# On Rejection Sampling in Lyubashevsky's Signature Scheme

2022/1249 on ePrint (updated Dec. 5)

**Julien Devevey** Omar Fawzi Alain Passelègue Damien Stehlé

ENS de Lyon, Laboratoire LIP (U. Lyon, CNRS, ENSL, Inria, UCBL), France

# Wh Questions

- Goal: Optimize
- What: Lattice-based Fiat-Shamir with Aborts
- Which: Both runtime and compactness (small $|\sigma|$ and $|\mathsf{vk}|$)
- How: Formal study of the use of rejection sampling
- Results:
  1. Runtime: Proof of its optimality
  2. Compactness: Lower bounds + how to reach them

# Wh Questions

- Goal: Optimize
- What: Lattice-based Fiat-Shamir with Aborts
- Which: Both runtime and compactness (small $|\sigma|$ and $|\mathsf{vk}|$)
- How: Formal study of the use of rejection sampling
- Results:
  1. Runtime: Proof of its optimality
  2. Compactness: Lower bounds + how to reach them

# Wh Questions

- Goal: Optimize
- What: Lattice-based Fiat-Shamir with Aborts
- Which: Both runtime and compactness (small $|\sigma|$ and $|\mathsf{vk}|$)
- How: Formal study of the use of rejection sampling
- Results:
  1. Runtime: Proof of its optimality
  2. Compactness: Lower bounds + how to reach them

# Wh Questions

- Goal: Optimize
- What: Lattice-based Fiat-Shamir with Aborts
- Which: Both runtime and compactness (small $|\sigma|$ and $|\mathsf{vk}|$)
- How: Formal study of the use of rejection sampling
- Results:
  1. Runtime: Proof of its optimality
  2. Compactness: Lower bounds + how to reach them

# Wh Questions

- Goal: Optimize
- What: Lattice-based Fiat-Shamir with Aborts
- Which: Both runtime and compactness (small $|\sigma|$ and $|\mathsf{vk}|$)
- How: Formal study of the use of rejection sampling
- Results:
  1. Runtime: Proof of its optimality
  2. Compactness: Lower bounds + how to reach them

# Why: Motivations

- Used by (future) NIST PQ standard:


- Rejection sampling has been widely used since its introduction in cryptography (Lyubashevsky; AC'09)...
- ... but mostly in a black-box manner, and only with very few distributions.

# On Rejection Sampling in Lyubashevsky's Signature Scheme

Lyubashevsky's Signature Scheme
(Lyubashevsky; AC'09), (Lyubashevsky; EC'12)...

Minimizing Number of Rejects

Minimizing Signature Size

# Lyubashevsky's Signature Scheme

(Lyubashevsky; AC'09), (Lyubashevsky; EC'12)...

Lyubashevsky's Signature Scheme
(Lyubashevsky; AC'09), (Lyubashevsky; EC'12)...

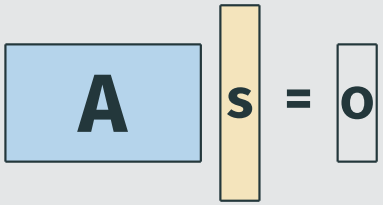
Minimizing Number of Rejects

Minimizing Signature Size

# Security Assumption

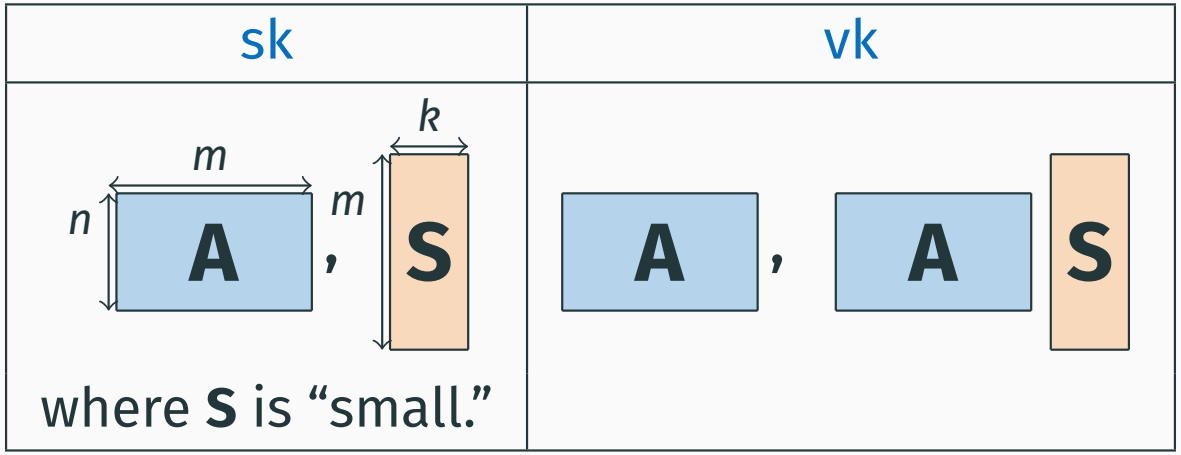
**$\mathrm{SIS}_{n,m,\beta}$**

Given uniform $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, find $\mathbf{s} \in \mathbb{Z}_q^m$ s.t. $0 < \|\mathbf{s}\| \leq \beta$ and




- Post-quantum assumption based on lattices.
- Gets harder when $\beta$ gets smaller.

# KeyGen



# Sign with Generic Distribution

On input sk, $\mu$, sample a small

$$\mathbf{y} \hookleftarrow Q$$

for a *free* distribution $Q$.

Signature $\sigma$ for message $\mu$ is

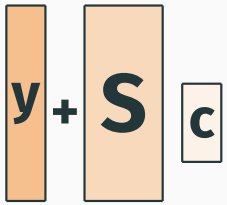
| $\mathbf{z}$ | $\mathbf{c}$ |
| --- | --- |
| $\mathbf{y} + \mathbf{S}\,\mathbf{c}$ | $\mathbf{H}\left(\mathbf{A}\,\mathbf{y}, \mu\right)$ |

# Properties

**Correctness**

$\exists \gamma : \Pr_{\mathbf{z}}(\|\mathbf{z}\| > \gamma) \leq \mathrm{negl}(\lambda) \implies$ the scheme is correct.

- Instantiated with $Q$ either Gaussian or $[-\eta, \eta]^m$-Uniform,
- This version is not secure:

$\mathbf{z} =$  depends on $\mathbf{S}$.

# Making the Scheme Secure

Goal: erase dependency on $\mathbf{S}$.

Done by enforcing $\mathbf{z} \sim P$.

Two solutions:

1. Flooding
   - $Q$ with large standard deviation
   - Used by (Damgård et al.; CRYPTO12), (Agrawal et al.; ICALP22)

   $\Longrightarrow$ large $\gamma$

2. Rejection Sampling
   (Lyubashevsky; AC'09)

# Making the Scheme Secure

Goal: erase dependency on $\mathbf{S}$.

Done by enforcing $\mathbf{z} \sim P$.

Two solutions:

1. Flooding
   - $Q$ with large standard deviation
   - Used by (Damgård et al.; CRYPTO12), (Agrawal et al.; ICALP22)

   $\Longrightarrow$ large $\gamma$

2. Rejection Sampling

   (Lyubashevsky; AC'09)

# Making the Scheme Secure

$\sigma = (\mathbf{z}, \mathbf{c})$ uncorrelated with $\mathbf{S} \implies$ signature queries are useless.

**Theorem** (Lyubashevsky; EC'12)

If $\mathcal{A}$ cannot query Sign, $\Pr(\mathcal{A} \text{ forges}) = \text{negl}(\lambda)$ under $\text{SIS}_{n,m,2\gamma}$.

# Minimizing Number of Rejects

Lyubashevsky's Signature Scheme

(Lyubashevsky; AC'09), (Lyubashevsky; EC'12)...

Minimizing Number of Rejects

Minimizing Signature Size

# Broader Context

- Given access to $(X_1, \ldots, X_i, \ldots)$ i.i.d. following $\tilde{D}$...
- ... How to find $X_j$ distributed as $D$ among the first $i^*$ samples?
- ⚠ Without modifying the samples!
- Goal: minimize $\mathbb{E}(i^*)$, expected number of samples

# Broader Context

- Given access to $(X_1, \ldots, X_i, \ldots)$ i.i.d. following $\tilde{D}$...
- ... How to find $X_j$ distributed as $D$ among the first $i^*$ samples?
- ⚠ Without modifying the samples!
- Goal: minimize $\mathbb{E}(i^*)$, expected number of samples

# Imperfect Rejection Sampling (Lyubashevsky; EC'11)

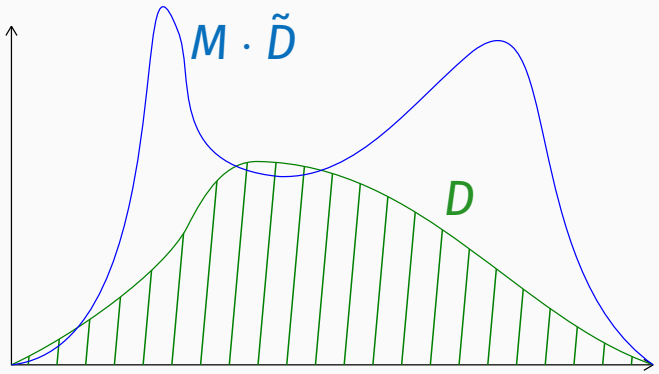



**Figure 1:** Acceptance zone and sampling domain

## Imperfect Rejection Sampling

$$R : X \mapsto \begin{cases} \mathrm{Acc} & \text{w.p. } \min\left(\frac{D(X)}{M \cdot \tilde{D}(X)}, 1\right), \\ \mathrm{Rej} & \text{otherwise.} \end{cases}$$

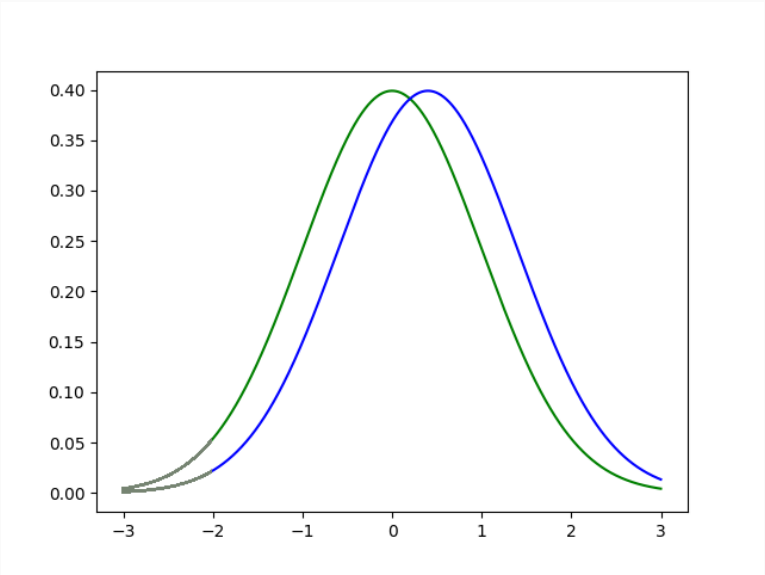
# Smooth Rényi Divergence

Our generalization of Rényi divergence for any $\varepsilon \geq 0$:

**$\varepsilon$-smooth Rényi divergence**

$$R^{\varepsilon}_{\infty}(D\|\tilde{D}) = \inf_{D(S)\geq 1-\varepsilon} \sup_{x\in S} \frac{D(x)}{\tilde{D}(x)}.$$

By tail-cutting, $R^{\varepsilon}_{\infty}(D_s\|D_{s,c}) < +\infty$ if $\varepsilon \neq 0$.



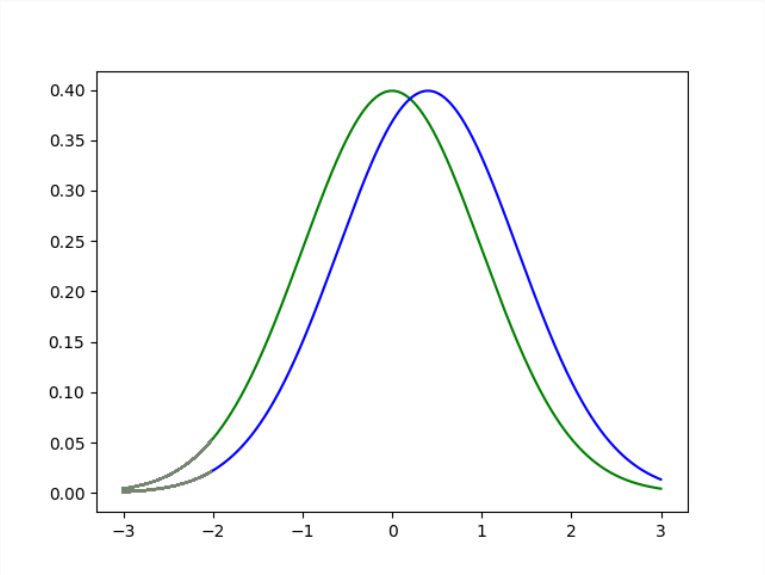
# Smooth Rényi Divergence

Our generalization of Rényi divergence for any $\varepsilon \geq 0$:

**$\varepsilon$-smooth Rényi divergence**

$$R_\infty^\varepsilon(D\|\tilde{D}) = \inf_{D(S)\geq 1-\varepsilon} \sup_{x\in S} \frac{D(x)}{\tilde{D}(x)}.$$

By tail-cutting, $R_\infty^\varepsilon(D_s\|D_{s,c}) < +\infty$ if $\varepsilon \neq 0$.



# Efficiency of Rejection Sampling

Given $\varepsilon \geq 0$ and $M \geq R_\infty^\varepsilon(D\|\tilde{D})$:

**Runtime: Average number of samples $\mathbb{E}(i^*)$**

$$\mathbb{E}(i^*) \leq \frac{M}{1-\varepsilon}.$$

(**Contribution:** optimal when $\varepsilon = 0$ among perfect strategies)

**Quality of resulting distribution $P^{out}$ (contribution)**

$$R_\infty(P^{out}\|D) \leq \frac{1}{1-\varepsilon}.$$

# Minimizing Signature Size

Lyubashevsky's Signature Scheme

(Lyubashevsky; AC'09), (Lyubashevsky; EC'12)...

Minimizing Number of Rejects

Minimizing Signature Size

# The Optimization Problem

Let $M > 1$ and $\varepsilon \leq 1/Q_s$.

Goal: Find $P, Q$ minimizing $\gamma$ under the constraints

1. $\Pr_{\mathbf{z} \hookleftarrow P}(\|\mathbf{z}\| > \gamma) = \mathrm{negl}(\lambda)$,
2. $\max_{\mathbf{S},\mathbf{c}} R_\infty^\varepsilon(P \| Q_{\mathbf{Sc}}) \leq M$.

# The Optimization Problem

Let $\mathbf{M} > \mathbf{1}$ and $\varepsilon \leq 1/Q_s$.

Goal: Find $P, Q$ minimizing $\gamma$ under the constraints

1. $\Pr_{\mathbf{z} \hookleftarrow P}(\|\mathbf{z}\| > \gamma) = \mathrm{negl}(\lambda)$,
2. $\max_{\mathbf{S},\mathbf{c}} \mathbf{R}^{\varepsilon}_{\infty}(\mathbf{P} \| \mathbf{Q_{Sc}}) \leq \mathbf{M}$.

- $\mathbf{M}$ represents the average number of rejects: "time" constraint.
- It must be satisfied for all $+\mathbf{Sc}$ shift.

# The Optimization Problem

Let $M > 1$ and $\varepsilon \leq 1/Q_s$.

Goal: Find $P, Q$ minimizing $\gamma$ under the constraints

1. $\Pr_{\mathbf{z} \hookleftarrow P}(\|\mathbf{z}\| > \gamma) = \mathrm{negl}(\lambda)$,
2. $\max_{\mathbf{S},\mathbf{c}} R^{\varepsilon}_{\infty}(P \| Q_{\mathbf{Sc}}) \leq M$.

**Reminder: Quality (contribution)**

$$R_{\infty}\left(Q_s \text{ signatures} \parallel (P \otimes U(\mathcal{C}))^{Q_s}\right) \leq \frac{1}{(1-\varepsilon)^{Q_s}}.$$

- Tighter security proof with RD than SD.

**Security (contribution)**

If $\varepsilon = O(1/Q_s)$, $\Pr(\mathcal{A}^{\mathrm{Sign}} \text{ forges}) \leq \mathrm{negl}(\lambda)$.

# The Optimization Problem

Let $M > 1$ and $\varepsilon \leq 1/Q_s$.

Goal: Find $P, Q$ **minimizing** $\gamma$ under the constraints

1. $\Pr_{\mathbf{z} \hookleftarrow \mathbf{P}}(\|\mathbf{z}\| > \gamma) = \mathrm{negl}(\lambda)$,
2. $\max_{\mathbf{S},\mathbf{c}} R^{\varepsilon}_{\infty}(P \| Q_{\mathbf{Sc}}) \leq M$.

- Condition needed for correctness.
- $\gamma$ drives the signature size ($|\mathbf{c}|$ is omitted).

# The Optimization Problem: Kiss Cool Effect

Let $M > 1$ and $\varepsilon \leq 1/Q_s$.

Goal: Find $P, Q$ minimizing $\gamma$ under the constraints

1. $\Pr_{\mathbf{z} \hookleftarrow P}(\|\mathbf{z}\| > \gamma) = \mathrm{negl}(\lambda)$,
2. $\max_{\mathbf{S},\mathbf{c}} R^{\varepsilon}_{\infty}(P \| Q_{\mathbf{Sc}}) \leq M$.

Minimize $\gamma$

$\Downarrow$

Cryptanalysis becomes more expensive

$\Downarrow$

Smaller parameters overall for the same level of security

# Optimality

**Contribution: Lower bounds on compactness**

- $\varepsilon = 0$,
- $M > 1$,
- $\max_{\mathbf{s},\mathbf{c}} R_\infty(P \| Q_{\mathbf{Sc}}) \leq M$,
- $t = \max_{\mathbf{s},\mathbf{c}} \|\mathbf{Sc}\|$,

$$\left[\Pr_{\mathbf{z} \hookleftarrow P}(\|\mathbf{z}\| > \gamma) = \mathrm{negl}(\lambda)\right] \Longrightarrow \gamma \geq \frac{t(m-1)}{\log M}.$$

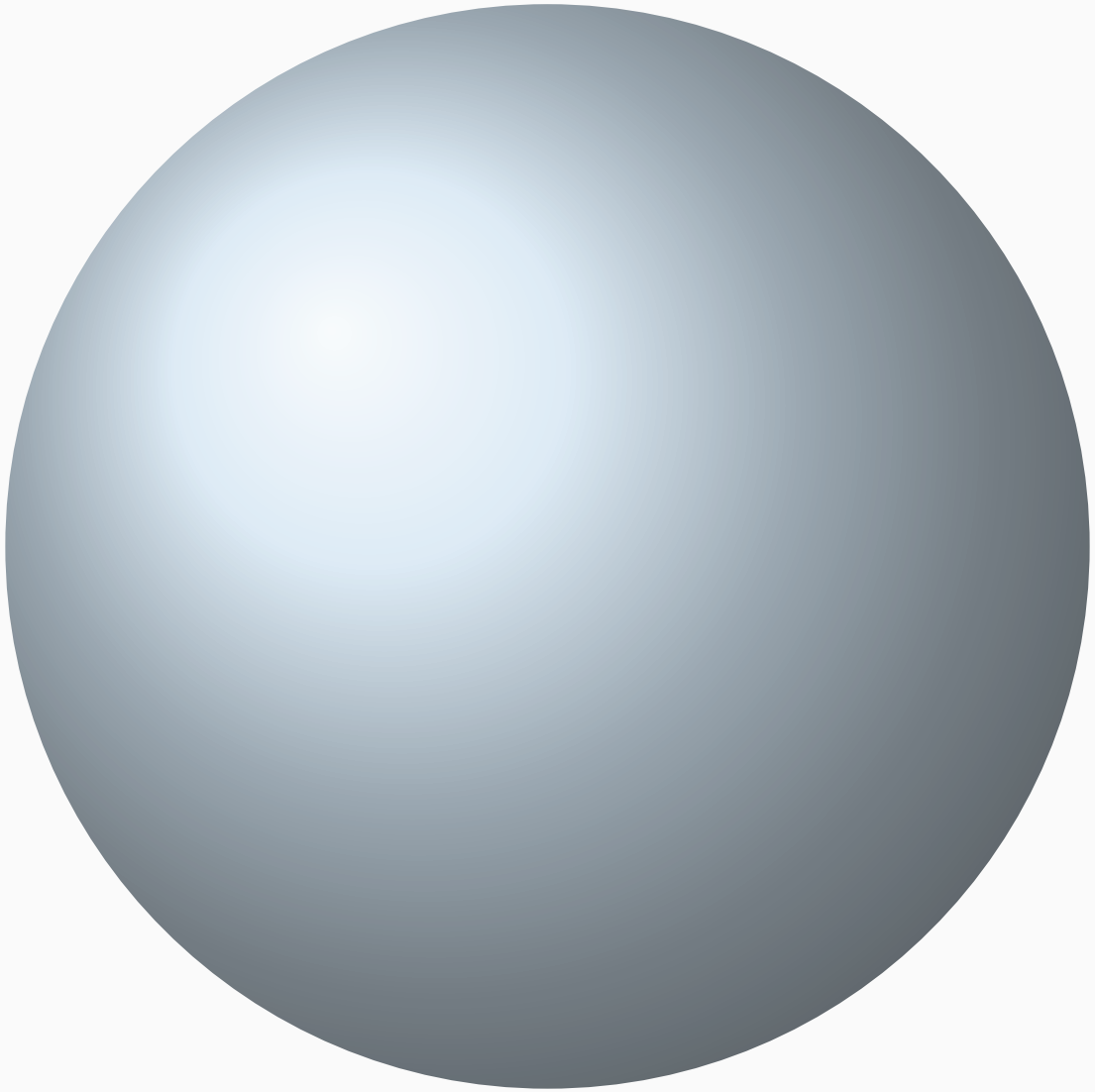
# Current Choices of Distributions

| $P, Q$ | Sampling | Rejection | $\gamma_{(\varepsilon=0)}$ | $\gamma_{(\varepsilon=1/Q_s)}$ |
|---|---|---|---|---|
| $U(\square)$ | Easy | Deterministic | $\frac{t\sqrt{m}m}{\log M}$ | $\frac{t\sqrt{m}m}{\log M}$ |
|  | Cumbersome | Probabilistic | $\infty$ | $\frac{t\sqrt{m \log \frac{1}{\varepsilon}}}{\sqrt{\log M}}$ |

(where $t = \max_{\mathbf{s},\mathbf{c}} \|\mathbf{Sc}\|$)

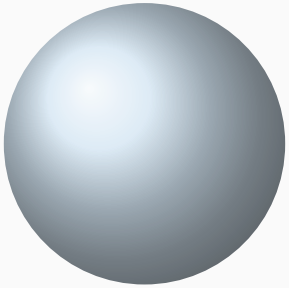
The first distribution is used in Dilithium.

# Our Proposal



# Our Proposal

Use the uniform distribution over



| $P, Q$ | Sampling | Rejection | $\gamma(\varepsilon=0)$ | $\gamma(\varepsilon=1/Q_s)$ |
|---|---|---|---|---|
| $U(\square)$ | Easy | Deterministic | $\frac{t\sqrt{m}m}{\log M}$ | $\frac{t\sqrt{m}m}{\log M}$ |
|  | Cumbersome | Probabilistic | $\infty$ | $\frac{t\sqrt{m \log \frac{1}{\varepsilon}}}{\sqrt{\log M}}$ |
| $U(\bigcirc)$ | Cumbersome | Deterministic | $\frac{tm}{\log M}$ | $\frac{t\sqrt{m \log \frac{1}{\varepsilon}}}{\log M}$ |

# Intuition

Hyperballs versus hypercubes:

- $\{\mathbf{Sc}\} \approx \mathcal{B}_m(t) \cap \mathbb{Z}^m$ and $\gamma$ is a bound on the Euclidean norm.
- Factor $\sqrt{m}$ gained because of $\|\cdot\| \leq \sqrt{m}\|\cdot\|_\infty$.

Cut and smooth divergence:

- Remove a hyperspherical cap opposite to $\mathbf{Sc}$.
- Volume allowed depends on $\varepsilon$.

# Intuition

Hyperballs versus hypercubes:

- $\{\mathbf{Sc}\} \approx \mathcal{B}_m(t) \cap \mathbb{Z}^m$ and $\gamma$ is a bound on the Euclidean norm.
- Factor $\sqrt{m}$ gained because of $\|\cdot\| \leq \sqrt{m}\|\cdot\|_\infty$.

Cut and smooth divergence:

- Remove a hyperspherical cap opposite to **Sc**.
- Volume allowed depends on $\varepsilon$.

# Practical Parameters

| Security (core-SVP) | 120 bits | | 180 bits | | 260 bits | |
|---|---|---|---|---|---|---|
| Size | $\lvert\sigma\rvert$ | $\lvert vk\rvert$ | $\lvert\sigma\rvert$ | $\lvert vk\rvert$ | $\lvert\sigma\rvert$ | $\lvert vk\rvert$ |
| $U($  $)$ | 2420 | 1312 | 3293 | 1952 | 4595 | 2592 |
|  | 1921 | 800 | 2462 | 1184 | 3553 | 1760 |
| $U($  $)$ | 1903 | 800 | 2473 | 1056 | 3461 | 1760 |

- Based on Dilithium and Gaussian/Hyperball variants.
- Plugs in *all* improvements we made.
  - Take $\varepsilon = 2^{-64}$ instead of $2^{-\lambda}$.
  - Improved constant factor in computation of $R_\infty^\varepsilon$ for Gaussians.

# Practical Parameters

| Security (core-SVP) | 120 bits | | 180 bits | | 260 bits | |
|---|---|---|---|---|---|---|
| Size | $\lvert\sigma\rvert$ | $\lvert\mathsf{vk}\rvert$ | $\lvert\sigma\rvert$ | $\lvert\mathsf{vk}\rvert$ | $\lvert\sigma\rvert$ | $\lvert\mathsf{vk}\rvert$ |
| $U(\square)$ | 2420 | 1312 | 3293 | 1952 | 4595 | 2592 |
| $\wedge$ | 1921 | 800 | 2462 | 1184 | 3553 | 1760 |
| $U(\bigcirc)$ | 1903 | 800 | 2473 | 1056 | 3461 | 1760 |

- Based on Dilithium and Gaussian/Hyperball variants.
- Plugs in *all* improvements we made.
  - Take $\varepsilon = 2^{-64}$ instead of $2^{-\lambda}$.
  - Improved constant factor in computation of $R_\infty^\varepsilon$ for Gaussians.

# Practical Parameters

| Security (core-SVP) | 120 bits | | 180 bits | | 260 bits | |
|---|---|---|---|---|---|---|
| Size | $\lvert\sigma\rvert$ | $\lvert\mathsf{vk}\rvert$ | $\lvert\sigma\rvert$ | $\lvert\mathsf{vk}\rvert$ | $\lvert\sigma\rvert$ | $\lvert\mathsf{vk}\rvert$ |
| $U(\square)$ | 2420 | 1312 | 3293 | 1952 | 4595 | 2592 |
|  | 1921 | 800 | 2462 | 1184 | 3553 | 1760 |
| $U(\bigcirc)$ | 1903 | 800 | 2473 | 1056 | 3461 | 1760 |

- Based on Dilithium and Gaussian/Hyperball variants.
- Plugs in *all* improvements we made.
  - Take $\varepsilon = 2^{-64}$ instead of $2^{-\lambda}$.
  - Improved constant factor in computation of $R_\infty^\varepsilon$ for Gaussians.

# Wrapping up

Other results in the paper:

- Similar results for BLISS (Ducas et al.; CRYPTO'13).
- Alternative version with bounded number of rejects: Compromise between rejection and flooding.
- Variant relying on continuous distributions.

# Thank you for your attention!

Any question?