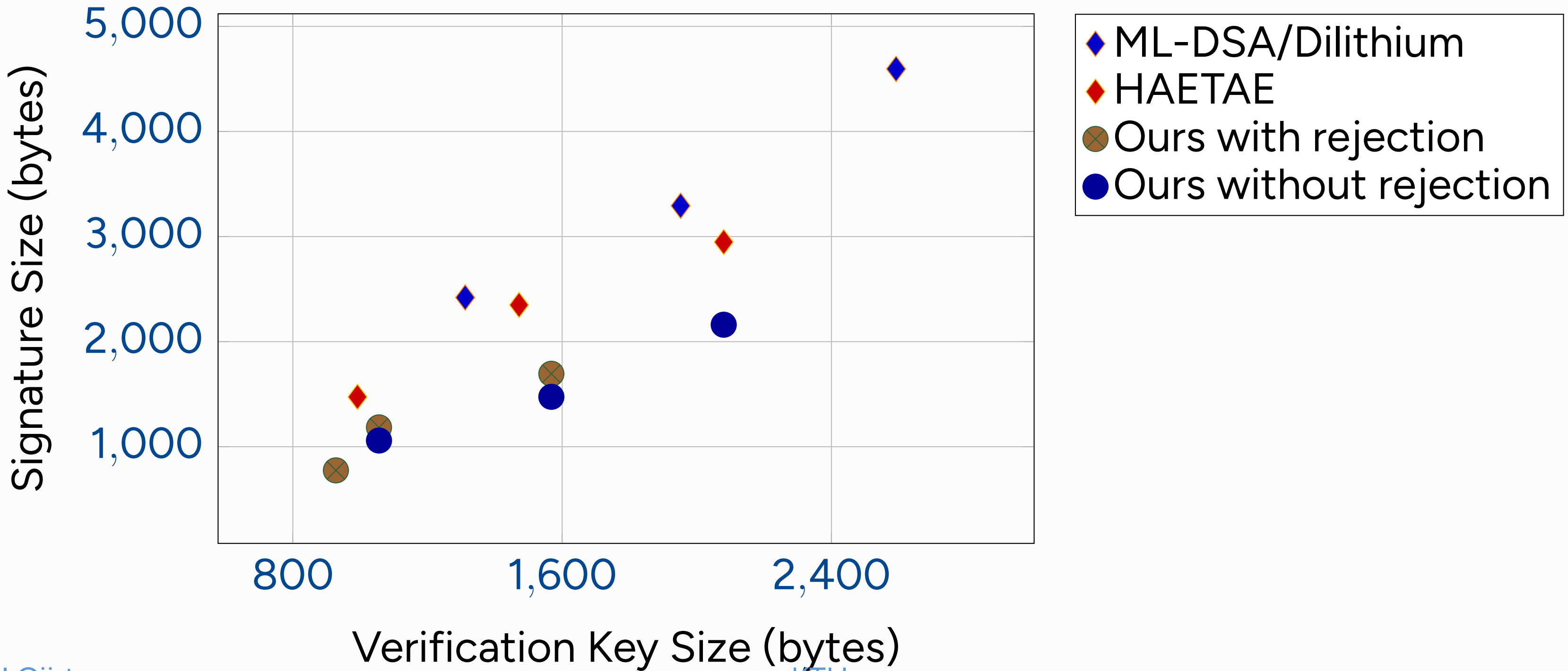
5,000
4,000
3,000
2,000
1,000
Signature Size (bytes)
800
1,600
2,400
Verification Key Size (bytes)
ML-DSA/Dilithium
HAETAE

Comparison

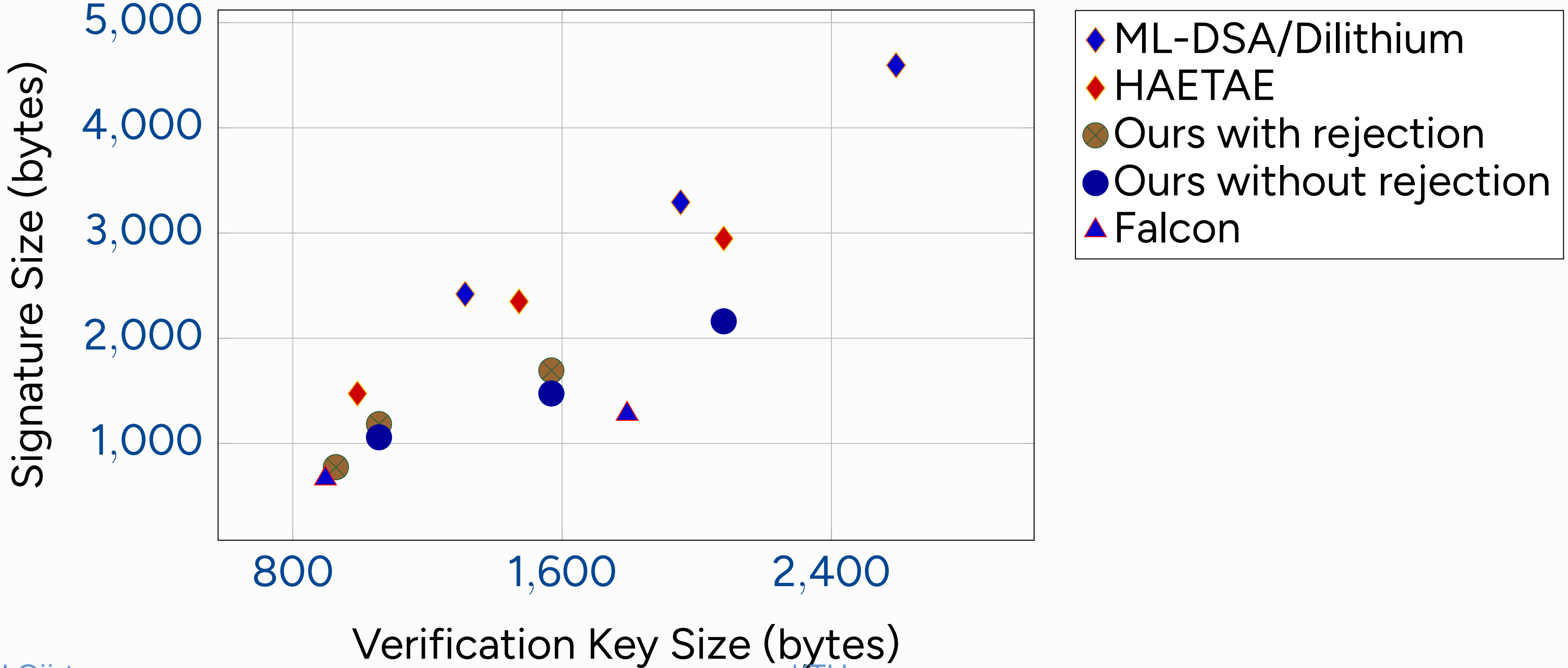

5,000
4,000
3,000
2,000
1,000
Signature Size (bytes)
800
1,600
2,400
Verification Key Size (bytes)
ML-DSA/Dilithium
HAETAE
Ours with rejection

Concrete Scheme

Comparison



Comparison



5,000
4,000
3,000
2,000
1,000
Signature Size (bytes)
800
1,600
2,400
Verification Key Size (bytes)
ML-DSA/Dilithium
HAETAE
Ours with rejection
Ours without rejection
Falcon

Secure Implementation

- Big concern with Falcon is that it seems hard to implement securely

Our scheme

- Non-trivial to securely implementing discrete Gaussian sampling
- New method for rejection sampling may complicate implementation
- Possibility to ignore rejection condition may simplify implementations

Conclusion

- Developed a new method for rejection sampling
- Allows us to construct a significantly more compact lattice-based Fiat–Shamir signature scheme
- Would be interesting if similar construction could improve rejection sampling from uniform distributions

	Level 2			Level 3			Level 5		
Scheme	VK	Sig	Comb	VK	Sig	Comb	VK	Sig	Comb
Falcon	897	666	1563	-	-	-	1793	1280	3073
HAWK	1024	555	1579	-	-	-	2440	1221	3661
Ours with rejection	928	775	1703	1056	1184	2240	1568	1694	3262
Ours without rejection	1056	1059	2115	1568	1475	3043	2080	2161	4241
HAETAE	992	1474	2466	1472	2349	3821	2080	2948	5028
G+G	1472	1677	3149	1952	2143	4095	2336	2804	5140
Dilithium	1312	2420	3732	1952	3293	5245	2592	4595	7187

Table: Sizes for Verification Key (VK), signatures (Sig) and combined (Comb) for different NIST security levels. All sizes are reported in bytes. The schemes in yellow are hash-and-sign-based.

	Level 2			Level 3			Level 5		
Scheme	VK	Sig	Comb	VK	Sig	Comb	VK	Sig	Comb
Falcon	897	666	1563	-	-	-	1793	1280	3073
HAWK	1024	555	1579	-	-	-	2440	1221	3661
Ours with rejection	928	775	1703	1056	1184	2240	1568	1694	3262
Ours without rejection	1056	1059	2115	1568	1475	3043	2080	2161	4241
HAETAE	992	1474	2466	1472	2349	3821	2080	2948	5028
G+G	1472	1677	3149	1952	2143	4095	2336	2804	5140
Dilithium	1312	2420	3732	1952	3293	5245	2592	4595	7187

Table: Sizes for Verification Key (VK), signatures (Sig) and combined (Comb) for different NIST security levels. All sizes are reported in bytes. The schemes in yellow are hash-and-sign-based.

Questions?

KTH
VETENSKAP
OCH KONST

[DDLL13] Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky, *Lattice signatures and bimodal Gaussians*, 2013, pp. 40–56.

[Gär23] Joel Gärtner, *NTWE: A natural combination of NTRU and LWE*, 2023, pp. 321–353.

[Lyu09] Vadim Lyubashevsky, *Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures*, 2009, pp. 598–616.

[Lyu12] ______, *Lattice signatures without trapdoors*, 2012, pp. 738–755.